

HORTA COMPARTILHADA: APLICAÇÃO DE
CRIPTOMOEDA IOTA EM INTERNET DAS COISAS
– ECONOMIA DAS COISAS

Fábio Carli Rodrigues Teixeira

Novembro de 2021

**Horta Compartilhada: Aplicação de
Criptomoedas Iota em Internet das Coisas –
Economia das Coisas**

Fábio Carli Rodrigues Teixeira

Dissertação apresentada ao Instituto Nacional de
Telecomunicações, como parte dos requisitos para
obtenção do Título de Mestre em Telecomunicações.

ORIENTADOR: Prof. Dr. Antônio Marcos Alberti

Santa Rita do Sapucaí

2021

Teixeira, Fábio Carli Rodrigues

T266h

Horta Compartilhada: Aplicação de Criptomoeda IOTA em Internet das Coisas – Economia das Coisas. / Fábio Carli Rodrigues Teixeira. – Santa Rita do Sapucaí, 2021.

144 p.

Orientador: Prof. Dr. Antônio Marcos Alberti.

Dissertação de Mestrado em Telecomunicações – Instituto Nacional de Telecomunicações – INATEL.

Inclui bibliografia.

1. Economia das Coisas. 2. IoT. 3. Horta Compartilhada. 4. IOTA. 5. Mestrado em Telecomunicações. I. Alberti, Antônio Marcos. II. Instituto Nacional de Telecomunicações – INATEL. III. Título.

CDU 621.39

FOLHA DE APROVAÇÃO

Dissertação defendida e aprovada em ____ / ____ / ____, pela comissão julgadora:

Prof. Dr. Antônio Marcos Alberti

INATEL

Prof. Dr. Danilo Henrique Spadoti

UNIFEI

Prof. Dr. Samuel Baraldi Mafra

INATEL

Prof. Dr. José Marcos Câmara Brito

Coordenador do Curso de Mestrado

*“Não é o muito saber que sacia e satisfaz a alma,
mas o sentir e saborear internamente as coisas”*

-- Santo Inácio de Loiola

Agradecimentos

Primeiramente agradeço a Deus, o Grande ‘Engenheiro’ do Universo, a Quem tudo devemos;

À minha família, pela qual tudo faço;

Ao Prof. Dr. Antônio Marcos Alberti, orientador e amigo;

Aos colegas do ICTLab do INATEL, companheiros de jornada;

À Escola Técnica de Eletrônica Francisco Moreira da Costa – ETE FMC, onde leciono, e que sempre me apoiou;

Ao INATEL, que sempre faz o melhor para incentivar seus discentes.

Índice

Lista de Figuras.....	x
Lista de Tabelasxi
Lista de Abreviaturas, Siglas e Símbolos	xii
Resumo.....	xv
Abstract	xvi
Publicação	xvii
Capítulo 1 – INTRODUÇÃO.....	1
1.1- Visão Histórica das Criptomoedas	8
Capítulo 2 – AGRICULTURA, CADEIAS PRODUTIVAS E TECNOLOGIA.....	16
2.1 Revisão de Literatura.....	18
2.2 Controle da Produção Agrícola	28
2.3 Armazenamento e Uso de Dados	31
2.4 Conectividade Agrícola.....	33
2.5 Desenvolvimento Sustentável.....	34
2.6 Relacionamento com o Mercado de Consumo	35
2.7 Serviços Digitais.....	37
2.8 Classificação de Hortaliças e Mercado	38
Capítulo 3 – ASPECTOS LEGAIS DAS CRIPTOMOEDAS.....	41
3.1- Conceito da Criptomoeda	42
3.2- Risco das Criptomoedas	44
3.3- ICO – Initial Coin Offering.....	45
3.4- DA REGULAÇÃO DAS CRIPTOMOEDAS.....	46
3.4.1- Regulação das Criptomoedas no Brasil.....	46
3.4.2- Panorama Global da Regulação	53
Capítulo 4 – DESCRIÇÃO DO BITCOIN, ETHEREUM E IOTA.....	57
4.1 Bitcoin.....	57
4.1.1 <i>Hashcode</i> e Encriptação	58
4.2 Ethereum.....	64
4.2.1 Conceitos Básicos	65
4.2.2 Transição de Estado	67
4.2.3 Ethereum Virtual Machine (EVM)	68
4.2.4 Mineração no Ethereum	69
4.2.5 <i>Smart Contracts</i> da Carteira de Contrato.....	70
4.2.6 Hard Forks	71

4.3 IOTA.....	72
4.3.1 <i>Tangle</i>	73
4.3.2 Termos Importantes.....	74
4.3.3 Estratégias para aprovar as TIPs.....	77
4.3.4 Crescimento do Peso Acumulado	78
4.4 Modelo da IoT	78
4.5 Comparações entre <i>Blockchain</i> e <i>Tangle</i>	82
Capítulo 5 – EXPERIMENTOS E ANÁLISE.....	87
5.1 Materiais e Métodos	87
5.1.1 Placa de <i>Hardware</i>	87
5.1.2 Componentes Físicos.....	89
5.1.3 Construção do Protótipo da Horta	94
5.2 Montagens e Códigos.....	96
5.2.1 Etapa 1 – Montagem Inicial para Testes de Latência.....	96
5.2.2 Etapa 2 – Montagem Final com as Funções da Horta	99
5.3 Resultados e Discussões.....	102
5.3.1 Etapa 1 – Testes de Latência Preliminares	102
5.3.2 Experimento da Horta e Análise de Desempenho	104
Capítulo 6 – CONCLUSÃO	113
Referências Bibliográficas	115

Lista de Figuras

Figura 1 - Uma horta de alface vertical indoor no Japão.	2
Figura 2 - Horta na Av. Paulista. Fonte:	3
Figura 3 - Horta Mariquinha Capistrano.	4
Figura 4 - 17 objetivos da Agenda 2030 da ONU [41].	18
Figura 5 - Desafios, tendências e oportunidades na agricultura [45].	19
Figura 6 - Crescimento dos dispositivos conectados [64]	23
Figura 7 - O processo de negócios de gestão da fazenda [87].	29
Figura 8 - Comparação de uma imagem com câmera RGB e câmera Multiespectral [89].	30
Figura 9 - Estrutura simplificada de blocos da cadeia [147]	60
Figura 10 - Árvore de Merkle [147].	61
Figura 11 - Uma fazenda de mineração. Fonte: www.genesis-mining.com	63
Figura 12 - Transação Ethereum, sem o valor do Gas [26].	67
Figura 13 - As três raízes no cabeçalho Ethereum [157].	70
Figura 14 - Exemplo de Contrato Inteligente Ethereum [77].	71
Figura 15 - DAG [35].	73
Figura 16 - A transação B aprova diretamente a transação A [35].	74
Figura 17 - Aprovação indireta de A por B [35].	74
Figura 18 - Pesos próprios no canto inferior e Pesos Cumulativos no canto superior [35].	75
Figura 19 - A TIP X chegou e os Pesos Cumulativos das transações anteriores aumentou [35].	75
Figura 20 - Pontuação no site A e no site C [35].	76
Figura 21 - Carga baixa [35].	77
Figura 22 - Carga alta [35].	77
Figura 23 - Crescimento do Peso acumulado em carga alta [35].	78
Figura 24 - Modelo de Referência da IoT [161].	79
Figura 25 - Modelo de negócio IoT com Blockchain [162].	81
Figura 26 - Velocidade e número de usuários [164].	83
Figura 27 - Raspberry Pi 3. Fonte: raspberrypi.org	87
Figura 28 - Pinagem do barramento da Raspberry Pi 3B+	88
Figura 29 - Sensor de Umidade.	89
Figura 30 - Circuito comparador de Sensor de Umidade	90
Figura 31 - Módulo Relé. Fonte: itelectroniccomp.com	90
Figura 32 - Esquema elétrico do módulo relé.	90
Figura 33 - Lâmpada Full Spectrum	91
Figura 34 - Demonstração de Engelmann.	92
Figura 35 - Reservatório e bomba d'água.	92
Figura 36 - Bico de gotejamento.	93
Figura 37 - Vaso de PVC.	93
Figura 38 - Preparação do vaso. Fonte: revistanatureza.com.br	94
Figura 39 - Construção da Maquete da horta.	95
Figura 40 - Primeira etapa de testes.	96
Figura 41 - Driver de Relé. A lâmpada simula a carga.	97
Figura 42 - Sequência lógica de funcionamento do acionador de cargas	97
Figura 43 - Código Python da Etapa 1.	98
Figura 44 - Set de testes da horta compartilhada.	99
Figura 45 - Fluxograma da horta compartilhada.	100
Figura 46 - Código utilizado no experimento da horta.	102
Figura 47 - Testes de latência.	103
Figura 48 - Tempo de confirmação de transação em janeiro de 2020.	103
Figura 49 - Confirmação de transação na carteira e no site thetangle.org	105
Figura 50 - Pacotes Wireshark de uma transação IOTA	106
Figura 52 - Tempo de confirmação de transação, em janeiro de 2021.	109
Figura 53 - Tempo de confirmação de transação, em julho de 2021.	110
Figura 54 - Medidor de umidade do solo Minipa MV-331. Fonte: eletropartcomponentes.com.br	112
Figura 55 - Controle da Umidade do solo.	112

Lista de Tabelas

<i>Tabela 1 - Benefícios na cadeia produtiva [40].</i>	17
<i>Tabela 2 - Classificação de hortaliças no Brasil (Embrapa).</i>	39
<i>Tabela 3 – Panorama global da regulação das criptomoedas.</i>	54
<i>Tabela 4 – Comparação entre Bitcoin, Ethereum e IOTA.</i>	85
<i>Tabela 5 – Tempos de confirmação de transações, em janeiro/20.</i>	103
<i>Tabela 6 - Tempo de confirmação de transações, em janeiro/21.</i>	108
<i>Tabela 7 - Tempo de confirmação de transações, em julho/21.</i>	109

Lista de Abreviaturas, Siglas e Símbolos

AgTech - Empresa de Tecnologia aplicada ao agronegócio

ASICs – Application Specific Integrated Circuits

BACEN – Banco Central do Brasil

BIP – Bitcoin Improvement Proposal

BNDES – Banco Nacional de Desenvolvimento Social

BTC – Bitcoin

CBDC – Central Bank Digital Currencies

CNA – Confederação da Agricultura e Pecuária do Brasil

COAF – Conselho de Controle de Atividades Financeiras

CRA – Cotas de Reserva Ambiental

CVM – Comissão de Valores Mobiliários

DAC – Distributed Autonomous Corporation

DAG – Directed Acyclic Graph

DAO – Decentralized Autonomous Organization

DDoS – Distributed Denial of Service

DeFi – Decentralized Finances

DLT – Distributed Ledger Technology

DSL – Digital Subscriber Line

ECDLP - Elliptic Curve Discrete Logarithm Problem

EMBRAPA – Empresa Brasileira de Pesquisa Agropecuária

EOA - Externally Owned Account

EVM – Ethereum Virtual Machine

FAIR – Findable, Accessible, Interoperable and Reusable

FAO – Food and Agriculture Organization

FMI – Fundo Monetário Internacional

FUST – Fundo de Universalização dos Serviços de Telecomunicações

GFIN – Global Financial Innovation Network

GPIO – General Purpose Input Output

GPS – Global Positioning System

HD – Hard Disk

IBGE – Instituto Brasileiro de Geografia e Estatística

ICO – Initial Coin Offering

IDH – Índice de Desenvolvimento Humano

IDoT – Identity of Things

IN – Instrução Normativa

IoT – Internet of Things

IPEA – Instituto de Pesquisa Econômica Aplicada

IPO – Initial Public Offering

IXI – IOTA EXtension Interface

LTE – Long Term Evolution

M2M – Machine to Machine

MAM – Mensagem Autenticada com Máscara

MAPA – Ministério da Agricultura, Pecuária e Abastecimento

MIOTA – Milhões de IOTAs

MS – Ministério da Saúde

ODS – Objetivos de Desenvolvimento Sustentável

OMS – Organização Mundial da Saúde

ONG – Organização Não Governamental

ONU – Organização das Nações Unidas

P2P – Peer to Peer

PBFT – Practical Byzantine Fault Tolerance

PC – Program Counter

PIB – Produto Interno Bruto

PL – Projeto de Lei

PNUD – Programa das Nações Unidas para o Desenvolvimento

PoC – Proof of Capacity

PoS – Proof of Stake

PoW – Proof of Work

PSA – Pagamento por Serviços Ambientais

PSTN – Public Switched Telephone Network

PRA – Programa de Regularização Ambiental

QR Code – Quick Response Code

RFID – Radio Frequency Identification

TCP/IP – Transmission Control Protocol / Internet Protocol

TIC – Tecnologia de Informação e Comunicação

UNGC – United Nations Global Compact

ZARC – Zoneamento Agrícola de Risco Climático

Resumo

Utilizando um cenário de uma horta comunitária urbana, este trabalho apresenta a aplicação da Internet das Coisas em um caso de Economia Compartilhada, fazendo uso da criptomoeda IOTA e seu protocolo de registros distribuídos, o *Tangle*, de forma a se ter o controle das funcionalidades da horta, seus pagamentos, a distribuição de produtos, e o monitoramento do desenvolvimento das plantas, a partir da disponibilidade de saldo em uma carteira digital associada ao código de controle da horta. A horta pode ser acomodada em um edifício, garagem e até mesmo em um terreno baldio, de forma a otimizar e a escalar o aproveitamento dos recursos utilizados e produtos oferecidos. A agricultura urbana e periurbana é apontada pela ONU como uma das soluções para a segurança alimentar e de problemas socioeconômicos em comunidades carentes. Esta monografia discute também as melhorias que o uso de tecnologias e novas formas de administração podem propiciar ao cenário agrícola nacional. Outra importante discussão necessária ao uso legal da moeda digital é sua regulamentação estatal, o que também é contemplado neste trabalho. Também são apresentadas as características das principais criptomoedas que utilizam *Blockchain* e da IOTA, justificando a escolha dessa última na aplicação da horta. Por fim, os resultados do experimento feito são apresentados e discutidos, comprovando que a proposta tem viabilidade de uso e pode ser facilmente adequada às particularidades de cada comunidade.

Palavras-chave: Economia das Coisas, IoT, Horta Compartilhada, IOTA

Abstract

Using a scenario of an urban community vegetable garden, this work presents the application of the Internet of Things in a case of Shared Economy, making use of the IOTA cryptocurrency and its distributed ledger technology, the Tangle, in order to control the functionalities of the vegetable garden, its payments, product distribution, and monitoring of vegetable development, based on the availability of a balance in a digital wallet associated with the vegetable garden control code. The vegetable garden can be accommodated in a building, garage and even in a vacant lot, in order to optimize and scale the use of resources used and products offered. Urban and peri-urban agriculture is identified by the UN as one of the solutions for food security and socioeconomic problems in poor communities. This work also discusses the improvements that the use of technologies and new forms of administration can bring to the national agricultural scenario. Another important discussion necessary for the legal use of digital currency is its state regulation, which is also covered in this work. The characteristics of the main cryptocurrencies that use Blockchain and IOTA are also presented, justifying the choice of the latter in the application of the vegetable garden. Finally, the results of the experiment carried out are presented and discussed, proving that the proposal is viable for use and can be easily adapted to the particularities of each community.

Keywords: Economy of Things, IoT, Shared Vegetable Garden, IOTA

Publicação

TEIXEIRA, Fábio C. R.; VILAS BOAS, Jonas L.; ALBERTI, Antônio M.. Horta Compartilhada com IOTA e Fuzzy – Um Projeto de Economia das Coisas para IoT. In **XXXIX Simpósio Brasileiro de Telecomunicações e Processamento de Sinais – SBrT 2021, 26 – 29 de setembro de 2021**, Fortaleza, CE.

Capítulo 1 – INTRODUÇÃO

‘Existem três eras da moeda: baseada em commodities, baseada na política, e agora, baseada na matemática’ (Chris Dixon – Investidor)

☉ inexorável avanço da tecnologia, tanto no mundo real, quanto no virtual, que tem sido observado em escalas exponenciais, e que remetem a Moore [1] e a Kurzweil [2], em especial no que se refere à IoT – *Internet of Things*, vem propiciando a elaboração de projetos com objetivos específicos voltados a pessoas e comunidades, e também à indústria e a gestão pública.

As transações financeiras feitas via Internet atualmente são bastante confiáveis, e utilizam ferramentas tradicionais reconhecidas. Na maioria das transações, são utilizadas as moedas oficiais dos países, passando pelo sistema bancário convencional e sendo reconhecidas pelos governos. Assim, as transações realizadas no mundo são, em sua esmagadora maioria, baseadas na intermediação bancária tradicional, e respaldadas pelos governos, garantindo assim a segurança das transações, na maioria das vezes.

A tecnologia, conforme mencionado, evolui de forma rápida. Há poucos anos, uma nova forma de efetivar as transações comerciais na rede foi desenvolvida, podendo ser aplicada tanto nos pagamentos comerciais, como também na troca de serviços e informações na Internet das Coisas [3], utilizando-se regras previamente estabelecidas para a transação e suas consequências, os chamados contratos inteligentes (*Smart Contracts*), para essa efetivação. A essa nova forma de pagamentos chamou-se moeda digital, ou criptomoeda, e seu controle é feito de forma descentralizada na própria rede, sem o intermédio de governos ou bancos. Naturalmente a moeda digital elenca muitas dúvidas a todos, principalmente no que se refere à garantia e à segurança da transação. É uma nova forma de pagamentos na rede, e que, sendo revolucionária e disruptiva, se propõe a substituir as transações financeiras convencionais [4].

Justamente pela facilidade de se utilizar as criptomoedas em transações financeiras entre objetos de IoT, e também pela possibilidade de não haver taxas proibitivas em transações de pequeníssima monta (ou melhor ainda: não haver taxas), o que, em geral, não ocorre nas transações bancárias convencionais, torna-se interessante

discutir o uso dessa forma de pagamento em aplicações que possam ser relacionadas à IoT, tal como é a proposta de monetização de uma horta compartilhada, urbana ou não, onde os produtos da horta possam ser comercializados mediante essa base digital de pagamentos. Naturalmente é necessária uma análise de qual criptomoeda se utilizar, uma vez que há uma grande quantidade delas no mercado, e outras tantas surgem todos os dias, cada uma com suas particularidades de uso e funcionamento. No caso da horta, tanto a comercialização dos produtos quanto a manutenção dos canteiros, compra de insumos, etc., podem ser contabilizados na base da moeda digital. Até mesmo a simples consulta a um sensor de umidade de solo pode ser precificada dessa forma, o que teria um valor muito pequeno, e a simples cobrança de uma taxa pode até mesmo inviabilizar esse pequeno serviço. Sendo assim, uma criptomoeda sem cobrança de taxas, com transação rapidamente confirmada pela rede e, de certa forma, já estabelecida no mercado, passa a ser uma escolha viável para a aplicação da horta.

As hortas comunitárias são relativamente recentes e são um fenômeno principalmente urbano ou periurbano, proporcionando a seus usuários alimentos frescos, livres de agrotóxicos, produzidos de forma sustentável, e também promovendo inclusão social e interação entre as pessoas da comunidade. A Figura 1 ilustra uma horta indoor que faz uso de tecnologias modernas para o cultivo:



Figura 1 - Uma horta de alface vertical indoor no Japão. Fonte: <caipirismo.wordpress.com>

A própria Organização das Nações Unidas – ONU, em seu Programa das Nações Unidas para o Desenvolvimento (PNUD) [5], considera a agricultura urbana e periurbana uma importante ação de desenvolvimento sustentável, que traz benefícios como segurança alimentar e nutricional, e promove o bem-estar social. É estimado pela UNFPA – United Nations Population Fund [6] que em mais 20 anos ter-se-á dois terços da

população mundial vivendo em cidades, o que resulta em impactos socioambientais relevantes, como a diminuição da fauna e flora, impermeabilização do solo (que impede a recarga dos aquíferos), geração de resíduos sólidos, geração de efluentes líquidos, e, aliado a explosão demográfica, proporciona também, a insegurança alimentar. Em apenas 50 anos houve um acréscimo de 1000% no número de pessoas subnutridas no mundo. Em 2010 foi inserida na Constituição Federal do Brasil, de 1988, a emenda número 64, que estabelece, dentre outras coisas, que a alimentação é um direito constitucional de todos, o que necessariamente implica em aplicação de políticas públicas efetivas no combate à fome. Neste contexto, a agricultura urbana e periurbana é uma das soluções para combater a insegurança alimentar.

Organizações e associações vêm surgindo para atender a essa premência da agricultura urbana e periurbana. Um exemplo disso é a Organização Cidades sem Fome, criada no Estado de São Paulo em 2004, e é uma organização não governamental (ONG) que desenvolve projetos de hortas comunitárias, escolares e estufas agrícolas, criando oportunidades de trabalho em comunidades com vulnerabilidade social e melhorando a alimentação desses locais. Atualmente, a Cidades sem Fome desenvolve projetos em diversos Estados do País, e já recebeu diversos prêmios por seu trabalho [7]. No Rio de Janeiro existe o projeto Hortas Cariocas, da Secretaria Municipal de Meio Ambiente, presente em 30 comunidades e na Rede Municipal de Ensino da capital, gerando empregos nas comunidades e dividindo a produção entre as escolas, creches e as famílias em risco social. O excedente da produção é comercializado [8]. Já os Hortelões Urbanos de São Paulo cuidam de diversas hortas na metrópole, sendo uma delas em plena Av. Paulista, no canteiro central, conforme a Figura 2 ilustra:

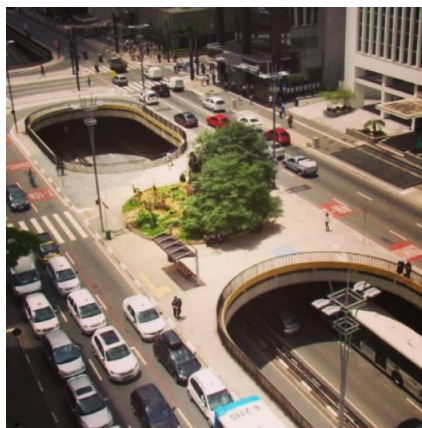


Figura 2 - Horta na Av. Paulista. Fonte: <facebook.com/groups/429537857165149/>

Em Jaraguá do Sul, SC, há o projeto Germinar, da prefeitura municipal, criado para aproveitar os espaços abandonados e estimular a alimentação orgânica [9]. O próprio INATEL criou, na Escola Municipal rural Mariquinha Capistrano, de Santa Rita do Sapucaí, MG, uma horta inteligente, que produz alimentos para consumo dos alunos da escola, mas que também objetiva testes de 5G em áreas remotas e rurais. A irrigação da horta pode ser controlada por meio de um aplicativo de celular, que também mostra os dados relacionados à umidade do solo. Esta iniciativa do INATEL está inserida no projeto 5G-Range, uma cooperação Brasil-União Europeia em TIC. A Figura 3 ilustra esta iniciativa:



Figura 3 - Horta Mariquinha Capistrano. Fonte: <inatel.br>

Os produtos da horta comunitária são destinados a consumo próprio da comunidade, podendo o excedente dos produtos ser comercializado, proporcionando uma forma de renda as pessoas que nela habitam. Podem ser cultivadas hortaliças, leguminosas, frutas, produção de mudas, plantas medicinais, etc.

A horta comunitária pode ser criada em um terreno baldio, em uma praça pública, uma escola, um condomínio, telhado de prédios, garagens, ou em qualquer local no entorno da comunidade que a manterá e usufruirá de seus resultados.

Alguns benefícios que podem ser destacados ao se fazer hortas comunitárias:

- Os espaços urbanos aproveitados para a horta não se tornarão depósito de lixo e entulhos;
- Segurança alimentar, que *‘é a situação na qual as pessoas, em todos os momentos, têm acesso físico, social e econômico a recursos suficientes, seguros e alimentos nutritivos que atendam às suas necessidades dietéticas e preferências alimentares para uma vida ativa e saudável’* (FAO – Food and Agriculture Organization);

-
- Desenvolvimento da comunidade, com aumento de oportunidades e trocas de conhecimento;
 - escoamento de águas das chuvas;
 - Reciclagem de resíduos orgânicos sólidos e líquidos;
 - Educação ambiental;
 - Redução da pobreza, a produção dos alimentos é utilizada para consumo próprio e ainda como doação para uso comunitário, em escolas, creches e associações da própria comunidade;
 - Geração de renda: em comunidades mais carentes, a possibilidade de venda dos produtos cultivados é uma opção muito praticada por meio de cooperativas e associações organizadas.

Alguns integrantes da comunidade, ou mesmo cooperativas de produção sustentável, se dispõem a gerenciar e manter a horta, desde o plantio até a colheita. Geralmente, o trabalho é fiscalizado pelo poder público. Outros membros da comunidade, ainda que não queiram ou não possam participar dos trabalhos, desejarão consumir os produtos da horta. Deste modo, a dinâmica de distribuição e venda de produtos é um desafio que pode ser contornado pelo estabelecimento de regras e condições para que todos possam receber os produtos de seu interesse e assim viabilizar a horta na comunidade. A monetização da horta passa assim a ser de fundamental importância e devem ser constantemente atualizados e divulgados a todos os membros da comunidade os valores dos produtos, assim como todas as informações de custos de produção, produtos disponíveis, datas de entrega de produtos, dados de sensores, etc. A monetização possibilita alcançar benefícios econômicos, por meio do uso dos dados gerados através da tecnologia embutida na horta. Além do próprio benefício econômico, a monetização da horta pode ajudar a calcular os indicadores de produtividade, otimizando a produção e evitando desperdícios. Com sensores IoT espalhados na horta, é possível avaliar a produção de forma mais eficiente: temperatura, umidade do solo e do ar, etc. Com essa base de dados o processo de tomada de decisão será mais efetivo, e a monetização será ainda maior. Todos os consumidores da horta desejarão a qualquer momento saber de todas essas informações, para que façam seus pagamentos e conseqüentemente recebam seus produtos. Isso propicia a rastreabilidade, a qualidade e a confiabilidade dos produtos

e fornecedores. Com acesso à *Internet* todas essas transações podem ser feitas rapidamente, e os serviços de IoT e as criptomoedas formam a base tecnológica que propicia essa organização social e comercial. As tecnologias hoje disponíveis para uso na agricultura, e que são fortemente incentivadas pela própria ONU em sua Agenda 2030 para o Desenvolvimento Sustentável, vêm a calhar para aumentar a produtividade, a rastreabilidade, melhorar a qualidade dos produtos, facilitar o trabalho e possibilitar o desejado desenvolvimento sustentável. É natural que hortas tecnológicas sejam monetizadas gerando renda, ao mesmo tempo em que beneficia a comunidade no aspecto alimentar e social.

Este trabalho, que ora se apresenta, trata da monetização de uma horta de produtos agrícolas, usando tecnologias recentes de telecomunicações, como a IoT e as criptomoedas, e demonstra as possibilidades de melhorias, tanto no aspecto de evolução, quanto na disrupção de processos convencionais. A esta junção de tecnologias da informação e das comunicações com os ambientes de produção, comércio, transportes, etc., dá-se o nome de Economia das Coisas ou ainda Economia Compartilhada [10]. Para que se escolha qual seria a criptomoeda adequada à proposição, serão descritas as características das principais moedas digitais utilizadas atualmente, suas tecnologias, sua adequação ao uso em contratos inteligentes de serviços de IoT, que, em uma desejada visão de futuro, serão totalmente autônomos em sua oferta, descoberta, negociação, e utilização por outras pessoas e/ou coisas na própria rede. Todo o ambiente físico da horta é compartilhado entre seus usuários, e os pagamentos são comunitários, pois diversos participantes podem pagar para a manutenção da horta.

Os questionamentos que motivaram o desenvolvimento deste trabalho são:

- Como fazer micropagamentos de IoT de forma a oportunizar uma horta comunitária urbana?
- Qual criptomoeda seria adequada para esses micropagamentos?

Desta forma, o objetivo principal deste trabalho é provar conceitualmente a possibilidade de se monetizar uma horta comunitária, utilizando a moeda digital IOTA, e a Internet das Coisas, gerando assim um caso de economia digital compartilhada.

A seguir, na Seção 1.1 será mostrada uma visão das moedas digitais e sua evolução no mundo. Esta visão, além de trazer o cunho histórico da evolução das criptomoedas e

mostrar em que momento o controle e registro das transações passou a ser descentralizado na rede e feito de forma imutável, fornece também um *background* para a escolha de uma criptomoeda interessante a ser utilizada na monetização da horta. No Capítulo 2 ter-se-á, na visão de um engenheiro, a noção básica de como a IoT, que é um cabedal tecnológico recente, pode ser útil no desenvolvimento e comercialização de produtos agrícolas, seja em uma pequena horta particular, urbana, rural, ou mesmo em uma grande plantação em ambientes *indoor* ou não, ainda que o escopo deste trabalho seja voltado para hortas comunitárias de pequeno porte. O Capítulo 3 discorrerá sobre os aspectos legais do uso das moedas digitais. Uma horta comunitária é um empreendimento social, e como tal, é importante que tudo esteja dentro dos princípios da legalidade. A legalidade dos criptoativos ainda está em discussão na maioria dos países, sendo que alguns as rejeitam, outros a regulamentaram, e a grande maioria ainda discute os termos dessa legalidade, ainda que já as aceitem em seu mercado. No Brasil, conforme se verá adiante, ainda não se chegou a um termo de legalidade na regulação dos criptoativos, mas já existem dispositivos jurídicos que permitem, de uma forma mais genérica, aceitar o uso dos mesmos. As *Exchange*, por exemplo, que são corretoras especializadas na intermediação da negociação de criptoativos, já estão em funcionamento regular no Brasil. No Capítulo 4 será feita uma exposição do funcionamento básico das criptomoedas Bitcoin, Ethereum, e IOTA, e suas possibilidades, e também as necessidades que a IoT tem em relação a transações na rede e aos *Smart Contracts*. Ainda no Capítulo 4 serão apresentadas as comparações decorrentes dos usos e arquiteturas da Bitcoin, Ethereum e IOTA. Essas três criptomoedas estão entre as mais conhecidas no mercado: o Bitcoin por ser a primeira de controle descentralizado e uso de *Blockchain*, e por sua projeção no mercado financeiro global; o Ethereum, por ser o ‘Bitcoin de segunda geração’, que permite em seu protocolo o uso dos *Smart Contracts*; e a IOTA, por não usar *Blockchain* e também por não cobrar taxas de confirmação de transação, além de ter um tempo de confirmação de transação bastante curto, relativamente. O Capítulo 5 irá apresentar o experimento especificamente desenvolvido para a comprovação científica da viabilidade da monetização de hortas com o uso de criptomoedas, com seus resultados e medições. E no Capítulo 6, final, são colocadas as conclusões feitas pelo autor de acordo com os resultados dos dados que comprovam a eficácia da proposta de monetização de uma horta comunitária com o uso de IoT e criptomoeda.

1.1- Visão Histórica das Criptomoedas

É interessante uma análise cronológica da evolução dos assuntos pautados. Dessa forma, o leitor poderá observar nuances que, por vezes, poderia se lhe escapar, devido à falta dessa revisão histórica. E nesse contexto, uma visão da evolução dos ativos digitais certamente enriquece o tema proposto. Muitas criptomoedas, por seu protocolo, centralização, taxas, e outras características, não seriam adequadas à monetização de hortas e similares, outras seriam razoavelmente favoráveis a esta aplicação, e algumas (ou alguma) trará certamente uma otimização na monetização, permitindo redução de custos e aumento de lucro, sem, no entanto, reduzir a qualidade e nem a quantidade da produção da horta. Naturalmente, busca-se uma criptomoeda que não sofra incidência de taxas em suas transações, tenha confirmação de transação rápida na rede, seja segura, de fácil aquisição e operação, e que também possa ser facilmente associada aos códigos e programações necessários em todas as etapas de produção e venda dos produtos da horta.

A ideia de se fazer uma moeda digital surgiu enquanto a Internet estava se expandindo ao redor do mundo. Nos anos de 1990s, com a bolha das empresas dot.com, muitas ideias surgiram. Algumas ideias eram boas e prosperaram, outras nem tanto, mas a moeda digital foi uma dessas ideias que, ao que tudo indica, veio para ficar [11]. São alguns exemplos:

- **E-gold:** Foi uma das primeiras moedas digitais de controle centralizado que surgiram. Foi criada em 1996 por um oncologista chamado Douglas Jackson, e gerenciada pelo advogado Barry Downey, chegou a ter mais de 5 milhões de contas de usuários [12]. O E-gold cresceu muito, e foi bem aceito por diversos mercados, até que os *hackers* e os cibercriminosos começaram os ataques à plataforma. O uso para extorsões e fraudes levou à queda do E-gold.
- **WebMoney:** esta moeda digital surgiu em 1998, e é uma moeda digital quase como as atuais criptomoedas, exceto no que se refere à descentralização das transações na rede [12]. A empresa é sediada em Moscou, e oferece uma ampla gama de serviços financeiros, incluindo *peer-to-peer*, soluções de pagamentos, serviços de comércio, faturamento *online* e pagamentos, e até mesmo comércio baseado na Internet. Uma vez que a plataforma E-gold havia sido legalmente desativada, o WebMoney atraiu seus usuários, tanto os bons quanto os ruins. No entanto, o WebMoney fez alterações em seus serviços para impedir o seu uso em atividades ilegais.

- **Q ou QQ Coins:** é outra moeda digital que é baseada em commodities na plataforma de mensagens do Tencent QQ (programa de mensagens instantâneas gratuitas mais popular da China) e surgiu no início de 2005 [14]. As moedas Q foram tão eficazes na China que chegaram a desestabilizar o yuan chinês devido à especulação [15].
- **Liberty Reserve:** Em 2006 foi fundado o serviço de moeda digital Liberty Reserve. Este serviço permitia que os usuários convertessem dólares ou euros em sua moeda (dólar ou euro *Liberty Reserve*). Após a conversão os usuários podiam trocar livremente, com uma taxa cobrada pela plataforma centralizada de 1%. Como o serviço era utilizado para lavagem de dinheiro, o governo americano encerrou- a [13].
- **Perfect Money:** lançada em 2007 [16]. Os clientes da Liberty Reserve a inundaram depois que a primeira foi fechada pelos reguladores. A Perfect Money também oferece serviços semelhantes aos da Liberty Reserve sem a verificação. No entanto, a Perfect Money não está disponível nos Estados Unidos e nem para cidadãos dos EUA localizados em qualquer parte do mundo [17].
- **Bitcoin:** Introduzido em 2009, a partir da publicação de Satoshi Nakamoto [18], é uma moeda digital amplamente aceita [19]. Em 2016, o governo da cidade de Zug, Suíça, aceitou pela primeira vez o pagamento de taxas da cidade em Bitcoins. A cidade aceita Bitcoins como um meio de pagar quantias pequenas, até 200 francos suíços, em um teste e uma tentativa de avançar em sentido a tecnologias futuras. Para reduzir o risco, Zug converte imediatamente qualquer Bitcoin recebido em moeda suíça convencional [20]. É importante mencionar o fato de que o protocolo Bitcoin é de código aberto, evitando assim que qualquer pessoa tenha o monopólio sobre o sistema. Além disso, a segurança e a transparência associadas ao Bitcoin também merecem ser mencionadas. Ou seja, o Bitcoin parece ter atingido um grau de confiança que satisfaz todas as dúvidas sobre as moedas digitais que foram construídas ao longo dos anos de experiência com plataformas de moedas digitais centralizadas e proprietárias. Seguindo a popularidade do Bitcoin, existem novas moedas digitais que surgiram, incluindo moedas nacionais. Por exemplo: o Equador adotou sua própria moeda digital e até Barcelona. A Espanha tem planos de incluir a moeda digital como sua moeda legal [21].

Além da Bitcoin, há uma variedade de criptomoedas atuando paralelamente, cada qual com características próprias, mas mantendo uma base comum ideológica e estrutural. Dentre esse grupo, conhecido como *altcoins* (por serem alternativas à Bitcoin), pode-se mencionar: Augur (REP), Dash (DASH), Digibyte (DGB), Factom (FCT), Lisk (LSK), Litecoin (LTC), Nem (XEM), Pascalcoin (PASC), Pivx (PIVX), Ripple (XRP), Synereo (AMP), SingularDTV, Stratis (STRAT), Vertcoin (VTC), Waves (WAVES), Zcash (ZEC), Zerocoin, Namecoin (NMC), Peercoin (PPC), Dogecoin (DOGE), Mastercoin (MSC), Nxt (NXT), Emercoin (EMC), Aeon (AEON), Auroracoin (AUR), BlackCoin (BC, BLK), Coinye (KOI, COYE), DigitalNote (XDN), MazaCoin (MZC), Monero (XMR), PotCoin (POT), E-Coins (ECS). Na realidade, em meados de 2021 [22], registrou-se um total de pouco mais de 6.000 moedas digitais catalogadas, e um valor total de mercado de trilhões de dólares [23]. Todas estas criptomoedas, e muitas outras que porventura não são aqui mencionadas, mantêm alguma semelhança com o Bitcoin original, em sua forma, encriptação, mineração, *Blockchain* [24], PoW (Prova de Trabalho), etc. O que varia, em geral, são os usos em comunidades específicas, para transações específicas; mas sendo todas derivações da ideia do Bitcoin [25]. A *Blockchain* é uma sequência de registros distribuída na rede, e feitos de forma imutável. Estes registros guardam a informação de todas as transações feitas na rede, de forma a se ter em qualquer momento o conhecimento de quem enviou ou recebeu ativos na rede. Já a PoW – *Proof of Work*, é um protocolo utilizado para o consenso das transações na rede, utilizando de funções hash. Para um usuário realizar alguma ação, ele deve ser capaz de provar que realizou alguma tarefa, essa prova é a garantia de que o usuário gastou tempo para gerar uma resposta que satisfaça algum requisito do avaliador. Para esse sistema funcionar, tal prova deve ser trabalhosa de ser criada, mas facilmente verificada pelo avaliador.

- **Litecoin:** O protocolo Litecoin foi desenvolvido por Charles Lee [29], então funcionário da Google, em 2011. É um projeto de código aberto, que na época foi lançado em plataformas de desenvolvimento colaborativas. O tempo de mineração deste protocolo gira em torno de 2 a 3 minutos, mais rápido que o Bitcoin. O algoritmo usado para estabelecer o processo de mineração é o Scrypt [30]. A diferença entre os algoritmos de PoW do Bitcoin e do Litecoin é que o SHA256 do Bitcoin é focado no uso intensivo de processadores, e o Scrypt do Litecoin tem seu foco no uso intensivo

de memória. Dessa forma, enquanto que no Bitcoin existem *hardware* específicos para a mineração, no Litecoin podem ser utilizados *hardware* genéricos [31].

- **Dash:** Foi introduzido no mercado, em 2013, com o nome de Xcoin. Em janeiro de 2014 mudou de nome para Darkcoin, e finalmente em 2015 virou Dash, diminutivo de Digital Cash. É uma plataforma de pagamento descentralizada, totalmente privada, e rápida (em relação ao Bitcoin). Há um recurso no Dash, denominado *PrivateSend*, pelo qual as transações são misturadas com outros pagamentos anônimos, tornando quase impossível que alguém consiga rastrear a mesma. Contudo, assim como no Monero, isso favorece as transações ilícitas [34].
- **Ethereum:** É considerada a segunda geração de *Blockchain*, lançada em 2013 por Vitalik Buterin [26], onde foi descrito detalhadamente o protocolo Ethereum e a arquitetura de contratos inteligentes [27]. Gavin Wood [28] publicou as especificações técnicas da EVM (Ethereum Virtual Machine). Assim, em 2014 o projeto Ethereum se iniciou como um *Crowdfunding Project*, algo como um projeto que precisa angariar fundos.

Na Ethereum a diferença de tempo entre os blocos gerados é algo em torno de 14 segundos (em teoria), enquanto que no Bitcoin isso leva aproximadamente 10 minutos. O tamanho do bloco Ethereum depende do contrato feito entre as partes. Foi criada no Ethereum uma medida para se determinar o tamanho do bloco, que pode variar significativamente a cada bloco. Esta medida é o Gas. No Ethereum, o Gas é uma medida do esforço computacional. Para cada operação, uma quantidade fixa de Gas é atribuída (por exemplo, adicionar dois números custa 3 Gas, calcular um hash custa 30 Gas, enviar uma transação custa 21.000 Gas). Uma vez que a computação é cara (considerando-se que ela deve ser feita em todos os nós da rede), o consumo excessivo de Gas precisa ser desencorajado. Portanto, cada unidade de Gas deve ser paga pelo remetente da transação que acionou o cálculo. Habitualmente, o tamanho máximo de um bloco Ethereum gira em torno de 1.500.000 Gas, ao passo que uma transação básica tem 21.000 Gas. Cerca de 71 transações se encaixam em um bloco. No Bitcoin ocorrem cerca de 1.500 a 2.000 transações em um bloco. Atualmente, a maioria dos blocos Ethereum possui menos de 2 KB.

- **Monero:** Foi lançada em 2014, e tem a característica de dificultar o rastreamento das transações, ao contrário de outras moedas, como o Bitcoin, que possuem registros públicos. O Monero não segue o protocolo Bitcoin, mas um outro, chamado CryptoNote, mas, no entanto, tem sua estrutura baseada também em *Blockchain*. A principal vantagem da Monero sobre o Bitcoin é a maior proteção à privacidade [32] de quem faz transações com a moeda. Enquanto o Bitcoin é distribuído em carteiras digitais – da carteira A para a carteira B – a Monero cria uma espécie de senha que muda a cada transação. Valores transferidos só são visualizados por quem tem acesso a essa chave, tornando a localização dos donos mais difícil. Em contrapartida, isso facilita as transações criminosas de transferência de valores ilícitos na rede. A Monero tem um sistema de "lavagem" integrado. O método agrega todos os valores transferidos pela *Blockchain* em diversas senhas diferentes e redistribui para os mesmos donos. A quantidade de Monero permanece a mesma em cada senha e não gera prejuízo para o dono. No entanto, a origem dos valores fica impossível de encontrar. Essa estratégia é usada há tempos por quem usa Bitcoin e quer o máximo de anonimato, mas, na Monero, o recurso já vem embutido no código [33].
- **IOTA:** A moeda digital IOTA inicialmente aborda duas questões: a escalabilidade e as taxas cobradas pelas transações de mineração, que são problemas decorrentes do uso de *Blockchain*. É introduzido um novo conceito: o *Tangle* [35], que é baseado em um Grafo Acíclico Dirigido (DAG – *Directed Acyclic Graph*), com registros distribuídos na rede, sem mineradores e tampouco *Blockchain*. Na matemática, particularmente na teoria dos gráficos e na ciência da computação, um DAG consiste em vértices e arestas (também chamados de arcos), com cada aresta direcionada de um vértice a outro, nunca formando um loop fechado. Um grafo direcionado é um DAG se, e somente se, puder ser ordenado topologicamente, organizando os vértices como uma ordem linear que é consistente com todas as direções das arestas. Os DAGs têm inúmeras aplicações científicas e computacionais, que vão da biologia (evolução, árvores genealógicas, epidemiologia) à sociologia (redes de citações) à computação (programação). Mais adiante, na secção 4.3, serão apresentados maiores detalhes sobre o uso do DAG em IOTA.

Como não há taxas de mineração no *Tangle*, fica mais fácil fazer micro e até mesmo nano pagamentos entre dispositivos IoT. A IOTA é uma entidade sem fins lucrativos registrada sob as leis da Alemanha [36].

Desta forma, a IOTA é uma tecnologia totalmente diferente da maioria das criptomoedas existentes [37], e consegue solucionar algumas limitações da *Blockchain*. Além da grande escalabilidade (e velocidade), e da inexistência de taxas de transações, ela é resistente a ataques por computação quântica e possui estrutura modular e leve, própria para os pequenos dispositivos de IoT. Como não há nós mineradores na IOTA, todos os nós têm igual poder, e a comprovação de trabalho existe em cada uma das transações realizadas, garantindo maior eficiência. Como a estrutura do protocolo é modular e leve, pode ser facilmente integrada a equipamentos eletrônicos e até mesmo a pequenos dispositivos de IoT, como sensores, e integra a ligação M2M (*machine-to-machine*). Também dispensa a necessidade de *backups*, pois não há arquivos que possam ser perdidos. Basta que se tenha uma senha e a guarde de forma segura.

Nas moedas baseadas em *Blockchain*, quanto mais transações são realizadas, mais caras ficam as tarifas, e mais lenta fica a rede. No protocolo Bitcoin, por exemplo, transações menores que 0,01 BTC (Bitcoin) dificilmente são aceitas pelos nós mineradores, devido à taxa cobrada. E quando são aceitas, entram em uma fila de processamento muito demorada. Há também a questão da segurança, pois como a *Blockchain* fica cada vez maior, a carteira ocupa cada vez mais espaço no computador, o que leva o usuário a tentar carteiras leves (*light nodes*), possibilitando ataques. Na IOTA, quanto mais transações ocorrem na rede, mais rápida ela fica, pois a comprovação é realizada justamente durante as transações. Como as micro e nano transações serão maioria na IoT, é vantajoso para a rede IOTA fazê-las, pois se beneficiará com isso. Outra característica interessante para a IoT, é que um nó da rede IOTA não necessariamente precisa estar ligado à Internet para ter sincronismo com a rede. Os nós podem estar interligados por diversas formas, inclusive *Bluetooth*, por exemplo.

- **IOT Chain:** A IOT Chain foi criada em 2017 na China, e em 2018 recebeu o *Blockchain Excellence Award*, do Fórum Econômico Mundial de Davos, devido a seu progresso em resolver problemas reais, principalmente os relacionados a velocidade e

segurança em IoT. Ainda é um projeto relativamente recente, e sem um produto em funcionamento. Apesar de ter origem chinesa, ela foi registrada em Singapura, que tem uma regulamentação mais favorável à existência de criptomoedas que a China. Porém o grande foco da IOT Chain é o mercado chinês, tendo algum alcance em Singapura e na Austrália, sendo assim uma moeda mais regional, por enquanto, diferentemente da IOTA, por exemplo, que já tem projeção mundial.

A IOT Chain não teve ICO (*Initial Coin Offering*), tendo uma venda direta privada em novembro de 2017, onde metade dos 100 milhões de *tokens* previstos entraram em circulação. A ICO é a oferta inicial da moeda, onde a *startup* que a lançou busca arrecadar fundos para seu projeto. Em geral a *startup* cria um *White Paper* que descreve o projeto, a necessidade que o projeto atenderá após a conclusão, quanto dinheiro é necessário, quantos *tokens* virtuais os fundadores manterão, que tipo de dinheiro será aceito e por quanto tempo durará a campanha da ICO. O *token* (ativo digital) da IOT Chain é chamado de ITC, e pode ser utilizado para transportar informações tanto de valores, quanto de propriedade entre os dispositivos da rede.

O foco da IOT Chain é desenvolver um sistema operacional leve e seguro para atender as conexões do mundo digital na IoT. A ideia é oferecer um pacote completo, com a parte de software e com a parte de hardware, tendo um chip implantado dentro de dispositivos eletrônicos.

A IOT Chain utiliza uma tecnologia híbrida, combinando *Blockchain*, PBFT (*Practical Byzantine Fault Tolerance*), e DAG, sendo uma rede que foca na segurança, inclusive contra computação quântica.

A IOT Chain também mira o mercado de economia compartilhada, mercado esse que cresce de forma exponencial a cada dia. Ela permite que haja compartilhamento de dados diretamente entre as coisas da rede, como por exemplo um carro que compartilha seus dados com os outros carros que estão na mesma localidade, facilitando as condições de tráfego, o que minimiza a necessidade de intermediários, tais como agentes de trânsito. Para incentivar o compartilhamento das informações, a proposta da IOT Chain é remunerar o compartilhamento dos dados. Assim, uma indústria de bicicletas por exemplo, pode monitorar o uso de seus produtos, com o intuito de aperfeiçoar o produto, fazendo a seus clientes uma oferta de compra e uso

dos dados de utilização das bicicletas. Como a bicicleta terá um chip de IOT Chain, a indústria poderá facilmente coletar os dados, após o acordo de uso com o cliente.

A IOT Chain aceita tanto transações sem custo quanto transações com custo. Transações de pequeníssima monta não serão cobradas, mas transações maiores serão, pois a IOT Chain considera que transações sem taxas podem comprometer a segurança da rede, uma vez que facilitam grandemente os ataques do tipo spam na rede. As taxas dependem somente do tamanho, em bytes, da transação, sendo altamente previsíveis, diferente por exemplo de criptomoedas que utilizam somente a *Blockchain*, onde as taxas variam dependendo da demanda e da oferta. Segundo a proposta da IOT Chain as taxas sempre serão muito baratas. Para o consenso de transação a IOT Chain utiliza os *Witness Nodes*, que são nós que testemunham as transações, não tendo o papel do minerador na rede. Esses nós são remunerados para fazer o papel de testemunhas das transações [38].

De todas as criptomoedas mencionadas, as que realmente obtêm destaque, por suas características específicas, ou por seu alcance global, são atualmente a Bitcoin, que praticamente originou o uso de *Blockchain*, a Ethereum, que é considerada a segunda geração do *Blockchain*, e a IOTA, que apresenta uma proposta de uso específica para IoT, sendo adequada a micro e nano transações financeiras, por não ter taxas de mineração associadas, e nem o uso de *Blockchain*. No capítulo 4 serão apresentadas de forma mais detalhada essas três criptomoedas, de uma forma suficiente para se entender a grande maioria das criptomoedas da atualidade.

Capítulo 2 – AGRICULTURA, CADEIAS PRODUTIVAS E TECNOLOGIA

‘Não existe qualquer tipo de dúvida que os desafios postos à agricultura somente serão superados com a adoção de tecnologias modernas.’ (EMBRAPA)

De hoje o Brasil é um dos líderes mundiais em produção e exportação agrícola, isso não se deve somente a suas condições naturais de clima, relevo, solo e outras; mas a ciência aliada ao empreendedorismo e também políticas de incentivo são quesitos importantes nessa equação. Praticamente todos os produtos agrícolas e pecuários estão em franco crescimento de produtividade, para atender tanto o mercado interno quanto as exportações. E essa aceleração do crescimento se deve, em grande parte, à aplicação de tecnologias que, ao mesmo tempo em que propiciam um aumento de produtividade e qualidade, reduzem o consumo de recursos naturais fundamentais, contribuindo também para a ecologia. O crescimento populacional, principalmente nos centros urbanos, as mudanças de hábitos alimentares, o poder econômico, os novos mercados internacionais, são fatores que implicam em uma maior demanda por energia, água e alimentos, e como a simples exploração de recursos naturais é limitada e gera degradação, então a saída é o uso da tecnologia para maior produção. A agricultura que faz uso das tecnologias digitais, chamada de ‘agricultura 4.0’, se aproveita desse arcabouço de recursos tecnológicos para atender a essa crescente demanda e ainda assim preservar melhor os recursos do planeta. Hoje, no campo, já se faz uso de genética, robótica, nanotecnologia, nanossatélites, inteligência artificial, DLTs e criptografia, sensoriamento, luminotécnica, GPS, computação em nuvem, bancos de dados, IoT, telemetria, drones, dentre outros, para o desenvolvimento e gestão desses sistemas agroalimentares [39]. E ainda há as tecnologias emergentes, que poderão trazer grandes mudanças que ainda não podem ser previstas, como a computação quântica, que pode acelerar o cálculo em sistemas que envolvam cálculos massivos, tais como simulação de cenários sobre impactos climáticos em diferentes áreas, volatilidade de preços e flutuações no mercado, e a robótica de enxame, em que um grande número de robôs age de forma associada para a coleta de dados. Essas são

tecnologias capazes de alterar significativamente o cenário atual, abrindo novas possibilidades ainda não viáveis no estágio atual. Naturalmente, nem todas essas citadas tecnologias são aplicáveis em hortas comunitárias urbanas e periurbanas, devido ao custo, área de plantio reduzida, dentre outros fatores, mas ainda assim é interessante que se discorra sobre essas possibilidades, uma vez que cada horta, em cada local ou região de plantação, pode fazer uso de diferentes acervos tecnológicos para sua instalação, operação, manutenção, e monetização.

Não é mais uma opção esse processo de transformação digital no campo, mas um caminho imprescindível para tornar a agricultura brasileira mais competitiva e com maior valor agregado [40].

Os benefícios na cadeia produtiva podem ser, a grosso modo, relacionados, conforme a Tabela 1 a seguir:

Tabela 1 - Benefícios na cadeia produtiva [40].

Fabricantes de insumos	Produtores	Processadores	Distribuidores	Consumidores
Eficiência produtiva	Aumento de produtividade	Planejamento e ações gerenciais	Diversidade de produtos	Conectividade urbano-rural
Otimização de recursos	Sustentabilidade	Agregação de valor	Novos nichos de mercado	Protagonismo digital
Novos produtos	Novas oportunidades	Redução de perdas	Plataformas de comercialização	Valorização cultural
Segurança e qualidade	Poder de decisão	Qualidade dos alimentos e bebidas	Eficácia nas entregas	Transparência e engajamento
	Sucessão rural	Segurança e Certificações	Rastreabilidade	Novos negócios

A transformação digital da agricultura também tem seus princípios embasados na proposição da ONU – Organização das Nações Unidas, que em sua Agenda 2030 propõe 17 Objetivos de Desenvolvimento Sustentável (ODS) para a erradicação dos problemas socioambientais, conforme a Figura 4 a seguir:



Figura 4 – 17 objetivos da Agenda 2030 da ONU [41].

De acordo com a UNGC – *United Nations Global Compact* [42], em 2021 o mercado global da agricultura digital irá movimentar 15 bilhões de dólares. Os recentes aspectos econômicos mundiais, e também a questão da pandemia do Covid-19, geram incertezas em torno desse número, podendo até aumentar essa estimativa.

2.1 Revisão de Literatura

A agricultura urbana tem-se apresentado atualmente como uma das soluções para a questão da insegurança alimentar. Pinderhughes [43] define agricultura urbana como a prática da produção de alimentos, plantas medicinais e materiais combustíveis na área de influência direta de uma cidade. A escala de produção é pequena e pode ser praticada em terrenos ociosos, terraços ou espaços públicos e privados. Seus benefícios incluem a diminuição dos impactos da agricultura convencional, a melhora das condições nutricionais dos usuários, a melhora das condições físicas e psicológicas dos praticantes envolvidos.

Discutir a agricultura urbana remete à ideia de hortas urbanas, que pode ser uma atividade agrícola de inclusão, pela sua importância econômica, pela geração de emprego e renda que ela pode proporcionar aos que dela fazem seu meio de vida, de acordo com Fernandes et al. [44].

Bolfe et al. [45] traçam um panorama dos desafios, das tendências e das oportunidades que a agricultura digital traz. Nesse trabalho, uma interessante Figura 5 elenca esses desafios, tendências e oportunidades:

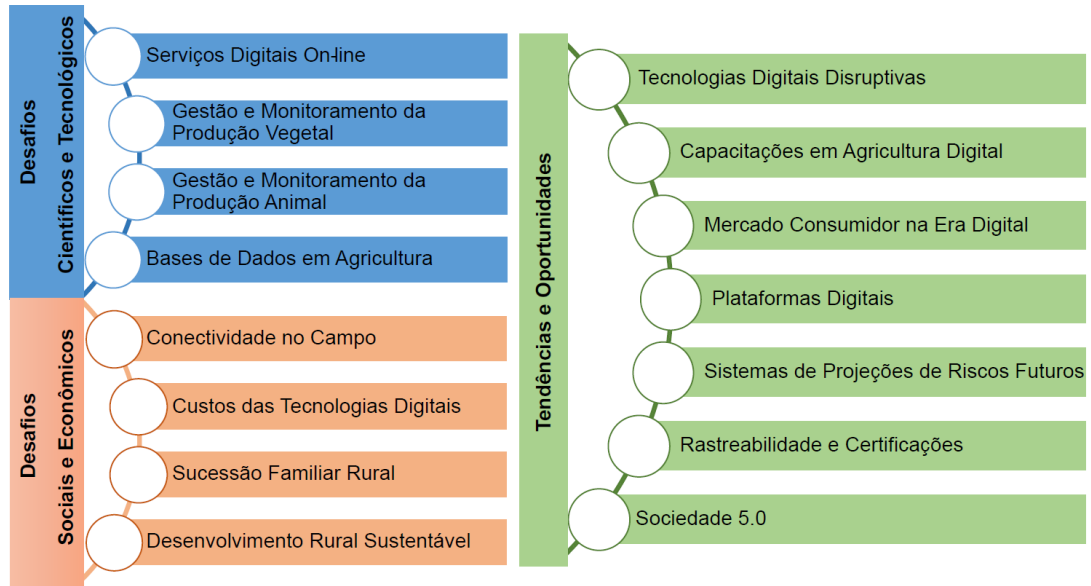


Figura 5 – Desafios, tendências e oportunidades na agricultura [45].

Em termos de planejamento e gestão urbana a implementação de projetos relacionados às hortas urbanas proporciona benefícios de caráter permanente, como o reaproveitamento dos resíduos provenientes da poda da arborização viária para formação do composto orgânico, aumento da permeabilidade do solo, ampliação das áreas verdes, limpeza de terrenos, combate as áreas de risco, proteção aos mananciais e, mudança na paisagem urbana, segundo Ribeiro [46].

Pinto [47] corrobora com tais afirmações quando cita que: “*entre os inúmeros benefícios das hortas urbanas destacam-se: a produção de alimentos de qualidade, a reciclagem de resíduos orgânicos, utilização racional de espaços, a educação ambiental, o desenvolvimento humano e qualidade de vida, a segurança alimentar, o desenvolvimento local, o recreio e o lazer, a farmácia caseira, a forma de microclimas e manutenção da biodiversidade, a infiltração de águas pluviais, a proteção do solo, o valor estético, a diminuição da pobreza, a geração de renda, a integração social, entre outros.*”

Hortas urbanas são consideradas áreas verdes urbanas e, sob o ponto de vista ambiental e da percepção das pessoas (usuários, produtores e transeuntes), podem representar diversos fatores, como: função química, através da absorção de gás carbônico e a liberação de oxigênio; função física, através da estabilidade climática, diminuição de temperatura e aumento da umidade do ar, melhoria das condições de solo urbano, do ciclo hidrológico redutor de poluição atmosférica e acústica; função paisagística, pela mudança de textura do elemento construído e aspectos estéticos; função psicológica, pelo conforto e bem estar que ela reproduz; e função ecológica proporcionado pelo abrigo e alimentação da fauna remanescente além de contribuir para o aumento da diversidade e da quantidade, relata Fátima [48].

Outros aspectos positivos relacionados às hortas urbanas são: ocupação de terrenos baldios, complementação da alimentação das famílias, acesso a alimentos frescos e saudáveis, qualidade regularizada aos produtos produzidos, mudança de hábitos e práticas alimentares saudáveis, inserção de indivíduos no mercado de trabalho e geração de renda. Da mesma forma, que as famílias envolvidas utilizam a área das hortas para o fortalecimento das relações sociais, realização de diálogos a respeito da conjuntura local comum a todos e o papel da organização social frente a esse panorama, relatam Fernandes et al. [49].

Contudo, as hortas urbanas podem ser focos de contaminação e poluição, pela presença de metais pesados provenientes da emissão atmosférica de veículos conforme estudos demonstrados por Varennes [50]; Dinardi et al., [51]; e Pinto e Ramos [52]. Nestes casos, diretrizes de escolha da área e plantio de espécies devem ser levadas em consideração.

A implantação das hortas urbanas exige a criação de uma infraestrutura de gestão e gerenciamento. Desta feita, é fundamental a aquisição de uma área, ferramentas, equipamentos, instalações, sistema de adubação, rede de abastecimento de água ou irrigação, aquisição de espécies e variedades, pré-disposição para controlar organicamente as pragas e doenças, bem como forma e reprodução das hortaliças, diz Francisco Neto [53]. Mas, o principal é que as hortas urbanas devem ser encaradas como políticas públicas.

Para explicitar os fenômenos pertencentes ao tema horta urbana, se faz necessário expor o tema que constitui e fornece elementos para a explicação das hortas:

as políticas públicas. De acordo com Souza [54], não existe uma única, nem melhor, definição sobre o que seja política pública. Suas discussões definem o termo como um campo dentro do estudo da política que analisa o governo à luz de grandes questões públicas, como um conjunto de ações do governo que irão produzir efeitos específicos. Sua discussão teórica em resumo relata que política pública é a soma das atividades dos governos, que agem diretamente ou através de delegação, e que influenciam a vida dos cidadãos.

Segundo a Fundação Magabeira [55], entende-se que a política pública, enquanto geração de emprego e renda, é parte de um conjunto maior denominado de política de trabalho, que inclui o emprego assalariado de boa qualidade, uma vez que a estratégia de desenvolvimento econômico deve contemplar um conjunto articulado de atividades produtivas, com ênfase naquelas que geram ocupações de alta qualidade. Pode-se entender que a política de geração de trabalho e renda para pessoas de baixo poder aquisitivo tem limites claros, sendo um dos mais significativos a incapacidade de, por si só, enfrentar a pobreza. De acordo, ainda, com a Fundação Magabeira essencialmente pode-se considerar os seguintes objetivos da política de geração de trabalho e renda:

- Proporcionar ganhos de renda para os destinatários dessas políticas;
- Ampliar a rede social de seus destinatários, entendida rede social como articulação de vínculos ou contatos sociais, expressos pela relação entre indivíduos e organizações; e,
- Estimular o protagonismo social de seus beneficiários.

A partir destes elementos, pode-se entender que as políticas públicas possuem relevância para a sociedade em geral, bem como para aquelas que necessitam da complementação da renda. Contudo, no caso brasileiro, muitas políticas públicas são confundidas como políticas de governo. Esta última se caracteriza como uma política que se restringe a continuidade apenas de um específico governo, ocorrendo sua continuidade somente se houver interesse por parte dos sucessores do poder político. Contudo, se existir pressão e ainda interesse de vários grupos de poder, pode-se transformar uma política de governo em política pública, garantindo assim, a

continuidade, independentemente de quem esteja no poder. Diante disso, um obstáculo encontrado pelos teóricos diz respeito a formação das políticas públicas que geralmente são organizadas e implementadas em sua grande maioria por burocratas, políticos locais e grupos de interesses. No que tange este fato, Kerbauy [56] relata que *apesar da existência de novas instâncias decisórias locais (Conselhos) e da entrada de novos atores políticos no cenário local, aparentemente a formação de políticas municipais continua sendo monopolizada pelos políticos locais, burocratas e grupos de interesse, com um baixo grau de institucionalização e de consolidação das práticas de negociação*. Diante do pressuposto, é consenso que muitas políticas públicas e decisões devem ser descentralizadas e assim posicionar-se no contexto local. O fato contribui para atender na sua essência as demandas que existem entre as diversas comunidades, já que a proximidade contribui com uma análise profícua de determinada realidade. Isso leva os diversos poderes a dialogar com a sociedade, já que antes, isso não ocorria. Como afirma Kerbauy, prefeitos, vereadores e sistema jurídico que, durante séculos, definiram o estruturado poder local no Brasil, agora são obrigados a dialogar e interagir com a sociedade, especialmente os conselhos gestores de políticas sociais e o orçamento participativo na busca de articulação entre atores sociais e políticos, além dos arranjos institucionais que permeiam o governo local.

No Brasil, a aplicação da tecnologia na agricultura rural ou urbana, e na pecuária, já se tornou uma política pública, e os incentivos governamentais à pesquisa e desenvolvimento tecnológico são cada vez maiores e alavancam a produção, com maior qualidade. A Embrapa Informática Agropecuária [57] realiza pesquisas em bioinformática aplicada, biologia computacional, geotecnologias, inteligência computacional, matemática computacional, modelagem agroambiental, novas tecnologias, organização e tratamento da informação eletrônica, software livre, e outros, e realiza a transferência de tecnologia para os setores privados e de produção. Especificamente, dentro das novas tecnologias, surgem pesquisas relacionadas a hortas urbanas, tratando de sensoriamento de solo e clima, irrigação, iluminação natural e artificial, adubação e controle de pragas de forma orgânica, compra de insumos, produtividade, comercialização e distribuição de produtos, etc. Soares [58] apresenta um estudo da utilização e impactos da Internet das Coisas em fazendas e hortas urbanas, para redução de custos, menor uso de químicos, e menor conflito com o meio

ambiente. Situa o uso da IoT na produção de alimentos urbanos e sua importância no planejamento da produção.

A Internet das Coisas é o conjunto de ações que são feitas para se conectar as coisas físicas à Internet, de acordo com Kranenburg et al. [59]. Um objeto a ser conectado na rede necessita de algum software associado ao mesmo, transformando-se em um *Smart Object*. Atualmente, além dos computadores convencionais, outros equipamentos já se conectam à Internet, tais como TVs, laptops, geladeiras, fogões, eletrodomésticos, automóveis, smartphones, sensores, atuadores, etc. Até aplicações em educação são elencadas na Internet das Coisas (Deidmar et al.) [60], e *smart cities* (Sun et al.) [61]. A *domótica* nas residências, a *robótica* nas indústrias, a chamada Agricultura 4.0, são exemplos de coisas que se conectam nas redes, e fazem uso dos dados que os dispositivos conectados transmitem e recebem, promovendo o avanço tecnológico desejado, relata Amorin [62]. A *Indústria 4.0*, termo de origem alemã, segundo Oliveira et al., é um conjunto de tecnologias utilizadas na indústria para automação, interoperabilidade e troca de dados entre dispositivos e sistemas: elementos computacionais colaborativos, Internet das Coisas e computação em nuvem. É importante que na IoT ocorra a convergência de três paradigmas: orientado para a Internet (*middleware*), orientado a coisas (sensores e atuadores), e orientado à semântica (representação e armazenamento das informações) [63].

De maneira semelhante à Lei de Moore [1], estudos realizados na China [64] mostraram que a Internet dobra de tamanho a cada 5,32 anos (Evans), conforme a Figura 6:

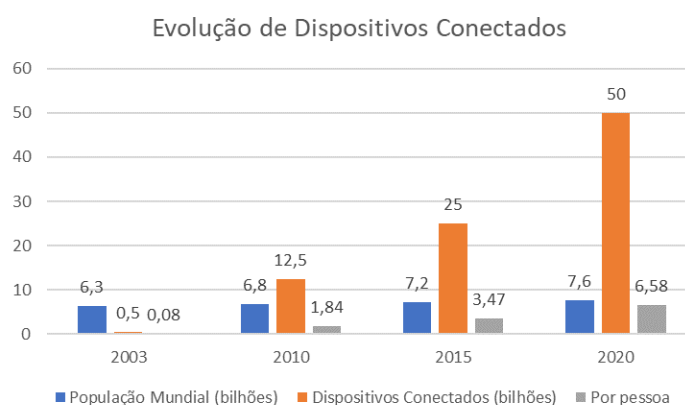


Figura 6 - Crescimento dos dispositivos conectados [64]

A IoT é a primeira evolução real da Internet, levando a aplicações revolucionárias da rede. A IoT já transformou a Internet em algo sensorial (temperatura, pressão, vibração, iluminação, umidade e estresse), permitindo que as ações sejam mais proativas e menos reativas.

Porém, da mesma forma que a IoT traz benefícios, ela também aumenta os riscos relacionados à segurança e privacidade, narra Leal [65]. As ameaças vão muito além do roubo de informações ou da impossibilidade do uso de alguns serviços, elas são ameaças reais, inclusive de segurança física, dizem Ahmed et al. [66]. E neste contexto as criptomoedas se inserem, pois, seus protocolos, além do *token* de moeda para pagamentos, podem também ser utilizados para autenticar, autorizar e auditar os dados gerados pelos dispositivos da rede. A natureza descentralizada desses protocolos (*Blockchain, Tangle*), elimina a necessidade do "terceiro de confiança", como por exemplo, um banco para realizar uma transação financeira, conforme Kramer [67].

Segundo Alberti [68], para que um pagamento entre coisas na rede possa ser efetivo e confiável, é necessário que princípios de segurança sejam observados:

- Integridade, que dá a certeza de que a informação não foi alterada, exceto por quem tem esse direito. Os mecanismos criptográficos de verificação da integridade são comumente utilizados nas criptomoedas para a confirmação;
- Disponibilidade, que garante que os usuários utilizem o sistema sempre que necessário. A criptomoeda permite que os usuários tenham a disponibilidade da rede sempre, pois estabelecem conexões com vários outros usuários, e mantêm as transações de maneira descentralizada com várias cópias na rede;
- Privacidade, que garante que a informação não será obtida por pessoas não autorizadas. Nas criptomoedas, os *hashes*, ou resumos criptográficos, garantem a privacidade;
- Autenticação, Autorização e Auditoria, para verificar a identidade de quem realiza uma função no sistema, verificar os direitos desse usuário, e armazenar as informações de uso do usuário. Tanto a *Blockchain* quanto o *Tangle* garantem estas funções, pois somente os usuários que possuem as chaves privadas podem realizar as transações, e todas as transações são públicas e auditáveis [69];

-
- Não Repúdio, que garante que um usuário não negue uma transação que realizou.

Na IoT a ideia é que a rede se torne uma rede de dispositivos autônomos [70], que interajam uns com os outros e com o ambiente, tomando decisões sem a intervenção humana quando for o caso, relatam Serra et al. [71]. E é justamente nisso que as tecnologias *Blockchain* e *Tangle* ajudarão a alavancar a IoT, formando uma base que suportará a economia compartilhada baseada em comunicações M2M (*machine-to-machine*).

Wörner and Von Bomhard [72] descrevem uma troca simples de dados por dinheiro eletrônico, entre um sensor e um requisitante, utilizando Bitcoin. O sistema descrito é composto de três partes:

- Dispositivo IoT: deve anotar uma solicitação de dados ao receber um pagamento e ser capaz de criar e publicar uma transação contendo os dados solicitados;
- Cliente requisitante: deve ser capaz de enviar o pagamento ao endereço do sensor, e deve monitorar as alterações na *Blockchain* até detectar a transação com os dados enviados pelo dispositivo IoT;
- Repositório de dispositivos IoT: Os sensores devem ser registrados no repositório, para serem encontrados pelos clientes. Uma entrada no repositório deve conter pelo menos o endereço do sensor, quais os dados que ele oferece, preço, e metadados adicionais, como localização, tags, etc.

A primeira versão da *Blockchain*, que é o Bitcoin, foi feita pensando na descentralização de dinheiro e de pagamentos [73], enquanto que a segunda versão, que está associada ao Ethereum, visa à descentralização de mercados, e permite a transferência de muito mais coisas que moeda, utilizando a cadeia de blocos [74]. A *Blockchain* pode assim ser utilizada para registrar, confirmar e transferir todo tipo de contratos e propriedades, em sua segunda versão. O contrato inteligente regula as transações entre as entidades na rede. Nick Szabo [75] definiu um *Smart Contract*

como "*um protocolo de transação computadorizado que executa os termos de um contrato*". Ele sugeriu a transposição de cláusulas contratuais em código para propriedades que possam executá-las [76], de modo a minimizar a necessidade de intermediários confiáveis entre as partes das transações, e a ocorrência de exceções maliciosas ou acidentais.

Três características dos contratos inteligentes que os diferenciam são: autonomia, autossuficiência e descentralização, dizem De Filippi e Mauro [77]. Autonomia significa que, depois de lançado e em execução, um contrato e seu agente iniciador não precisam estar em contato. A segunda característica é que os contratos inteligentes podem ser autossuficientes em sua capacidade de gerar recursos, isto é, arrecadar fundos ao fornecer serviços ou emitir equidade e gastá-los em recursos necessários, como o poder de processamento ou o armazenamento. E a terceira característica é que os contratos inteligentes são descentralizados, na medida em que não subsistem em um único servidor centralizado, sendo distribuídos e auto executados em nós de rede [78].

Barros et al. [79] relatam a preocupação com a valorização da água consumida na formação do preço de hortaliças. Para determinar o volume de água virtual das hortaliças, no trabalho desse autor a irrigação foi monitorada durante 35 dias, tempo para completar o ciclo de vida da cultura. Feito isso, calculou-se o volume da evapotranspiração da cultura, o que resultou na quantidade de água que é perdida para o ambiente e não é computada no volume de água virtual. A quantidade de água gasta na irrigação foi de 137.320 litros, com uma perda de 15,01% do volume para o ambiente, o que resultou 116.710,44 litros de água virtual gasta na produção. Também preocupado com o desperdício de água na irrigação, Santos e De Bone [80] apresentam um sistema de irrigação automático e inteligente, com o uso de Internet das Coisas, aplicado a estufas de ambiente controlado em temperatura e umidade, fazendo uso de sensores e atuadores. Camargo et al. [81] propõem uma rede de sensores eletrônicos de baixo custo, *open source*, baseados na tecnologia Arduino, desenvolvendo um sistema de coleta, armazenamento e análise de indicadores em tempo real para monitorar os parâmetros de temperatura, umidade, luminosidade e umidade do solo, além de controlar a aplicação de insumos em hortas cultivadas nas escolas municipais de Bagé-RS, tendo como intuito a melhoria no rendimento das culturas, bem como, o uso consciente dos recursos naturais, o principal deles, a água. Utiliza Internet das

Coisas e Sensoriamento. Os dados coletados são mantidos em um servidor Raspberry com banco de dados Mongo DB e, os gráficos gerados dinamicamente utilizando Chart.JS.

Yang et al. [82] apresentam um aplicativo de manejo de hortaliças, que permite o rastreamento desde a produção nos canteiros, consumo de insumos, armazenamento, transporte, distribuição e vendas, com os dados armazenados em nuvem, e com uso de QR Codes e RFID.

Ribeiro [83] apresenta um projeto de rastreabilidade de hortaliças, com o desenvolvimento de um aplicativo multiplataforma, onde toda cadeia produtiva de hortaliças é identificada e protocolada. O sistema é desenvolvido em linguagem de Programação C# (C-Sharp), plataforma ASP.NET, como Aplicação WebForms em Banco de Dados SQL Server 14 fundamentado para apresentar dados de rastreamento de hortaliças evidenciado com o acesso informativo de cada fase do processo produtivo e logístico disponível no relatório acessível ao usuário final.

Silvano et al. [84] demonstram que a tecnologia IOTA e seu sistema de registros distribuídos, o *Tangle*, é bastante adequada ao acompanhamento da situação de produtos, sendo melhor que a tecnologia *Blockchain*, dando suporte a um grande volume de transações advindas de dispositivos de IoT. No sistema IOTA/*Tangle*, são permitidas transações de valor zero, uma vez que não há taxas de transação, e as informações relacionadas aos produtos, data, hora, situação de carga, etc., podem ser obtidas e validadas por meio do *Tangle*.

Já Nakada et al. [85] mencionam que os micropagamentos de IoT podem ser habilitados com as criptomoedas e as tecnologias de registros distribuídos (DLT – *Distributed Ledger Technologies*), mas que as criptomoedas baseadas em *Blockchain* apresentam a limitação das taxas de transação e da latência. A IOTA, que não requer um processo de mineração, pode fazer as micro transações sem taxas e com alta velocidade. É apresentado pelos autores um estudo de viabilidade da IOTA em dispositivos de IoT, usando um sistema de micropagamento em um Raspberry PI, e são feitas medidas de tempos de transação. Concluem os autores pela viabilidade dos micropagamentos com IOTA, mas em dispositivos de menor poder de computação a latência aumenta, devido à tarefa de cálculo de *hash*.

Elsts et al. [86] alertam justamente para a questão da computação em dispositivos pequenos de IoT, principalmente aqueles alimentados por baterias, onde o esforço computacional pode reduzir a duração da carga da bateria, e apresentam uma solução, onde um servidor *proxy* possa ser utilizado para esse processamento, ao invés de os próprios dispositivos de IoT o fazerem.

Conforme vimos, em termos de aplicação de tecnologias de IoT em hortas de pequeno porte, comunitárias ou não, a literatura é bastante vasta, mas a maioria dos estudos apresentam o uso da tecnologia somente para controle de irrigação, temperatura e iluminação. A maior parte dos estudos usa o Arduíno como plataforma, mas o Raspberry também é bastante citado. Porém, o que é difícil de se encontrar na literatura é a associação dos controles das funções citadas de uma horta com sua monetização com ativo digital, sendo que este trabalho que ora se apresenta traz como diferencial justamente essa associação das funções de IoT de uma horta compartilhada com sua monetização, gerando um ambiente de economia digital compartilhada.

2.2 Controle da Produção Agrícola

Gerenciar uma fazenda de produção agrícola, ou mesmo uma horta comunitária, não é uma tarefa simples. Na Figura 7 abaixo vê-se de forma abrangente o processo de negócio no manejo de uma produção de hortaliças. Manejar a safra é uma das atividades, mas também precisa-se gerenciar os insumos, a qualidade, analisar a lucratividade, etc. Atualmente o gerenciamento de uma produção agrícola não é feito somente dentro da propriedade, como era antigamente, é importante observar e acompanhar o mercado, o transporte da produção, a distribuição, vendas, etc. A produção agrícola, em grande, média, ou pequena escala, deve sempre estar associada a métodos modernos e eficientes de gestão, para se obter melhores resultados, com menor custo, e maior qualidade.

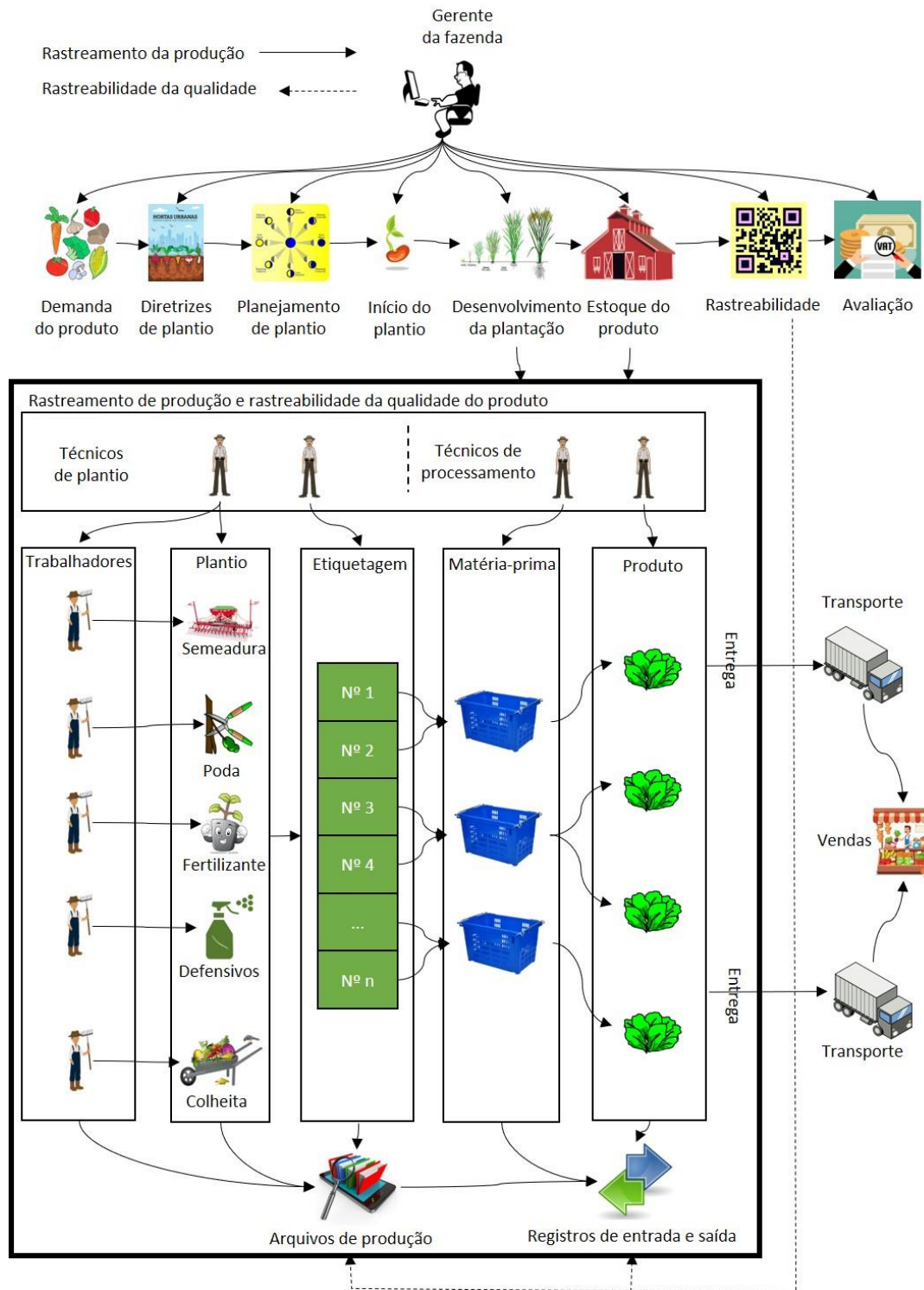


Figura 7 - O processo de negócios de gestão da fazenda [87].

Até uma ou duas décadas atrás a monitoração da produção agrícola era feita de forma totalmente manual, *in loco*. Tudo tinha que ser verificado pessoalmente, como por exemplo: falta de irrigação adequada, ataque de pragas, doenças, crescimento de mato e ervas daninhas, controle de minerais e nutrientes do solo, dentre outros. Ainda hoje uma grande parte desse controle é feita de forma manual, mas aos poucos os processos estão sendo automatizados, e já existem muitas empresas trabalhando nessa automação. Diversas *Startups* desenvolvem soluções para os processos de produção agrícola. São as chamadas ‘AgTechs’ as empresas de tecnologia aplicada ao agronegócio [88].

O uso de imagens obtidas por drones ou satélites tem sido cada vez mais importante na gestão das lavouras, principalmente na detecção de eventos indutores de estresse na plantação. As câmeras multiespectrais aplicadas em drones têm sido amplamente utilizadas no monitoramento da saúde da plantação por imagens. Essas câmeras contam com múltiplos sensores e filtros de alta qualidade que interagem com a luminosidade gerada pelas plantas (invisível a olho nu) para captar diferentes bandas com largura estreita, permitindo acompanhar o desenvolvimento das plantas. A Figura 8 ilustra:

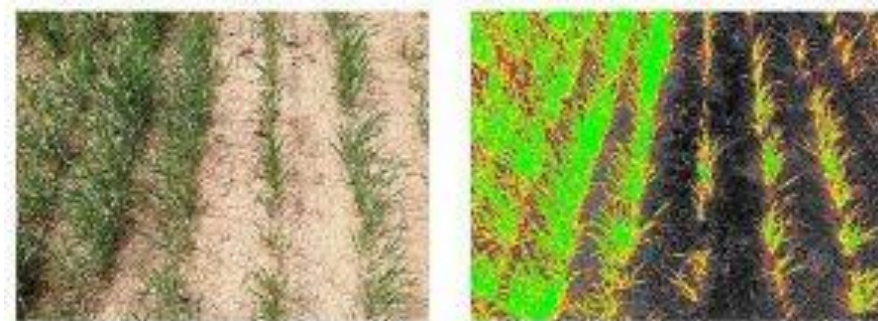


Figura 8 – Comparação de uma imagem com câmera RGB e câmera Multiespectral [89].

Já as câmeras hiperespectrais são ainda mais eficientes que as multiespectrais, pois além de fazer uma estimativa da área plantada, um levantamento do número de plantas em determinada área, verificar a saúde das plantas e da cultura, detectar pragas na plantação e gargalos no processo produtivo, elas têm também o potencial de prover detalhes sobre as propriedades físico-químicas dos materiais presentes na superfície filmada, incluindo composição química/bioquímica, grau de cristalinidade e

morfologia desses materiais [90]. A Inteligência Artificial é de grande valia no processo, pois ela pode combinar os resultados da análise das imagens com outras informações, tais como condições climáticas, dados históricos do manejo da lavoura, sensoriamento das condições do solo, etc., de forma a tornar o processo cada vez mais autônomo [91]. A correção dos fatores de estresse da plantação, e mesmo sua prevenção, também podem ser determinadas pela Inteligência Artificial, que pode acionar veículos autômatos, aéreos ou não, para o controle de pragas, adição de nutrientes no solo etc. Esses veículos são monitorados por localização GPS, telemetria e outros meios.

2.3 Armazenamento e Uso de Dados

Uma base de dados muito sólida é de fundamental importância para que as ferramentas de Inteligência Artificial e Aprendizado de Máquina sejam utilizadas de forma confiável na prática. A gama extensa e altamente variável de fatores que influenciam nas condições da plantação torna necessária a coleta de muitos milhares de amostras, sejam imagens, medições de sensores, análises, etc. Outro fator importante é o cadastramento dessas informações quanto à sua representatividade de local, clima, temperatura e outras características que as tornem particulares. É bastante complexa essa aquisição e classificação de dados [92]. A EMBRAPA [93] menciona uma iniciativa proposta por Alan Irwin [94], chamada de ‘*Citizen Science*’, na qual ele sugere o uso de dados coletados por voluntários para formação de bancos de dados. Por exemplo: os dispositivos de comunicações móveis com capacidade de adquirir imagens hoje já são presença quase que global, e poderiam ser utilizados por produtores e trabalhadores rurais para enviar imagens de plantas com estresse ou doenças para um servidor específico, onde os estudiosos de plantas poderiam realizar a classificação dessas imagens e sua inserção no banco de dados. Mas a própria EMBRAPA acredita que é mais factível o compartilhamento de bases de dados geradas por grupos distintos, e ela já contribui com esse compartilhamento em plataformas tais como o Digipathos [95] que está integrada à Rede de Repositórios de Dados Científicos do Estado de São Paulo [96].

Um passo complementar para o compartilhamento de bases de dados é a adesão aos princípios FAIR (*Findable, Accessible, Interoperable and Reusable*) [97]. OS princípios FAIR foram inicialmente criados porque a produção de conhecimento baseada em dados tem se acelerado muito, e as novas tecnologias de acesso, transferência e análise de dados criam oportunidades inéditas para o avanço do conhecimento científico. Mas, para tanto, é importante que os dados coletados estejam bem estruturados, armazenados de forma apropriada e disponíveis para uso. A boa gestão de dados passou a seguir estes princípios. A palavra ‘FAIR’ é um acrônimo, cujas letras significam:

- F – *Findable* (Achável): Os dados ficam disponíveis para serem descobertos por outros. Os dados e metadados devem adotar um Identificador persistente único; os metadados devem ser ricos e ambos indexados em repositórios confiáveis, de forma que os mecanismos de busca possam encontrá-los facilmente;
- A – *Accessible* (Acessível): Outros podem acessar os dados, mediante o uso de protocolos padronizados, abertos e gratuitos, que ofereçam autenticação e acesso aos metadados mesmo quando o dado não estiver mais disponível, sendo necessário o uso de um conjunto de estratégias de preservação;
- I – *Interoperable* (Interoperável): Os dados podem ser integrados com outros dados ou facilmente “entendidos” por computadores. Implica no uso de linguagem de representação do conhecimento, vocabulários e/ou ontologias que adotem os princípios FAIR. É necessário referenciar o conjunto de dados, possibilitando que aqueles gerados a partir de outros conjuntos, sejam interligados. Assegurando a ligação semântica entre eles;
- R – *Reusable* (Reusável): Os dados podem ser reutilizados em outras pesquisas, com o uso de licenças apropriadas, informação de procedência, e o alinhamento com os padrões de seu domínio, observando as práticas de arquivamento e compartilhamento específicas da área de pesquisa.

2.4 Conectividade Agrícola

O perfil do agricultor brasileiro é, em sua maioria, de pessoas com idade inferior a 45 anos, sendo esse um dos motivos que facilitam as inovações que as novas tecnologias imprimem no campo e também nas produções urbanas e periurbanas. Em 2017 o censo agropecuário do IBGE [98] apontou que 30% dos agricultores possuíam acesso à Internet, entre banda larga e redes móveis. Ainda havia 70% do total sem acesso. Esses números, naturalmente mudaram muito desde então, e atualmente 47% dos agricultores já fazem uso de pelo menos uma ferramenta de precisão, e 33% já usam duas ou mais ferramentas. A falta de conectividade é um grande desafio que tem sido enfrentado com investimentos públicos e privados. O próprio BNDES [99] estima que o uso da IoT em larga escala na agricultura poderia gerar um impacto de 50 a 200 bilhões de dólares na economia, em 2025.

Um exemplo de iniciativa privada que visa melhorar a conectividade rural no Brasil é a ConectarAGRO [100]. Grandes empresas (AGCO, Climate, CNH Industrial, Jacto, Nokia, Solinftec, Tim e Trimble) estruturaram essa associação visando promover tecnologias abertas em todas as áreas rurais do país. A tecnologia que melhor atende, no momento (abril de 2021), a todas as premissas vislumbradas pelo ConectarAGRO é a LTE 4G 700 MHz, a mesma utilizada na cidade. Isto significa dizer que os mesmos equipamentos (smartphones, tablets, modems etc.) usados na cidade também funcionam no campo. Esta tecnologia proporciona grandes alcances de cobertura nas áreas rurais ou remotas, podendo atingir milhares de hectares com apenas uma simples infraestrutura, formada por torre, rádio e antenas. E a chegada da 5G, com o leilão em 2021, será de grande valia para ampliar a conectividade rural brasileira.

Possíveis recursos públicos para melhorar a infraestrutura de Internet podem se originar a partir do projeto de lei nº 172/2020 [101], que tramita no Congresso Nacional, e pretende modificar a Lei Geral das Telecomunicações para acessar os recursos do Fundo de Universalização dos Serviços de Telecomunicações (FUST), e prover o financiamento da expansão da infraestrutura nas regiões de zona rural ou urbana com baixo Índice de Desenvolvimento Humano (IDH), estimulando o uso e o desenvolvimento de novas tecnologias de conectividade para promoção de desenvolvimento econômico e social. A maior conectividade no meio rural também

está apontada no Plano Nacional de Internet das Coisas [102] e nas discussões da Câmara Agro 4.0, na qual existe um grupo de trabalho em Conectividade no Campo [103].

2.5 Desenvolvimento Sustentável

Uma das metas brasileiras na Agenda 2030 é ‘acabar com a fome, alcançar a segurança alimentar e melhoria da nutrição e promover a agricultura sustentável’ [104]. Especificamente em agricultura, alguns desafios são “*garantir sistemas sustentáveis de produção de alimentos, por meio de políticas de pesquisa, de assistência técnica e extensão rural, entre outras, visando implementar práticas agrícolas resilientes que aumentem a produção e a produtividade e, ao mesmo tempo, ajudem a proteger, recuperar e conservar os serviços ecossistêmicos, fortalecendo a capacidade de adaptação às mudanças do clima, às condições meteorológicas extremas, secas, inundações e outros desastres, melhorando progressivamente a qualidade da terra, do solo, da água e do ar*” e “*aumentar a produtividade agrícola e a renda dos pequenos produtores de alimentos, particularmente de mulheres, agricultores familiares, povos e comunidades tradicionais, visando tanto à produção de autoconsumo e garantia da reprodução social dessas populações quanto ao seu desenvolvimento socioeconômico*” (IPEA 2021). O desafio é associar os dados de sensoriamento com as imagens coletadas, os algoritmos de processamento e as demais tecnologias, a um nível de precisão tal que permita o uso racional dos recursos naturais e favoreça a sustentabilidade agrícola [105].

A EMBRAPA [106] cita os desafios mais prementes:

- Uso eficiente da água em sistemas de irrigação de grãos, hortaliças, frutíferas, pastagens e cana-de-açúcar;
- Elevar a capacidade adaptativa e a resiliência dos sistemas de produção agrícola com maior impacto econômico projetado e relevância para segurança alimentar a partir de cenários de mudanças climáticas;
- Fazer a orientação do uso e a ocupação das terras em áreas de conversão de uso e de expansão da fronteira agrícola nos biomas Cerrado, Caatinga e Amazônia.

2.6 Relacionamento com o Mercado de Consumo

Não há dúvida de que os consumidores, atualmente muito mais informados pela própria mídia digital disponível, desejam que os produtos agrícolas à sua mesa sejam de maior qualidade e com origem comprovada. As TICs (Tecnologias de Informação e Comunicação) propiciam um contato mais direto com o produtor, e alteram drasticamente a relação de consumo. Dessa forma, os negócios convencionais estão sendo cada vez mais criados em bases de mercados digitais, com uso intensivo de automação e da convergência das TICs na agricultura [107].

Outra consequência interessante do uso das novas tecnologias é o grande impulso que terão as cooperativas produtivas, que, usando a economia digital associada às criptomoedas, já estão em processo de relacionamento direto com os consumidores. Uma horta urbana, por exemplo, como é o caso da proposta deste trabalho, irá vender seus produtos diretamente aos consumidores finais. Isso possibilitará que a produção seja direcionada especificamente às necessidades do mercado, e os produtores poderão coletar diretamente dos consumidores as informações de qualidade, preços, etc., o que será decisivo nas tomadas de decisões de produção, fazendo assim uso de uma irrigação de precisão, com redução de custos, menor utilização de produtos químicos, e reduzindo os conflitos socioambientais. Uma horta urbana, que atende um bairro, uma comunidade, ou uma localidade, deve ter uma produção rápida, de qualidade, custo acessível, e com facilidade de distribuição de seus produtos, e o uso das tecnologias de produção e pagamentos vem a calhar em um mercado desse tipo, propiciando uma nova forma de economia compartilhada.

A população urbana, em 2050, segundo estimativas da ONU [108], chegará a 70% do total, o que obviamente causará mudanças nos padrões de produção e consumo. A tecnologia é a grande aliada que, além de favorecer a aumento necessário da produção e da qualidade, ainda trará efeitos ambientais, tais como: a redução da pegada de carbono; as ilhas urbanas verdes – como exemplo o uso de tetos verdes; as hortas e fazendas urbanas; e também o plantio de mais árvores. O desenvolvimento de aplicativos e sensores de IoT para redução do impacto ambiental e as tecnologias ecoeficientes, podem ser importantes para a sobrevivência nos âmbitos sociais,

ecológicos e econômicos, uma vez que a geração e consumo de bens é decisiva. Exemplo disso é que atualmente os consumidores estão mais sensíveis a questões ambientais. Em 2018, o Instituto Akatu, de São Paulo, uma organização privada sem fins lucrativos, realizou uma pesquisa que demonstrou que 40% dos consumidores mudam sua intenção de compra para produtos que visam proteger o meio ambiente. Empresas e associações que não levam em conta a reciclagem, que não avaliam o uso de poluentes e ignoram medidas que fazem bem para a saúde do planeta, provocam olhares de reprovação de um nicho crescente de consumidores e perdem a chance de se posicionar com uma vantagem competitiva. Hoje em dia, diante da velocidade da informação em vídeos, redes sociais e blogs, fica difícil reparar os danos que uma má reputação pode provocar na marca de uma empresa. Por causa disso, priorizar a sustentabilidade deve ser parte da cultura da organização [109]. O uso correto de recursos para a agricultura pode ser mensurado pelos sensores de IoT, e os aplicativos podem atender aos mais variados objetivos, como, por exemplo, facilitar à empresa o entendimento do consumo de recursos (sejam energéticos ou de suprimentos) revelando todos os gastos e permitindo um planejamento mais sustentável e otimizado.

Uma questão já mencionada, mas que é uma circunstância muito recente e ainda não pode ser mensurada é a pandemia de Covid-19, que trouxe consigo a questão do isolamento social. Esse isolamento fechou restaurantes, feiras livres, lanchonetes, etc. Os produtores, em especial os pequenos, não conseguiram escoar suas vendas, por semanas. No início da pandemia o Ministério da Agricultura, Pecuária e Abastecimento (MAPA) agiu para definir as atividades essenciais que não poderiam parar, garantindo assim a continuação do abastecimento. Em seguida, um protocolo de transporte de cargas foi preparado, no sentido de garantir os cuidados adequados frente ao risco da pandemia. Novas regras de produção e distribuição de alimentos foram estabelecidas pela Confederação da Agricultura e Pecuária do Brasil (CNA). Tudo indica que ocorrências como essa irão potencializar as alterações nos hábitos de higiene e saúde pública, e surgirão protocolos de saúde mais rígidos na produção, comercialização e consumo de produtos agrícolas e outros [110]. A transparência dos processos produtivos se torna assim uma condição primordial para o comércio dos produtos. É fundamental que os produtos tenham informações de rastreabilidade com dados de seu local de origem, insumos utilizados, colheita, processamento, conserva-

ção, qualidade, armazenamento e transporte. O mercado cada vez mais pressiona o setor produtivo para que os produtos tenham certificações de garantia sanitária e alimentar. Uma tecnologia do tipo *Blockchain* ou *Tangle*, de registros distribuídos, pode ser adequada ao processo de rastreabilidade dos produtos.

2.7 Serviços Digitais

Naturalmente os produtores agrícolas não são, em sua esmagadora maioria, desenvolvedores de seus próprios serviços digitais. Surge então um novo mercado, de desenvolvimento de soluções integradas para a gestão da produção e da comercialização dos produtos, disponibilizadas aos produtores via acesso digital em computadores e *smartphones*. Diversas empresas, instituições de pesquisas, universidades, cooperativas e outras, investem no desenvolvimento dessas soluções, integradas em uma plataforma que pode ir desde a coleta de dados *in loco*, até o processamento desses dados com inteligência artificial, associando dados meteorológicos, condições de solo, modelos de previsão de doenças, pragas, sazonalidade, etc.

As plataformas digitais integradas devem ser abrangentes, e devem oferecer [111]:

- Suporte à análise de dados e à tomada de decisão da propriedade, com informações geoespaciais de agricultura, vegetação, solo e recursos hídricos para apoio aos Programas de Regularização Ambiental (PRA), Cotas de Reserva Ambiental (CRA) e Pagamentos por Serviços Ambientais (PSA);
- Conectividade entre produtores rurais e consumidores, favorecendo o processo de rastreabilidade e a certificação de qualidade e origem de produtos como leite, mel, ovos, carnes, grãos, frutas, açúcar, biocombustíveis, fibras, madeiras e celulose;
- Suporte à tomada de decisão e à gestão de políticas públicas agrícolas, baseadas em modelos matemáticos, estatísticos e computacionais, com o uso de

inteligência artificial, visão computacional e processamento de imagens de sensoriamento remoto.

Um fator importante na produção agrícola, seja no campo ou em área urbana, em ambientes *outdoor*, e que pode estar incorporado em uma plataforma digital, é a previsão de riscos às atividades agrícolas. Por exemplo, as condições climáticas são altamente variáveis, e uma precipitação com granizos danifica grandemente uma plantação. Um modelo climático regional permite avaliar as possibilidades desse risco. A EMBRAPA [112] desenvolve atualmente um Simulador de Cenários Agrícolas (ScenAgri) que incorpora os aspectos citados e associa a fundamentação do ZARC (Zoneamento Agrícola de Risco Climático). O sistema é baseado em computação de alto desempenho para apoiar os pesquisadores na investigação dos impactos das mudanças climáticas na agricultura brasileira. Alguns estudos já evidenciaram a importância dessa projeção futura de médio e longo prazo para doenças de plantas, forrageiras, eucalipto, grãos e cana-de-açúcar [113].

2.8 Classificação de Hortaliças e Mercado

Especificamente no escopo deste trabalho, que trata de aplicação de tecnologias das TICs em hortas, é necessário que se classifique os produtos de uma horta, seja ela urbana ou não. A EMBRAPA [114] faz uma classificação dos principais tipos de hortaliças plantados e consumidos no Brasil de acordo com sua variedade e tipo, conforme a Tabela 2 a seguir. O clima moderado, com chuvas leves e frequentes, é o melhor para o desenvolvimento das hortaliças, sendo a alface a campeã brasileira de vendas e consumo.

Tabela 2 - Classificação de hortaliças no Brasil (Embrapa)

Classificação	Tipo
Hortaliças Folhosas	Acelga, Agrião, Alface, Almeirão, Alho-Porró, Bertalha, Cebolinha, Coentro, Couve, Couve-chinesa, Chicória, Espinafre, Repolho, Rúcula, Salsa, Taioba
Hortaliças Flores	Alcachofra, Brócolis e Couve-Flor
Hortaliças Frutos	Abóbora, Abobrinha, Berinjela, Chuchu, Jiló, Maxixe, Melancia, Melão, Milho-verde, Morango, Moranga, Pimenta, Pimentão, Pepino, Quiabo e Tomate
Hortaliças Legumes	Ervilha, Fava, Feijão vagem
Hortaliças Raízes	Batata-baroa (Mandioquinha-salsa), Batata doce, Beterraba, Inhame (Cará), Cenoura, Nabo e Rabanete
Hortaliças Tubérculos	Batata
Hortaliças Bulbos	Alho e Cebola
Hortaliças Hastes	Aspargo e Salsão
Hortaliças Temperos	Açafrão, Alecrim, Alho, Cebola, Cebolinha, Coentro, Cominho, Gengibre, Hortelã, Louro, Manjerição, Manjerona, Mostarda, Orégano, Páprica (Colorau), Pimenta, Salsa, Sálvia, Tomilho

Em 2015 a China era o principal produtor mundial de hortaliças, com 51% da produção. A produção mundial naquele ano foi de 11,5 bilhões de toneladas, sendo as principais hortaliças produzidas o alho, tomate, melancia e batata [115]. No Brasil o consumo de hortaliças permanece muito abaixo dos valores diários preconizados por instituições nacionais e internacionais, como o Ministério da Saúde (MS) e a Organização Mundial da Saúde (OMS), respectivamente. A OMS recomenda o consumo diário de 400 gramas de frutas e hortaliças, em cinco ou mais dias da semana. No nosso país, segundo a FAO, o consumo de hortaliças por pessoa/dia é de apenas 141 gramas, ficando atrás, inclusive, de alguns países mais pobres da Ásia e da América Latina. Em países mais desenvolvidos, o consumo de hortaliças é maior; por exemplo, o Japão consome o dobro do que é consumido no Brasil, isto é, 280

gramas/pessoa/dia. Países como Portugal e Itália consomem, respectivamente, 416 e 353 gramas/pessoa/dia.

Grande parte da produção nacional é destinada ao mercado de exportação, principalmente ao mercado asiático. A qualidade desses produtos precisa ser garantida, e as tecnologias de produção e rastreabilidade são fundamentais para que os consumidores se sintam seguros ao comprar suas hortaliças.

A EMBRAPA afirma que 60% da produção nacional é garantida pela agricultura familiar, e que esse volume representa 2% do PIB do agronegócio brasileiro. 2,4 milhões de empregos são gerados por essa produção.

Dentro desse contexto revisado neste capítulo, é intuito deste trabalho relacionar a agricultura familiar, ou comunitária, às tecnologias de IoT e Criptomoedas, objetivando a afirmação deste modelo de negócio agrícola no mercado, e apoiando a criação de oportunidades de emprego e renda nas comunidades urbanas e seu entorno, melhorando a condição social da comunidade e sua segurança alimentar, colaborando assim, para que se atinja os objetivos da Agenda 2030 da ONU. Mas sempre trazendo à luz as aplicações práticas dos conceitos das TICs em ambientes diversos, como a agricultura urbana e periurbana, e comprovando que essa associação é benéfica em todos os aspectos, sejam eles sociais, econômicos, culturais, ambientais, etc.

Capítulo 3 – ASPECTOS LEGAIS DAS CRIPTOMOEDAS

*‘Estar por dentro das tendências é importante para toda empresa, startup ou outro negócio. Mas, tão fundamental quanto isso, é estar atento às implicações jurídicas dessas inovações.’
(Koboldt Advogados)*

É notório que a agricultura urbana e periurbana, onde se localizam a grande

maioria das hortas comunitárias, está cada vez mais sendo tratada como uma necessidade na solução de questões alimentares, sociais e econômicas das populações, chegando ao ponto de já estarem incluídas nas políticas públicas de todas as esferas de governo nacionais, e até de órgãos internacionais, como a ONU, por exemplo. A monetização desse modelo de negócio é uma consequência natural e esperada na obtenção dos objetivos propostos de melhoria das condições de vida das comunidades. Claro que em uma proposta de uso de tecnologias de TIC em hortas compartilhadas, onde a monetização é baseada em criptomoeda, torna-se relevante conhecer a situação do uso da criptomoeda em termos de legalidade e regulação estatal. Sendo assim, este capítulo versa justamente sobre os aspectos legais da criptomoeda, e a evolução de seu uso no Brasil e no mundo, e justifica sua aplicação de forma lícita, podendo ser utilizada em hortas públicas, de associações, comunidades, e até particulares, e criando um mercado digital de produtos agrícolas totalmente aberto e legal.

No início da década de 1990, havia um grupo de pessoas, ligadas às famosas empresas *dot.com*, que era uma bolha de sucesso à época, que não estavam muito satisfeitas com as políticas econômicas existentes. Passaram a criar então sistemas de trocas de pagamentos independentes dos sistemas tradicionais, tais como bancos, financeiras, etc. A intenção era de se ter sistemas de trocas de valores independentes, que não tivessem o controle de terceiros, e que garantisse as transações efetuadas, preservando a identidade de seus usuários. Essas pessoas desenvolveram vários projetos, entre eles um bastante interessante, denominado *Hashcash*, que tinha o intuito de evitar ataques com *Spam* e DDOS. Esse algoritmo apresentava a PoW

(*Proof-of-Work*) que, como se sabe, foi posteriormente utilizado na estrutura do Bitcoin [116]. Projetos como esses trouxeram alternativas interessantes ao sistema monetário tradicional, e serviram como base para o desenvolvimento da mais conhecida criptomoeda do mundo atualmente, que é o Bitcoin.

Diante dos sinais de declínio econômico das grandes potências mundiais, grandes bancos em situação de insolvência, estouro de bolhas especulativas, surge, em 31 de outubro de 2008, em uma lista de discussão online acerca de criptografia, o usuário conhecido como “Satoshi Nakamoto”, que lançou na rede um *paper* de sua autoria, afirmando ser “*Uma versão puramente ponto-a-ponto de dinheiro eletrônico, que permitiria que os pagamentos online fossem enviados diretamente de uma parte para outra, sem passar por uma instituição financeira*” [117]. De acordo com Faé: ‘*Satoshi explicita notoriamente sua crítica ao sistema financeiro e monetário ao registrar a primeira transação no sistema Bitcoin acompanhada da mensagem ‘The Times 03/Jan/2009 Chancellor on brink of second bailout for banks’ em referência à capa do jornal britânico The Times que anunciava mais uma tentativa do governo em salvar bancos da falência*’ [118].

Especula-se [119] que o pseudônimo Satoshi Nakamoto tenha sido usado por um grupo de libertários, associados a ‘*cyberpunks*’ (O termo *cyberpunks* teve origem nos anos 90, na região da baía de São Francisco, na Califórnia, por um grupo de matemáticos, criptoanarquistas e hackers que começaram a reunir-se em suas casas. Os membros desse grupo fechado passaram a ser conhecidos como *cyberpunks*. Os membros originais não tinham ideologia social, eram mais preocupados com a matemática complicada da tecnologia criptográfica e a filosofia mais ampla da anonimidade, liberdade individual e privacidade.

3.1- Conceito da Criptomoeda

Para que se possa estudar os fenômenos econômicos e jurídicos decorrentes das criptomoedas, é imperativo que seja definido inicialmente o que são as criptomoedas: ‘*Criptomoeda (ou Moeda digital virtual) é uma moeda emitida eletronicamente cuja transferibilidade para moeda fiat (moeda fiduciária ou legal) não é garantida pelo estado (European Banking Authority, 2014). Moedas digitais podem ser divididas em*

tipos centralizados e descentralizados [120]. A criptomoeda deve atender as condições:

- 1) O sistema não requer uma autoridade central, sendo o consenso sobre o estado do sistema distribuído no próprio sistema;
- 2) O sistema mantém uma visão geral das unidades de criptomoeda e sua propriedade;
- 3) O sistema define se novas unidades de criptomoeda podem ser criadas. Se puder, o sistema define as circunstâncias de sua origem e como determinar a propriedade dessas novas unidades;
- 4) A propriedade de unidades de criptomoeda pode ser comprovada exclusivamente por criptografia;
- 5) O sistema permite que transações de mudança de propriedade das unidades sejam realizadas. Uma declaração de transação só pode ser emitida por uma entidade que prove a propriedade atual dessas unidades;
- 6) Se duas instruções diferentes para alterar a propriedade das mesmas unidades criptográficas forem enviadas simultaneamente, o sistema realiza no máximo uma delas.

Fernando Ulrich [121], a define como “[...] *uma moeda digital, peer-to-peer, (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central.*” Esse conceito traz sutil carga de dúvida, pois trata-se de um tema relativamente atual e de raízes tecnológicas, Internet, linguagem de programação computacional, entre outros temas complexos e impopulares, que sem dúvida não fazem parte do conhecimento da sociedade em geral. Sendo uma moeda, em princípio não haveria dúvidas ao público comum, porém, é moeda virtual, não materializada em cédulas ou níquel, e que existe somente pelos meios digitais, ou seja, dispositivos digitais (telefones celulares, computadores, tablets, etc.) conectados à Internet, por onde se dará a transmissão das transações. O termo “*peer-to-peer*”, trata-se de uma forma de conexão descentralizada via Internet em que todos os usuários se interligam, ao contrário das conexões convencionais, as quais se ligam a um servidor central [122]. O Sistema *Peer-to-peer*, com a sigla P2P, é uma rede de computadores onde cada um dos pontos, ou nós da rede, funciona tanto como cliente, quanto como servidor;

permitindo o compartilhamento de serviços, compra, venda e trocas; bem como o fornecimento e checagem de dados sem a necessidade de um servidor central.

Há muitas vezes uma falsa sensação de anonimato com a criptomoeda, pois, para obtê-la não é necessária a identificação, mas apenas a utilização de um pseudônimo. Porém, isso não garante o anonimato total; somente dificulta a sua descoberta. Todas as transações feitas são registradas, e esses registros são públicos, podendo ser acessados pelas autoridades competentes. Tratando de uma moeda digital de código aberto, sua linguagem de programação é irrestrita; portanto, pode ser alterada pela comunidade, sem nenhum intuito lucrativo, compartilhada entre os usuários e aprimorada constantemente. Importante frisar que apesar disso, nenhum usuário pode forçar a modificação do protocolo da moeda, pelo fato da criptomoeda ser controlada por todos os usuários, em sua rede, os quais têm liberdade de escolha do software, sendo necessário apenas que cumpram as mesmas regras, requisitos mínimos de compatibilidade [123].

3.2- Risco das Criptomoedas

As criptomoedas facilitam as transações de vendas, compras e trocas, sem o controle do sistema financeiro tradicional. De certo modo, isso é até bom, pois dá mais liberdade para que os usuários façam suas transações na rede, mas por outro lado propicia que criminosos façam uso dessa facilidade para as transações ilegais, ainda que a moeda fiduciária também o faça. A *deep web*, também chamada de *Deepnet*, *Web Invisível*, *Undernet*, *Web Obscura* ou *Web Oculta*) se refere ao conteúdo da *World Wide Web* que não é indexado pelos mecanismos de busca padrão, ou seja, não faz parte da *Surface Web*. Não deve ser confundida com a *Dark Internet*, que está relacionada à porção da Internet que não pode ser acessada ou que se tornou inacessível por meios convencionais. Também não se confunde com a *Darknet*, que não é uma simples rede de compartilhamento de arquivos, mas uma rede subjacente ou em camadas, onde existem grandes esforços no sentido de se manterem anônimos os dados de seus utilizadores. Mike Bergman, fundador da BrightPlanet e autor da expressão, afirmou que a busca na Internet atualmente pode ser comparada com o arrastar de uma rede na superfície do oceano: pode-se pescar um peixe grande, mas há uma grande quantidade de informação que está no fundo, e, portanto, faltando. A maior parte da

informação da *Web* está enterrada profundamente em sites gerados dinamicamente, não sendo encontrada pelos mecanismos de busca padrão. Estes não conseguem "enxergar" ou obter o conteúdo na *Deep Web* - aquelas páginas não existem até serem criadas dinamicamente como resultado de uma busca específica. A *Deep Web* possui um tamanho muito superior ao da *Surface Web*. O risco da *Deep Web* é, basicamente, a intenção com que o usuário a acessa. Por conter páginas com conteúdo ilegal, as mesmas podem conter vírus, prejudicando a segurança do computador. Vale lembrar que ela também, por ser criptografada e anônima, é muito usada por criminosos. Os criminosos, com o uso da *Deep Web*, conseguem vender e comprar seus produtos ilícitos, e utilizam-se das criptomoedas para as transações. Naturalmente as criptomoedas não tem em seu princípio a ideia de facilitar esse comércio ilegal, mas é bastante adequada a esse uso, e dificulta grandemente a fiscalização.

A grande vantagem das criptomoedas, que é a descentralização do controle sobre as transações, acaba sendo também um ponto que dificulta e muito o seu uso nas transações legalmente amparadas.

3.3- ICO – Initial Coin Offering

Initial Coin Offering (ICO) é um mecanismo que tem se desenvolvido com o crescimento das diferentes aplicações para a tecnologia do *Blockchain*. O nome remete ao IPO, ou *Initial Public Offering*, que é a oferta pública inicial de ações, mas não parece ser o nome mais adequado, já que não é apenas esse o objetivo do ICO, apesar de ser um deles. Trata-se de um modelo descentralizado de levantamento de fundos para novos projetos relacionados a criptoativos. Ao invés de se colocar à venda para os investidores ações de uma empresa, disponibilizam-se unidades de uma nova criptomoeda ou token digital. Devido à ascensão do Bitcoin, e sua rápida valorização no mercado, o número de novas criptos lançadas aumentou grandemente, em um curto espaço de tempo. Assim, aos poucos foram surgindo novas moedas virtuais, programadas, em sua maioria, com base nas linguagens trazidas pelo Bitcoin, mas também possuindo particularidades, provavelmente almejando o mesmo sucesso do Bitcoin. Assim, de 2013 em diante, as novas moedas virtuais começaram a fazer uso das ICO's para arrecadação de fundos. A moeda já tinha dessa forma uma definição prévia, e atraía um grupo específico de investidores. Assim como em um IPO, a

criptomoeda nova é oferecida para alguns investidores, em troca de outros ativos existentes, em moedas tradicionais, ou mesmo em criptomoedas existentes e estabelecidas. Uma ICO que merece ser citada como exemplo foi a Ethereum, que em 2014 promoveu um investimento milionário. Isso gerou segurança e estabilidade para a plataforma, que atualmente é uma das mais valorizadas do mercado. Cada vez mais a ICO é utilizada para financiar o desenvolvimento de projetos de criptomoedas, com a liberação de *token* que está no projeto. Os *tokens* são os ‘ativos digitais’, que se assemelham a títulos financeiros. Quem possui um *token* de um determinado projeto é um financiador desse projeto.

3.4- DA REGULAÇÃO DAS CRIPTOMOEDAS

Desde o momento em que as moedas virtuais passaram a receber destaque no mundo, seja pelos aspectos positivos ou negativos, estudiosos e governos passaram a observá-las mais de perto, ante sua imaturidade e potencial inexplorado. Havia muitas incertezas acerca do que esse fenômeno poderia causar à economia e aos governos; aos poucos foram surgindo estudos acerca da regulamentação destas, inclusive no Brasil. Isto posto, a seguir será abordado projeto de lei brasileiro tendente a regulamentar as criptomoedas no Brasil, além de traçado um panorama acerca da regulação e possíveis efeitos em todo o mundo.

3.4.1- Regulação das Criptomoedas no Brasil

O Projeto de Lei nº 2303/2015, de autoria do Deputado Federal Áureo Ribeiro (RJ), apresentado em 08 de julho de 2015, possui a seguinte ementa: “Dispõe sobre a inclusão das moedas virtuais e programas de milhagens aéreas na definição de “arranjos de pagamento” sob a supervisão do Banco Central”. O projeto consiste em quatro artigos, em que três deles trazem as alterações legislativas desejadas para o fim a que se propõe, nos seguintes termos:

Art. 1º Modifique-se o inciso I do art. 9º da Lei 12.865, de 09 de outubro de 2013:

Art. 9º.....
.....

I - disciplinar os arranjos de pagamento; incluindo aqueles baseados em moedas virtuais e programas de milhagens aéreas;'

Art. 2º Acrescenta-se o seguinte §4º ao art.11 da Lei 9.613, de 03 de março de 1998:

*'Art.11.....
.....*

§ 4º As operações mencionadas no inciso I incluem aquelas que envolvem moedas virtuais e programas de milhagens aéreas'

Art. 3º *'Aplicam-se às operações conduzidas no mercado virtual de moedas, no que couber, as disposições da Lei no 8.078, de 11 de setembro de 1990, e suas alterações.'*

Art. 4º *Esta Lei entra em vigor na data de sua publicação [124].*

Já em 2015 o referido deputado viu a necessidade da regulamentação estatal do fenômeno das criptomoedas e seu efeito revolucionário na economia.

3.4.1.1- Justificação do projeto de regulação

A proposta do projeto de lei inicia sua justificativa em razão do ganho de destaque por parte das “moedas virtuais” nas transações financeiras da atualidade. Adiciona ainda que, não obstante ainda não haver regulamentação nacional e nem internacional (em 2015) a respeito do assunto, há preocupação emergente com os efeitos das transações realizadas através de referidos meios (Obs.: Atualmente já há regulamentação internacional sobre as criptomoedas [125]. Diz ainda a justificativa que o tema então foi tratado com atenção pelo Banco Central Europeu (BCE), tendo elaborado relatórios em 2012 [126] e 2015 [127], expondo os muitos riscos que deveriam ter monitoramento adequado; todavia, esses relatórios concluíram que naquele momento não havia necessidade de uma intervenção direta no sentido da criação de regras mais eficientes para as criptomoedas. É importante mencionar que durante a tramitação do projeto de lei, em 2016 o Banco Central Europeu emitiu parecer definitivo acerca das criptomoedas [128], no sentido de que estas devem ser reguladas, a fim de se evitar o uso do sistema financeiro para a lavagem de dinheiro e financiamento do terrorismo. Em suma, o projeto legislativo justificava que o Banco Central do Brasil, o Conselho de Controle de Atividades Financeiras (COAF) e os órgãos de proteção ao consumidor, são capazes de exercer fiscalização e regulação sobre as moedas virtuais, mas para evitar inconvenientes discussões judiciais, defendeu a regulamentação das normas propostas.

Todavia, essa proposta inicial do referido deputado veio a ser arquivada pelo congresso, e ainda que hoje o Brasil seja o segundo maior investidor global em criptomoedas [129] ainda não há uma regulamentação estatal definida para o tema. Na sequência é mostrada uma linha do tempo de como a questão está sendo encaminhada no país [130]:

- Janeiro/19: PL 2303/2015 é arquivado;
- Março/19: PL 2303/2015 é desarquivado por seu relator, deputado Áureo Ribeiro (RJ);
- Abril/19: O deputado Áureo Ribeiro apresenta um segundo projeto, o PL 2060/2010;
- Junho/19: A CVM (Comissão de Valores Mobiliários – entidade autárquica vinculada ao Ministério da Economia) divulga ação para implementação de *sandbox* regulatório para o mercado financeiro;
- Julho/19: Senador Flávio Arns (PR) protocola o PL 3825/2019, para regular a atividade da *exchanges* sob supervisão do Banco Central;
- Agosto/19: A Instrução Normativa 1888/2019 entra em vigor e torna obrigatório o reporte mensal de movimentação com criptoativos;
- Agosto/19: Bacen inclui a compra e venda de criptomoedas na balança comercial do país;
- Setembro/19: a Comissão de Valores Mobiliários submeteu à audiência pública, a criação de um *sandbox* regulatório;
- Novembro/19: Banco Central abre audiência pública para criação de open banking e *sandbox* regulatório;

3.4.1.2- PL 2303/2015 e o 2060/2019

O Projeto de Lei 2303/2015, anteriormente mencionado, passou por inúmeras reviravoltas e em dezembro de 2017, o deputado Expedito Neto (RO), na época, relator da Comissão Especial da Câmara dos Deputados, propôs um substitutivo voltado à proibição do uso das moedas virtuais no Brasil. Em janeiro de 2019, o PL foi arquivado.

Em abril de 2019, o deputado Áureo apresentou um novo projeto, o PL 2060/2019, bastante diferente do projeto anteriormente apresentado pelo mesmo deputado. Enquanto o PL 2303/2015 buscava regulamentar os criptoativos a partir de sua inclusão na categoria de programas de milhagens aéreas, o novo projeto propõe classificar esses ativos como reserva de valor, meio de pagamento e *commodity* digital. Essa nova classificação, juridicamente mais madura, muda a forma de se ver os criptoativos e suas características. Essa nova proposta de projeto de lei, o PL 2060/2019, traz uma classificação para os ativos digitais, dividindo-os em unidade de valor, unidades representativas de bens e tokens virtuais (de acesso ou de utilidade). Outra diferença deste novo PL é o tratamento dos crimes digitais, que fazem uso das criptomoedas em esquemas fraudulentos e de pirâmides financeiras. De acordo com o PL, os autores de crimes dessa natureza poderão ser penalizados desde multas até reclusão por um período de até cinco anos. Sem dúvida, houve um grande avanço entre a primeira proposta e esta última, mas ainda são necessários mais esforços para melhorias da proposta. Por exemplo, no Art. 4º do PL 2060/2019, é dito que a emissão de criptoativos só "*poderá ser realizada por pessoas jurídicas de direito público ou privado, estabelecidas no Brasil*" [131]. Os projetos de ativos digitais são feitos, por vezes, por pessoas cuja real identidade não é conhecida (vide Satoshi Nakamoto), ou, na sua grande maioria, são estrangeiros. Com isso, a aplicação desse ponto pode travar a aplicação da lei na prática.

No dia 18 de setembro de 2019, durante audiência pública da Comissão Especial formada para debater o PL 2303/2015, o presidente da comissão de criptomoedas e *Blockchain* da Ordem dos Advogados do Brasil, Antônio Eduardo Gonçalves de Rueda [132], defendeu uma regulação branda para o setor. Para Rueda, uma regulação reativa ou uma autorregulação do mercado seriam as melhores soluções no momento.

3.4.1.3- A Instrução Normativa 1888/2019

A Instrução Normativa (IN) 1888/2019, que entrou em vigor a 1º de agosto de 2019 [133], e alterada pela IN 1899/2019, é uma obrigação acessória da Receita Federal, e formalizou a obrigação de que as instituições e investidores que fazem uso

das criptomoedas informem mensalmente toda e qualquer transação realizada. A IN determina que as corretoras (*exchanges*) de criptoativos, pessoas físicas e jurídicas domiciliadas no Brasil reportem as transações. Entre as declarações que precisam ser realizadas pelas pessoas físicas, estão as operações que forem realizadas em *exchanges* domiciliadas no exterior ou as operações que não forem realizadas em *exchanges*, cujo valor mensal das operações isolado ou conjuntamente, ultrapassar R\$ 30.000,00. E as operações que precisam ser informadas incluem compra e venda, permuta, doação, transferência e retirada para *exchanges*, cessão temporária, doação, emissão e qualquer outra operação que implique em transferência das criptomoedas. As *exchanges* são obrigadas a relatar quaisquer movimentações que ocorram em suas plataformas. Se um usuário realiza uma compra com um negociante peer-to-peer (P2P), independente, e esse negociante não é uma pessoa jurídica, a obrigação passa a ser do investidor, caso contrário, a obrigação é do negociante P2P.

3.4.1.4- Banco Central do Brasil, Balança Comercial e Recomendação do FMI

No dia 26 de agosto de 2019, o Banco Central do Brasil (BACEN) publicou um documento classificando criptomoedas como “ativos não-financeiros produzidos”. Seguindo a recomendação do Comitê de Estatísticas de Balanço de Pagamentos, órgão consultor do Departamento de Estatística do Fundo Monetário Internacional (FMI), o BACEN passou a incluir a compra e venda de criptoativos na balança comercial do país. A atividade de mineração também passou a ser classificada como “processo produtivo” [134]. Segundo o documento do BACEN, o Brasil tem sido importador líquido de criptoativos, contribuindo para reduzir o superávit comercial na conta de bens da balança de pagamento e por isso, passou a ser incluído na conta.

3.4.1.5- O Sandbox Regulatório: CVM E BACEN

No dia 13 de junho de 2019, a Comissão de Valores Mobiliários divulgou a intenção de implementar um modelo de *sandbox* regulatório para o mercado financeiro, securitário e de capitais brasileiros. No comunicado, a CVM cita que o ‘*uso*

de tecnologias inovadoras, como distributed ledger technology – DLT, blockchain, roboadvisors e inteligência artificial, têm permitido o surgimento de novos modelos de negócios, com reflexos na oferta de produtos e serviços de maior qualidade e alcance. Como resultado, esse cenário impõe aos reguladores o desafio de atuar com a flexibilidade necessária para adaptar suas regulamentações às mudanças tecnológicas e constantes inovações, principalmente sob as perspectivas da segurança jurídica, da proteção ao cliente e investidor e da segurança, higidez e eficiência dos mercados. O interessante dessa ação é que ela está sendo desenvolvida em conjunto com outras instâncias do poder público, como a Secretaria Especial de Fazenda do Ministério da Economia, Banco Central do Brasil e a Superintendência de Seguros Privados.

No dia 27 de setembro de 2019, a Comissão de Valores Mobiliários (CVM) submeteu à audiência pública, a criação de um ambiente regulatório experimental (“*sandbox* regulatório”) em que poderão ser concedidas autorizações temporárias para testes de modelos de negócio inovadores em atividades regulamentadas no mercado de valores mobiliários. A elaboração da minuta da instrução da CVM foi elaborada com base nos *sandbox* regulatórios do Reino Unido, Singapura, Austrália e México. E a autarquia também planeja se integrar à rede global de *sandbox*, conhecida como *Global Financial Innovation Network* (GFIN). O *sandbox* faz parte de uma estratégia do governo para incentivar o empreendedorismo digital no Brasil e pode representar um ambiente mais promissor para o desenvolvimento das iniciativas da criptoeconomia.

Em novembro de 2019, o Banco Central do Brasil também abriu consultas públicas para implementação do Sistema Financeiro Aberto (*Open Banking*) e do Ambiente Controlado de Testes para Inovações Financeiras e de Pagamento (*Sandbox* Regulatório).

No dia 01 de abril de 2020, o CEO da *Colb Blockchain Experts*, Yulgan Lira, enviou uma carta ao Ministro da Economia do Brasil, Paulo Guedes, sobre o *sandbox* regulatório envolvendo *Blockchain*. Para Yulgan, a tecnologia *Blockchain* pode ser grande aliada no combate ao coronavírus. Ela poderia ser usada por exemplo, para aproximar o agente deficitário ao capital de particulares de maneira mais rápida, simples e segura [135].

3.4.1.6- O Projeto de Lei 3825/2019

No dia 02 de julho de 2019, o Senador Flávio Arns (PR) protocolou um novo Projeto de Lei voltado especificamente para regular a atividade das *exchanges*. O Projeto de Lei 3825/2019 busca instituir o Banco Central do Brasil como o responsável por regular a fiscalizar as operações das *exchanges* de Bitcoin e de criptomoedas que operam no Brasil [136]. O PL cria a obrigação de que as *exchanges* sejam autorizadas pelo Banco Central do Brasil para poderem operar, "*Art 3 - O funcionamento da Exchange de criptoativos depende de prévia autorização do Banco Central do Brasil*". A autorização só deverá ser concedida às empresas (operantes ou não) que respeitarem e procedimentos determinados pelo BACEN. Em suma, o esforço regulatório deste PL busca estabelecer diretrizes que devem orientar o mercado de criptografia por meio da criação de um sistema de licenciamento para as transações, que ficará sob a supervisão do Banco Central do Brasil; inclusive definindo que os criptoativos não devam ser objeto de fiscalização pela Comissão de Valores Mobiliários, exceto quando possuírem característica de valor mobiliário.

O ano de 2019 foi marcado por forte regulamentação mundial dos ativos digitais, o que foi agravado com o lançamento do *whitepaper* da criptomoeda do Facebook, a Libra. Após esse lançamento, governos do mundo inteiro manifestaram suas opiniões sobre o setor, desenvolvendo guias e diretrizes para o mercado. O ano também foi marcado pela forte pressão em cima das empresas que lançaram ICO's durante 2017 e 2018 [137]. A maioria dos governos ainda está discutindo a taxonomia da nova classe de ativo. Eles buscam ferramentas para classificar *tokens* e definir seu enquadramento ou não enquanto ativo mobiliário. A atenção dos reguladores também é forte ao monitorar as transações de criptomoedas. Eles querem garantir que os ativos digitais não estejam sendo usadas para fomentar a lavagem de dinheiro e financiamento de terrorismo.

Os bancos centrais dos países estão, já há uns dois anos, rapidamente se movimentando no sentido de lançar suas próprias criptomoedas. São as CBDC – *Central Bank Digital Currencies*. Ao adicionar o desenvolvimento do "dólar digital" entre as medidas para se combater o Covid-19, os EUA lançaram a discussão para o

mundo inteiro. Acredita-se que dado o atual panorama político internacional, as CBDC devem ganhar ainda mais atenção [138].

As discussões regulatórias são longas e difíceis, ainda mais em um tema tão dinâmico e que envolve tanta tecnologia quanto esse em discussão. Enquanto os reguladores ainda estão tentando estabelecer as bases mínimas de funcionamento regular desse mercado, a tecnologia dá passos adiante, trazendo já ecossistemas de *Decentralized Finance* (DeFi), criptomoedas focadas em privacidade, BIPs (*Bitcoin Improvement Protocols*) e *Sidechains* (uma forma de testar novas funcionalidades para *Blockchain* sem realmente integrá-los no código). A velocidade exponencial das inovações e a tendência do setor para a privacidade é um grande desafio para os reguladores. E é claro que os avanços tecnológicos vão continuar. A questão é acompanhar de perto os modelos adotados em cada país e construir alternativas que não sufoquem a inovação. E mais do que isso, dado o tamanho do mercado brasileiro, os ativos digitais podem ser um grande aliado no desenvolvimento de novos mercados que apresentam grande potencial de captação.

3.4.2- Panorama Global da Regulação

Com base em um artigo da pesquisadora de análise antropológica e sociológica, Rafaela Romano [139], pode-se traçar um panorama comparativo da questão da regulação global das criptomoedas. Ainda há muita incerteza no que se refere à regulamentação dos governos no uso das criptomoedas, pelos mais variados motivos, como insegurança jurídica, receio de criminalidade, ameaça à soberania da moeda local, entre outros. A incrível velocidade com que a tecnologia avança pode tornar qualquer tentativa de regulamentação obsoleta em um curto tempo também. Ainda assim, muitos países tornaram o uso regular das criptomoedas, enquanto que outros as proibiram, pelo menos até que se possa ter uma maior percepção desse fenômeno tão revolucionário e suas implicações políticas, econômicas, sociais, geográficas, etc. Outrossim, deve-se esclarecer que qualquer moeda digital, assim como o dinheiro vivo, pode ser aplicada em boas ou más ações. O resultado depende de como ele é usado. E isto evidencia o óbvio. Não se pode condenar as criptomoedas com base em intransigência. A Tabela 3 a seguir mostra esse panorama, em abril de 2021:

Tabela 3 – Panorama global da regulação das criptomoedas

Continente	País	Situação	Observações
Américas	Argentina	Sem regulação	Somente o Banco Central pode emitir moeda
	Bahamas	Em tramitação	Projeto de Lei em discussão
	Brasil	Em tramitação	<i>Exchanges</i> podem operar no país
	Bolívia	Proibidas	Não há permissão do Banco Central
	Canadá	Sem regulação	Possibilidade de transação mediante análise
	Colômbia	Sem regulação	Proibidos os investimentos em criptomoedas
	Estados Unidos	Em tramitação	Divergências de classificação das criptos
	Ilhas Cayman	Sem regulação	Há leis que podem ser aplicáveis ao caso
	Chile	Sem regulação	<i>Exchanges</i> podem operar no país
	México	Em tramitação	<i>Sandbox</i> regulatório em testes
	Peru	Sem regulação	Banco Central estuda uso de <i>Blockchain</i>
Venezuela	Proibidas	Há uma criptomoeda estatal, a <i>Petro</i>	
Ásia	Abu Dhabi	Regular	Depende da natureza do produto/serviço
	Bangladesh	Proibidas	Violação de legislação
	Camboja	Regular	Sob licença estatal
	China	Proibidas	Criptomoeda estatal em desenvolvimento
	Coréia do Sul	Permitidas	Operações fiscalizadas por bancos
	Hong Kong	Regular	Operações dependem de licença
	Índia	Proibidas	Posição estatal hostil
	Irã	Parcial	Uso em situações específicas
	Japão	Permitidas	Supervisão do Departamento Financeiro
	Singapura	Permitidas	Operações são tributadas
Europa	Alemanha	Regular	Licenciadas e tributadas
	Espanha	Em tramitação	Há tributação
	Estônia	Regular	Registro no Dep. de Lavagem de Dinheiro
	França	Regular	Há um planejamento de uso
	Finlândia	Permitidas	Moedas virtuais são mercadorias
	Itália	Sem regulação	Autoridade Fiscal monitora operações
	Irlanda	Sem regulação	Grupo de trabalho estuda o setor
	Lituânia	Sem regulação	Identificação de usuários é obrigatória
	Malta	Permitidas	Necessário licença para operações
	Reino Unido	Parcial	Algumas criptos são permitidas
Suíça	Regular	Governo incentiva o uso	
África	Argélia	Proibidas	Sem uso
	África do Sul	Sem regulação	Operações são tributadas
	Egito	Proibidas parc.	Rigidez para obtenção de licença de operação
	Quênia	Sem regulação	Não há proibição, mas alertas sobre ICO's
Oceania	Austrália	Regular	Lei contra lavagem de dinheiro e terrorismo

Como grande defensor das criptomoedas, Fernando Ulrich [121] cita: ‘[...] é importante notar que muitas das desvantagens do Bitcoin são as mesmas enfrentadas pelo dinheiro vivo; este tem sido historicamente o veículo escolhido por traficantes e lavadores de dinheiro, mas políticos jamais seriamente considerariam banir o dinheiro vivo. À medida que os reguladores comecem a contemplar o Bitcoin, eles deveriam ser cautelosos com os perigos da regulação excessiva.’

Recentemente, o presidente do Banco Central do Brasil, Ilan Goldfajn [140], afirmou que as criptomoedas não são bem vistas pelos bancos centrais, em razão de

diversos problemas, dentre eles “a possibilidade de esconder transações que não podem ser vistas à luz do dia” e “a ideia de que as criptomoedas sirvam como pirâmides”. Corroborando as palavras do Presidente, em audiência pública da Comissão Especial da Câmara dos Deputados com propósito debater a respeito do projeto de lei aqui abordado, o consultor do departamento de regulação do sistema financeiro do Banco Central do Brasil, Mardilson Fernandes Queiroz informou que a entidade é contrária ao desejo dos legisladores. Inclusive, declarou que o Banco Central não reconhece as criptomoedas como espécie de moeda, justificando-se com o seguinte argumento: *‘Na dimensão jurídica, não tem o condão de ser moeda de curso forçado, nem lastro na moeda soberana, que é o real. Na dimensão econômica, ela pode até ter reserva de valor, mas podemos citar vários ativos que também podem ter, como uma casa ou apartamento. Como meio de pagamento, já restringe bastante os ativos possíveis de serem aceitos dentro de uma sociedade para ser utilizadas como meio de troca. Elas também não preenchem a função de unidade de conta’* [141].

Relevante pontuar que além do Banco Central do Brasil, atualmente outros Bancos Centrais do mundo têm dado atenção especial às moedas virtuais, assim como o da Holanda, que criou uma criptomoeda própria, restrita à circulação interna, com intuito de entender seu funcionamento. Entidades privadas também têm lançado suas próprias criptomoedas, como é o caso da ‘Libra’, a criptomoeda do Facebook anteriormente mencionada, que é lastreada em dólar, que mesmo antes de seu lançamento oficial já trouxe muita discussão e a preocupação dos reguladores e bancos centrais de que a moeda pode perturbar a estabilidade financeira [142].

Como se vê, diante da variedade de opiniões que se prolonga pelo tempo, algumas pessoas de destaque, tanto na área econômica, como tecnológica e de negócios, vêm manifestando-se acerca do assunto. Steve Wozniak, cofundador da Apple, e John McAfee, criador do antivírus McAfee e CEO da MGT Capital Investments Inc. são assíduos defensores das criptomoedas, inclusive afirmaram terem investido e esperam seu crescimento. Por outro lado, há opiniões contrárias a respeito das criptomoedas, como recentemente afirmaram Jamie Dimon, CEO, presidente e chairman do Banco JP Morgan e Warren Buffet, um dos maiores investidores do mundo, que declararam profunda aversão ao sistema e previram seu fim [143].

O principal motivo para que governos e bancos centrais tenham aversão aos criptoativos é o chamado desacoplamento governo/moeda, no qual os governos ficam de fora da questão monetária, sendo essa descentralizada, não mais controlada pelo estado. Os próprios governos (que existem para servir ao povo) passam a utilizar moedas descentralizadas, sendo clientes dessas. Tudo indica que esse será um dos grandes embates do século XXI.

Capítulo 4 – DESCRIÇÃO DO BITCOIN, ETHEREUM E IOTA

*‘Em retrospecto, era inevitável’ (Elon Musk –
Frase gravada na Blockchain do Bitcoin, ao
comentar sobre uma briga vencida por
investidores de varejo contra Wall Street, pela
primeira vez)*

No contexto da discussão das criptomoedas que podem ser utilizadas de forma mais eficaz na aplicação da horta compartilhada, que já se iniciou na seção 1.1 do Capítulo 1 anterior, decidiu-se que este trabalho se aterá aos detalhes das três criptomoedas de maior alcance mercadológico e/ou com características interessantes ao uso em questão, tais como, por exemplo, as taxas de transação e a baixa latência de resposta. Assim, serão apresentadas as características do Bitcoin, do Ethereum e da IOTA, de forma a se construir um cenário onde as mesmas possam ser comparadas, e que permita escolher a mais indicada para uso na monetização da horta compartilhada.

4.1 Bitcoin

Em seu livro "*Internet of Money*", Antonopoulos [144] faz uma descrição do Bitcoin: "*Bitcoin não é uma empresa. Não é uma organização. É um protocolo padrão, assim como o TCP/IP, ou a Internet. Ele não é de propriedade de ninguém. Ele opera por regras matemáticas simples que todos que participam da rede concordam. Através desse mecanismo simples, invenção de Satoshi Nakamoto, Bitcoin é capaz de permitir que uma rede completamente descentralizada de computadores concorde sobre quais transações ocorreram na rede, essencialmente concordando em quem atualmente possui o dinheiro*".

Porém, o que permite que o Bitcoin funcione de forma segura, imutável e descentralizada é a tecnologia *Blockchain*. O *World Economic Forum*, em 2016 [145], definiu as três características básicas da *Blockchain*: "*A tecnologia distributed ledger (da qual a Blockchain é um exemplo) usa ferramentas criptográficas e um processo*

de consenso para criar uma inovação significativa na forma de se manter registros. Ela possui três características principais: Veracidade, Transparência e Descentralização. Cópias múltiplas do histórico completo dos registros de entrada são verificadas individualmente por consenso (entradas incorretas são identificadas e eliminadas). Isto promove a Veracidade. Para a Transparência, registros públicos de atividades são disponibilizados a todos os participantes. A operação é feita de forma peer-to-peer, ao invés de requisitar uma organização específica e centralizadora." A Blockchain é assim, uma forma disruptiva de se armazenar dados, garantindo a continuidade e a imutabilidade das transações [146]. Porém isso tem um custo, principalmente em espaço de armazenamento e tempo de processamento, pois várias réplicas de um mesmo registro são feitas na rede [145]. Assim, a transação é feita de forma distribuída, pelos nós que têm cópias da Blockchain da mesma. A Blockchain então possui a sequência de registros de todas as transações ocorridas. Podem ocorrer erros ou tentativas de uso fraudulento, como por exemplo, a utilização duplicada de uma mesma unidade da criptomoeda em duas transações diferentes, o chamado "problema do duplo gasto". Por isso, uma transação só é considerada efetiva se mais da metade dos participantes da rede concordarem que a mesma ocorreu de fato, gerando o consenso [144].

4.1.1 Hashcode e Encriptação

O *hashcode* é a saída de uma função matemática, um número plano único que resume digitalmente os dados de entrada. Assim, pode-se comparar o *hash* recebido em uma transação com o *hash* calculado, a fim de se averiguar a autenticidade e a integridade do arquivo. As características que o algoritmo de *hash* deve possuir são [147]:

- Unidirecionalidade: É computacionalmente difícil encontrar a entrada que originou o *hashcode*;
- Compressão: O tamanho do *hashcode* deve representar uma pequena parte dos dados de origem;
- Cálculo fácil: o cálculo do *hashcode* deve ser relativamente simples;

- Difusão: para dificultar a descoberta da entrada de dados a partir do *hashcode*, ao se mudar um único bit dos dados de entrada, o *hashcode* deve ser alterado em aproximadamente 50% de seus *bits*;
- Colisão: para um mesmo *hashcode* gerado, deve ser computacionalmente muito difícil encontrar dois valores de entrada diferentes que o gerem.

A criptografia faz com que a leitura da mensagem seja possível somente se o receptor possuir a chave para decifrar a codificação matemática feita. A criptografia assimétrica, adotada pelo Bitcoin, usa um par de chaves, sendo uma chave pública utilizada no processo de encriptação, e uma chave privada para a deciptação. A função matemática usada é a ECDLP (*Elliptic Curve Discrete Logarithm Problem*), definida em um padrão chamado *secp256k1*. Maiores informações podem ser encontradas em Hankerson et al, [148].

A assinatura digital é a cifragem do *hashcode* usando uma chave privada, de tal forma que a chave pública seja utilizada para provar a origem do documento. Uma assinatura válida não pode ser refutada pelo nó originador, pois só ele tem a chave privada daquela assinatura. Assim, a assinatura digital provê integridade, autenticidade, e não-repúdio [149]. Desta forma, o nó, que já possui um par de chaves, pode gerar o endereço. O endereço é um número obtido usando a chave pública do nó. Ele é usado para informar ao sistema quem é o dono daquela transação, pois somente quem possuir a chave privada que gerou aquele endereço poderá usar o que estiver na transação, seja um valor monetário ou um dado. Para gerar o endereço o nó deve realizar uma operação de duplo *hash*, primeiro SHA-256 depois RIPEMD160 = RIPEMD160(SHA256(Chave Pública)), após isso deve converter o resultado para Base58. Este é o endereço Bitcoin criado pela carteira do usuário, e é a única informação usada para definir onde os Bitcoins serão alocados e para onde serão enviados.

As chaves precisam ser armazenadas, e geralmente são armazenadas em uma carteira digital. A carteira tem a função de gerar as chaves dos usuários. Existem dois tipos de carteira: as determinísticas e as aleatórias. As determinísticas usam uma chave inicial, chamada de semente, para criar as demais através de uma função *hash*. Armazena apenas a primeira chave, pois todas as outras podem ser recalculadas. As

carteiras Aleatórias precisam usar algum algoritmo de geração de números aleatórios para gerar as chaves, e precisam armazenar todas as chaves criadas.

Como a rede deve ser descentralizada, e deve haver o consenso [150] na rede, foi criada uma rede P2P (*peer-to-peer*) [151], sendo todos os nós da rede iguais e não havendo nenhum nó centralizador. Qualquer nó da rede pode assumir uma ou mais de quatro funções: roteamento, base de dados, mineração e carteira digital. Todos os nós possuem ao menos a função de roteamento, porém nem todos precisam executar todas as funções. Um usuário mais simples necessita apenas das funções de roteamento e de carteira digital, podendo realizar transações até mesmo com um celular somente, sem necessitar armazenar toda a cadeia de blocos. Os nós que se interconectam para formar a rede são chamados de vizinhos [152]. Os registros descentralizados da cadeia de blocos permitem que haja consenso entre os nós, e mesmo que cada um desses nós não seja isoladamente confiável, o consenso traz a confiabilidade necessária. Em um sistema convencional, os bancos e cartórios são os responsáveis de confiança pela guarda da informação, o que já não mais é necessário quando se utiliza registros na *Blockchain*, eliminando assim a necessidade das instituições convencionais [153].

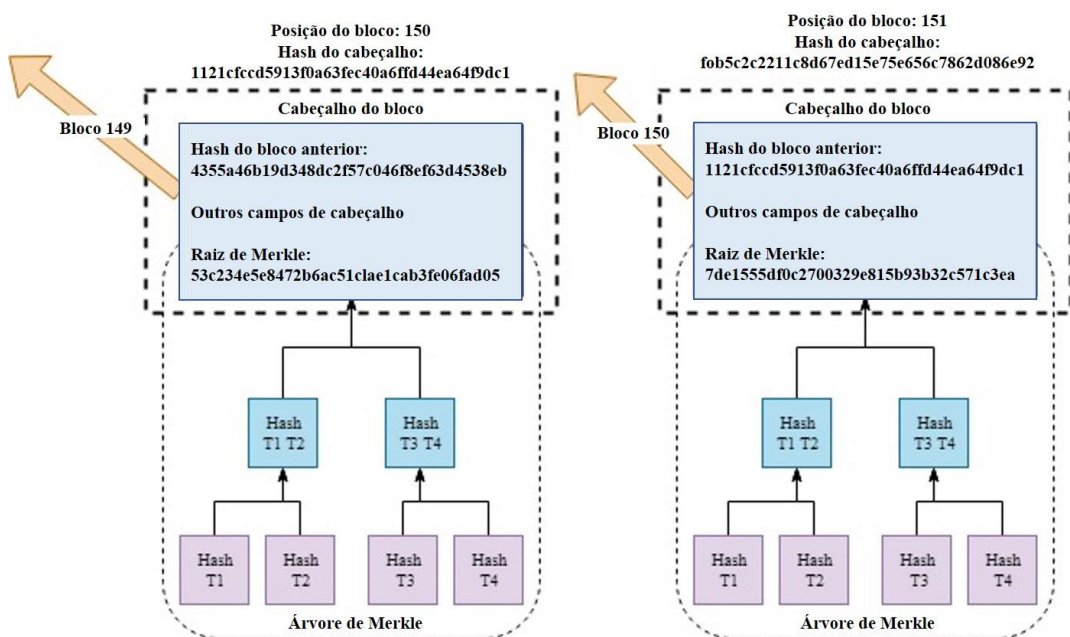


Figura 9 - Estrutura simplificada de blocos da cadeia [147]

Conforme a Figura 9 acima, a *Blockchain* armazena transações de forma concatenada com os blocos anteriores, montando um registro distribuído. O bloco tem duas partes: cabeçalho e transações. É possível associar uma transação ao seu endereço

de origem e de destino. Cada bloco possui um *hashcode* único, que é armazenado no cabeçalho do bloco seguinte da cadeia, formando uma ligação entre os mesmos. Daí o nome cadeia de bloco ou, em inglês, *Blockchain*.

A árvore de Merkle, resumidamente, permite a verificação da presença de uma informação em um dado local. Inicialmente tendo uma grande quantidade de informação, esta será quebrada em várias partes, mantidas em ordem. A seguir, aplica-se uma função de *hash* a cada uma destas partes. O próximo passo consiste em, seguindo a ordem original, concatenar estes *hashes* dois a dois (ou três a três ou mais, dependendo do tipo de árvore que se deseja obter) e aplicar a função de *hash* a esta concatenação. O resultado será o nó de uma árvore e os *hashes* que o originaram, seus filhos. Esse procedimento é repetido com todas as partes e depois com os nós gerados pelas partes, e assim sucessivamente, até que se obtenha o nó raiz. Ou seja, é uma árvore construída de baixo para cima. O motivo para se utilizar esta estrutura é que ela permite um procedimento chamado Prova de Merkle. Neste procedimento, um cliente deseja verificar que certa informação se encontra em uma dada posição da árvore. O cliente precisa possuir o *hash* da raiz fornecido por alguma fonte confiável e a parte que está sendo inquirida precisa enviar apenas os *hashes* complementares ao longo do ramo que leva da folha até a raiz. A Figura 10 ilustra:

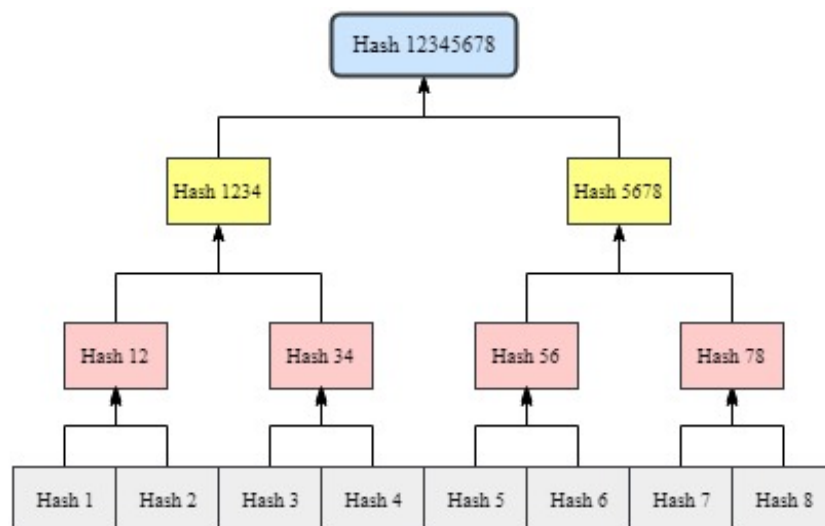


Figura 10 - Árvore de Merkle [147].

O processo de consenso de uma criptomoeda pode ser implementado através de diferentes regras e algoritmos que influenciam diretamente no seu nível de descentralização e controle, seja para confirmar transações, seja para “emitir” novas unidades de moedas e adicioná-las ao sistema, processo chamado de “mineração” [154].

A PoW (*Proof-of-Work*), utilizada no Bitcoin, é um processo de mineração, para confirmar uma transação [155]. Neste processo os nós realizam diversos cálculos matemáticos até que se descubra um novo bloco da cadeia. O processo envolve tomar a função *hash* criptografada (no caso do Bitcoin usa-se o algoritmo SHA-256) do último bloco da *Blockchain*, adicionar novas transações e resolver uma nova função criptografada. É fácil verificar se o resultado da função resolvida é correto, porém é muito complexa a resolução, o que exige um esforço de processamento enorme. Atualmente usam-se ASICs (*Application-Specific Integrated Circuits*) para esse fim. Quem resolver a função será o criador do próximo bloco da cadeia, e receberá uma recompensa, além das taxas inclusas nas transações. O PoW é muito criticado pelo alto consumo de energia, mas torna a *Blockchain* bastante segura. No Bitcoin, essa prova consiste em adicionar um *nonce* (isto é, um número arbitrário que só será usado uma vez) ao cabeçalho e então obter o *hash* do cabeçalho usando o algoritmo SHA256. Se o resultado obtido for menor do que certo valor alvo, a prova é aceita. Caso contrário, muda-se o *nonce* e tenta-se novamente (como esse número é de apenas 32 bits, é comum que os valores possíveis se esgotem, o que exige que alguma outra parte do cabeçalho, como a marca de tempo, seja alterada para tentar novamente). Como o SHA256 é um algoritmo pseudoaleatório com resultado imprevisível, não há qualquer maneira de se obter uma Prova de Trabalho válida exceto por tentativa e erro alterando o *nonce* a cada tentativa. O valor alvo é redefinido a cada 2016 blocos para aumentar ou diminuir a dificuldade, de modo que seja criado em média um bloco a cada dez minutos. Para incentivar os mineradores, estes adicionam uma transação ao bloco no qual se recompensam pela criação do mesmo antes de iniciar a criação do cabeçalho. Assim, todo dia milhões de nós competem entre si na mineração de blocos a fim de ganhar esta recompensa e auditam uns aos outros para garantir que ninguém está “roubando”. Um exemplo de fazenda de mineração é visto na Figura 11:



Figura 11 - Uma fazenda de mineração. Fonte: www.genesis-mining.com

Outra forma de confirmação de transação existente, mas que não é utilizada pelo Bitcoin, é a PoS (*Proof-of-Stake*). Esta forma faz um sorteio para decidir quem será o minerador do próximo bloco. Nesse modelo, o potencial criador já deve contar com ativos da moeda específica, e quem tiver mais moedas terá mais chances de ser sorteado. É necessário alocar uma quantidade de moedas para este processo, e caso tente corromper o bloco, perderá essas moedas, o que, em tese, garante a integridade dos participantes. O bloco resultante é denominado bloco "forjado", e não mais "minado". O PoS é mais eficiente que o PoW em termos de energia gasta.

A terceira forma de consenso conhecida é a PoC (*Proof-of-Capacity*). É ainda menos utilizada, e o nó sorteado para criar o próximo bloco é escolhido por sua capacidade de HD disponível. Usa bem menos energia que as anteriores, mas também não é utilizada no Bitcoin [156].

A validação do novo bloco é simples: verifica-se se o bloco anterior é válido, verifica-se a marca temporal do novo bloco, que deve ser maior que a anterior e não deve estar muito distante no tempo, verificam-se as informações adicionais do cabeçalho, verifica-se o mecanismo de consenso do novo bloco, verifica-se o banco de dados do bloco anterior e compara-se com o do novo bloco. Caso haja alguma inconsistência, a validação é falha. Caso contrário, o novo bloco se localizará ao final

da cadeia. Esta validação deve ser executada por todos os nós que receberem o novo bloco criado, para que se tenha o consenso da maioria. Por se tratar de uma rede distribuída, frequentemente acontece de dois ou mais blocos diferentes, todos legítimos, serem criados quase que simultaneamente e adicionados à mesma posição da cadeia em nós diferentes da rede. Isso cria uma divisão (*fork*) temporária do banco de dados, pois duas ou mais versões competem para serem aceitas. Cada rede deve ter definido algum algoritmo que permita avaliar estas versões e decidir uma pontuação para elas, decidindo então a vencedora. Por exemplo, em *Blockchains* que usam Prova de Trabalho, tal pontuação é calculada como o trabalho total acumulado em uma cadeia. Blocos criados que acabam ficando de fora da rede após este “desempate” são chamados blocos órfãos. Em geral, estes algoritmos são desenvolvidos de modo tal que essa pontuação continue crescendo à medida que se adicionam novos blocos, de modo que a possibilidade de certo bloco se tornar órfão diminui exponencialmente quanto mais a cadeia cresce [157].

4.2 Ethereum

A linguagem do Bitcoin não chega a ser uma linguagem de Turing completa. Por exemplo, não há *loops* no Bitcoin. Outras limitações do Bitcoin são: inabilidade de uma unidade de valor se fragmentar; impossibilidade de a unidade ter vários estados intermediários (no *Bitcoin*, uma unidade está gasta ou não gasta); e inacessibilidade pela unidade a algumas informações da *Blockchain*.

Vitalik Buterin [26], após perceber que o Bitcoin carecia de uma linguagem de *scripts* mais robusta, decidiu criar uma nova plataforma dedicada ao desenvolvimento de aplicações descentralizadas, tecendo assim o *White Paper* do Ethereum. Ele promoveu um processo muito eficaz de captação de investidores e criou a Ethereum Foundation, para implementar sua proposta. Buterin partiu do princípio de que qualquer um poderia desenvolver um sistema baseado em *Blockchain* e executá-lo no ambiente Ethereum, não tendo custos de desenvolvimento. Existem diversos sistemas parecidos, utilizando o Bitcoin, mas que são limitados em capacidade pelos scripts do mesmo.

O Ethereum é, portanto, uma plataforma dedicada ao desenvolvimento e implantação de aplicações descentralizadas de alta confiabilidade. Em seu âmbito, tais aplicações são conhecidas como *Smart Contracts*. O Ethereum utiliza uma *Blockchain* para executar esses contratos de maneira inviolável, uma vez que todos os nós da rede deverão entrar em consenso sobre o resultado de cada computação. Para participar da sua rede, cada nó deve possuir uma implementação da *Ethereum Virtual Machine* (EVM), uma máquina virtual Turing completa definida por Gavin Wood [28]. Na realidade, a criptomoeda do sistema Ethereum é a *Ether*, que é utilizada para compensar as computações realizadas pelos nós, e também para a transferência de valores entre contas.

4.2.1 Conceitos Básicos

a. Gas

A plataforma Ethereum define o Gas como sendo um mecanismo de preço interno, com o objetivo de medir o esforço computacional para realizar as transações e se tentar evitar ataques de negação de serviço e outros tipos de *spam*. O valor do Gas para processamento interno, é diferente de como os *tokens* de Ether avaliam a valoração real da criptomoeda, desagregando a camada de valor e a camada de processamento da plataforma Ethereum. Sempre que algum pedaço de código vai ser executado, a parte que está solicitando tal execução deve estabelecer a quantidade máxima de unidades de Gas que está disposta a utilizar e qual o valor em Ether que irá pagar por cada unidade gasta. Parte básica da verificação inicial consiste em checar se o solicitante de fato possui a quantidade necessária de moeda e subtraí-la de sua conta para pagar as taxas de transação (isto é, o custo do Gas). Se for necessário mais Gas que o enviado para executar o código, os efeitos deste serão revertidos, mas o solicitante perde o valor das taxas de transação. Por outro lado, se sobrar Gas, o valor em excesso será devolvido ao solicitante no final da transação. Cada nó decide se aceita o valor proposto para o serviço. Assim, fica inviável para algum possível invasor tentar sobrecarregar o sistema com computações inúteis, pois perderia muito dinheiro com isso, ou seria ignorado se oferecesse muito pouco pelo Gas. Dessa forma, *loops* infinitos são barrados pois não é possível enviar Gas infinitamente.

b. Contas

As contas definem o estado do sistema, sendo as transições de estado definidas pela transferência de valores e informação entre contas. Existem dois tipos de contas: contas externas, controladas por quem possui a chave privada; e contas de contrato, controladas por seu próprio código. As contas possuem quatro campos:

- *Nonce*, um contador que garante que não se processe a mesma transação várias vezes;
- A quantidade de Ether atual da conta;
- O código do contrato da conta (*Smart Contract*), se houver;
- O armazenamento da conta (inicialmente vazio).

Uma conta externa (EOA – *Externally Owned Account*) não tem código interno e pode enviar transações de acordo com o controle do seu usuário, detentor de sua chave privada. Uma conta de contrato por outro lado deve conter um código e irá executá-lo sempre que receber uma transação ou mensagem proveniente de uma EOA. Tal execução pode ler e escrever no seu armazenamento (em pares de chave-valor), enviar novas mensagens, criar novos contratos, dentre outras coisas. O termo popular ‘contrato inteligente’ (*Smart Contract*) refere-se ao código da conta de contrato, e é um programa executado quando uma transação é enviada para essa conta.

c. Transações

A transação é a forma como uma conta externa envia um pacote de dados a outras contas (sejam externas ou de contrato). Os campos da transação são:

- Destinatário,
- Assinatura do remetente,
- Quantidade de Ether a ser transferida,
- Um campo de dados opcional,
- A quantidade de Gas enviada,
- O valor do Gas.

A Figura 12 ilustra:

Transaction
From: 14c5f88a
To: Bb75a980
Value: 10
Data: 2, CHARLIE
Sig: 30452fdedb3d F7959f2ceb8al

Figura 12 - Transação Ethereum, sem o valor do Gas [26].

d. Mensagens

As contas externas se comunicam por transações, porém as contas de contrato, entre si, se comunicam por mensagens. As mensagens são objetos virtuais, que existem apenas no ambiente Ethereum, e contêm:

- Remetente,
- Destinatário,
- Quantidade de Ether transferida,
- Campo de dados,
- Quantidade de Gas enviada.

4.2.2 Transição de Estado

A mudança de estado necessariamente deve começar com o envio de uma transação, uma vez que as contas de contrato só executam seu código quando recebem a solicitação de uma EOA, de forma estritamente determinista. Inicialmente, verificam-se os campos da transação que deu origem ao processo. Todos os campos devem estar corretos, com sua assinatura válida, e o *nonce* da transação deve coincidir

com o *nonce* do remetente. Caso contrário, já houve erro. É calculada a taxa de transação, multiplicando-se a quantidade de Gas enviada pelo seu preço. Este valor é subtraído da conta do remetente, e o *nonce* é incrementado, para se evitar que a mesma transação seja processada duas vezes. Se o remetente não tiver Ether suficiente, não há transição. Sabendo a quantidade disponível de Gas, é subtraída da conta do remetente a taxa a ser paga pelo total de bytes da transação. O valor da transação é transferido do remetente para o destinatário. Caso o remetente não possua o valor para a transferência, tudo volta ao estado inicial, mas o minerador do bloco ficará com as taxas de Gas da transação. Se o destinatário for uma conta de contrato, executa-se o seu código até que este retorne, ou até que a quantidade de Gas se esgote. Se o Gas se esgotar antes do fim, também se revertem todas as mudanças, exceto pelas taxas que ficam com o minerador. Se a execução terminar normalmente, o minerador fica com o valor do Gas que foi gasto nas computações e o restante é devolvido ao remetente. A duração de execução do processo pode ser bem longa, uma vez que o código do contrato pode enviar mensagens para outros contratos, que executarão seus códigos, e assim por diante, até que tudo se encerre ou o Gas acabe. Importante observar que caso este esgotamento ocorra durante uma computação de uma mensagem, apenas os efeitos desta mensagem serão revertidos, pois a conta que enviou a mensagem pode ainda ter Gas que não tinha sido enviado.

4.2.3 Ethereum Virtual Machine (EVM)

Para garantir que todos os contratos sejam executados da mesma maneira em qualquer nó, cada um destes deve possuir uma implementação da EVM definida no *Yellow Paper* de Gavin Wood [28]. A EVM permite que a *Blockchain* Ethereum não armazene somente valores e transações, mas também códigos de programação e instruções específicas, sendo assim uma *Blockchain* melhorada e mais inteligente [158]. Embora existam várias linguagens de programação disponíveis para o Ethereum, todas são compiladas para a mesma linguagem de *bytecode* baseada em pilhas conhecida como EVM *code*. Sua operação é bastante semelhante à de computadores modernos, onde se tem uma série de instruções básicas em sequência, um *program counter* (PC) que aponta para a próxima instrução a ser executada e é

incrementado ao final de cada instrução, e a execução segue até que as instruções acabem (fim do programa), ou até que se detecte um erro (falha no programa), ou se encontre uma instrução de parada ou de retorno (programa concluído ou interrompido). Porém, diferentemente de computadores modernos, a EVM não tem registradores, mas apenas três tipos de espaços onde guardar informações: a) Uma pilha com as operações típicas de *push* e *pop*; b) A memória, que é organizada como um arranjo de bytes que teoricamente pode ser expandido indefinidamente; c) O armazenamento do contrato (o campo possuído por todas as contas, onde pares chave-valor são guardados). Os dois primeiros são temporários (como a memória RAM de um computador) e resetados ao final de cada computação. Já o último é persistente até que seja mudado (equivalente ao disco rígido de um computador). O EVM *code* possui as instruções típicas de linguagens de *assembly* para operações matemáticas básicas, comparações e lógicas bit a bit, armazenamento na memória, uso da pilha e movimentação do *program counter* (*jumps*). Além destas, também possui instruções para determinar a quantidade de Gas disponível e o seu preço, para enviar mensagens para outra conta, para criar uma nova conta e para obter vários tipos de informações sobre o ambiente, como por exemplo: o bloco atual (informações do cabeçalho); o código de uma conta (podendo inclusive copiá-lo para a memória); a transação ou mensagem que iniciou a atual execução (remetente, balanço, e etc.); e o valor enviado. Existe também uma instrução especificamente para aplicar o algoritmo de *hash* criptográfico SHA3 e uma variedade de instruções para propósitos de *log* (isto é, registrar eventos ao longo da execução do programa). Ao final, a execução deste código pode retornar um arranjo de bytes como saída.

4.2.4 Mineração no Ethereum

A mineração no Ethereum consiste em acumular uma certa quantidade de transações, limitadas por valor de Gas máximo que cada bloco pode ter e aplicá-las, obtendo os próximos estados. A *Blockchain* do Ethereum possui a particularidade de guardar todo o estado atual em cada bloco, embora utilize recursos para minimizar o espaço gasto com isso. O cabeçalho de um bloco no Ethereum possui, além das informações básicas, as raízes de três árvores de Merkle: a primeira, como no Bitcoin,

para armazenar todas as transações contidas no bloco; a segunda contendo o estado atual, que utiliza uma estrutura modificada conhecida como árvore Patrícia; a terceira e última é uma árvore de recibos que, na prática, são informações mostrando o efeito de cada transação. A Figura 13 mostra:

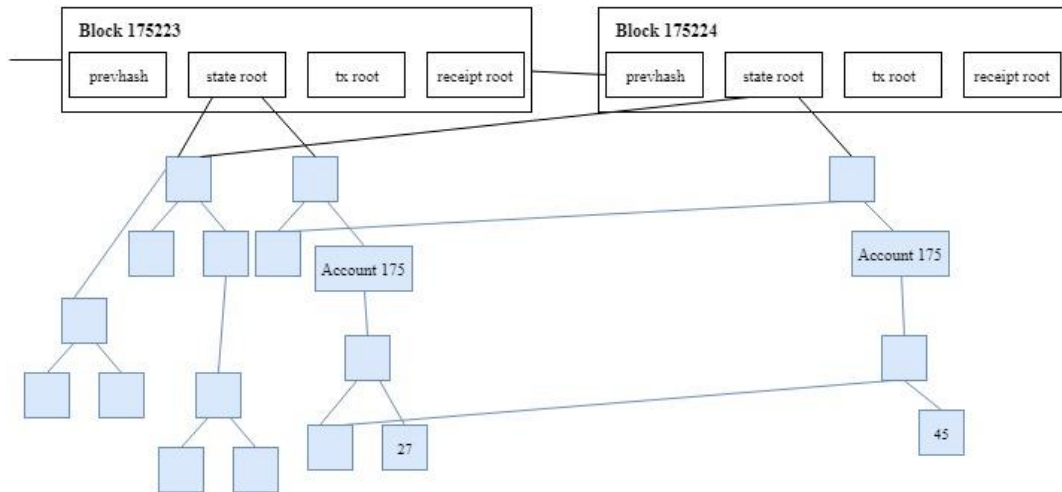


Figura 13 – As três raízes no cabeçalho Ethereum [157].

O Ethereum usa a Prova de Trabalho para realizar o consenso, de forma bastante semelhante ao Bitcoin, mas com algumas pequenas modificações que tornam mais difícil a criação de ASICs para Ethereum. O grau de dificuldade da mineração é ajustado para se manter a taxa de criação de blocos em torno de 12 a 15 segundos por bloco. O processo de validação de um bloco inclui checar todas as computações desencadeadas por cada transação, de modo que no final, cada nó terá realizado praticamente o mesmo trabalho que o minerador (exceto a prova de trabalho, cuja verificação é mais simples), embora apenas este receba as taxas de transação e a recompensa pela mineração.

4.2.5 Smart Contracts da Carteira de Contrato

Os contratos inteligentes formam a base da plataforma Ethereum, e basicamente são *scripts* para transferência de valores, que conversam entre si. São três tipos básicos de contratos: aplicações financeiras, aplicações parcialmente financeiras, e aplicações não-financeiras [159]. As aplicações financeiras envolvem todo tipo de fundos de investimentos, de cobertura, bolsas de valores, e até mesmo contratos de emprego. As

aplicações semifinanceiras envolvem alguma troca de dinheiro, mas a aplicação em si não é voltada para dinheiro, como por exemplo, o pagamento de uma taxa de resolução de um problema computacional. Já as aplicações não-financeiras envolvem casos tais como sistemas de votação e governança, sem troca de dinheiro. Qualquer um pode escrever um *smart contract* no Ethereum, mas precisa ter Ether para pagar o Gas necessário para a execução do contrato. Um exemplo é visto na Figura 14:

```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
    ) {
        balanceOf[msg.sender] = initialSupply;          // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);      // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;              // Subtract from the sender
        balanceOf[_to] += _value;                      // Add the same to the recipient
    }
}
```

Figura 14 - Exemplo de Contrato Inteligente Ethereum [77].

Um caso particular de *smart contract*, bastante popular, é o chamado ICO (Initial Coin Offerings), onde uma empresa emite uma nova criptomoeda para oferta aos investidores. Assim a empresa obtém capital para financiar seu crescimento e os investidores aguardam a valorização para ter retorno. Esse foi o caso da própria plataforma Ethereum, que em sua ICO arrecadou 18 milhões de dólares. O valor do Ether à época era de 40 centavos de dólar.

4.2.6 Hard Forks

Quando uma mudança abrupta na plataforma Ethereum é feita, pelos próprios mantenedores, por questões de atualizações e/ou melhorias, esta mudança é denominada *Hard Fork*. Isso gera uma derivação na *Blockchain*, uma vez que muitos usuários podem não querer atualizar seus sistemas e se manter na *Blockchain* anterior. Porém, as transações destes usuários não serão mais validadas na *Blockchain*

atualizada. Um exemplo disso é a *Hard Fork* que acabou gerando duas plataformas distintas: a Ethereum Classic (original), e a Ethereum (atualizada). Essa *Hard Fork* foi necessária devido a uma aplicação que rodava de forma autônoma na plataforma, chamada *The DAO*, ter tido uma falha que levou à perda de 50 milhões de dólares da mesma. A falha não foi da plataforma Ethereum, mas sim da aplicação, mas ainda assim a comunidade optou em restituir o prejuízo e criar uma *Hard Fork* para prevenir novos casos. Como muitos usuários não quiseram seguir a atualização, criou-se a Ethereum Classic, que todavia é incompatível com a nova plataforma Ethereum.

4.3 IOTA

O protocolo IOTA foi criado em 2015, na cidade de Berlim, Alemanha, por David Sønstebø, Sergey Ivancheglo, Dominik Schien, e Sergei Popov. É um protocolo criado especialmente para transações entre objetos, na Internet das Coisas [160]. A IoT tem crescido rapidamente, e a demanda por micropagamentos, e até mesmo nanopagamentos está cada vez maior. A IOTA é diferente da maioria das criptomoedas existentes, pois não se baseia no uso de *Blockchains*, o que, em princípio, soluciona as limitações das moedas baseadas em Bitcoin, que apresentam duas características bastante limitantes para seu uso em IoT:

- Taxas cobradas pesadas, pois à medida que o valor do pagamento a ser feito diminui, sua taxa para ser processado pela rede *Blockchain* aumenta, quando deveria ser exatamente ao contrário;
- Funções dos usuários: na *Blockchain* são necessários dois tipos de usuários, os mineradores, que verificam as transações e cobram as taxas, e os usuários normais, que emitem as transações. Isso aumenta a chance de conflitos e acarreta em maiores gastos de recursos.

A tecnologia utilizada na IOTA é o *Tangle*, que, de acordo com Popov [35], permite as seguintes qualidades:

- Grande velocidade nas transações e enorme escalabilidade;
- Inexistência de taxas cobradas nas transações, facilitando as micro e nano transações;

- Mais resistente a ataques oriundos de computação quântica, que no futuro serão um grande problema para as criptografias, devido à Inteligência Artificial. A Inteligência Artificial pode utilizar uma série de critérios para derrubar uma conta, trabalhando de forma automática e promovendo adaptações aos ataques, de forma a possibilitar a efetividade dos ataques;
- Estrutura modular e leve, bastante apropriada para integração em pequenos dispositivos de IoT;
- Não há *forks* na IOTA, garantindo uma imutabilidade e maior segurança nas transações;
- Todos os nós da rede são iguais, sem mineradores para censurar a rede, uma vez que não há a necessidade de mineração, pois todos os tokens IOTA já foram emitidos na pré-venda. Existe um total de 2,779,530,230 bilhões de MIOTA (milhões de IOTAs).

4.3.1 Tangle

Considerando todos estes aspectos, a IOTA *Tangle* apresenta uma melhor solução para transações de IoT. A *Blockchain* é substituída pelo *Tangle*, que é um DAG (Grafo Acíclico Dirigido).

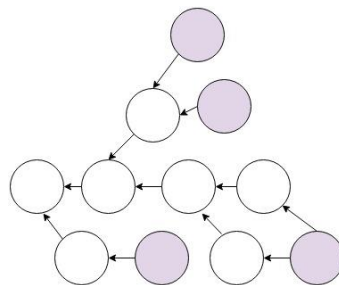


Figura 15 – DAG [35].

O *Tangle* é feito de *Sites* e Nós. Os *Sites* contêm uma ou algumas transações relacionadas entre si, e os Nós são os usuários IOTA que emitem e recebem as transações. Por via de regra na IOTA, uma nova transação emitida na rede deve aprovar duas transações mais antigas. E todos os nós da rede são responsáveis por aprovar as transações, o que remove o papel dos mineradores na rede. Existem duas

maneiras de uma transação aprovar outra. A primeira maneira é a aprovação direta, conforme a Figura 16:

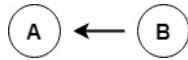


Figura 16 - A transação B aprova diretamente a transação A [35].

A segunda maneira é a aprovação indireta, onde transações intermediárias fazem a ponte para a aprovação, conforme a Figura 17:

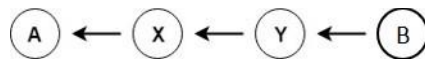


Figura 17 - Aprovação indireta de A por B [35].

A primeira transação que ocorre no *Tangle* é denominada transação do *Genesis*, e é direta ou indiretamente aprovada por todas as outras subsequentes. Esta transação envia *tokens* de um endereço contendo todos os *tokens* para outros endereços do *fundador*. No estágio inicial, não se escolhem as transações para aprovação. Todos os nós seguem algumas regras de referência, pois geralmente são dispositivos locais que pertencem a uma mesma região. A transação recém-emitida, que ainda não recebeu nenhuma aprovação é denominada TIP. Há um algoritmo de seleção de TIP, que resolve os conflitos de aprovação de TIPs. Este algoritmo roda diversas vezes para verificar qual das TIPs tem maior probabilidade de ser aprovada pelo nó. O *Tangle* atua de forma assíncrona e tolera duas transações conflitantes, pois supõe que a transação incorreta será considerada órfã ou até mesmo apagada, à medida que o *Tangle* for crescendo.

Um nó será descartado pelo nó vizinho, quando mostrar preguiça em relação à propagação de transações. O incentivo mantém todos os nós funcionando, embora eles não emitam transações frequentes.

4.3.2 Termos Importantes

Os termos descritos na sequência são considerados essenciais em uma transação, que aqui será chamada de transação A.

- a. **Peso próprio:** O peso da transação A é proporcional ao esforço que o nó emissor da mesma tem que fazer, que pode ser assumido como sendo 3^n , onde n é um número inteiro positivo, que se relaciona com a importância da transação. A ideia é de que quanto maior for o Peso próprio da transação, maior será sua importância. Para se evitar ataques de *spam* ou outros, é assumido, por exemplo, que nenhum nó da rede pode gerar um grande número de transações com pesos "aceitáveis" em um curto período de tempo.
- b. **Peso Cumulativo:** É o Peso próprio da transação A mais a soma dos Pesos próprios das transações seguintes que aprovaram direta ou indiretamente a transação A. Na figura seguinte a transação D tem Peso próprio igual a 1, e Peso cumulativo de 6, que é o Peso próprio de D mais os Pesos próprios de A, B, e C, ou seja: $1 + 1 + 3 + 1$.

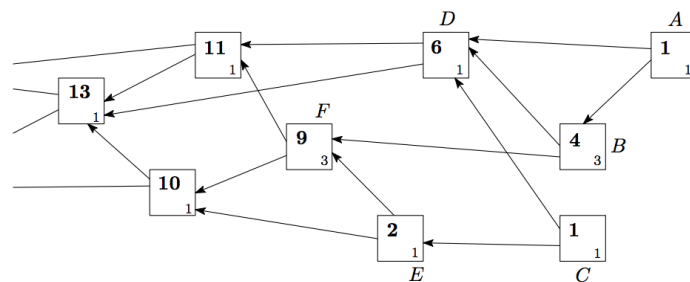


Figura 18 - Pesos próprios no canto inferior e Pesos Cumulativos no canto superior [35].

Na figura 18 acima as transações A e C ainda não foram aprovadas e, portanto, são TIPS. Ao se chegar uma transação nova, X, que aprova as transações A e C anteriores, X passará a ser a TIP, e as transações anteriores terão seu Peso cumulativo acrescido do Peso próprio de X, como na Figura 19 a seguir.

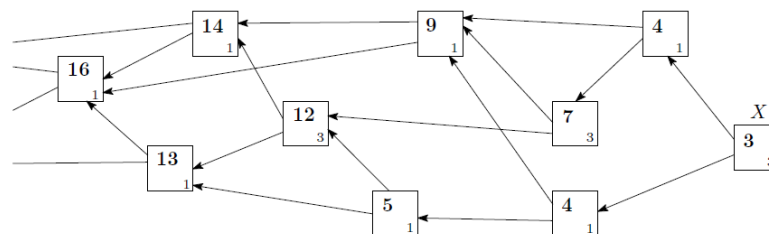


Figura 19 - A TIP X chegou e os Pesos Cumulativos das transações anteriores aumentou [35].

- c. **Pontuação:** É o Peso próprio da transação mais a soma de todos os Pesos próprios das transações anteriores que foram aprovados pela mesma. Por exemplo, na Figura 20 seguinte a transação A aprovou B, D, F, e G, então sua pontuação é $1 + 3 + 1 + 3 + 1 = 9$.

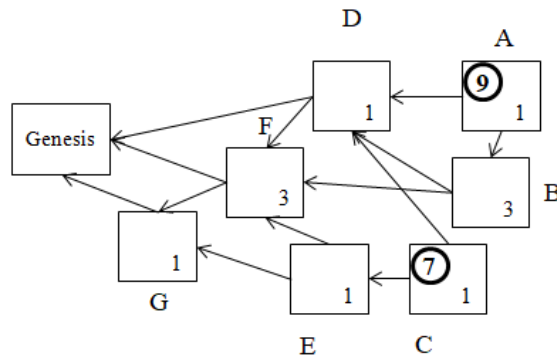


Figura 20 - Pontuação no site A e no site C [35].

- d. **Altura:** É o comprimento, em quantidade de sites, do caminho mais longo até a transação *Genesis*. No exemplo da figura acima G tem uma Altura de 1, enquanto que D tem uma altura de 3 (D, F, e G).
- e. **Profundidade:** É o tamanho do caminho mais comprido, do site até uma TIP. Na figura acima, G tem a Profundidade de 4 (F, D, B, A), e D tem a Profundidade de 2 (B, A).
- f. **Cutset:** assumindo que o tempo médio para se emitir uma nova transação seja H, *Cutset* é o grupo de TIPs existentes no intervalo de tempo t até t + H, e define que:
- Qualquer caminho de uma nova transação para o *Genesis* deve passar pelo *cutset*;
 - Quanto menor o tamanho do *cutset*, maior a chance de uma nova transação ser aprovada. Ou seja, uma nova transação tem menos concorrentes;
 - Ele é usado como um *checkpoint* para podar o DAG e controlar o crescimento do *Tangle*.

4.3.3 Estratégias para aprovar as TIPS

A nova transação emitida por um usuário deve sempre primeiramente aprovar duas TIPS existentes, e isso pode ser feito de forma aleatória ou quase aleatória, uma vez que um algoritmo decide a melhor TIP a ser aprovada, evitando nós preguiçosos, que poderiam sempre aprovar um par fixo de transações antigas, e também evitando que entidades maliciosas inflem artificialmente o número de TIPS tornando possível que transações futuras selecionem as TIPS maliciosas e abandonem as TIPS honestas.

A carga, ou o tamanho do *Tangle*, influencia em sua eficiência, viabilidade e segurança. Com carga baixa, o número de TIPS é bem baixo, sendo normalmente uma ou duas. É improvável que várias transações diferentes aprovevem a mesma TIP. Isto ocorre quando a latência da rede é baixa e o poder de computação é alto, fazendo com que o fluxo de novas transações seja pequeno.

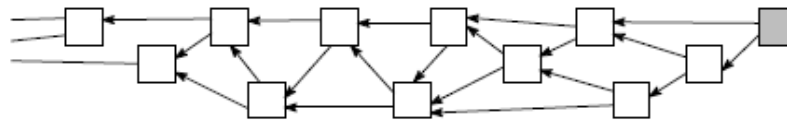


Figura 21 - Carga baixa [35].

Se a latência da rede for alta, e o poder computacional dos nós for baixo, o regime se torna de carga alta. O número de TIPS fica alto, e algumas novas transações podem esperar bastante até serem aprovadas.

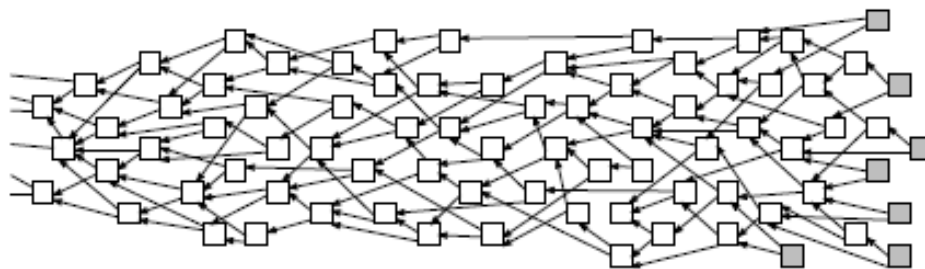


Figura 22 - Carga alta [35].

Em carga alta, caso uma transação que não seja considerada uma das melhores a ser aprovada, e fique algum tempo esperando aprovação, um nó da rede pode criar uma chamada "transação vazia", apenas com o intuito de aprovar a transação que está aguardando. Como a nova transação sempre aprova duas transações anteriores, a

transação vazia aprovará a transação que estava parada, e também uma outra, dentre as consideradas "melhores" a ser aprovadas. A transação vazia não envolve nenhuma transferência de *token*, e contribui para a segurança da rede.

O autor do *White Paper IOTA Tangle* [35] considera que a estratégia de aprovação das TIPs é o fator mais importante na construção da criptomoeda baseada em *Tangle*, uma vez que é lá que a maioria dos ataques estarão escondidos. O mesmo autor discute, em seu *White Paper*, possíveis cenários de ataques e os algoritmos de seleção das TIPs que os contornem.

4.3.4 Crescimento do Peso Acumulado

Em um regime de carga baixa, a transação, após aprovada várias vezes pelas transações subsequentes, terá seu peso acumulado crescendo de forma constante, em uma velocidade proporcional ao Peso médio de uma transação genérica da rede. Em carga alta, após um período de adaptação, onde o Peso acumulado cresce de forma lenta, a velocidade de crescimento desse Peso irá aumentar de forma similar ao regime de carga baixa. Esse período de adaptação é o tempo que a transação aguarda para ser aprovada pela maioria das TIPs atuais.

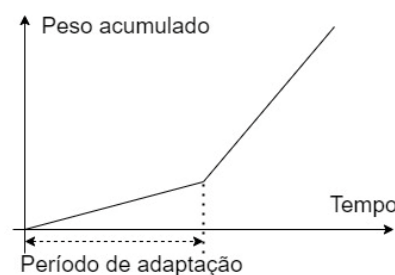


Figura 23 - Crescimento do Peso acumulado em carga alta [35].

4.4 Modelo da IoT

O ITU-T propôs, em 2012 [161], que o Modelo de Referência da IoT fosse construído com quatro camadas, envolvidas por recursos de segurança e de gerenciamento, conforme a Figura 24:

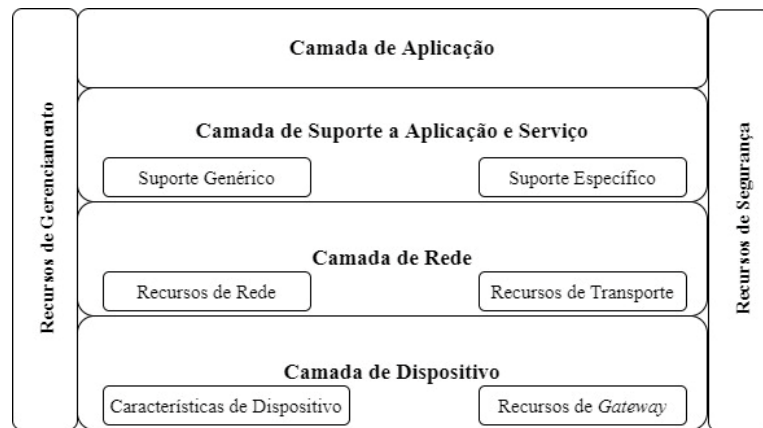


Figura 24 - Modelo de Referência da IoT [161].

- A camada de Aplicação é responsável pelos serviços oferecidos ao cliente.
- A camada de Suporte a Aplicação e Serviço consiste em suporte genérico e suporte específico. Suporte genérico é aquele em que os recursos de suporte são comuns que podem ser usados por diferentes aplicações de IoT, como processamento ou armazenamento de dados. Suporte específico é aquele que possui recursos particulares que atendem aos requisitos de aplicações específicas, eles podem consistir em vários grupos com recursos detalhados, a fim de fornecer diferentes funções de suporte.
- A camada de Rede é responsável por funções relevantes de controle de conectividade de rede, tais como funções de controle de recursos de acesso e transporte, gerenciamento de mobilidade ou autenticação, autorização e contabilidade, fornecimento de conectividade para o transporte do serviço IoT e informações de dados específicos da aplicação, bem como o transporte de informações de controle e gerenciamento relacionadas ao IoT.
- A camada de dispositivos envolve os recursos dos dispositivos, e pode ser dividida em recursos de dispositivos e recursos de *gateway*:
 - ✓ Recursos de dispositivos: Interação direta com a rede de comunicação, sendo os dispositivos capazes de coletar e fazer upload de informações diretamente, sem usar recursos do *gateway*, para a rede de comunicação e podendo receber diretamente informações (por exemplo, comandos) da rede de comunicação. Interação indireta com a rede de comunicação, onde os dispositivos são capazes de coletar e fazer o upload de informações para a rede de comunicação, através

de recursos do *gateway*. Rede *ad hoc* em que os dispositivos podem ser capazes de construir redes de forma *ad hoc* em alguns cenários que precisam de escalabilidade aumentada e implantação rápida. *Sleeping and waking-up* onde os recursos do dispositivo podem utilizar mecanismos de "dormir" e "acordar" para economizar energia;

- ✓ Recursos de *Gateway*: Suporte a várias interfaces, por exemplo, na camada de dispositivos, os recursos do *gateway* suportam dispositivos conectados através de diferentes tipos de tecnologias com ou sem fio, ZigBee, Bluetooth ou Wi-Fi e na camada de rede, os recursos do *gateway* podem se comunicar através de várias tecnologias, como rede telefônica comutada (PSTN), redes de terceira geração ou quarta geração (3G ou 4G), Ethernet ou assinante digital linhas (DSL). Conversão de protocolo, quando as comunicações na camada do dispositivo usam diferentes protocolos, por exemplo, protocolos de tecnologia ZigBee e protocolos de tecnologia Bluetooth e quando comunicações envolvendo camada de dispositivo e camada de rede usam protocolos diferentes, por exemplo, um protocolo de tecnologia ZigBee na camada de dispositivo e um protocolo de tecnologia 4G na camada de rede.

Os recursos de gerenciamento que permeiam as quatro camadas do modelo cobrem as classes tradicionais de falhas, configurações, contabilidade, desempenho e segurança, e são divididos em recursos genéricos e específicos:

- ✓ Recursos Genéricos de Gerenciamento: gerenciamento de dispositivos, como ativação e desativação remota de dispositivos, diagnóstico, atualização de firmware e/ou software, gerenciamento de status de funcionamento do dispositivo; gestão de topologia de rede local; gerenciamento de tráfego e congestionamento, como a detecção de condições de transbordamento de rede e a implementação de reserva de recursos para fluxos de dados críticos de tempo e/ou vida;
- ✓ Recursos Específicos de Gerenciamento: permitem o gerenciamento de requisitos específicos da aplicação, como por exemplo, monitoramento de energia em uma linha de transmissão.

Os recursos de segurança também podem ser divididos em genéricos e específicos:

- ✓ Recursos Genéricos de Segurança: não dependem da aplicação, e incluem na camada de aplicação: autorização, autenticação, confidencialidade e proteção de integridade dos dados da aplicação, proteção de privacidade, auditoria de segurança e antivírus. Na camada de rede incluem: autorização, autenticação, confidencialidade dos dados de uso e da sinalização e proteção da integridade de sinalização. Na camada do dispositivo: autenticação, autorização, validação da integridade do dispositivo, controle de acesso, confidencialidade de dados e proteção de integridade;
- ✓ Recursos Específicos de Segurança: associados aos requisitos específicos da aplicação, como por exemplo, uma aplicação de pagamento com mobilidade.

Zhang and Wen [162] propõem uma arquitetura de comércio eletrônico projetada especificamente para as mercadorias IoT, baseada no protocolo do Bitcoin. Foram utilizadas Corporações Autônomas Distribuídas (DAC - *Distributed Autonomous Corporation*) como a entidade de transação para lidar com os dados de dispositivos e propriedade inteligente negociados. Nesse modelo as pessoas podem negociar com DACs para obter mercadorias IoT, utilizando criptomoedas baseadas no protocolo da *Blockchain*. Para trocar os dados do dispositivo são usados chaves eletrônicas e contratos inteligentes. A Figura 25 ilustra:

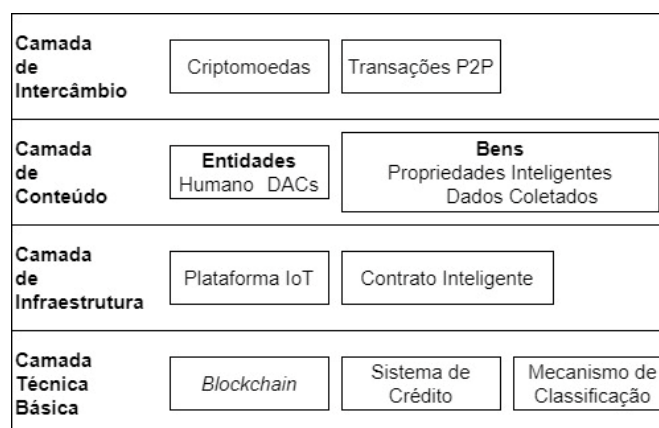


Figura 25 - Modelo de negócio IoT com Blockchain [162].

-
- A Camada Técnica Básica inclui o mecanismo de classificação das mercadorias, o algoritmo de crédito para efetuar o gerenciamento das carteiras, e a *Blockchain* do Bitcoin, que foi a criptomoeda escolhida pelo projeto citado.
 - A Camada de Infraestrutura contém a plataforma de serviço IoT e o contrato inteligente.
 - A Camada de Conteúdo envolve as entidades participantes e as mercadorias de IoT. Se a entidade for uma DAC, ela é executada automaticamente, sem a intervenção humana. Cada DAC pode comprar produtos de outras DACs, e todos podem emitir suas próprias mercadorias IoT. As mercadorias são propriedades inteligentes e dados coletados de sensores. As propriedades inteligentes podem ser obras de arte, bens duráveis (carros, casas), energia (eletricidade, água, gás, óleo), que podem ser controladas e quantificadas por dispositivos digitais com chaves eletrônicas ou sistemas de controle de acesso.
 - A Camada de Intercâmbio inclui o sistema de transações P2P que é o núcleo do modelo de negócios da IoT juntamente com a criptomoeda escolhida, que no caso é a Bitcoin.

4.5 Comparações entre *Blockchain* e *Tangle*

Uma comparação entre as tecnologias *Tangle* e *Blockchain* é interessante sob certos aspectos, mas existem diferenças significativas que fazem com que os usos das mesmas nem sempre sejam para os mesmos fins [163].

Na *Blockchain* todas as transações estão conectadas umas às outras por intermédio dos blocos. Dessa forma, com o aumento do número de usuários, a cadeia de blocos aumenta, e o sistema fica cada vez mais lento, e os nós mineradores passam a preferir as melhores transações para aprovar. As transações de baixo custo, que serão a maioria na IoT, são ignoradas pelos mineradores o tanto quanto possível, e quando são aprovadas, custam taxas significativas que desencorajam essas microtransações. Somente os mineradores podem criar o consenso distribuído para as transações, deixando assim a rede dependente dos nós mineradores. Obviamente, os mineradores preferem as transações melhores a serem aprovadas.

No *Tangle*, as transações são conectadas umas às outras por *edges*. Uma transação se conecta a somente duas outras anteriores. Quanto mais usuários houver no sistema, mais rápido o mesmo ficará. Devido à grande escalabilidade da rede, os usuários podem fazer uso da mesma sem se preocupar com a quantidade de máquinas. As chances de manipulação maliciosa da rede realmente são baixas. O *Tangle* aprova rapidamente as transações novas, funcionando mais rápido à medida que o número de transações novas cresce. Não há taxas de mineração, porque não há nós mineradores na rede. Todos os nós têm o mesmo poder. A Figura 26 mostra:

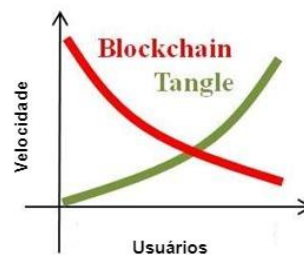


Figura 26 - Velocidade e número de usuários [164].

As características que ajudam o *Blockchain 2.0* (Ethereum) a atingir seus objetivos de atendimento a aplicações descentralizadas, são:

- A EVM (*Ethereum Virtual Machine*), um software completo de Turing que permite que qualquer serviço centralizado seja descentralizado sem ter que desenvolver uma *Blockchain* totalmente nova;
- O *Smart Contract*, que é o protocolo com as instruções contratuais e atua de forma autoexecutável;
- A DAO (*Decentralized Autonomous Organization*), toda uma organização escrita em um ou mais *Smart Contracts*, o que elimina a necessidade da interação humana;

As características que permitem que a *Tangle* (IOTA) seja voltada à IoT são:

- Não há nós mineradores, e as transações são aprovadas pelas transações subsequentes;
- A velocidade de aprovação da transação é bem mais rápida que em *Blockchain*;

- Não há taxas pelos serviços de rede, possibilitando as micro transações;
- Não necessita de quantidades massivas de energia, sendo mais eficiente.

Quanto aos esforços que as plataformas Ethereum e IOTA têm feito para melhorar o desempenho, nota-se que enquanto a Ethereum se preocupa em melhorar a escalabilidade e a eficiência energética, a IOTA ainda precisa alcançar o estágio final de sua proposta para ser utilizada amplamente por todos os setores. O foco da Ethereum é ter uma plataforma mais leve, rápida e segura. O estágio que se encontra agora é a versão *Metropolis*, que já passou pela etapa denominada Bizâncio, e está agora em uma etapa chamada *Constantinople* (na sequência virão as etapas *Istanbul* e *Muir Glacier*), que permitirá à plataforma:

- Um novo protocolo de consenso chamado *Casper*, que substituirá o algoritmo de PoW por uma combinação mais barata e eficiente de PoS e proteção contra falha *Byzantine* [165] (*Serenity*). Isso era esperado para 2018, mas deve acontecer agora em 2021. Atualmente está em testes (junho/julho de 2021) a atualização *London*, que ao ser implantada na rede principal irá gerar uma *hard fork*, e que trata da troca do algoritmo de PoW para PoS e também traz mudanças nas taxas de transação, que até então são negociadas com os mineradores em Gas, mas terão seus valores básicos estabelecidos (fixos) e o usuário que desejar acelerar a aprovação de sua transação poderá negociar uma espécie de 'gorjeta' com o minerador;
- Um processo denominado *Sharding*, que dividirá a *Blockchain* em pedaços menores, permitindo que os nós armazenem e computem apenas alguns desses blocos, ao invés de toda a *Blockchain*;
- outro processo chamado *Plasma*, que permite a criação de várias *Blockchains* separadas, mas interconectadas, que impedem que os nós tenham que confirmar e verificar cada transação individual.

A jornada da IOTA para estabelecer um "*Ledger of Things*" padronizado está apenas começando. 2017 foi gasto principalmente em pesquisa e criação da Fundação.

O ano de 2018 se concentrou no desenvolvimento e implementação dos resultados da pesquisa de 2017. Abaixo está o roteiro compartilhado por David Sønstebø [166]:

- Core Client Development: Java, C ++, Rust, Go;
- Módulos *IOTA eXtention Interface (IXI): Identidade de Coisas (IDoT), Permanodes, Rede Flash, Mensagens autenticadas com máscara (MAM), Transações privadas, Oracles;*
- Ferramentas e bibliotecas: JavaScript, Python, Java, Go;
- Projetos: Teste de estresse, estimulação pública, *Sandbox, Learn.*

Em uma tabela comparativa, pode-se relacionar as características do Bitcoin, Ethereum e IOTA, de forma a subsidiar a opção feita neste trabalho pela criptomoeda IOTA, para a monetização da horta compartilhada, conforme a Tabela 4:

Tabela 4 – Comparação entre Bitcoin, Ethereum e IOTA.

	Bitcoin	Ethereum	IOTA
Criptomoeda nativa	Bitcoin	Ether	IOTA Token
Aplicações descentralizadas	Muito limitada	Sim	Muito limitada
Taxa de transação	Sim	Sim	Não
Tipo de rede	Pública	Pública/Privada	Pública
Tipo de acesso	Sem permissão	Sem permissão	Permitido/Sem permissão
Contas anônimas	Sim	Sim	Sim/Não
Adequada para IoT	Não	Restrita	Sim
Adequada para DApps	Não	Sim	Não
Tecnologia de Registros	Blockchain 1.0	Blockchain 2.0	Tangle
Eficiência energética	Ruim	Baixa	Melhor
Assíncrona	Não	Não	Sim
Escalabilidade	Não	Em implantação	Sim
Velocidade de transação	Lenta	Média	Rápida
Dependência de ‘mineradores’	Sim	Sim	Não
Micropagamentos	Não	Caro	Sim
Linguagens compatíveis	C++	C++, Python, Go	Python, C, Java

O Tipo de Rede mostra que qualquer pessoa pode acessar a rede, caso seja pública. O Tipo de Acesso à rede também mostra se o acesso deve ser feito diretamente à rede,

ou se é necessário acessar primeiramente um nó de entrada para se acessar a rede. As Contas Anônimas mostram se o usuário pode ou não ser identificado na rede. A adequação à IoT mostra a possibilidade de se utilizar a cripto em transações financeiras entre objetos de IoT, assim com a adequação às DApps o fazem para aplicações distribuídas. Esta Tabela 4 demonstra que, comparativamente, a IOTA apresenta uma melhor adequação para o uso em IoT, tendo uma boa eficiência energética, o que facilita o uso de pequenos dispositivos alimentados por baterias e que ficam à distância, sendo altamente escalável, e não cobrando taxas de transações devido à comprovação de suas transações não ser feita por nós mineradores.

Para a horta compartilhada, os requisitos importantes da criptomoeda são a compatibilidade com os dispositivos de IoT (sensores, atuadores, etc.), a ausência de taxas de transação para possibilitar micropagamentos, a baixa latência de rede para rápida confirmação de transações, e a fácil integração da criptomoeda com os códigos de programação das funções da horta, em processadores de pequeno porte que possam estar instalados *in loco* com a horta, ou em um dispositivo do tipo *proxy*. A vantagem de se fazer a comprovação das transações em dispositivos *proxy* e não no próprio dispositivo de IoT é relacionada ao consumo de energia do dispositivo e ao seu poder computacional. Para se ter um poder computacional grande a ponto de fazer uma comprovação de transação de maneira rápida, o consumo de energia será maior, e os pequenos dispositivos de IoT geralmente não possuem alto poder computacional e nem energia disponível (se forem alimentados com baterias) para tanto. Portanto, o consumo energético também é importante de ser levado em consideração na escolha da criptomoeda a ser utilizada. Em suma, pesando todas estas necessidades para a associação da criptomoeda com o gerenciamento da horta compartilhada, a tecnologia que melhor se encaixa neste projeto é a IOTA/Tangle.

Capítulo 5 – EXPERIMENTOS E ANÁLISE

‘Uma única demonstração impressiona-me mais do que cinquenta fatos.’ (Denis Diderot)

*P*ara a comprovação da possibilidade de monetização de uma horta compartilhada e sua eficiência, um protótipo de horta foi desenvolvido, e um dispositivo de *hardware* do tipo *Raspberry Pi 3* é utilizado como base para rodar o software de gerenciamento das funções de controle de umidade do solo dos canteiros e de iluminação artificial. Todas as funções de controle da horta foram feitas mediante a existência de saldo, em IOTA, na carteira associada ao software de gerenciamento, estabelecido em linguagem *Python*. São descritos na sequência deste Capítulo os materiais e métodos utilizados, a construção do protótipo, os códigos e bibliotecas usados no software de gerenciamento, e os resultados são apresentados e discutidos.

5.1 Materiais e Métodos

5.1.1 Placa de *Hardware*

A placa *Raspberry Pi 3*, vista na Figura 27, é a base de *hardware* deste sistema, e deverá estar equipada com um cartão SD compatível, para armazenamento em massa. Para esta proposta, foi utilizado um cartão SD de 8 GB.



Figura 27 – *Raspberry Pi 3*. Fonte: raspberrypi.org

Ainda que a *Raspberry Pi* tenha um custo um pouco superior a um Arduíno, por exemplo, seu poder computacional é relativamente grande, rodando em frequências de *clock* elevadas (700 MHz ou mais), e utiliza um Sistema Operacional de propósito geral, tal como a distribuição Raspbian Linux. Em contrapartida, o uso de Sistema

Operacional genérico apresenta uma pequena latência, que impede o uso *'hard real time'*, o que, todavia, não chega a ser crítico no caso da proposta da horta compartilhada. Outra característica interessante da *Raspberry Pi* é a possibilidade de se utilizar linguagens de programação *open source*, e também a vastidão da comunidade mundial de desenvolvimento, que fornece suporte, bibliotecas e exemplos diversos.

Em apoio ao funcionamento da placa *Raspberry Pi* foi utilizado um monitor de vídeo, conectado à porta HDMI da placa, um *mouse*, conectado a uma das portas USB e um teclado USB. A alimentação do monitor de vídeo é feita diretamente na rede 110/220V, e a alimentação da placa *Raspberry Pi* necessita de uma fonte de 5 Vdc. A conexão da placa de *hardware* à rede, para monitoração da carteira IOTA é feita por conexão Wi-Fi.

A placa *Raspberry Pi 3* possui um barramento de 40 pinos GPIO (*General Purpose Input/Output*), para a comunicação de entrada e saída dos sinais digitais. Nestes pinos é possível ligar sensores de medidas distintas, acionar relés, motores, dentre outros. Estes pinos são distribuídos conforme mostra a Figura 28:

3,3V	1	⊠ ⊠	2	5V
GPIO02	3	⊠ ⊠	4	5V
GPIO03	5	⊠ ⊠	6	GND
GPIO04	7	⊠ ⊠	8	GPIO14
GND	9	⊠ ⊠	10	GPIO15
GPIO17	11	⊠ ⊠	12	GPIO18
GPIO27	13	⊠ ⊠	14	GND
GPIO22	15	⊠ ⊠	16	GPIO23
3,3V	17	⊠ ⊠	18	GPIO24
GPIO10	19	⊠ ⊠	20	GND
GPIO09	21	⊠ ⊠	22	GPIO25
GPIO11	23	⊠ ⊠	24	GPIO08
GND	25	⊠ ⊠	26	GPIO07
ID_SD	27	⊠ ⊠	28	ID_SC
GPIO05	29	⊠ ⊠	30	GND
GPIO06	31	⊠ ⊠	32	GPIO12
GPIO13	33	⊠ ⊠	34	GND
GPIO19	35	⊠ ⊠	36	GPIO16
GPIO26	37	⊠ ⊠	38	GPIO20
GND	39	⊠ ⊠	40	GPIO21

Figura 28 – Pinagem do barramento da *Raspberry Pi 3B+*.

Por cores, tem-se:

- Vermelho: Pinos de alimentação de 5V;
- Laranja: Pinos de alimentação de 3,3V, que também podem ser conectados a outros pinos, usando resistor limitador de corrente;

- Preto: Aterramento (GND – *Ground*);
- Azul: Podem ser programados para interface I2C, que é um protocolo criado pela Philips para conexão entre periféricos de baixa velocidade. Usa um barramento de dois fios, um de dados e outro de *clock*, para comunicação *serial* entre circuitos integrados montados em uma mesma placa;
- Amarelo: Portas *serial*, que utilizam protocolo RS-232;
- Verde: São configuráveis como entrada ou saída, e servem para envio e recebimento de sinais digitais;
- Rosa: Além de entrada e saída de sinais digitais, podem também fazer comunicação *serial Full Duplex* síncrona, permitindo ao *Raspberry* comunicar com algum periférico externo de forma bidirecional, caso o protocolo seja implementado;
- Cinza: Portas de ID EEPROM (*Electrically Erasable Programmable Read Only Memory*). Memória que pode ser programada e apagada através de uma tensão elétrica interna ou externa.

5.1.2 Componentes Físicos

a. Sensores de Umidade

O protótipo utilizou sensores de umidade de solo convencionais, do tipo FC-28, que consiste em duas sondas em forma de hastes, que são usadas para medir o conteúdo volumétrico da água presente no solo. As duas sondas permitem que a corrente passe pelo solo e, em seguida, obtenha o valor da resistência para medir o valor da umidade. Quando houver mais água, o solo conduzirá mais eletricidade, o que significa que haverá menos resistência. Portanto, o nível de umidade será maior. O solo seco apresenta menor condução elétrica, e uma maior resistência se apresentará entre as pontas das sondas. A Figura 29 abaixo ilustra o sensor:

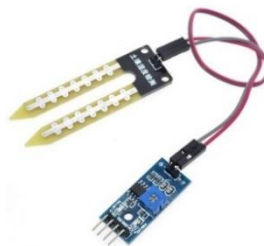


Figura 29 – Sensor de Umidade.

A saída do sensor pode ser analógica ou digital, sendo que um comparador de tensão com Amplificador Operacional LM393 é utilizado para a saída digital de dados, e um potenciômetro de ajuste de nível de referência pode ser regulado, conforme a figura 30 abaixo:

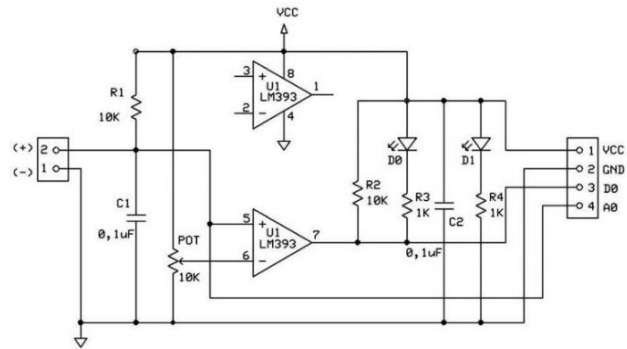


Figura 30 – Circuito comparador de Sensor de Umidade

b. Módulo Relé

O módulo relé utilizado para o acionamento da irrigação e da iluminação foi um módulo de um canal, alimentado com 5V, que suporta em seus contatos uma corrente de 10A em 250Vac, conforme a Figura 31:



Figura 31 – Módulo Relé.

O esquema elétrico do módulo relé está na Figura 32 abaixo:

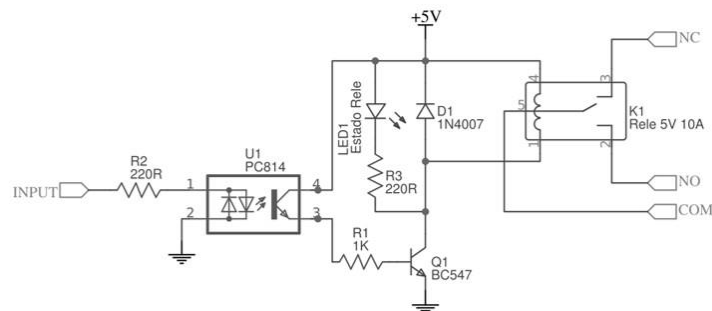


Figura 32 – Esquema elétrico do módulo relé. Fonte: tecnicas.com

c. Lâmpada de Espectro Solar

A iluminação artificial da horta foi feita com lâmpada que simula o mesmo espectro de iluminação da luz solar e permite a fotossíntese das plantas e seu crescimento, mesmo que a horta esteja em ambiente *indoor* e não receba a luz natural do dia. A Figura 33 ilustra:



Figura 33 – Lâmpada Full Spectrum.

A lâmpada foi alimentada com tensão da rede 110/220V, e tem soquete E27, adequado ao padrão nacional.

É importante que as lâmpadas de iluminação artificial sejam do tipo *Full Spectrum*, pois simulam melhor o espectro de luz solar. As plantas, quando em estado vegetativo, absorvem mais alguns espectros da luz ambiente (cores azuladas), que favorecem seu crescimento, e quando em estado de floração, outras frequências de luz são mais absorvidas pelas plantas, favorecendo a floração (cores avermelhadas). A própria luz solar que incide no globo terrestre fica mais azulada na primavera e avermelhada no outono, razão pela qual as plantas crescem mais na primavera e florescem/frutificam no outono. Naturalmente essa variação espectral depende da posição da terra em relação ao sol, da atmosfera, etc.

Theodore Engelmann foi um botânico e microbiólogo alemão do século XIX que em 1882 elaborou uma experiência com uma alga filamentosa, a *Spirogyra* e com bactérias aeróbias (utilizam o oxigênio na respiração). O objetivo era relacionar os comprimentos de onda da luz com a eficácia da fotossíntese [167]. Ele colocou numa lâmina a *Spirogyra* e água com bactérias. Cobriu a preparação com uma película transparente e fina, e verificou que as bactérias se encontravam uniformemente espalhadas em toda a preparação. Num microscópio tinha adaptado um prisma ótico que permitia a decomposição da luz branca. No final da experiência Engelmann verificou que

as bactérias se deslocaram para zonas onde incidiam as radiações vermelho-alaranjada e azul-violeta. (As bactérias deslocaram-se à procura de oxigênio fornecido pela *Spirogya* através da fotossíntese), conforme a Figura 34:

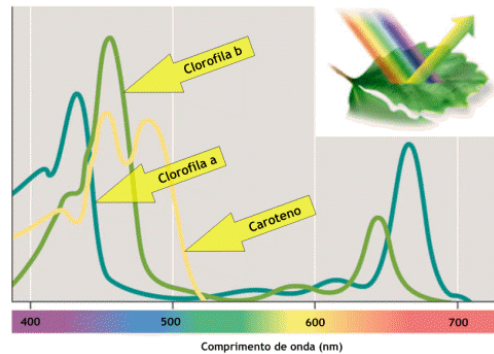


Figura 34 - Demonstração de Engelmann. Fonte:cientic.com

Pode ele concluir que estas radiações eram as mais absorvidas pelas plantas de cor verde, uma vez que a maiores taxas fotossintéticas correspondem as maiores taxas de absorção de radiação. As radiações com comprimentos de onda correspondentes à cor verde não são absorvidas, são refletidas, e por isso vemos a cor verde nas plantas.

d. Bomba e Tanque de Água

Para o protótipo optou-se pelo uso de água armazenada em tanque, em benefício da portabilidade do protótipo da horta, que poderá dessa forma ser deslocado para as demonstrações que se fizerem necessárias. O sistema de bomba e tanque utilizado foi o mesmo que se utiliza em limpadores de parabrisas de automóveis, sendo que a bomba funciona com uma tensão de 12 Vdc, e, portanto, foi necessária a utilização de uma fonte de 12 Vdc para essa alimentação. A Figura 35 abaixo mostra o conjunto bomba e tanque:



Figura 35 – Reservatório e bomba d'água.

e. Bicos de Gotejamento de Água

Dentre muitas possibilidades de irrigação optou-se pelo gotejamento de água vertical, sendo os bicos de distribuição da água instalados em cima dos canteiros da horta. Este sistema é bastante utilizado atualmente, por ser um sistema que pode ser controlado de forma automatizada e possibilitar uma grande economia de recursos hídricos. Ao se entregar a quantidade certa de água para as plantas, reduz-se a incidência de pragas e doenças e também o desenvolvimento de ervas daninhas nos canteiros. A Figura 36 ilustra:



Figura 36 – Bico de gotejamento.

Nesse tipo de bico de gotejamento a quantidade de água liberada pode ser manualmente regulada rosqueando-se a parte inferior do bico, vista na Figura 36 acima. Isto possibilita que, mesmo tendo diversos bicos acionados por uma mesma linha d'água, as quantidades de água liberadas por cada bico possam ser individualmente controladas, conforme a necessidade do canteiro irrigado.

f. Vasos e Terra dos Canteiros

O protótipo da horta, construído de forma a ser portátil, fez uso de vasos suspensos para a plantação, e pode ser alocado em qualquer ambiente interno ou externo, de acordo com a necessidade. Vasos retangulares de PVC, de 15 x 40 cm foram utilizados, conforme mostra a Figura 37:



Figura 37 – Vaso de PVC.

O substrato que preenche os vasos foi feito com uma mistura de terra vegetal (60%) e adubo orgânico (40%), que foram sobrepostos a uma manta de retenção e uma camada de pedras de argila expandida. A função da manta de retenção é segurar o substrato por cima da argila quando da irrigação, e as pedras de argila formam uma camada denominada ‘bica corrida’, onde a água em excesso correrá até um dreno no vaso, isolando as raízes das plantas do excesso de umidade e evitando apodrecimento. A Figura 38 abaixo ilustra as etapas de preparação de um vaso:



Figura 38 – Preparação do vaso. Fonte: *revistanatureza.com.br*.

5.1.3 Construção do Protótipo da Horta

O protótipo compõe o cenário de testes, onde as experiências são feitas e a comprovação necessária das questões propostas é observada, permitindo dessa forma que as discussões de funcionamento sejam estabelecidas e conclusões sejam tiradas. É, portanto, um meio de se obter a prova de conceito da proposição, sendo muito eficaz para ilustrar a ideia apresentada. E justamente no intuito de se ter uma ilustração esclarecedora das vantagens da monetização digital de uma horta compartilhada, optou-se pela construção de um cenário portátil, que pode ser transportado e demonstrado com facilidade. A única conexão física necessária para o funcionamento do protótipo é à rede elétrica, pois a conexão de Internet é Wi-Fi, e a água para irrigação é armazenada em um pequeno tanque agregado ao conjunto montado. A Figura 39 a seguir mostra as etapas de construção da maquete:

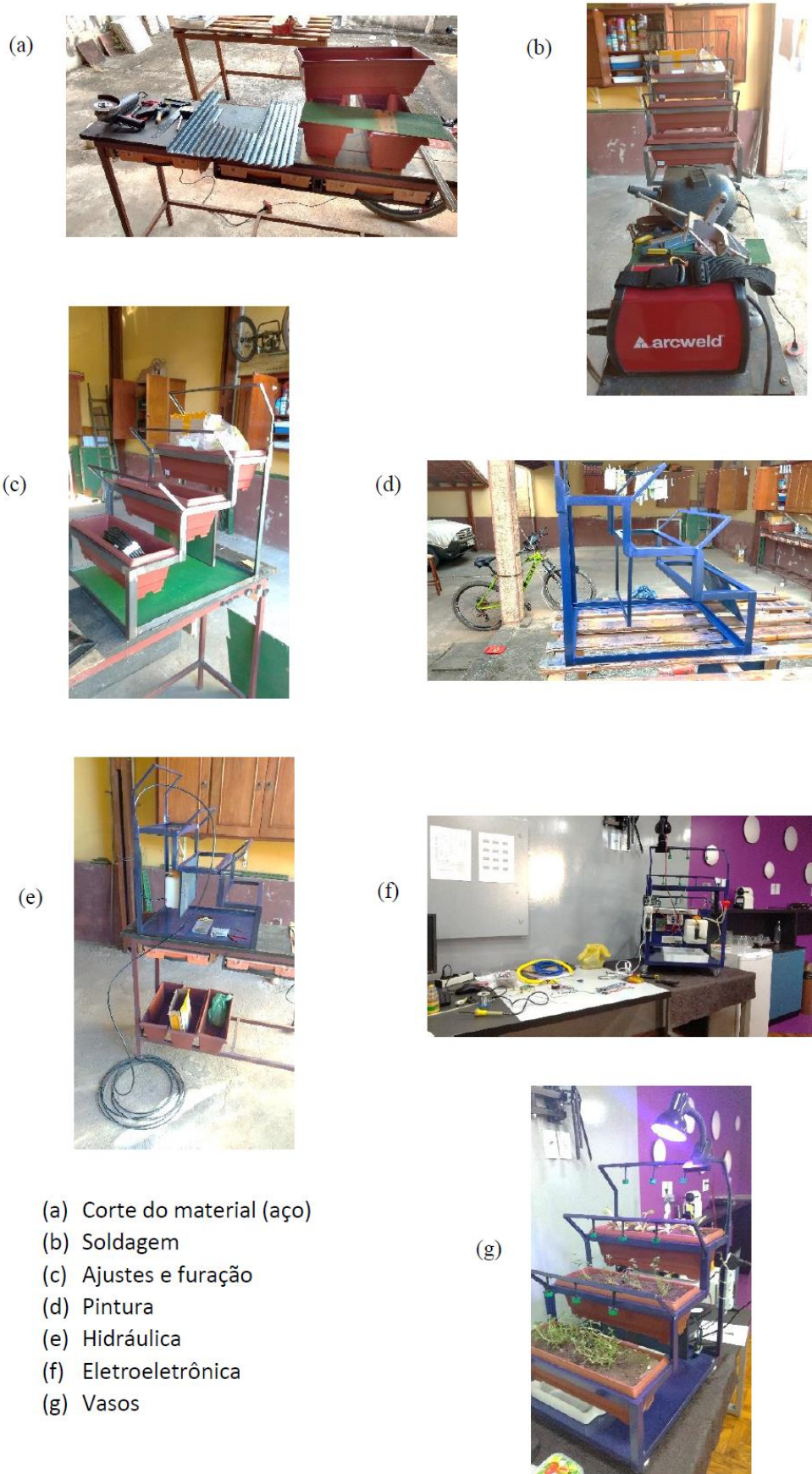


Figura 39 – Construção da Maquete da horta.

5.2 Montagens e Códigos

O sistema operacional utilizado é a distribuição Linux *Raspbian*, que é o SO oficial da Fundação *Raspberry*. As instruções de instalação estão detalhadas no *site* da Fundação [168]. A linguagem Python, a ser utilizada, já está pré-instalada no *Raspbian*. Para que se tenha acesso ao *Tangle* da IOTA, é necessário que se instale a biblioteca *API PyOTA*, que está disponível no GitHub [169].

Para os testes de desempenho do projeto, duas etapas foram executadas, conforme descrito nos itens 5.2.1 e 5.2.2 a seguir. Os resultados e discussões serão apresentados no item 5.3, na sequência.

5.2.1 Etapa 1 – Montagem Inicial para Testes de Latência

Em um primeiro momento havia a preocupação da latência de resposta da rede, do ponto de vista do usuário, ou seja, a partir do momento em que uma transação for inserida na rede, pela *Wallet* do usuário, em quanto tempo a carteira do recebedor irá acusar o recebimento. Para esta etapa de testes foi montado o seguinte *set* da Figura 40:



Figura 40 – Primeira etapa de testes.

Como o objetivo desta etapa era somente a verificação da latência do sistema, foi usada apenas uma lâmpada como carga, sem ainda se preocupar com a ativação de funções da horta propriamente dita. Na verdade, este sistema poderá acionar qualquer tipo de carga, desde que se utilize um *driver* de relé, uma vez que os pinos de saída do *Raspberry* possuem tensão de 5 [V] e baixa corrente. Para cargas pequenas, um simples *driver* poderá ser utilizado, conforme se vê na Figura 41:

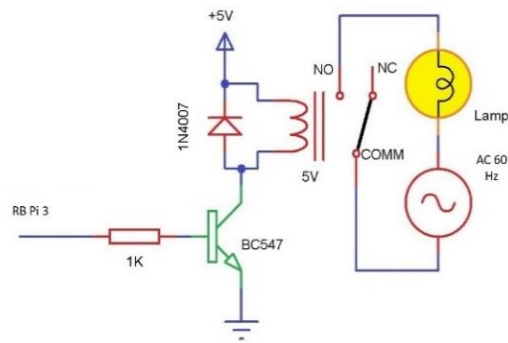


Figura 41 – Driver de Relé. A lâmpada simula a carga.

Antes de mostrar o Código utilizado para os testes, é necessário visualizar a sequência lógica de operação, conforme o fluxograma visto na Figura 42 a seguir:

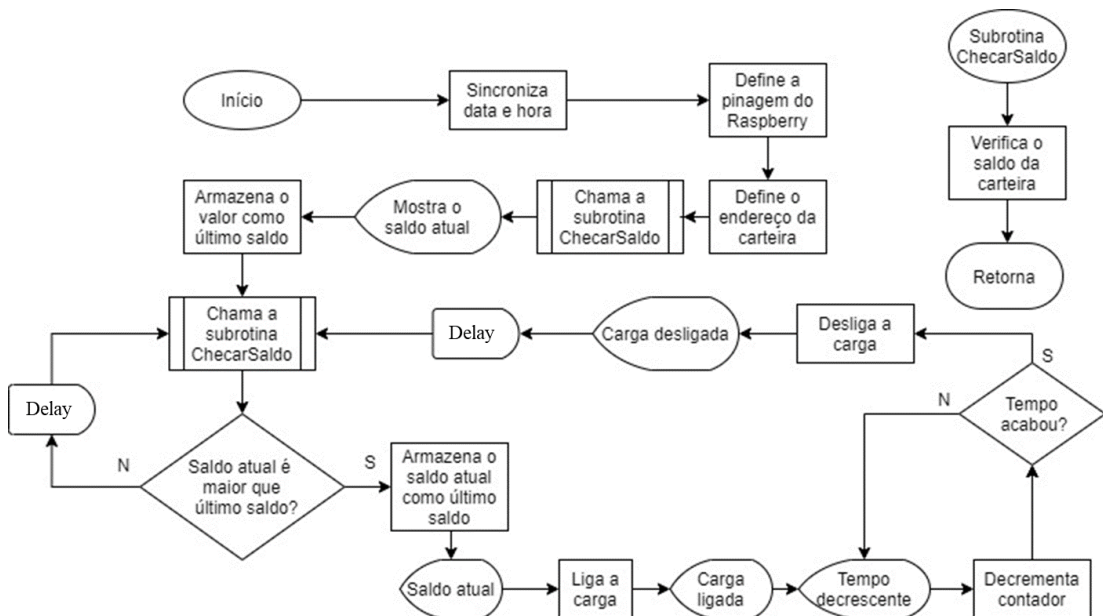


Figura 42 – Sequência lógica de funcionamento do acionador de cargas.

Diversos códigos Python relacionados a IOTA podem ser instalados e executados na *Raspberry Pi*. No próprio GitHub [170] há vários exemplos diferentes para se executar, mas nesse controle de horta inteligente o código utilizado foi o da Figura 43 abaixo:

```
# Importando algumas funções de data e hora do Python
import time
import datetime
# Importando a biblioteca GPIO
import RPi.GPIO as GPIO
```

```

# Importando a biblioteca PyOTA
from iota import Iota
from iota import Address
# Escolhendo os pinos O/I
LEDPIN = 18
GPIO.setmode(GPIO.BCM)
GPIO.setwarnings(False)
GPIO.setup(LEDPIN, GPIO.OUT)
GPIO.output(LEDPIN, GPIO.LOW)
# Função para verificar o balanço do endereço no tangle IOTA
def checarSaldo():
    print("Verificando se há novos fundos na
          carteira")
    saldoverificado =
        api.get_balances(address)
    balanço = saldoverificado['balances']
    return (balanço[0])
# URL para o nó completo IOTA usado ao verificar o saldo
iotaNode = 'https://nodes.thetangle.org:443'
# Criar um objeto IOTA
api = Iota(iotaNode, '')
# Endereço IOTA a ser verificado o balanço
# (Este endereço pode ser criado usando a carteira IOTA)
address =
[Address(b'KSNWNNLGLHIBVFMULCEXDQLXMGVKLACPPDNKSQYLBPPHISXGCNDZHEGCTQII9PRMRB9TXXBZ9BZTOSGW')]
#(obs.: Este endereço aqui utilizado é um endereço qualquer, mas deve-se usar o endereço da
carteria IOTA desejada)
# Obtendo o saldo atual do endereço na inicialização e usando como base para medir novos
fundos sendo adicionados
saldoatual = checarSaldo()
print('O saldo atual da carteira é', saldoatual, 'iotas')
ultimosaldo = saldoatual
# Definindo algumas variáveis
saldocarga = 0
contador = 0
statuscarga = False
# Loop principal executado a cada 1 segundo
while True:
    # Verificando se há novo saldo e adicionando ao saldo da carga quando encontrado
    if contador == 5:
        saldoatual = checarSaldo()
        if saldoatual > ultimosaldo:
            saldocarga = saldocarga +
            (saldoatual - ultimosaldo)
            print('Houve uma nova entrada
                  de:', saldoatual - ultimosaldo,
                  'iotas. O saldo atual
                  agora é de:', saldoatual,
                  'iotas')
            ultimosaldo = saldoatual
            contador = 0
        # Gerenciar o saldo e ligar/desligar a carga
        if saldocarga > 0:
            if statuscarga == False:
                print("Carga Ligada")
                GPIO.output(LEDPIN, GPIO.HIGH)
                statuscarga = True
            saldocarga = saldocarga - 1
        else:
            if statuscarga == True:
                print("Carga Desligada")
                GPIO.output(LEDPIN, GPIO.LOW)
                statuscarga = False
        # Mostrando o saldo remanescente
        print(datetime.timedelta(seconds=saldocarga))
        # Aumentar contador de verificação de saldo
        contador = contador + 1
        # Pausa de 1 segundo
        time.sleep(1)

```

Figura 43 – Código Python da Etapa 1.

5.2.2 Etapa 2 – Montagem Final com as Funções da Horta

A segunda etapa de testes de comprovação do conceito apresentado foi feita já utilizando a maquete desenvolvida e apresentada no item 5.1.3 anterior. As funções de irrigação do solo e iluminação artificial foram implementadas. A Figura 44 a seguir mostra o *set* desenvolvido:

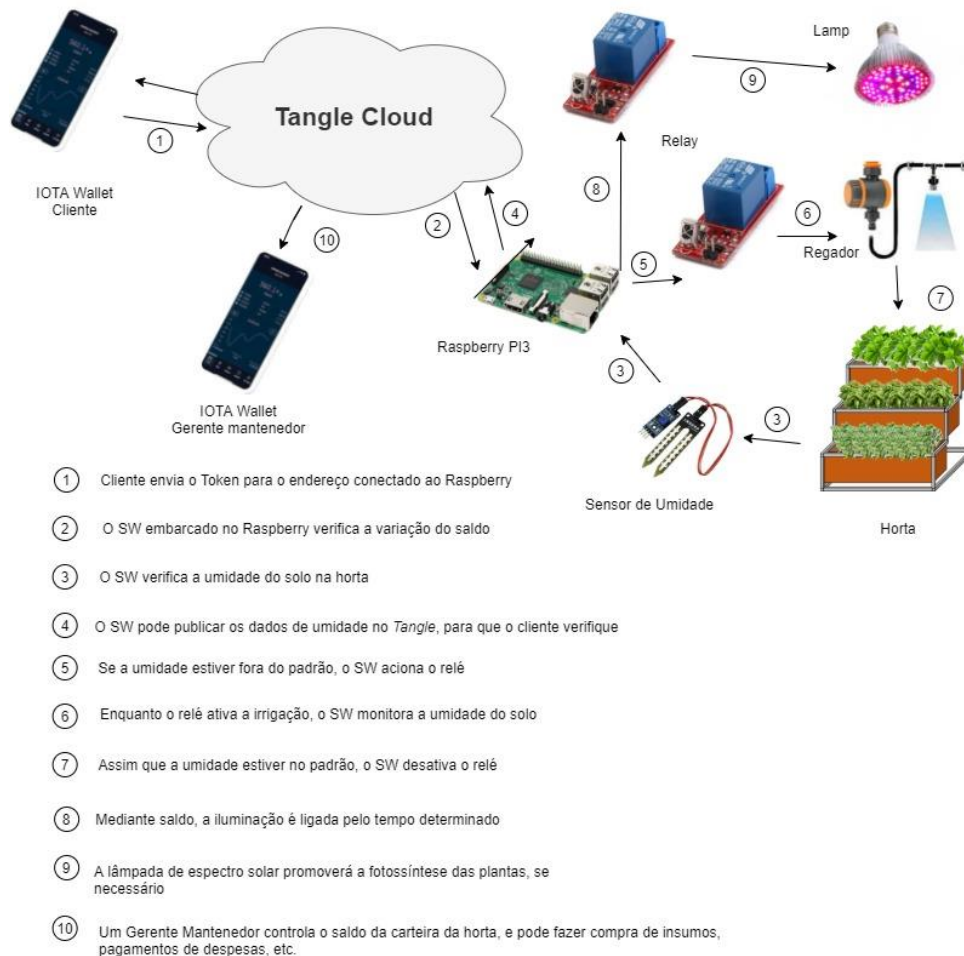


Figura 44 – Set de testes da horta compartilhada.

Para o desenvolvimento do código a sequência lógica de funcionamento mostrada no fluxograma da Figura 45 abaixo foi utilizada:


```

# Escolhendo os pinos O/I
SENSOR_1 = 21
SENSOR_2 = 20
SENSOR_3 = 16
GPIO.setmode(GPIO.BCM)
GPIO.setup(SENSOR_1, GPIO.IN)
GPIO.setup(SENSOR_2, GPIO.IN)
GPIO.setup(SENSOR_3, GPIO.IN)
RELE_LUZ = 18
GPIO.setmode(GPIO.BCM)
GPIO.setwarnings(False)
GPIO.setup(RELE_LUZ, GPIO.OUT)
GPIO.output(RELE_LUZ, GPIO.LOW)
RELE_AGUA = 24
GPIO.setmode(GPIO.BCM)
GPIO.setwarnings(False)
GPIO.setup(RELE_AGUA, GPIO.OUT)
GPIO.output(RELE_AGUA, GPIO.LOW)
# Entrar com a informação de tempo de iluminação artificial ligada:
TEMPO_LUZ = input("Quanto tempo (em segundos) a iluminação deverá ficar acesa?")
# Função de checar umidade do solo. True se tiver OK
def checarUmidade():
    if GPIO.input(SENSOR_1):
        print("Sensor de solo 1: seco")
        resultado_coleta_1 = "solo seco"
    else:
        print("Sensor de solo 1: úmido")
        resultado_coleta_1 = "solo umido"
    if GPIO.input(SENSOR_2):
        print("Sensor de solo 2: seco")
        resultado_coleta_2 = "solo seco"
    else:
        print("Sensor de solo 2: úmido")
        resultado_coleta_2 = "solo umido"
    if GPIO.input(SENSOR_3):
        print("Sensor de solo 3: seco")
        resultado_coleta_3 = "solo seco"
    else:
        print("Sensor de solo 3: úmido")
        resultado_coleta_3 = "solo umido"
    if GPIO.input(SENSOR_1) or GPIO.input(SENSOR_2) or GPIO.input(SENSOR_3):
        return False
    else:
        return True
# Função para verificar o balanço do endereço no tangle IOTA
def checarSaldo():
    print("Verificando se há novos fundos na carteira")
    saldoverificado = api.get_balances(address)
    balanço = saldoverificado['balances']
    return (balanço[0])
# URL para o nó completo IOTA usado ao verificar o saldo
iotaNode = 'https://nodes.thetangle.org:443'
# Criar um objeto IOTA
api = Iota(iotaNode, "")
# Endereço IOTA a ser verificado o balanço
# (Este endereço pode ser criado usando a carteira IOTA)
address =
Address('b'SZGSOHZTHSXHDKWXLWSWNMJX9WFHZQZIRXW9QIRKNSYFOZCEPYRANZGHFUOKYIMPBZYAOYS
BCGXZIHYYOLWN9PKAYQVA'])
# Obtendo o saldo atual do endereço na inicialização e usando como base para medir novos fundos sendo adicionados
saldoatual = checarSaldo()
print('O saldo atual da carteira é', saldoatual, 'iotas')
ultimosaldo = saldoatual
# Definindo algumas variáveis
saldocarga = 0
contador = 0
statuscarga = False
statusluz = False
auxiliar_luz = int(TEMPO_LUZ)
# Loop principal executado a cada 1 segundo
while True:
# Verificando se há novo saldo e adicionando ao lightbalance quando encontrado
    if contador == 5:
        saldoatual = checarSaldo()
        if saldoatual > ultimosaldo:

```

```

    saldocarga = saldocarga + (saldoatual - ultimosaldo)
    print('Houve uma nova entrada de:', saldoatual - ultimosaldo, 'iotas. O saldo atual agora é de:', saldoatual, 'iotas')
    ultimosaldo = saldoatual
    contador = 0
# Gerenciar o saldo e ligar/desligar a iluminação e irrigação
if saldocarga > 0:
#Controlar a iluminação artificial
    if auxiliar_luz > 0:
        if statusluz == False:
            print("Iluminação acesa")
            GPIO.output(RELE_LUZ, GPIO.HIGH)
            statusluz = True
            auxiliar_luz = auxiliar_luz - 1
        else:
            if statusluz == True:
                print("Iluminação apagada")
                GPIO.output(RELE_LUZ, GPIO.LOW)
                statusluz = False
#Controle da Irrigação:
    statuscarga = checarUmidade()
    if statuscarga == False:
        print("Irrigação Ligada")
        GPIO.output(RELE_AGUA, GPIO.HIGH)
        statuscarga = True
    else:
        print("Não é necessário irrigar")
        GPIO.output(RELE_AGUA, GPIO.LOW)
        statuscarga = False
    saldocarga = saldocarga - 1
    print("Tempo restante",timedelta(seconds=saldocarga))
    else:
        print("Favor colocar saldo na carteira para o funcionamento da horta")
        GPIO.output(RELE_LUZ, GPIO.LOW)
        statusluz = False
# Aumentar contador de verificação de saldo
    contador = contador + 1
# Pausa de 1 segundo
    time.sleep(1)

```

Figura 46 – Código utilizado no experimento da horta.

5.3 Resultados e Discussões

5.3.1 Etapa 1 – Testes de Latência Preliminares

É evidente que o tempo que a rede demora para aprovar e mostrar a transação na carteira de destino da transferência como saldo, é importante para a proposta deste artefato. Um *site*, denominado *tanglemonitor* [170], apresentava, em 2020 algumas métricas de desempenho, em tempo real, da rede *Tangle* ao redor do globo, e nele podiam ser escolhidos os endereços desejados para se monitorar o desempenho. A Figura 47 ilustra a montagem desta Etapa em funcionamento:



Figura 47 – Testes de latência.

Para o endereço utilizado, foram feitas 100 medições de tempo de confirmação de transação, em um período de dez dias, de 8 de janeiro a 17 de janeiro de 2020, em horários distintos, que podem ser vistas na Tabela 5 e no gráfico da Figura 48 a seguir:

Tabela 5 – Tempos de confirmação de transações, em janeiro/20

Número da medição	Dia 1 08/01/20	Dia 2 09/01/20	DIA 3 10/01/20	Dia 4 11/01/20	Dia 5 12/01/20	Dia 6 13/01/20	Dia 7 14/01/20	Dia 8 15/01/20	Dia 9 16/01/20	Dia 10 17/02/20
1	38,40	229,80	113,40	54,60	205,80	79,80	61,80	28,20	48,60	146,40
2	37,20	199,80	108,60	51,00	121,80	46,80	60,00	28,20	48,60	133,80
3	33,60	91,20	108,60	43,20	60,00	45,60	51,60	44,40	45,60	130,20
4	30,00	82,20	88,80	87,60	56,40	113,40	261,00	63,60	169,20	93,60
5	119,40	79,20	85,80	80,40	97,20	86,40	47,40	103,80	168,60	81,00
6	115,20	78,00	79,20	99,00	92,40	85,20	46,80	87,00	167,40	72,60
7	184,80	73,20	75,60	107,40	73,20	84,60	34,20	61,20	164,40	52,20
8	112,80	65,40	73,20	157,80	136,20	84,00	82,80	60,00	163,20	112,80
9	112,20	63,60	63,60	229,20	104,40	82,80	82,80	51,60	149,40	100,20
10	83,40	132,00	55,20	148,20	91,80	78,00	31,80	113,40	147,60	42,00
										(Medidas em Segundos)
Média	86,70	109,44	85,20	105,84	103,92	78,66	76,02	64,14	127,26	96,48
Desvio Padrão	51,28	59,15	19,84	58,02	43,71	19,72	67,28	29,21	55,48	35,04
Intervalo de Confiança	36,68	42,32	14,19	41,51	31,27	14,11	48,13	20,89	39,68	25,06
Máximo	123,38	151,76	99,39	147,35	135,19	92,77	124,15	85,03	166,94	121,54
Mínimo	50,02	67,12	71,01	64,33	72,65	64,55	27,89	43,25	87,58	71,42

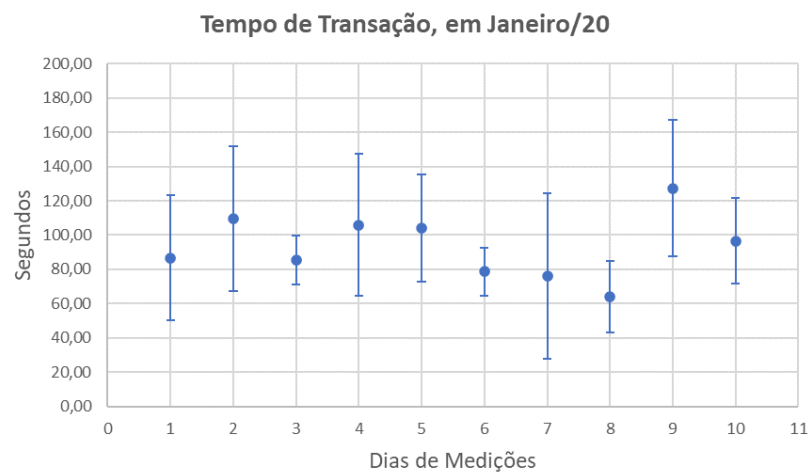


Figura 48 – Tempo de confirmação de transação em janeiro de 2020.

Vale lembrar que há um Nó coordenador da rede *Tangle*, que emite marcos de tempo (*milestones*) a cada minuto, aproximadamente, e as atualizações de *status* de aprovação ou não das transações são feitas por estes marcos de tempo, que atuam como um sincronismo de *status* da rede. Sendo assim, a atualização de saldo na carteira receptora ocorre na emissão do marco seguinte à aprovação da transação.

Todavia, em 12 de fevereiro de 2020 a Fundação IOTA informou que as transações na rede ficariam suspensas por um certo tempo, devido a ataques *hacker* que algumas carteiras de grande monta sofreram. Em alguns dias a rede voltou a operar normalmente, com as falhas corrigidas, porém, após isso, o *site tanglemonitor* parou de mostrar as métricas de desempenho anteriormente fornecidas, e dessa forma, as medidas aqui apresentadas servem como um registro histórico, feito antes do citado ataque [171].

5.3.2 Experimento da Horta e Análise de Desempenho

Na seção 5.3.1 foram feitos testes preliminares do tempo de confirmação de transação na rede. Estes testes ocorreram em janeiro de 2020, usando o *site tanglemonitor* para se medir os tempos. Agora, em 2021, novas medições de tempo foram tomadas, e apresentadas nesta seção. As medições foram feitas em duas etapas: a primeira em janeiro de 2021, com a carteira Trinity, e a segunda em julho de 2021, já com a carteira Firefly, que é a atualmente recomendada pela Fundação IOTA. Como agora o *site tanglemonitor* não mais apresenta as medidas de tempo de confirmação de transações, o monitoramento de tempo foi feito coletando-se o endereço de envio na carteira utilizada, e fazendo-se uma busca deste endereço no *site thetangle.org*. Aparecerão neste site as informações de horário de envio e de recebimento, o que permite a medição do tempo de confirmação da transação. A Figura 49 ilustra uma das transações feitas em julho de 2021, vendo-se os detalhes da transação na carteira Firefly, e sua confirmação no *tangle*, por intermédio do *site thetangle.org*. Os *prints* das telas foram feitos posteriormente, em setembro de 2021, o que demonstra a possibilidade de se verificar qualquer transação a qualquer tempo em que se necessite.

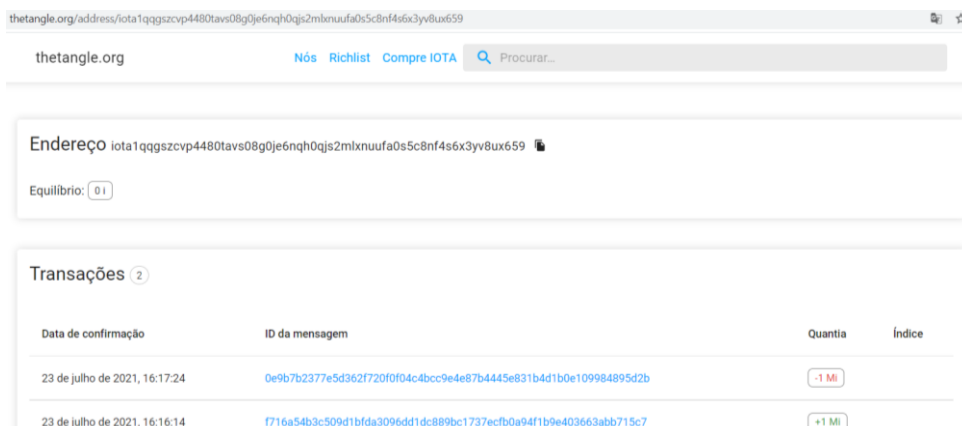
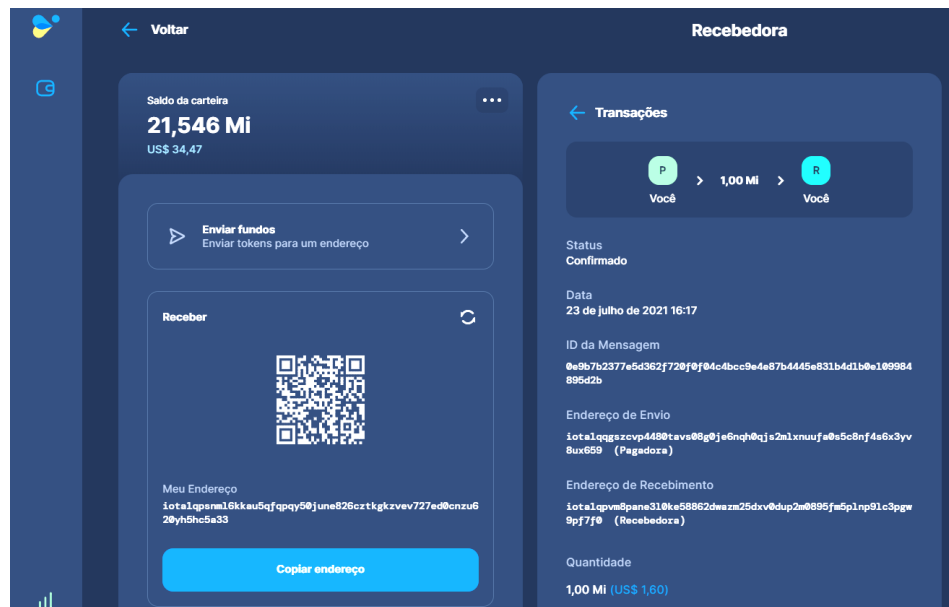
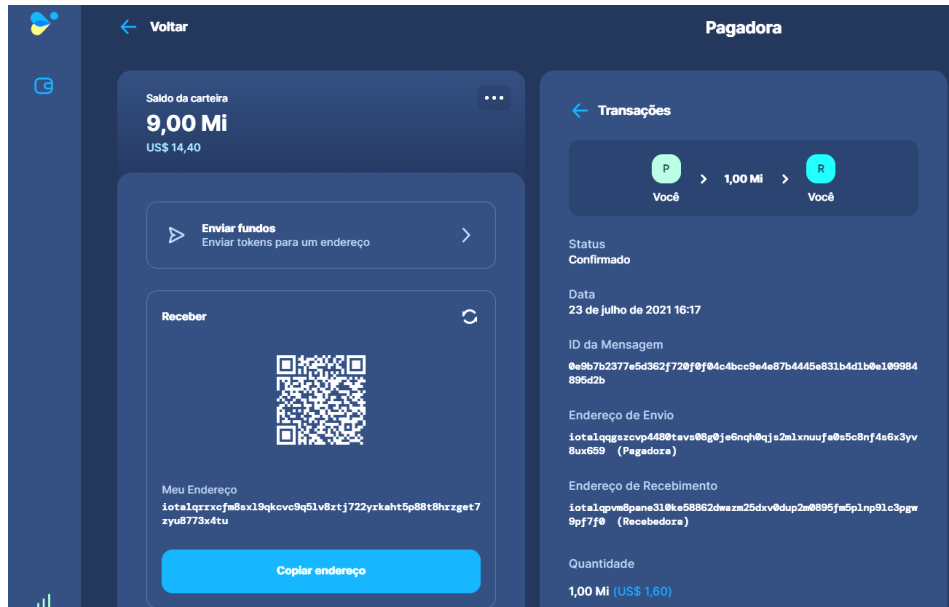


Figura 49 - Confirmação de transação na carteira e no site thetangle.org.

Também é possível monitorar e capturar a troca de pacotes em uma transação de transferência entre duas carteiras IOTA. Utilizando um aplicativo de análise de protocolo de rede, o Wireshark, é possível acompanhar a troca de pacotes na rede. Foram registrados 158 pacotes capturados durante uma transação de transferência de IOTA, desde o momento em que se iniciou a *Wallet Firefly* até o momento em que apareceu a mensagem de confirmação de recebimento na carteira receptora. A carteira receptora é a carteira associada à horta compartilhada, porém, para que se pudesse visualizar tanto os pacotes relativos à carteira pagadora, quanto os relativos à carteira receptora em uma mesma sequência de captura do Wireshark, e de forma a não perder a contagem de tempo, ambas as carteiras foram instaladas em uma única *Firefly*. Pode-se observar na Figura 50 a seguir que o pacote inicial, de número 104, ocorreu no instante 7,003443 [s], e o pacote final, de número 4331, ocorreu no instante 58,960563 [s]:

```
No.    Time      Source      Destination  Protocol Length Info
  104  7.003443  192.168.0.102  192.168.0.1  DNS      106    Standard query 0xb0c9 A iotaledger-files.s3.eu-central-1.amazonaws.com
Frame 104: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BEA6D778-99C5-493B-AD02-8F318AA29546}, id 0
Ethernet II, Src: IntelCor_8b:53:b2 (e4:70:b8:8b:53:b2), Dst: Tp-LinkT_d4:0d:3a (90:9a:4a:d4:0d:3a)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 92
  Identification: 0x0115 (277)
  Flags: 0x00
  Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0xb7c4 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.102
  Destination Address: 192.168.0.1
User Datagram Protocol, Src Port: 60608, Dst Port: 53
Domain Name System (query)
...

Frame 4331: 323 bytes on wire (2584 bits), 323 bytes captured (2584 bits) on interface \Device\NPF_{BEA6D778-99C5-493B-AD02-8F318AA29546}, id 0
Ethernet II, Src: IntelCor_8b:53:b2 (e4:70:b8:8b:53:b2), Dst: Tp-LinkT_d4:0d:3a (90:9a:4a:d4:0d:3a)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 157.90.246.211
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 309
  Identification: 0x178f (6031)
  Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x8cf7 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.102
  Destination Address: 157.90.246.211
Transmission Control Protocol, Src Port: 59670, Dst Port: 443, Seq: 1, Ack: 1, Len: 269
Transport Layer Security
```

Figura 50 - Pacotes Wireshark de uma transação IOTA

O código da Figura 46 inicialmente carrega a data e hora, determina a pinagem a ser utilizada do *Raspberry*, e carrega a biblioteca *PyOTA*. Uma função de verificação do saldo da carteira utilizada é implementada no código, e será utilizada para as consultas de saldo feitas enquanto o código estiver rodando. O endereço da carteira utilizada, que está explícito no código, é o endereço associado à horta, onde são feitos os recebimentos de criptomoeda. Naturalmente, o endereço pode ser alterado para qualquer endereço que se deseje monitorar. Ao se rodar o código, as diferenças de saldo positivas verificadas na carteira ativam a iluminação artificial e o loop de verificação de umidade e consequente irrigação, se necessário. A horta fica ligada por um tempo proporcional à quantidade de IOTA transferida (aqui a proporção utilizada é de um segundo para cada IOTA, o que pode ser alterado ajustando-se o código).

Um QR code pode ser associado ao endereço IOTA, facilitando as transferências feitas por outras carteiras instaladas em *smartphones*. Enquanto a carga estiver acionada, caso haja um novo acréscimo de saldo, o tempo de funcionamento da horta se estende proporcionalmente a este acréscimo. Ao se consumir a diferença de saldo, a horta se desativa, e o processo continua em um *loop* de verificação de saldo e acionamento e desligamento da horta. A Figura 51 mostra o experimento em funcionamento:



Figura 51 – Experimento em funcionamento.

Agora, em 2021, em que este trabalho comprova o funcionamento do projeto da horta, as medições de tempo de transação se tornam ainda mais importantes. Para as novas medições de latência foi utilizada a seguinte metodologia: duas carteiras IOTA foram criadas, ambas utilizando a *Wallet Trinity*, recomendada pela Fundação IOTA, em janeiro de 2021. Uma das carteiras foi associada à horta, para receber os pagamentos. A outra carteira seria um cliente qualquer da horta, que faz os pagamentos. Na *Wallet Trinity*, além do valor monetário transferido, é possível também associar mensagens de texto, onde o cliente pode se identificar e especificar o pagamento também. A carteira recebedora consegue ler essas informações. Outra informação interessante é que os tempos medidos se referem a toda a transação, de ponta a ponta, ou seja, do momento em que o cliente pressiona o ‘Enviar’ de sua carteira até o momento em que a carteira recebedora acusa o recebimento. É uma análise do ponto de vista dos usuários da rede. Foram feitas 100 medições de tempo de confirmação de transação, em um período de dez dias, de 12 de janeiro a 21 de janeiro de 2021, em horários distintos, que podem ser vistas na Tabela 6 e no gráfico da Figura 52 a seguir:

Tabela 6 - Tempo de confirmação de transações, em janeiro/21

Número da medição	Dia 1 12/01/20	Dia 2 13/01/20	DIA 3 14/01/20	Dia 4 15/01/20	Dia 5 16/01/20	Dia 6 17/01/20	Dia 7 18/01/20	Dia 8 19/01/20	Dia 9 20/01/20	Dia 10 21/02/20
1	192,00	83,40	74,40	83,40	80,40	83,40	146,40	87,00	129,60	182,40
2	91,80	79,20	126,00	76,20	84,60	129,60	155,40	132,60	87,00	135,00
3	189,00	120,60	85,80	89,40	88,20	84,60	124,80	87,60	136,20	84,60
4	183,00	79,80	85,20	80,40	122,40	69,00	90,60	93,00	141,60	82,20
5	75,60	122,40	90,00	133,80	86,40	81,00	126,60	123,00	145,20	81,60
6	78,00	147,00	128,40	76,20	87,60	120,60	91,80	122,40	202,20	78,60
7	79,80	74,40	82,80	74,40	94,20	77,40	124,20	127,20	255,00	125,40
8	80,40	81,60	74,40	88,80	74,40	124,80	81,60	148,20	123,00	126,00
9	121,80	123,00	88,20	76,20	94,20	81,00	199,20	198,00	126,60	136,20
10	94,80	127,80	81,00	82,80	129,00	85,80	82,20	126,00	136,20	87,60
									(Medidas em Segundos)	
Média	118,62	103,92	91,62	86,16	94,14	93,72	122,28	124,50	148,26	111,96
Desvio Padrão	49,72	26,65	19,46	17,56	17,71	22,18	37,74	33,01	46,97	34,51
Intervalo de Confiança	35,57	19,07	13,92	12,56	12,67	15,87	27,00	23,61	33,60	24,69
Máximo	154,19	122,99	105,54	98,72	106,81	109,59	149,28	148,11	181,86	136,65
Mínimo	83,05	84,85	77,70	73,60	81,47	77,85	95,28	100,89	114,66	87,27

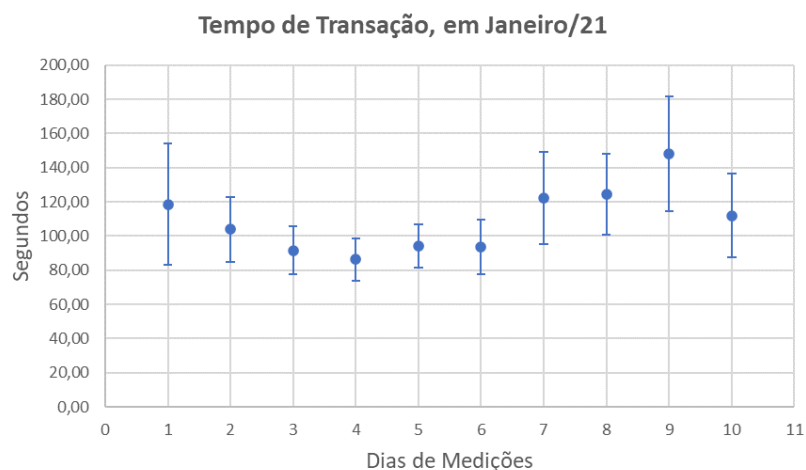


Figura 512 – Tempo de confirmação de transação, em janeiro de 2021.

Em abril de 2021 a Fundação IOTA começou a migrar a rede para a etapa denominada *Chrysalis*, e uma nova *wallet* foi lançada, em substituição à *Trinity*. Esta nova *wallet*, denominada *Firefly*, pelas medições vistas na Figura 52 abaixo, apresenta uma latência menor que a *Trinity*, deixando os tempos de transação mais curtos ainda, o que melhora o desempenho da solução no quesito latência. Novamente, foram feitas 100 medições de tempo de transação, no período de 21 a 30 de julho de 2021, sendo 10 medidas em cada dia, conforme pode ser visto na Tabela 7 e no gráfico da Figura 53 a seguir:

Tabela 7 - Tempo de confirmação de transações, em julho/21

Número da medição	Dia 1 21/07/21	Dia 2 22/07/21	DIA 3 23/07/21	Dia 4 24/07/21	Dia 5 25/07/21	Dia 6 26/07/21	Dia 7 27/07/21	Dia 8 28/07/21	Dia 9 29/07/21	Dia 10 30/07/21
1	38,50	52,20	37,80	36,50	38,60	40,60	38,40	39,70	11,80	13,30
2	41,70	46,30	22,90	36,90	38,80	44,90	43,20	43,00	11,90	42,10
3	37,20	41,60	38,40	15,30	36,70	40,30	20,80	42,80	62,90	42,20
4	47,30	34,40	36,50	44,80	37,90	8,10	11,70	42,90	23,90	41,10
5	35,80	17,00	35,30	18,00	36,40	20,80	11,90	40,60	11,40	38,20
6	38,30	18,30	31,00	40,30	34,70	42,80	39,50	46,10	13,90	35,80
7	31,00	34,20	31,00	9,40	31,30	38,90	12,50	33,50	12,20	42,70
8	46,00	36,50	37,70	35,00	39,00	36,40	14,80	39,10	34,00	41,00
9	35,60	38,60	32,80	42,00	41,50	36,30	43,50	41,90	39,90	12,70
10	41,10	36,00	33,70	32,10	36,90	39,00	10,70	40,40	37,60	37,30
	(Medidas em Segundos)									
Média	39,25	35,51	33,71	31,03	37,18	34,81	24,70	41,00	25,95	34,64
Desvio Padrão	4,93	10,98	4,68	12,30	2,76	11,44	14,50	3,33	17,35	11,63
Intervalo de Confiança	3,53	7,85	3,35	8,80	1,98	8,18	10,38	2,38	12,41	8,32
Máximo	42,78	43,36	37,06	39,83	39,16	42,99	35,08	43,38	38,36	42,96
Mínimo	35,72	27,66	30,36	22,23	35,20	26,63	14,32	38,62	13,54	26,32

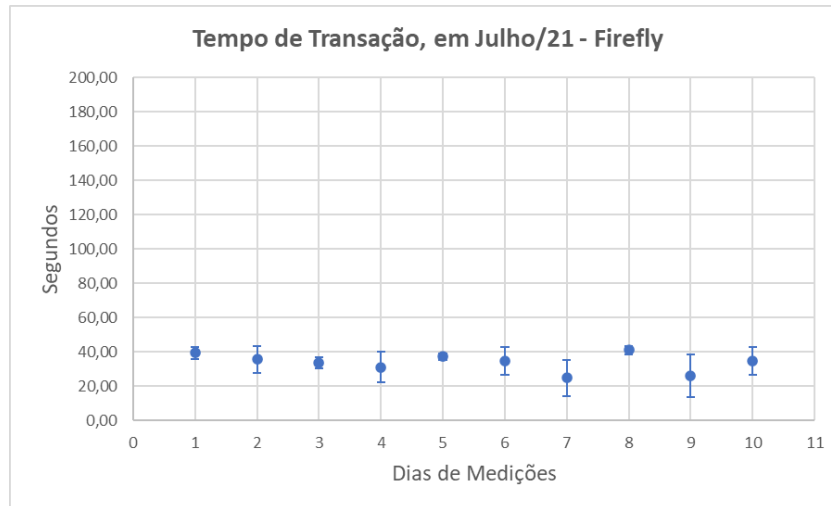


Figura 523 – Tempo de confirmação de transação, em julho de 2021.

Naturalmente, as medições de janeiro de 2020, da Figura 48 foram feitas com método distinto, e não devem ser comparadas com as duas outras, das Figuras 52 e 53. Mas, do ponto de vista dos usuários, estas últimas medições, de janeiro de 2021, com a *wallet Trinity*, e depois julho de 2021, com a nova *wallet Firefly*, são bem realistas, e trazem uma boa noção de como a aplicação dos usuários (no caso, a horta) vai demorar para reagir aos pagamentos recebidos.

Em teoria, o tempo de confirmação é de 2 milissegundos [172], mas as medições do próprio *Tangle*, conforme a Figura 53 acima, mostram que na prática isso ainda não acontece. Nos casos em que a transação demore muito tempo para ser confirmada, ocorre o que se descreveu no Capítulo 2 anterior, e a transação precisa ser recolocada ou referenciada explicitamente em outra transação (transação vazia). À medida em que mais transações ocorrem, mais rapidamente ocorrerão as confirmações, pois elas serão mais rapidamente confirmadas pelas transações subsequentes. A rigor, o limite de velocidade de confirmação de transação é tão somente o limite físico da rede. Com o crescimento da rede IOTA, existirão mais dispositivos, que acelerarão o processo de confirmação da transação, ficando a rede cada vez mais rápida.

Quanto ao controle de irrigação, as condições de umidade do solo da horta e o valor do saldo são monitorados, e a bomba de irrigação é ligada toda vez que a umidade do solo estiver abaixo do valor regulado no próprio comparador do sensor de umidade, e houver saldo suficiente na carteira da horta. Um mecanismo de irrigação eficiente deve analisar outras condições além da umidade do solo, o que ainda não está contemplado nesta implementação. Algumas soluções propostas na literatura

aplicando a lógica *fuzzy* consideram a temperatura do ambiente e a umidade do ar [173]. Outras condições também podem ser utilizadas, como luminosidade, volume acumulado de água usada na irrigação, etc.

A horta-tempero escolhida para este trabalho foi o orégano, a fim de ajustar o sistema para tomar decisões mais precisas. Todas as regras do sistema podem ser ajustadas de acordo com a variedade de hortaliças produzidas. O ambiente de cultivo se assemelha a um ambiente doméstico, ou seja, um ambiente interno com pouca ou nenhuma exposição ao sol. As plantas de orégano se ajustam melhor com solo úmido, consumindo cerca de 200 l/m² ao ano de água no cultivo. A temperatura do ambiente adequada pode variar de 4°C a 32°C, respondendo melhor a temperaturas entre 21°C e 25°C, e a umidade do ar ideal está entre 60% e 65%.

Outra condição particular desse trabalho que deve ser considerada é o valor do saldo. A horta será mantida com depósitos realizados pelas pessoas da comunidade. Por isso, o saldo também deve ser analisado no momento do controle da irrigação. Foi considerado que cada unidade do saldo corresponde a um segundo de funcionamento da bomba, que tem uma vazão de 20ml/s. Para o cenário proposto, existem três vasos com plantas de orégano de 0,375m², consumindo um total de 200 ml de água por dia. Dessa forma, seria necessário um saldo de cerca 70 IOTAs por semana para irrigar a horta (Em 14 de setembro de 2021 cada MIOTA – Milhão de IOTAs – estava custando US\$ 1,51).

O estado da horta será verificado a cada ciclo do código desenvolvido. Se houver saldo disponível, a iluminação será mantida ligada durante um intervalo previamente estabelecido, podendo totalizar 6, 8, ou mais horas de exposição à iluminação artificial. A iluminação não decrementa o saldo, mas não será acionada se o saldo for nulo. Em cada intervalo as condições serão verificadas e o sistema irá acionar a bomba para irrigar as plantas até que a umidade do solo chegue ao nível estabelecido. Durante dezenove dias, de 09 a 27 de abril de 2021, foi monitorada a condição de umidade do solo, nos três canteiros da horta, sempre com saldo disponível na carteira da horta. Para o orégano, o solo precisa estar bastante úmido, mas não encharcado (60% a 70%), segundo a EMBRAPA. A umidade do solo foi monitorada com o uso de um medidor de umidade do solo Minipa MV-331, conforme a Figura 54:



Figura 534 - Medidor de umidade do solo Minipa MV-331. Fonte: eletropartcomponentes.com.br.

Os resultados observados foram os da Figura 55:

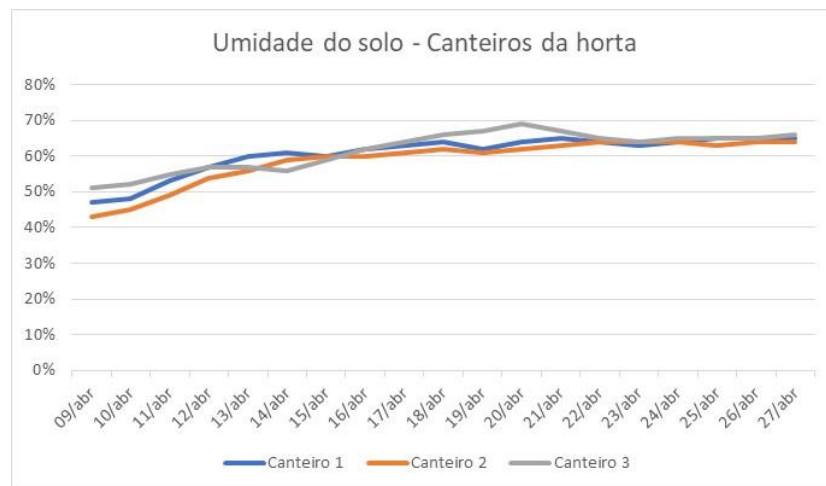


Figura 545 - Controle da Umidade do solo.

Estes resultados mostram que, desde que haja saldo na carteira associada à horta, a umidade do solo pode ser controlada e mantida dentro dos parâmetros considerados normais para a planta em questão, no caso, o orégano. Uma reserva de saldo pode ser estabelecida pelo gerente mantenedor da horta, para que, se houverem longos intervalos de entrada de novos valores na carteira da horta, o próprio gerente possa realizar essa transferência e dessa forma manter o nível de umidade do solo dentro dos valores necessários.

Capítulo 6 – CONCLUSÃO

Objetivo de provar conceitualmente a possibilidade de se monetizar uma horta

comunitária, utilizando a moeda digital IOTA, e a Internet das Coisas, gerando assim um caso de economia digital compartilhada, foi atingido com o desenvolvimento deste trabalho. Ficou estabelecido que a criptomoeda escolhida para a proposta, a IOTA, é bastante adequada aos micropagamentos envolvidos nas trocas financeiras da horta e de seus usuários, uma vez que, por não haver cobrança de taxas nas transações dessa criptomoeda em sua rede *Tangle*, esses micropagamentos não são inviabilizados pela própria rede, e até transações que não envolvem valores financeiros são incentivadas pela rede, pois quanto mais transações houverem mais rápida fica a rede, pois a comprovação das transações é feita pelas transações subsequentes. Também a latência da rede, do ponto de vista do receptor da transação, é bem baixa.

As implementações envolvidas nesta monografia foram: construir um protótipo de horta apropriado para o monitoramento da umidade do solo dos canteiros e da iluminação recebida pelas plantas para a fotossíntese, embarcar a solução em um *hardware* Raspberry Pi, de forma que o controle da umidade e da iluminação sejam feitos mediante a disponibilidade de saldo na carteira IOTA associada à horta; saldo esse sustentado pelas transferências feitas pelos clientes da horta; desenvolvendo assim uma aplicação utilizada para os testes e experimentações necessárias.

Como um trabalho futuro, seria uma sequência lógica realizar o experimento da horta utilizando o protocolo Ethereum, para uma comparação prática de tempos de confirmação, eficiência, custos e taxas, etc. Ainda que o protocolo Ethereum cobre taxas para as transações em sua *Blockchain*, há um grande esforço da Fundação Ethereum na redução dessas taxas, e até mesmo a eliminação futura dessas taxas, o que certamente o tornará interessante nas pequenas transações de IoT, tanto em hortas compartilhadas quanto em outras aplicações.

Outra sequência natural deste trabalho seria a inclusão dos princípios de Inteligência Artificial ao controle das funções da horta, aplicando a lógica *fuzzy* nas tomadas de decisões, também um interessante trabalho futuro. O uso dos princípios *fuzzy* trariam um controle mais eficiente na irrigação e iluminação artificial,

possibilitando maior eficiência, com custos reduzidos, melhor desenvolvimento das plantas e maior qualidade.

Outro trabalho futuro que deve ser realizado para a aplicação da horta em situações reais é o desenvolvimento da tela (*dashboard*) para o cliente da horta, na qual ele poderá controlar seus pagamentos, receber informações da horta, fotos, dados, etc. Esta *dashboard* poderá ser integrada à própria rede *tangle*, ou feita em uma aplicação independente. Mas sempre com acesso via *Internet*.

A horta comunitária faz uso da IoT e gera uma economia compartilhada, que traz diversos benefícios à comunidade e às pessoas envolvidas. Alimentos saudáveis e frescos, revitalização de espaços, integração da comunidade, rendimento e sustentabilidade para pessoas e grupos em situação de fragilidade socioeconômica e consequente aumento da qualidade de vida da comunidade, são alguns dos benefícios. A agricultura urbana e periurbana, proposta pela ONU como uma das alternativas de melhoria socioambientais para as comunidades carentes, alcança um patamar muito mais abrangente quando assistida pelas tecnologias modernas de informação e comunicação, melhorando a qualidade e a quantidade da produção, facilitando a distribuição e comercialização dos produtos

O presente trabalho concluí que a criptomoeda IOTA é uma solução interessante que permite a monetização das atividades e produtos de uma horta comunitária que integra IoT e outros ingredientes. A umidade do solo se mantém dentro dos parâmetros adequados ao tipo de hortaliça cultivada, e a iluminação artificial propicia o desenvolvimento das plantas no padrão adequado. Assim, este trabalho contribui no sentido de abrir a possibilidade do desenvolvimento de soluções comerciais para hortas comunitárias urbanas, periurbanas e até mesmo rurais, que sejam monetizadas com IOTA e estabeleçam um ambiente de economia compartilhada. A IOTA é bastante adequada ao ambiente da IoT, e permite que os objetos inteligentes se relacionem entre si, sem interferências externas e nem cobrança de taxas para as transações, o que é bastante interessante para uma prestação de um serviço de IoT ou até mesmo um compartilhamento de um bem. No caso específico da horta, o operador da horta fornece os produtos, e os clientes pagam proporcionalmente a seu consumo, criando a economia distribuída, ou descentralizada.

Referências Bibliográficas

- [1] Moore, G. E. **Cramming more components onto integrated circuits**. Electronics Magazine, volume 38, number 8, PP. 4-7. Abril 19, 1965.
- [2] Kurzweil R. **The Singularity is Near: When Humans Transcend Biology**. Viking Press, ISBN 0670033847. 2005
- [3] Atzori, L., Iera, A., & Morabito, G. **The internet of things: A survey**. Computer networks, 54(15), 2787-2805. 2010.
- [4] Clark, D. D., Wroclawski, J., Sollins, K. R., & Braden, R.. **Tussle in cyberspace: defining tomorrow's internet**. In ACM SIGCOMM Computer Communication Review (Vol. 32, No. 4, pp. 347-356). ACM. 2002.
- [5] UNDP. **Programa das Nações Unidas para o Desenvolvimento – Brasil**. Disponível em <<https://www.br.undp.org/>>, acesso em 08 de junho de 2021.
- [6] UNFPA. **Estado de la población mundial 2011: Liberar El potencial Del crecimiento urbano**. Fondo de Población de La Naciones Unidas. New York, USA, 2011. Disponível em: https://www.unfpa.org/sites/default/files/pub-pdf/SP-SWOP2011_Final.pdf. Acesso em junho de 2021.
- [7] Organização Cidades sem Fome. **Trabalho, renda e garantia de alimentação: Tudo começa com uma horta**. Disponível em: <<https://cidadessemfome.org/pt-br/>>, acesso em junho de 2021.
- [8] Secretaria Municipal do Meio Ambiente da Cidade do Rio de Janeiro. **Hortas Cariocas**. Disponível em: <https://www.rio.rj.gov.br/web/smac/hortas-cariocas>, acesso em junho de 2021.
- [9] Prefeitura de Jaraguá do Sul. **Projeto Germinar Implanta Novas Hortas Comunitárias**. Disponível em: <<https://www.jaraguadosul.sc.gov.br/news/projeto-germinar-implanta-novas-hortas-comunit-rias>>, acesso em junho de 2021.
- [10] Huckle, Steve, et al. **Internet das coisas, aplicativos de blockchain e economia compartilhada**. *Procedia computer science* 98: 461-466. 2016
- [11] Rabah, K.. **Digital Cryptoeconomics Powered by Digital Cryptocurrency**. Mara Research Journal of Computer Science & Security-ISSN 2518-8453, 1(1), 107-131. 2017.
- [12] Mullan, P. C. **E-gold. In The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations** (pp. 20-29). Palgrave Macmillan US. 2014
- [13] Trautman, L. J.. **Virtual Currencies; Bitcoin & What Now after Liberty Reserve**. Silk Road, and Mt. Gox. Richmond Journal of Law and Technology, 20(4). 2014
- [14] Wang, Y., & Mainwaring, S. D.. **Human-Currency Interaction: learning from virtual currency use in China**. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 25-28). ACM. 2008.
- [15] ATO. **China's virtual currency threatens the Yuan**. Asia Times Online. December 5, 2006.
- [16] Moore, T.. **The promise and perils of digital currencies**. IJCIP, 6(3-4), 147-149. 2013.
- [17] Barhum, R. M.. **Criptomoedas e a Regulação Estatal**. Trabalho de Conclusão de Curso de Direito. Intertem@s ISSN 1677-1281, 34(34). Centro Universitário Antônio Eufrásio de Toledo. Presidente Prudente 2018.
- [18] Nakamoto, S.. **Bitcoin: a peer-to-peer electronic cash system**. Disponível em: < <http://www.bitcoin.org/bitcoin>>. Pdf. (cited on pp. 15 and 87). 2008.
- [19] Grinberg, R.. **Bitcoin: An innovative alternative digital currency**. Hastings Sci. & Tech. LJ, 4, 159]. 2012.
- [20] RABAH, Kefa. **Criptoeconomia digital alimentada por criptomoeda digital**. Mara Research Journal of Computer Science and Information Security , v. 1, n. 1, pág. 107-131, 2016.
- [21] Dwyer, G. P.. **The economics of Bitcoin and similar private digital currencies**. Journal of Financial Stability, 17, 81-91. 2015.
-

-
- [22] COINMARKETCAP. **Cryptocurrency Market Capitalizations**. Disponível em: <<https://coinmarketcap.com>>. Acesso em: 1 Fev. 2021.
- [23] Kranenburg, R.V.; Caprio, D.; Anzelmo, E.; Dodson, S.; Bassi, A.; Ratto, M., **The Internet of Things**. 1ST Berlin Symposium on Internet na Society. October 2011.
- [24] Conoscenti, M., Vetro, A., & De Martin, J. C.. **Blockchain for the Internet of Things: A systematic literature review**. In Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of(pp. 1-6). IEEE. 2016.
- [25] Barhum, R. M.. **Criptomoedas e a Regulação Estatal**. Intertem@ s ISSN 1677-1281, 34(34). 2018.
- [26] Buterin, V.. **A next-generation smart contract and decentralized application plataform**. Whitepaper. 2014.
- [27] Mueller, P., Rizk, A., & Steinmetz, R.. **Blockchain a new foundation for building trustworthy and secure distributed applications (DAPP's) of the future**. Technische Universität Darmstadt. Frankfurt. 2017.
- [28] Wood, G. **Ethereum: A secure decentralised generalised transaction ledger**. Ethereum Project Yellow Paper, 151, 1-32. 2014.
- [29] Bradbury, D.. **Litecoin Founder Charles Lee on the Origins and Potential os the World´s Second Largest Cryptocurrency**. 2013. Disponível em <www.coindesk.com>, acesso em nov, 2020.
- [30] Percival, C.. **Stronger key derivation via sequential memory-hard functions**. Self-published, 1-16. 2009.
- [31] Silva, G. A. B., & Rodrigues, C. K. D. S.. **Mineração individual de bitcoins e litecoins no mundo**. In XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Workshop de Trabalhos de Iniciação Científica e de Graduação (SBSeg), Niterói, RJ, novembro (pp. 524-533). 2016.
- [32] Ali, M. S., Dolui, K., & Antonelli, F.. **IoT data privacy via blockchains and IPFS**. In Proceedings of the Seventh International Conference on the Internet of Things (p. 14). ACM. 2017.
- [33] Alves, P.. **O que é Monero**. Disponível em: <www.techtudo.com.br>, 2017. Acesso em maio, 2020.
- [34] Rolim, L.. **Dash: Entenda o que é e como funciona**. Disponível em: <www.atlasproj.com>, 2018. Acesso em maio, 2020.
- [35] Popov, S.. **The tangle**. Disponível em: <https://iota.org/IOTA_Whitepaper.pdf> [Popov, S., Saa, O., & Finardi, P. (2017). Equilibria in the Tangle. arXiv preprint arXiv:1712.05385. Acesso em junho de 2017.
- [36] Lucas, Y., **Tudo sobre IOTA: A Criptomoeda das Máquinas**. Disponível em: <www.medium/cibercultura>, em 02/18/2017. Acesso em maio 2020.
- [37] Divya, M., & Biradar, N. B.. IOTA-Next Generation Blockchain. International Journal of Engineering and Computer Science, 7(04), 23823-23826. 2018.
- [38] IoT Chain Whitepaper. **IoT Chain - A High-Security Lite IoT OS - ITC**, Disponível em: <https://iotchain.io/>. Acessado em 20 de fevereiro de 2021.
- [39] KLERKXA, L.; ROSEB, D. **Dealing with the game-changing technologies of Agriculture 4.0**. Global Food Security, v. 24, n.3, p. 1-7, Mar. 2020. DOI: 10.1016/j.gfs.2019.100347.
- [40] BOLFE, E.; MASSRUHÁ, S. **A transformação digital e a sustentabilidade agrícola**. Agroanalysis, v. 40, p. 32-34, mar. 2020.
- [41] NACÕES UNIDAS. **Objetivos de Desenvolvimento Sustentável**. 2015. Disponível em: <https://nacoesunidas.org/pos2015/>. Acesso em: 5 maio 2020.
- [42] UNITED NATIONS GLOBAL COMPACT - UNGC. **Digital agriculture**. 2017. <http://breakthrough.unglobalcompact.org/disruptive-technologies/digital-agriculture>. Acesso em: 19 maio 2020.
- [43] PINDERHUGHES, R. **Urban Futures: Planning for sustainable development in cities throughout the world**. Rowman & Littlefield Publishers: Maryland, USA, 2004.
-

-
- [44] FERNANDES, R. A.; SILVA, M.; COSTA, C. C.; SANTOS, D. P.; ARAÚJO, E. A.; MARTINS, J. M. A. **Projeto alimento verde: implantação de hortas urbanas em Pombal-PB**. Informativo técnico do Semiárido (INTESA), v. 3, N. 1, p. 07-10, 2010.
- [45] BOLFE, E. L. et al. **Desafios, tendências e oportunidades em agricultura digital no Brasil**. Embrapa Informática Agropecuária-Capítulo em livro científico (ALICE), 2020.
- [46] RIBEIRO, S. M. **Agricultura urbana agroecológica sob o olhar da promoção da saúde: a experiência do projeto colhendo sustentabilidade** – Embu das Artes - SP. Dissertação (Mestrado em Ciências) - USP, São Paulo (SP) 2013.
- [47] PINTO, R. **Hortas Urbanas: Espaços para o Desenvolvimento Sustentável de Braga**, Dissertação (mestrado em Engenharia Municipal). Departamento de Civil, Escola de Engenharia, Universidade do Minho, Braga, 2007.
- [48] FÁTIMA, M. **Estudos dos impactos ambientais da interação da rede de distribuição de energia elétrica coma arborização urbana nos municípios da região metropolitana do Recife**. Dissertação (Mestrado em Gestão e Políticas Ambientais) Universidade Federal de Pernambuco, Recife, Pernambuco, 2005.
- [49] FERNANDES, R.; SOUZA, N. R. P. G.; MARTINS JÚNIOR, J. **Benefícios da implantação do programa hortas comunitárias em Maringá-Paraná**. Brazilian Journal of surgery and clinical research - BJSCR, Maringá, V. 4, nº 1, p. 79-82, 2013.
- [50] VARENNES, A. **Produtividade dos Solos e Ambiente**. Escolar Editora: Lisboa, Portugal, 2003.
- [51] DINARDI, A. L.; FORMAGI, V. M.; CONEGLIAN, C. M. R.; BRITO, N. N.; SOBRINHO, G. D.; TONSO, S.; PELEGRINI, R. **Fitorremediação**. In: III FÓRUM DE ESTUDOS CONTÁBEIS, 2003, Rio Claro. Anais... Rio Claro: Faculdades Integradas Claretianas, 2003.
- [52] PINTO, R. F.; RAMOS, R. A. R. **Viabilidade ambiental de hortas urbanas: o caso de Braga, Portugal**. In: PLURIS, 3º CONGRESSO LUSO BRASILEIRO PARA O PLANEJAMENTO URBANO, REGIONAL, INTEGRADO E SUSTENTÁVEL, 2008., Santos. Anais... Santos: USP, UNESP, UFSCar, Universidade do Minho, 2008.
- [53] FRANCISCO NETO, J. **Manual de horticultura ecológica: guia de autossuficiência em pequenos espaços** - São Paulo: Nobel, 1995.
- [54] SOUZA, C. **Políticas públicas: uma revisão da literatura**. In.: Revista Sociologias, Porto Alegre, vol.16, p.20-45, jul. 2006.
- [55] FUNDAÇÃO MAGABEIRA, **Políticas públicas: elementos para organização do programa de governo**. In.: BACHIEGA, Carlos Alberto; SIQUEIRA, Carlos; PEREIRA, Marcelo Peron; BATISTA, Sinoel. São Paulo: Ed. Quanta, 2012, p. 58-63.
- [56] KERBAUY, M. T. M. **Descentralização, processos decisórios e Políticas Públicas locais**. In.: Revista Estudos de Sociologia, Araraquara, vol.16, p.151-163, 2004.
- [57] EMBRAPA. **Informática Agropecuária**. Disponível em: <<https://www.embrapa.br/informatica-agropecuaria/pesquisa-e-desenvolvimento>>, acesso em junho de 2021.
- [58] SOARES, J. F. **Os impactos da utilização da internet das coisas em fazendas e hortas urbanas**. 2020. Disponível em: <<http://www.riuni.unisul.br/handle/12345/10533>>, acesso em junho de 2021.
- [59] Kranenburg, R.V.; Caprio, D.; Anzelmo, E.; Dodson, S.; Bassi, A.; Ratto, M., **The Internet of Things**. 1ST Berlin Symposium on Internet na Society. October 2011.
- [60] Deidmar, G.L.C.; Lima, W.D.; Sobreira, D.S., **Internet das Coisas na Educação**. Revista Tecnologias em Projeção, v. 8, n. 2, ano 2017, p 67.
- [61] Sun, J., Yan, J., & Zhang, K. Z.. **Blockchain-based sharing services: What blockchain technology can contribute to smart cities**. Financial Innovation, 2(1), 26. 2016.
-

-
- [62] Amorin, C., **A Revolução Blockchain – Como essa tecnologia vai mudar os negócios, os governos e as pessoas**. Blockchain Research Institute, Disponível em: <www.blockchainresearchinstitute.org>, acesso em 04 de dez. 2020.
- [63] Oliveira, A. H., de Barros Neves, J., Rezende, T. T., & Teixeira, P. A.. **Aplicações de Automação em Iot–Internet Of Things**. Revista Científica e-Locução, 1(10). 2016.
- [64] Evans, D.. **Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo**. Cisco Internet Bussiness Solutions Group-IBSG, 11(1), 4-11. 2011.
- [65] Leal, R.L.V., **Whitepaper Blockchain e IoT – Aplicações e Iniciativas**. Disponível em: <www.cpqd.com.br>, Acesso em 20 de Abr. 2018.
- [66] Ahmed, A.H.; Omar, N.M.; Ibrahim, H.M., **Modern IoT Architectures Review: A Security Perspective**. 8th Annual International Conference on ICT: Big Data, Cloud and Security (ICT- BDCS 2017), 2017.
- [67] Kramer, J., **A Blockchain-Based Micro Economy Platform for Distributed Infrastructure Initiatives**. Master Thesis. Departament of Information and Computing Sciences, Utrecht University, 2017.
- [68] Alberti, A. M.. **A conceptual-driven survey on future internet requirements, technologies, and challenges**. Journal of the Brazilian Computer Society, 19(3), 291-311. 2013.
- [69] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S.. **Towards Blockchain-based Auditable Storage and Sharing of IoT Data**. In Proceedings of the 2017 on Cloud Computing Security Workshop (pp. 45-50). ACM. 2017.
- [70] Futere Internet PPP. **Future internet - public-private partnership**. Disponível em: <https://www.fi-ppp.eu/>. Acesso em 25 jan. 2021.
- [71] Alberto Serra, Antonio Pintus (CRS4), Nenad Gligoric (DNET). **User Environment**. Fórum Brasileiro de IoT. Slides de Suporte 1. Novembro/2015. Disponível em: <http://www.iotbrasil.com.br/new/wp-content/plugins/download-monitor/download.php?id=212>. Acesso em outubro 2019.
- [72] Wörner, D. and von Bomhard, T.. **When your sensor earns money: exchanging data for cash with bitcoin**. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, pages 295–298. ACM. 2014.
- [73] Vicente, R.J., **The Cryptocurrency as an Alternative Method for Making Financial Transactions**. Revista Maiêutica, Indaial, v. 2, n. 01, p 85-94, 2017. ISSN 2525-8397.
- [74] Dorri, A., Kanhere, S. S., & Jurdak, R.. **Blockchain in internet of things: challenges and solutions**. arXiv preprint arXiv:1608.05187. 2016.
- [75] Szabo, N.. **Smart contracts**. Unpublished manuscript. 1994.
- [76] Szabo, N.. **The idea of smart contracts**. Nick Szabo’s Papers and Concise Tutorials, 6. 1997.
- [77] De Filippi, P. and Mauro, R.. **Ethereum: the decentralized platform that might displace today’s institutions**. Internet Policy Review, 25. 2014.
- [78] DA SILVA RODRIGUES, Carlo Kleber. **Uma Análise Simples de Eficiência e Segurança da Tecnologia Blockchain**. Revista de Sistemas e Computação-RSC, v. 7, n. 2, 2017.
- [79] Barros, K.F.G., Santana, A.C., Martins, C.M., Campos, P.S.S.. **Valor da Água Virtual de Hortaliças Comercializada em Benevides – PA**. Revista Científica da Fundação Educacional de Ituverava – Nucleus, v. 15, n. 1, 2018.
- [80] Santos, O. L.; De Bone, A. C. C.; **REDES DE SENSORES APLICADAS À AGRICULTURA**. Revista Científica FAESA, v. 15, n. 2 Especial, p. 99-120, 2019.
- [81] CAMARGO, L.; CAMARGO, M.; CAMARGO, S.; **Smart irrigation-uma proposta para o uso eficiente da água em hortas escolares**. In: X Congreso de AgroInformática (CAI)-JAIIO 47 (CABA, 2018). 2018.
-

-
- [82] YANG, Feng et al. **A cloud-based digital farm management system for vegetable production process management and quality traceability**. Sustainability, v. 10, n. 11, p. 4007, 2018.
- [83] RIBEIRO, Maurício Santana. **Desenvolvimento de um sistema para rastreabilidade de hortaliças: inovação tecnológica aplicada à agricultura**. 2020. Universidade Federal do Tocantins, Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação, Palmas, 2020.
- [84] Silvano, W.F., Marcelino, R., Vigil, M.A.G., **Tecnologia Blockchain – IOTA Aplicada a Rastreabilidade de Produtos**. Revista Tecnologia e Sociedade, v. 17 n. 46, 2021.
- [85] NAKADA, Ryota; NGUYEN, Kien; SEKIYA, Hiroo. **Feasibility Study of Micropayment on IoT device**. IEICE Technical Report; IEICE Tech. Rep., v. 120, n. 258, p. 56-61, 2020.
- [86] ELSTS, Atis; MITSKAS, Efstathios; OIKONOMOU, George. **Distributed ledger technology and the internet of things: A feasibility study**. In: Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. 2018. p. 7-12.
- [87] YANG, Feng et al. **A cloud-based digital farm management system for vegetable production process management and quality traceability**. Sustainability, v. 10, n. 11, p. 4007, 2018.
- [88] WOLFERT, S.; GE, L.; VERDOUW, C.; BOGAARDT, M. J. **Big data in smart farming – a review**. Agricultural Systems, v. 153, p. 69-80, May 2017. DOI: 10.1016/j.agsy.2017.01.023.
- [89] Drone Mania. **Câmera Digital Multiespectral**. Disponível em:
<<https://lojadronemania.com.br/produto/camera-multiespectral-micasense-rededge/>>, acesso em 13 abr. 2021.
- [90] BARBEDO, J. G. A. **A review on the use of unmanned aerial vehicles and imaging sensors for monitoring and assessing plant stresses**. Drones, v. 3, n. 2, article 40, 2019a. DOI: 10.3390/drones3020040.
- [91] BOCK, C. H.; BARBEDO, J. G. A.; DEL PONTE, E. M.; BOHNENKAMP, D.; MAHLEIN, A.-K. **From visual estimates to fully automated sensor-based measurements of plant disease severity**. Phytopathology Research, v. 2, n. 9, Apr. 2020. DOI: 10.1186/s42483-020-00049-8.
- [92] BARBEDO, J. G. A. **Detection of nutrition deficiencies in plants using proximal images and machine learning: A review**. Computers and Electronics in Agriculture, v. 162, p. 482-492, July 2019b. DOI: 10.1016/j.compag.2019.04.035.
- [93] EMBRAPA. **Visão 2030: o futuro da agricultura brasileira**. Brasília, DF, 2018a. 212 p.
- [94] IRWIN, A. **Citizen science: a study of people, expertise and sustainable development**. London: Routledge, 2002. 216 p.
- [95] EMBRAPA. **Portfólios de P&D da Embrapa: desafios de inovação**. Brasília, DF: SPD/Ideare, 2019.
- [96] FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DE SÃO PAULO. **Rede de repositório de dados**. São Paulo, 2019. Disponível em: <http://agencia.fapesp.br/fapesp-lanca-rede-de-repositorios-de-dados-cientificos-do-estado-de-sao-paulo/32251/>. Acesso em: 09 Abr. 2021.
- [97] WILKINSON, Mark D. et al. **The FAIR Guiding Principles for scientific data management and stewardship**. Scientific data, v. 3, n. 1, p. 1-9, 2016
- [98] IBGE **Senso**. Disponível em: <<https://censos.ibge.gov.br/agro/2017/>>. Acesso em: 12 abril 2021.
- [99] BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL. **Internet das Coisas: um plano de ação para o Brasil**. Brasília, DF: BNDES; MCTIC: McKinsey/Fundação CPqD: Pereira Neto Macedo, 2017. 65 p. Disponível em: <https://www.bndes.gov.br/wps/portal/site/home/onde-atuamos/inovacao/internet-das-coisas>. Acesso em: 14 out. 2020.
- [100] CONECTARAGRO. **Agricultura 4.0**. Disponível em: <<https://conectaragro.com.br/>>. Acesso em: 12 abril 2021.
-

-
- [101] Senado Brasileiro. **Projeto de Lei nº 172 de 2020. Altera a Lei Geral de Telecomunicações e a Lei do Fust.** Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/140555>>. Acesso em: 12 abril 2021.
- [102] Governo Federal. **Decreto Presidencial nº 9.854 de 2019a. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara 4.0.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. Acesso em: 12 abril 2021.
- [103] Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC; Ministério da Agricultura, Pecuária e Abastecimento - MAPA. **Câmara Agro 4.0.** Disponível em: <<https://www.embrapa.br/busca-de-noticias/-/noticia/47656442/mapa-e-mctic-promovem-primeira-reuniao-da-camara-do-agro-40>>. Acesso em: 12 abril 2021.
- [104] Instituto de Pesquisa Econômica Aplicada, **Agenda 2030.** disponível em <<http://www.agenda2030.org.br/>>, acesso em 12 abril 2021.
- [105] BOLFE, E. **Application of geotechnologies in the development of sustainable agriculture in Brazil.** International Journal of Advanced Engineering Research and Science, v. 6, p. 458-463, 2019. DOI: 10.22161/ijaers.612.53.
- [106] EMBRAPA. **Portfólios de P&D da Embrapa: desafios de inovação.** Brasília, DF: SPD/Ideare, 2019.
- [107] EMBRAPA. **Rede AP.** 2018. Disponível em: <<https://www.embrapa.br/tema-automacao-e-agricultura-de-precisao>>. Acesso em: 13 abril 2021.
- [108] ONU News. **ONU prevê que cidades abriguem 70% da população mundial até 2050.** Disponível em: <<https://news.un.org/pt/story/2019/02/1660701>>. Acesso em 13 de abr. 2021.
- [109] Fundação Akatu. **Consumo Cosnciente.** Disponível em: <<https://akatu.org.br/>>. Acesso em junho de 2021.
- [110] Masson, S.. **O Impacto do Coronavírus no Agronegócio** – Disponível em: <<https://www.dinheirorural.com.br/o-impacto-do-coronavirus-no-agronegocio/>>. Acesso em junho de 2021.
- [111] EMBRAPA. **Visão 2030: o futuro da agricultura brasileira.** Brasília, DF, 2018. 212 p.
- [112] EMBRAPA TERRITORIAL. **Soluções tecnológicas.** Disponível em: <<https://www.embrapa.br/territorial/solucoes-tecnologicas>>. Acesso em: 13 abril 2021.
- [113] GHINI, R.; BETTIOL, W.; HAMADA, E. **Diseases in tropical and plantation crops as affected by climate changes: current knowledge and perspectives.** Plant Pathology, v. 60, p. 122-132, 2011.
- [114] Embrapa. **Catálogo Brasileiro de Hortaliças.** Disponível em: <https://www.embrapa.br/busca-de-publicacoes/-/publicacao/887213/catalogo-brasileiro-de-hortalicas-saiba-como-plantar-e-aproveitar-50-das-especies-mais-comercializadas-no-pais>, acesso em 14 abr. 2021.
- [115] CAMARGO FILHO, Waldemar Pires. CAMARGO, Felipe Pires. **Acomodação da produção olerícola no Brasil e em São Paulo, 1990- 2010 – análise prospectiva e tendências 2015.** IEA: São Paulo, 2015.
- [116] Back, Adam et al. **Hashcash-a denial of service counter-measure.** 2002.
- [117] NAKAMOTO, Satoshi; **BITCOIN, A peer-to-peer electronic cash system.** Bitcoin. Disponível em: <<https://bitcoin.org/bitcoin>>. pdf, v. 4, 2008.
- [118] FAÉ, J. P. **A ascensão das criptomoedas. consequências para o regime monetário internacional.** 2014. 26 f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Santa Catarina, Florianópolis, 2014.
- [119] Foxbit. **Quem é Satoshi Nakamoto.** Disponível em: <<https://foxbit.com.br/blog/quem-e-satoshi-nakamoto-veja-algumas-teorias/>>, acesso em 26 de março de 2021.
- [120] LANSKY, Jan. **Possible state approaches to cryptocurrencies.** Journal of Systems Integration, v. 9, n. 1, p. 19-31, 2018.
- [121] ULRICH, Fernando. **Bitcoin-a moeda na era digital.** Journal, volume, v. 2, p. 239, 1892. 2014.
-

-
- [122] HONORATO, Y. et al. **A criptomoeda Bitcoin: cooperação ou concorrente da moeda oficial dos países.** Trabalho apresentado ao VII Congresso Internacional de História, XXXV Encuentro de Geohistoria Regional, XX Semana de História da Universidade de Maringá, Maringá, 2015.
- [123] BARHUM, R. M., **Criptomoedas E A Regulação Estatal.** Interem@ s ISSN 1677-1281, v. 34, n. 34, 2017
- [124] Câmara dos Deputados **PL 2303/2015..** 2015. Disponível em:<http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1358969&filename=PL+2303/2015>. Acesso em: 10 ago. 2017.
- [125] Cointelegraph. **Resumo sobre a regulamentação de Bitcoin e criptomoedas no Brasil e no mundo.** Disponível em:< <https://cointelegraph.com.br/news/summary-of-bitcoin-and-cryptocurrency-regulations-in-brazil-and-worldwide> >. Acesso em: 29 mar. 2021.
- [126] EUROPEAN CENTRAL BANK. **Virtual currency schemes.** 2012. Disponível em:<<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>. Acesso em: 27. mar. 2021.
- [127] EUROPEAN CENTRAL BANK. **Virtual currency schemes – a further analysis.** 2015. Disponível em: <<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>>. Acesso em: 22. mar. 2021.
- [128] EUROPEAN CENTRAL BANK. **Opinion of the european central bank of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.** 2016. Disponível em:< <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016AB0049&from=EN>>. Acesso em: 29 mar. 2021.
- [129] Cointelegraph. **Ranking coloca Brasil como segundo país que mais possui investidores em criptomoedas,** disponível em <<https://cointelegraph.com.br/news/brazil-ranks-second-in-list-of-countries-with-more-crypto-investors>>, acesso em 29 mar. 2021.
- [130] Cointelegraph. **Resumo sobre a regulamentação de Bitcoin e criptomoedas no Brasil e no mundo.** Disponível em:< <https://cointelegraph.com.br/news/summary-of-bitcoin-and-cryptocurrency-regulations-in-brazil-and-worldwide> >. Acesso em: 29 mar. 2021.
- [131] Câmara dos Deputados. **Proposição de Lei 2196875.** Disponível em <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2196875>>, acesso em 30 mar. 2021.
- [132] Justiça em Foco. **Rueda toma posse.** Disponível em: <https://justicaemfoco.com.br/desc-noticia.php?id=135994&nome=rueda_toma_posse_como_presidente_da_comissao_especial_de_criptomoedas_e_blockchains_da_oab_nacional>, acesso em 30 mar. 2021.
- [133] Receita Federal. **Instrução Normativa 1888.** Disponível em: <<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>>, acesso em 30 mar. 2021.
- [134] Mello, L. F.. **Banco Central passa a contabilizar operações com criptomoedas na balança de pagamentos.** Disponível em: <<https://www.moneytimes.com.br/banco-central-passa-a-contabilizar-operacoes-com-criptomoedas-na-balanca-de-pagamentos/>>, acesso em 29 mar. 2021.
- [135] Blockinfo. **Especialista pede que Paulo Guedes instaure imediatamente sandbox sobre criptomoedas.** Disponível em: <<https://blockinfo.com.br/especialista-pede-que-paulo-guedes-instaure-imediatamente-sandbox-sobre-criptomoedas/>>, acesso em 30 mar. 2021.
- [136] Senado Federal. **Projeto de Lei 3825.** Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/137512>>, acesso em 30 mar. 2021.
-

-
- [137] Romano, R.. **Overview da Regulamentação dos Ativos Digitais no Brasil e no Mundo (2019-2020)**. Disponível em: <<https://rafaelaromano.jusbrasil.com.br/artigos/828490692/overview-da-regulamentacao-dos-ativos-digitais-no-brasil-e-no-mundo-2019-2020>>, acesso em 30 mar. 2021.
- [138] Purchio, L.. **As moedas virtuais ganham força e mercado**. Disponível em: <<https://veja.abril.com.br/economia/as-moedas-virtuais-ganham-forca-e-mercado/>>, acesso em 30 mar. 2021.
- [139] Cointelegraph. **Resumo sobre a regulamentação de Bitcoin e criptomoedas no Brasil e no mundo**. Disponível em: < <https://cointelegraph.com.br/news/summary-of-bitcoin-and-cryptocurrency-regulations-in-brazil-and-worldwide> >. Acesso em: 29 mar. 2021.
- [140] Bastiani, A.. **Presidente do Banco Central diz que Blockchain tem futuro brilhante**. Disponível em: <<https://www.criptofacil.com/presidente-do-banco-central-diz-que-blockchain-tem-futuro-brilhante/>>, acesso em 29 mar. 2021.
- [141] Câmara dos Deputados. **PL 2303/15**. Disponível em : <<https://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=11&nuSessao=1203/17>>, acesso em 29 mar. 2021.
- [142] Tecnoblog. **Facebook deve lancar criptomoeda Libra usando dólar como base**. Disponível em: <<https://tecnoblog.net/388938/facebook-deve-lancar-criptomoeda-libra-usando-dolar-como-base/>>, acesso em 01 abr. 2021.
- [143] Reis, T.. **Vale a pena investir em Bitcoin? Veja a opinião de grandes nomes do mercado**. Disponível em: <<https://www.sun0.com.br/artigos/vale-pena-investir-em-bitcoin-veja-opinio-de-grandes-nomes-do-mercado/>>, acesso em 01 abr. 2021.
- [144] Antonopoulos, A. M.. **The internet of money**. Merkle Bloom LLC. 2016.
- [145] EVANS, P. et al. **Thinking Outside the Blocks**. BCG Perspectives, 2016. Disponível em: <<https://www.bcg.com/blockchain/thinking-outside-the-blocks.html>>, acesso em 19 Abr. 2021.
- [146] PIRES, H. F. **Bitcoin: a moeda do ciberespaço**. Geosp – Espaço e Tempo (Online), v. 21, n. 2, p. 407-424, agosto. 2017. ISSN 2179-0892. Disponível em: < <http://www.revistas.usp.br/geosp/article/view/134538>. doi: 10.11606/issn.2179-0892. geosp.2017.134538. Acesso em janeiro 2021.
- [147] Jesus, E.F.; Chicarino, V.R.L.; Albuquerque, C.V.N.; Rocha, A.A.A., **A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack**. Hindawi Security and Communication Networks, Volume 2018, Article ID 9675050, 27 pages. <https://doi.org/10.1155/2018/9675050>, 2018.
- [148] Hankerson, D., Menezes, A. J., and Vanstone, S.. **Guide to elliptic curve cryptography**. Springer Science & Business Media. 2006.
- [149] Chitchyan, R., & Murkin, J.. **Review of Blockchain Technology and its Expectations: Case of the Energy Sector**. arXiv preprint arXiv:1803.03567. 2018.
- [150] Nelson, J., Ali, M., Shea, R., & Freedman, M. J.. **Extending existing blockchains with virtualchain**. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16),(Chicago, IL). 2016.
- [151] Chen, J..**Flowchain: A Distributed Ledger Designed for Peer-to-Peer IoT Networks and Real-time Data Transactions**. In Proceedings of the 2nd International Workshop on Linked Data and Distributed Ledgers (LDDL2). 2017.
- [152] Bjørnstad, M. V., Krogh, S., & Harketstad, J. G.. **A study on blockchain technology as a resource for competitive advantage** (Master's thesis, NTNU). Norwegian. 2017.
- [153] Contractnet **White Paper**. Disponível em: <<https://contractnet.com/documents/>>, acesso em 04 de set. 2019.
- [154] Subramanian, R. **The State of Cryptocurrencies**, Their Issues and Policy Interactions. v. 24, n. 3, p. 24–40, 2015.
-

-
- [155] BIRYUKOV, A.; PUSTOGAROV, I. **Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay BT** - Financial Cryptography and Data Security. (R. Böhme, T. Okamoto, Eds.)Berlin, Heidelberg: Springer Berlin Heidelberg, 2015.
- [156] Cruz, E. **Formas de Mineração e Diferenças entre PoW, PoS, PoC**. Disponível em <https://medium.com>, acesso em 05 de maio 2020.
- [157] Ferreira, F. L. **Blockchain e Ethereum Aplicações e Vulnerabilidades**. Universidade de São Paulo, 2017.
- [158] Lucas, Y. **Tudo Sobre Ethereum**. Disponível em: < <https://portaldobitcoin.uol.com.br/tudo-sobre-ethereum/>>, com acesso em 07/nov/2020.
- [159] Andersen, M. P., Kolb, J., Chen, K., Fierro, G., Culler, D. E., & Popa, R. A.. **WAVE: A decentralised authorization system for IoT via blockchain smart contracts**. Technical Report No. UCB/EECS-2017-234. Electrical Engineering and Computer Sciences University of California at Berkeley. 2017.
- [160] Hu, J. (2017). **IOTA Tangle**. Disponível em <https://medium.com>, acesso em 05 de Abr 2020.
- [161] Recommendation, Y. **«overview of internet of things»**. ITU-T, Geneva. 2012
- [162] Zhang, Y. and Wen, J.. **An iot electric business model based on the protocol of bitcoin**. In Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, pages 184–191. IEEE. 2015.
- [163] Han, R., Gramoli, V., & Xu, X.. **Evaluating Blockchains for IoT**. In New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on(pp. 1-5). IEEE. 2018.
- [164] Schueffel, P.. **Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph-A High-Level Overview and Comparison**. Haute école de gestion (HEG) de Fribourg 2017.
- [165] Clement, A., Wong, E. L., Alvisi, L., Dahlin, M., & Marchetti, M.. **Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults**. In NSDI (Vol. 9, pp. 153-168). 2009.
- [166] Sønstebø, D.. **The Transparency Compendium**. IOTA Blog. June, 16. 2017.
- [167] Vasco da Gama. **ALGUNS CONCEITOS PARA COMPREENDER A FOTOSSINTESE**. Disponível em: <<https://colegiovascodagama.pt/ciencias3c/decimo/unidade113a.html>>, acesso em junho de 2021.
- [168] Fundação Raspberry Pi. **Raspberry Pi 3**. Disponível em www.raspberrypi.org. Acesso em agosto de 2020.
- [169] Github – Iotaledger. **API PyOTA**. Disponível em <<https://github.com/iotaledger/iota.py/projects/1>>, acesso em agosto de 2020.
- [170] Github – Cyclux. **Tanglemonitor**. Disponível em <https://github.com/cyclux/tanglemonitor>, acesso em janeiro de 2020.
- [171] Brave New Coin. **A IOTA Foundation irá se recuperar após invasão à carteira?** Disponível em <<https://www.moneytimes.com.br/a-iota-foundation-ira-se-recuperar-apos-invasao-a-carteira/>>, acesso em março 2020.
- [172] IOTA Stack Exchange. Disponível em: <https://iota.stackexchange.com/>, acesso em fevereiro de 2020.
- [173] Alomar, B., & Alazzam, A., **A smart irrigation system using IoT and fuzzy logic controller**. In 2018 Fifth HCT Information Technology Trends (ITT) (pp. 175-179). IEEE. 2018.