

Universidade Paulista - UNIP

Guilherme de Albuquerque Grandmaison

Analise comparativa das tecnologias Blockchain e Tangle

Limeira

2017

Universidade Paulista - UNIP

Guilherme de Albuquerque Grandmaison

Análise comparativa de fluxo das tecnologias Blockchain e Tangle

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da computação sob a orientação dos professores Me. Prof. Antônio Mateus Locci, Me. Prof. Sandra Maria Crippa e Me. Prof. Sergio Eduardo Nunes.

Limeira

2017

Guilherme de Albuquerque Grandmaison

Análise comparativa de fluxo das tecnologias Blockchain e Tangle

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da Computação sob a orientação dos professores Me. Prof. Antônio Mateus Locci, Me. Prof. Sandra Maria Crippa e Me. Prof. Sergio Eduardo Nunes.

Aprovada em XX de XXXXX de 2017.

BANCA EXAMINADORA

Prof. Dr. Nome completo

Prof. Me. Nome completo

Prof. Esp. Nome completo

DEDICATÓRIA

Dedico este trabalho aos meus orientadores, amigos e pais.

“Sábio é aquele que conhece os limites da própria ignorância”.

Sócrates

RESUMO

A grande revolução monetária nos dias atuais é denominada por criptomoedas, apresentada pela primeira vez com o *Bitcoin*. A tecnologia por trás do *Bitcoin* é chamada de *blockchain*, é por meio dele que é possível executar uma operação totalmente virtual sem depender de um terceiro financeiro e além disso, garante proteção por intermédio da criptografia e consequentemente anonimato. Com o crescente uso desta moeda digital, problemas de atraso vem surgindo quando há uma enorme demanda de transações no sistema, resultando em horas ou até mesmo dias para que se concretizasse a operação, desta forma, demonstrando problemas de escalabilidade em seu fluxo. Tendo em vista esta dificuldade, o trabalho procura explicar o funcionamento do núcleo do *blockchain*, efetuar uma comparação analítica com uma evolução de seu sistema chamado *tangle* com a moeda *IOTA* e apresentar uma pesquisa atual comprovando o problema de escalabilidade, retirando os dados do próprio site do *blockchain*, onde é demonstrado todas as informações em tempo real das transações, blocos e até mesmo da rede. Esclarecendo a dúvida anteriormente podemos apontar que o *Bitcoin* necessita de alterações em seu código aperfeiçoando a sua movimentação de operações, assim como a *IOTA* desempenhou com a *Tangle*.

Palavra-Chave: *Backbone*; livro-razão.

ABSTRACT

First introduced with *Bitcoin* the great monetary revolution nowadays is denominated by cryptocurrency. The technology behind *Bitcoin* is called *blockchain*, it is through it that is possible to perform a totally virtual operation without relying on a financial third party and, furthermore, guarantees protection through encryption and therefore anonymity. With the increasing use of this digital currency, delay problems have arisen when there is a huge demand for transactions in the system, resulting in hours even days to accomplish an operation and thereby, demonstrating scalability problems in its flow. Given this difficulty, the paper seeks to explain the operation of the *blockchain* core, to make an analytical comparison with an evolution of its system called "*tangle*" with the *IOTA* currency and present a current research proving the problem of scalability removing the data from the site itself of the *blockchain*, where all the real-time information of transactions, blocks and even the network is demonstrated. To make it clear the previous doubt, we can point out that *Bitcoin* needs changes in its code to improve its operations movement, just as *IOTA* performed with the "*tangle*".

Key Words: general ledger

SUMÁRIO

INTRODUÇÃO	9
OBJETIVO	10
JUSTIFICATIVA.....	10
METODOLOGIA	11
1. CRIPTOMOEDAS.....	12
1.1 Bitcoin	13
1.2 Altcoins	14
2. BLOCKCHAIN.....	16
2.1 Informações do bloco	17
2.1.1 Cabeçalho do bloco.....	18
2.2 Hash	19
2.3 Timestamp	22
2.4.1 Algoritmo do proof of work.....	24
2.5 Arvore de merkle	26
2.6 Mineradores	28
3. IOTA	30
3.1 Gráfico acíclico direto (GAD)	30
4. Análise Comparativa	32
4.1 Escalabilidade	32
4.1.1 Análise de fluxo	33
5. CONCLUSÃO.....	38
6. REFERÊNCIAS BIBLIOGRÁFICAS	39

INTRODUÇÃO

Um dos maiores problemas no início das sociedades, era criar uma equivalência na troca de mercadorias, pois nos primórdios a “compra” de produtos era por meio apenas da troca, desta forma, não se existia um item que era valorizado globalmente. No decorrer do século VII a.C, os gregos criaram a primeira maneira de troca de mercadorias por um item específico, que seria a moeda cunhada. Conforme os séculos passaram uma nova maneira surgiu, transferindo a moeda cunhada, ao papel-moeda, que se fixou até os dias atuais.

Com a tecnologia evoluindo de maneira muito rápida nas últimas décadas, era inevitável a modernização do uso do dinheiro, assim surgir-se os cartões de crédito e os métodos de pagamento via internet, onde podemos usar o dinheiro de forma prática e rápida sem nos preocuparmos do modo que é feito.

No entanto, os bancos atualmente, monopolizam o mercado, de forma que estes ditam taxas, a ingressão de usuários, pedem dados pessoais, armazenam suas informações e utilizando ao favor deles. Até o fim do ano de 2008, não existia outra opção exceto os órgãos bancários, em relação ao uso do dinheiro com sua facilidade, através dos cartões de crédito e proteção ao poder aquisitivo com o depósito. Posteriormente, Satoshi Nakamoto, revolucionaria o sistema bancário, desenvolvendo um modelo que poderá substituir ao qual utilizamos atualmente.

Nakamoto, disponibilizou uma nova moeda de forma puramente eletrônica que se chamaria *Bitcoin*, onde qualquer pessoa poderia participar e não dependeria de nenhum órgão ou terceiro no uso da moeda. Ele criou o seu próprio sistema bancário, que é chamado de *blockchain*, este programa de computador, moderniza ainda mais o uso do dinheiro, garantindo anonimato através de criptografia e o total controle sobre o poder aquisitivo.

Com o passar dos anos, o *Bitcoin* começou a ganhar visibilidade e mais adeptos ao sistema, deste modo, ocorreu um aumento significativo de usuários executando inúmeras operações, logo, sucedeu uma grande demanda de transações na rede, em que o fluxo não suportava a enorme quantidade de transferências, resultando em horas ou até mesmo dias até que se confirmasse uma transação.

Posto isso, presenciamos os problemas de escalabilidade, demonstrando que a moeda ainda não tem a total capacidade de se tornar o dinheiro universal, entretanto, pessoas se basearam na tecnologia do *blockchain* e começaram a criar suas próprias versões do *Bitcoin*.

Por conseguinte, uma nova moeda chamada *IOTA*, propôs uma evolução ao sistema *blockchain*, chamado *Tangle*, resolvendo todos os problemas de escalabilidade e até mesmo de taxas.

OBJETIVO

O foco deste trabalho é explicar os processos que levam uma transação ser registrada nas criptomoedas *Bitcoin* e *IOTA*, com seus respectivos núcleos *blockchain* e *tangle*, após a compreensão de seus funcionamentos, será apresentado uma análise comparativa entre as tecnologias e suas escalabilidades de fluxo, desta forma, apontar suas diferenças e demonstrar os pontos em que elas se destacam, revelando a modernização da moeda *IOTA*.

JUSTIFICATIVA

Com a revolução iminente das criptomoedas no mercado, é inevitável não escutar em certo momento, alguém dizer *bitcoin* por meio de um noticiário, blog ou até mesmo na rua, assim, surge o questionamento, o que é isso? Como ela funciona? Isso é seguro? Desta forma, nasce os primeiros passos para um investidor em potencial.

O *Bitcoin* atua no mercado deis de 2009, e até os dias atuais ele vem crescendo de maneira irrefreável, tomando proporções inimagináveis se comparado ao seu início. Com sua influência de uso aumentando dia a dia, a nova tecnologia vem apresentando atrasos em transações onde anteriormente não se demonstrava de forma tão comum. Por meio desta dúvida, este trabalho visa compreender os processos que levam uma transação ser registrada no sistema *Bitcoin*, verificando se o problema está relacionado a sua escalabilidade de fluxo. Além disso, executar

uma comparação entre uma nova tecnologia da moeda *IOTA* lançada no ano de 2015 com sua evolução ao *blockchain* chamado *tangle*.

METODOLOGIA

Sumariamente a primeira etapa consiste em explicar os processos que fazem uma transação ser registrada e validada nas criptomoedas *Bitcoin* e *IOTA*, em seguida, comparar o funcionamento dos sistemas distribuídos *blockchain* da *Bitcoin* e *tangle* da *IOTA*. Após a compreensão dos núcleos que rodam por trás destas moedas, será apresentada uma pesquisa de escalabilidade da moeda *Bitcoin* com os dados da própria *blockchain*, adquiridos por meio do site do próprio sistema, onde ele demonstra informações de estatística do mercado, dos blocos, da rede e dos mineradores.

1. CRIPTOMOEDAS

A ideologia por trás das criptomoedas nasceu muito antes mesmo de ser lançado o plano real no Brasil em 1994, ela apareceu no fim da década de 80 com um movimento chamado *Cypherpunk*, fazendo um trocadilho ao *Cyberpunk* que nasceu no início daquela década, “*cypher* é uma referência a criptografia, e *Cyberpunk*, nome da subcultura *underground* aliada às tecnologias de informação e cibernética, conhecida também pela sua resistência ao “*establishment*” e ao “*mainstream.*”” (HAAS, 2013)

Este grupo tinha como foco devolver ao usuário o poder de liberdade em relação aos ambientes da internet, pois, até mesmo quando a rede era recente, já existiam agentes governamentais, institucionais ou até mesmo setores comerciais que analisavam seus tráfegos de dados, portanto, a liberdade já estava comprometida. (HAAS, 2013) Em 1993, foi publicado um manifesto do grupo *Cypherpunk* por Eric Hughes, que o primeiro parágrafo diz o seguinte:

A privacidade é necessária para termos uma sociedade aberta na era eletrônica. Privacidade não é o mesmo que segredo. Um assunto privado é uma coisa que alguém não quer que o mundo inteiro saiba; um assunto secreto é uma coisa que alguém não quer que ninguém saiba. A privacidade é o poder de revelar-se seletivamente para o mundo. (Hughes,1993).

A maneira encontrada pelos *cyphers* de garantir a privacidade das transições anônimas na internet, foi escrever códigos de criptografia que dificultavam o monitoramento via internet. John Gilmore diz o seguinte como integrante do grupo:

Nós libertamos a criptografia do controle governamental para um mundo livre em termos comerciais e de programação. Nós construímos uma criptografia forte o suficiente para contornar e mudar o regime dos Estados Unidos de tal forma que a criptografia hoje pode ser desenvolvida e implantada por qualquer pessoa do mundo. (SIRIUS, 2013, tradução por GUILHERME HAAS).

Fernando Collor de Mello, então presidente da república naquela época, tomou do povo brasileiro algo que não lhe pertencia, causando um mal generalizado que levaria ao seu *impeachment*.

Sexta-feira, 16 de março de 1990, feriado bancário. Um dia após tomar posse como o primeiro presidente eleito no país de forma direta após quase 30 anos, Fernando Collor de Mello anunciou um pacote radical de medidas econômicas, incluindo o confisco de depósitos bancários e das até então intocáveis cadernetas de poupança dos brasileiros. O plano, que poucos meses depois começou a fazer água e seria substituído pela sua segunda

versão, em fevereiro de 1991, foi considerado duro demais por empresários e até pelo ex-ministro Octávio Gouvêa de Bulhões. (VILLELA, 2015).

Com este poder, Collor simplesmente “tomou” o dinheiro de seus cidadãos para aplicar uma reforma financeira, ignorando o fato de que ele não era o dono daquele dinheiro. É através desta ocorrência histórica que podemos enxergar claramente que quando precisamos confiar em terceiros, como as instituições financeiras, para garantir segurança de nossos bens, *nós* integrantes do sistema bancário, não temos o total poder sobre aquilo que é de direito nosso.

Desta maneira, percebemos que o intuito das criptomoedas é possibilitar que nosso dinheiro continue sendo de seus respectivos donos, impossibilitando que alguém tome por meio de terceiros que detêm o poder bancário ou até mesmo político, garantindo sua segurança através da criptografia e anonimato.

1.1 Bitcoin

O *Bitcoin* foi desenvolvido por Satoshi Nakamoto, pseudônimo de um brilhante engenheiro da computação, tendo sua primeira aparição funcional com sua invenção em 03 de janeiro de 2009.

À PRIMEIRA VISTA, ENTENDER O QUE É BITCOIN não é uma tarefa fácil. A tecnologia é tão inovadora, abarca tantos conceitos de distintos campos do conhecimento humano – e, além disso, rompe inúmeros paradigmas – que explicar o fenômeno pode ser uma missão ingrata. (ULRICH, 2014, p. 15)

De maneira sucinta, podemos dizer que o *Bitcoin* é uma moeda digital, e apesar de seu sucesso estrondoso nos dias atuais, ela não foi a primeira moeda digital a ser apresentada. As primeiras moedas a serem inventadas foram o DigiCash e E-gold, porém, por que elas não obtiveram o mesmo sucesso que o *Bitcoin*? Acredita-se que por causa da tecnologia apresentada através do *white paper* de Satoshi, que solucionava o problema conhecido como “gasto duplo”, sem a necessidade de um terceiro para solucioná-la.

Resumidamente, “gasto duplo” é a tentativa de se utilizar o valor do dinheiro de uma transação duas vezes, Nakamoto cita nas primeiras páginas de sua publicação o que seria necessário para evitar esse tipo de falha nas moedas digitais:

Nós precisamos de uma forma de o recebedor saber que os donos anteriores não assinaram nenhuma nova transação. Para este propósito, a transação mais antiga é a transação que conta, então nós não nos

importamos sobre novas tentativas de gasto duplicado. A única forma de confirmar a validade de uma transação e estar ciente de todas as transações. Em um modelo baseado em emissor, o emissor está ciente de todas as transações e sabe qual delas chegou primeiro. Para atingir o objetivo sem um intermediário confiável, as transações precisam ser publicamente anunciadas, e nós precisamos de um sistema em que os participantes concordem em um único histórico da ordem em que elas foram recebidas. O recebedor precisa provar que no tempo de cada transação, a maioria dos nós concordou que ele foi o primeiro a receber. (NAKAMOTO, 2008, p. 2)

Em outras palavras, Satoshi diz que é necessário criar um consenso de todos os integrantes que realizam as transações através do livro-razão¹, que quando um dos participantes sinaliza aquela transação até que seja confirmada, ela ignora as possíveis tentativas seguintes se aquela operação foi contabilizada pela maioria dos integrantes da rede.

1.2 Altcoins

Assim como o projeto de Satoshi Nakamoto era dar a liberdade de se realizar transações via web sem depender da utilização de um terceiro, ele disponibilizou para todos, as linhas de código de sua invenção.

Com o código aberto, era inevitável que surgisse outras criptomoedas, e tudo que se precisava era a curiosidade e a determinação de entendê-lo, podendo assim, criar sua própria derivação da moeda, portanto, todas as criptomoedas que vieram após o *Bitcoin* são chamadas de *altcoins*.

Como o *Bitcoin* é um sistema distribuído e não passa por nenhum órgão regulamentador, não há nenhuma pessoa por trás que dite mudanças ou atualizações no sistema, desta forma, apenas algumas pessoas sinalizadas pela comunidade poderiam escrever diretamente nos códigos da criptomoeda e implementar as *bips*. *Bips*² são um conjunto de sugestões apresentadas pela comunidade *bitcoin* para a melhoria do sistema, o nome *bip* pode variar em relação a criptomoeda. (ANTONOPOULOS, 2014, p. XVII).

Essas melhorias poderiam ser apresentadas por qualquer integrante da comunidade, o problema é que nem todas as *bips* apresentadas são adicionadas, então, sempre haverá uma pessoa ou grupo que discordam ou aceitam implementar

¹ “Lista de todos os registros das transações realizadas por uma empresa ou companhia”.

² “*Bitcoin Improvement Proposals*. A set of proposals that members of the *Bitcoin* community have submitted to improve *bitcoin*.”

certas mudanças ao sistema, conseqüentemente, elas podem se derivar do código aberto de Satoshi e criar sua própria criptomoeda, com suas próprias visões de melhoria.

Hoje já existe mais de mil criptomoedas de acordo com o site *Coin Market Cap*³, todas procuram criar sua própria identidade, por exemplo, a Litecoin e Ripple, foram criadas para terem transações mais rápidas e baratas; a moeda Monero procura embaralhar transações e evitar rastreamento; a Gridcoin usa sua parte de computação dos *nós* para manter o *blockchain*, enquanto a maior parte é usada para projetos científicos, que não têm verba para usar supercomputadores; e a *IOTA* que usa uma nova geração de *blockchain* que é mais leve e requer menos poder computacional (LAMARINO, 2017).

³ Disponível em: www.coinmarketcap.com

2. BLOCKCHAIN

Sumariamente, o *blockchain* é o núcleo de quase todas as criptomoedas até o momento, a única moeda que utiliza um sistema paralelo ao *blockchain*, é a criptomoeda *IOTA* com a *Tangle*.

Blockchain ou “protocolo de confiança” é um sistema de computador que se deriva de um conjunto de funcionalidades como, banco de dados, sistema distribuído, segurança através de criptografia e rede *peer to peer*⁴ (P2P). Realizando a tradução direta do inglês para o português, a palavra *blockchain*, que é “cadeia de blocos” ou “encadeamento de blocos”, podemos compreender a concepção do próprio sistema, que é um inventário organizado na forma de pilha, onde cada bloco está interligado um com ou outro, armazenando as operações realizadas, podendo ser arquivado de maneira simples no modo de um arquivo ou em banco de dados simples. (ANTONOPOULOS, 2016, p. 163)

A maneira em que os blocos criam sua conexão é através de uma função que chamamos de *hash*, esta informação fica localizada no cabeçalho do bloco, portanto, cada novo bloco adicionado à rede, deve referenciar o anterior com o seu *hash*, assim, criando um consenso entre os objetos adicionados. A forma em que o *blockchain* utiliza o *hash* em relação a sua segurança, é que ele é mutável, se qualquer número do *hash* do último bloco for alterado, os dígitos de seus antecessores mudam, criando uma reação em cadeia de sua linhagem até o primeiro bloco, que é chamado de bloco gênese, desta forma, torna inviável a adulteração da informação, devido ao consenso dos *nós*. (ANTONOPOULOS, 2014, p. 163-164).

Como o *blockchain* é um sistema distribuído utilizando uma rede *peer to peer*, ou seja, para que a rede se torne funcional, é necessário no mínimo dois *nós*, não tendo limitação a quantidade de *nós* adicionados, além do mais, quanto maior a quantidade de pessoas utilizando a rede, mais ela estará protegida, pois todos aqueles que ingressam a ela, devem ter obrigatoriamente um backup inteiro da *blockchain*, ou seja, quando se conecta no sistema, você pede para os outros pontos lhe forneçam a lista atualizada deis do bloco gênese, até o último item adicionado,

⁴ Modelo em que a conexão de rede é de formato descentralizado e os integrantes do sistema, executam funções de servidor e cliente.

resultando em um consenso de todos os *nós* sobre livro-razão, portanto, se houver algum tipo de desastre é muito improvável que se perca os registros já feitos (CARNUT, 2016).

2.1 Informações do bloco

Um bloco na *blockchain* é um conjunto de transações válidas, que possuem um peso em bytes, essas operações quando atingem o tamanho médio de 1 megabyte, podendo variar até no máximo 1,08 megabytes, completa um novo bloco ao encadeamento da pilha, portanto, esse peso das transações não é nada menos de um aglomerado de informações, que são adicionados ao bloco, e o bloco é apenas metadados do agrupamento das informações contidas nele, ou seja, são dados sobre outros dados, assim como descreve Antonopoulos em seu livro *Mastering Bitcoin*.

O bloco é composto por um cabeçalho, contendo metadados, e por uma longa lista de transações que constituem a maior parte de seu tamanho. O cabeçalho do bloco tem 80 bytes, enquanto uma transação em média tem pelo menos 250 bytes e um bloco em média contém mais de 500 transações. Um bloco completo, com todas as transações, consequentemente é 1.000 vezes maior do que o cabeçalho do bloco (ANTONPOULOS, 2014, p. 164).

Como todos os participantes da rede possuem uma cópia inteira do banco de dados, que são todas as transações válidas divididas em blocos, Satoshi se preocupa com o uso de disco e definiu em seu *white paper* que.

Um cabeçalho de bloco sem transações deve ter em torno de 80 bytes, se nós supusermos que os blocos são gerados a cada 10 minutos, $80 \text{ bytes} * 6 * 24 * 365 = 4.2\text{MB}$ por ano. Com os sistemas de computador típicos a venda em 2008 com 2GB de RAM, e a lei de Moore prevendo um aumento de 1.2GB por ano, armazenamento não deve ser um problema mesmo se os cabeçalhos dos blocos forem mantidos na memória (NAKAMOTO, 2008, p. 4, tradução Daniel Ribeiro)

A tabela a seguir detém as informações que serão contidas no bloco do sistema *blockchain*.

Tabela 1 – Estrutura do bloco.

Tamanho	Campo	Descrição
4 Bytes	Tamanho do bloco	O tamanho do bloco, em bytes após esse campo
80 bytes	Cabeçalho do bloco	Vários campos formam o cabeçalho do bloco
1-9 bytes (VarInt)	Contador de transações	Quantas transações seguem
Variável	Transações	As transações registradas nesse bloco

Fonte: ANTONOPOULOS, *Mastering Bitcoin* p 164.

2.1.1 Cabeçalho do bloco

A forma em que é concebida as informações do cabeçalho, são apresentadas em três funções de metadados do bloco. A primeira é a utilização da sinalização do *hash* do bloco antecessor, o segundo é o *timestamp*⁵ e o terceiro é a utilização da árvore de merkle, que serão explicados de forma mais aprofundada nos próximos capítulos. (ANTONOPOULOS,2014, p. 164-165)

⁵ Registro de data e hora em uma informação eletrônica.

Tabela 02 – Informações contidas no cabeçalho do bloco.

Tamanho	Campo	Descrição
4 bytes	Versão	Um número de versão para servir como referência nas atualizações de software/protocolo
32 bytes	<i>Hash</i> do bloco Anterior	Uma referência ao <i>hash</i> do bloco anterior (bloco pai) na <i>blockchain</i>
32 bytes	Raiz de Merkle	Um <i>hash</i> da raiz da árvore de merkle das transações desse bloco
4 bytes	Data e Hora (<i>timestamp</i>)	O momento aproximado em que este bloco foi criado (em segundos, usando Unix Epoch)
4 bytes	Dificuldade Alvo	O alvo de dificuldade do algoritmo de prova-de-trabalho deste bloco
4 bytes	Nonce	Um contador usado para o algoritmo de prova-de-trabalho

Fonte: Antonopoulos, *Mastering Bitcoin* p 165.

2.2 Hash

Primeiramente, o conceito da função *hash* é facilmente explicável, trata-se apenas uma um conjunto de letras e números escrita de forma hexadecimal que representa algum tipo informação como textos ou arquivos.

O *Hash* é gerado a partir de um algoritmo preestabelecido, o uso mais comum que temos de utilização de *hash* ou dígitos verificadores é o nosso CPF, o CPF

utiliza apenas 2 dígitos verificadores que são após o hífen, e os números antes do hífen é chamado de “mensagem”, por exemplo, “897.235.177”-“43”, o número “43” é o *hash* da mensagem “897.235.177”, se alguém tentar forjar de forma arbitrária em questão de probabilidade apenas irá achar uma vez em cem tentativas o *hash*. (CARNUT, 2016).

Em relação ao *Bitcoin*, ele utiliza 77 dígitos verificadores e com essa quantidade são quase nulas as duplicatas e as chances de se forjar um *hash*, portanto, é improvável achar o *hash* devido a criptografia usada pela moeda, que se chama SHA-256, esta segurança garante que é impossível descriptografar após a transformação e quase sempre a saída será no tamanho de 32-bytes, portanto, independente da extensão da mensagem irá garantir um peso fixo e uma segurança inquebrável se houver a tentativa de alteração em qualquer tipo de informação da mensagem que está no bloco. (CARNUT, 2016).

No exemplo a seguir, podemos constatar a transformação de uma *string*⁶ na criptografia SHA-256, e se for alterado qualquer tipo de dado, a mensagem será totalmente diferente da versão original.

⁶ Em computação, *string*, é uma cadeia de caracteres que pode ser escrito de forma alfanumérico, sem a necessidade de formar ou não uma palavra.

Figura 1 – Transformação de uma *string* na criptografia SHA-256
SHA-256 hash calculator

SHA-256 produces a 256-bit (32-byte) hash value.

Data

Guilherme de Albuquerque Grandmaison

SHA-256 hash

715fb20b3233c25d02d64e810548817776feece092135f8b27106d063d94b319

Calculate SHA256 hash

Fonte: XORBIN <<http://www.xorbin.com/tools/sha256-hash-calculator>>, acessado em 8 de novembro, 2017.

Figura 02 – Alteração na *string* resulta em um “*hash*” totalmente diferente ao original.
SHA-256 hash calculator

SHA-256 produces a 256-bit (32-byte) hash value.

Data

Guilherme de Albuquerque Grandmaiso

SHA-256 hash

102ae3bf477981b1d706f2c32328cbf3336f14c29641bd2e5aebd53f7ca04a9

Calculate SHA256 hash

Fonte: XORBIN <<http://www.xorbin.com/tools/sha256-hash-calculator>>, acessado em 8 de novembro, 2017.

2.3 Timestamp

Resumidamente, o *timestamp* é um programa simples utilizado para registrar digitalmente data e horário nas transações da rede *bitcoin*, a forma em que é “carimbada” a operação, é através do *hash*, após executada o carimbo no *hash*, ela é exibida para todos na rede, comprovando que aquela transação é verdadeira e existe na *blockchain*. (FERREIRA, 2017).

Existem três principais benefícios na utilização do “carimbo” do *hash*, a primeira é que informação a ser registrada pode ser mantida em segredo e separada do meio utilizado para garantir o horário. A segunda é o peso do *hash*, pois a mensagem que foi gerada aquele *hash*, é significativamente maior do que sua saída no SHA-256, resultando em um benefício de armazenamento. E por último, as assinaturas digitais ou *timestamp* funcionam melhor com dados com um tamanho predeterminado, que em nosso caso, sempre será uma saída de 32-bytes (FRANCO, 2015, p. 99, minha tradução).

Satoshi descreve em seu *white paper* a utilização do servidor de *timestamp* para que crie mais segurança e um registro em tempo das transações executadas.

A solução que nós propomos começa com um servidor de carimbos de tempo. Um servidor de carimbos de tempo funciona pegando a codificação de um bloco de itens a serem “carimbados” e publicando largamente esta codificação, como em um jornal ou post na Usenet [2-5]. O carimbo de tempo prova que os dados precisam ter existido naquele tempo, obviamente, para que sejam incluídos na codificação. Cada carimbo de tempo inclui o carimbo de tempo de anterior em sua codificação, formando uma corrente, onde cada carimbo de tempo adicional reforçará os blocos anteriores. (NAKAMOTO, 2008, p. 2)

Portanto, todo bloco gerado na rede possui um registro de tempo, podemos ver de maneira pública essa informação de todos os blocos já criados como segue na Figura 3.

Figura 03 – Informação do *timestamp* no bloco.

Bloco #495049

Resumo		Hashes	
Número de Transações	990	Jogo da velha	000000000000000000000000c342e73ca0a4ebc85753461611f5c08ca6dba345ed8d6a
Total de Saída	\$ 107,326,567.44	Bloco Anterior	0000000000000000000000001a2920f7328e051a7878ab14b7c3b85ec4a2c8b6279826
Volume Estimado de Transações	\$ 1,229,081.05	Próximo(s) Bloco(s)	000000000000000000000000119991bcd77bd29fcbdb009a21c8693ee9ad490352c93d
Taxas de Transação	\$ 3,517.88	Raiz de Merkle	49dc5cb50d90f054d1fb0dbf5dce893b9d8d23a1544ef8235f0692d557223d21
Altura	495049 (Sequência Principal)		
Timestamp	2017-11-19 06:47:45		
Hora de Recepção	2017-11-19 06:47:45		
Transmitido Por	BTC.com		
Dificuldade	1,364,422,081,125.15		
Bits	402705995		
Tamanho	1008.517 kB		
Peso	3992.923 kWU		
Versão	0x20000000		
Nonce	1587178553		
Recompensa Pelo Bloco	\$ 96,287.25		

Fonte: BLOCKCHAIN INFO
<https://blockchain.info/pt/block/000000000000000000000000c342e73ca0a4ebc85753461611f5c08ca6dba345ed8d6a> acessado em: 19 de novembro, 2017.

2.4 Proof of work

A forma em que Satoshi encontrou para proteger seu sistema, é literalmente a união faz a força, tudo que se faz na rede *blockchain* é distribuído entre todos os participantes da rede, ele vai deis da implementação de novos blocos e das transações com o uso do *proof of work*.

Para que uma transação na rede *Bitcoin* seja considerada verdadeira, o *nó* da rede precisa apresentar para todos os usuários a resolução matemática de um algoritmo, que é chamada de *proof of work*, ou se preferir, prova de trabalho, Alex Ferreira, explica em poucas palavras utilizando uma analogia o *proof of work*.

Uma Analogia para isso seria um professor dar uma lição de casa difícil para um estudante. O estudante pega essa lição gasta seu tempo calculando a solução para o problema e então apresenta a resposta ao professor. O professor então checa a resposta do estudante e caso esteja correta, isso prova ao professor que o estudante gastou uma quantidade de trabalho suficiente para ser recompensado. (FERREIRA, 2017).

Sumariamente, após que um *nó* da rede completa o seu “dever de casa”, ele passa adiante sua resposta, para que os outros integrantes da rede verifiquem se a

“resposta” dele está correta, refazendo a mesma “tarefa de casa”, assim para chegar em um consenso daqueles que fizeram a conta matemática, ou em nosso caso, executaram a validação da transação na rede *Bitcoin*. Para que seja validada a operação, é necessário passar mínimo seis vezes nos nós da rede, tendo o mesmo resultando todas as vezes em que foi passada adiante, assim, garantindo a veracidade da transação, e se resultar em algo diferente dos outros, o ato é considerado inválido e é descartado (CARNUT, 2017).

2.4.1 Algoritmo do proof of work

Basicamente, o algoritmo do *proof of work*, utiliza o *hash*, ele é um ponto crucial para o funcionamento da *blockchain*. Como dito anteriormente no capítulo 2.2, qualquer tentativa de adulteração por menor que seja da mensagem, resulta em um *hash* totalmente diferente, então, nosso *hash*, pode ser considerado uma assinatura digital, após a transformação do SHA-256, que é a criptografia usada pelo *Bitcoin*.

Todo bloco que entra no encadeamento, precisa passar pelo *proof of work*, a forma em que é denominada a dificuldade, é através de um alvo, onde o alvo é definido por uma quantidade de zeros em sequência com base na quantidade de *hash power* em que a rede possui.

Por exemplo, na figura 01, a transformação da mensagem “Guilherme de Albuquerque Grandmaison” resultou no *hash* criptográfico com a sequência “715fb20b3233c25d0264e...” suponhamos que o alvo de nossa mensagem seria encontrar uma sequência que comece com o número 0, desta forma, o bloco precisa criar um loop até que ache o alvo desejado, a variável usada é chamada de *nonce*, apresentada na tabela 02, então, será adicionado contadores na mensagem até que encontremos um *hash*, que comece com 0, e é só na sexta tentativa que podemos encontrar o nosso alvo com o seguinte *hash* “01ae1093e62c7e7ecc52e073...”

Figura 4 – Tentativas para achar o alvo (nonce).

SHA-256 produces a 256-bit (32-byte) hash value.

Data

Guilherme de Albuquerque Grandmaison 6

SHA-256 hash

01ae1093e62c7e7ecc52e073d43d5bae9b3b79dff3b4616a21d0926123ead243

Calculate SHA256 hash

Fonte: XORBIN <<http://www.xorbin.com/tools/sha256-hash-calculator>> acessado em 19 de novembro, 2017.

Portanto, após encontrarmos o nosso alvo, nossa prova de trabalho seria considerada válida, e o bloco entraria na *blockchain*. (ANTONOPOULOS, 2014, p. 193-98)

A maneira em que o *blockchain* dificulta o alvo é aumentando um bit, em nosso caso é o aumento de zeros em sequência, isso resulta em crescimento exponencial em relação a quantidade de tentativas que levaria para achar uma mensagem que se encaixa com o que é solicitado. Na Figura 04, podemos verificar que o alvo é uma sequência de 18 bits seguidos de zeros, onde o nosso contador o *nonce*, chegou a realizar mais de 158 milhões de tentativa para que achasse um alvo que se adequasse aos 18 bits (ANTONOPOULOS, 2014, p. 193-198). Conseqüentemente, os mineradores que possuem mais poder computacional, que é medido em *hash* por segundo, que é quantidade de gerações de *hash* que se realiza em um segundo, tende a ganhar mais em relação as taxas de transação e as adições de blocos, onde ele é recompensado se adicionar ao encadeamento, e a dificuldade é baseada no poder computacional da rede, portanto, quanto mais a rede tem de poder, maior será a dificuldade de se encontrar o *hash* do alvo. (CARNUT, 2016).

Figura 5 – sequências de zeros do *hash*, em um bloco no próprio *blockchain*.

Hashes	
Jogo da velha	00000000000000000000c342e73ca0a4ebc85753461611f5c08ca6dba345ed8d6a
Bloco Anterior	000000000000000000001a2920f7328e051a7878ab14b7c3b85ec4a2c8b6279826
Próximo(s) Bloco(s)	00000000000000000000119991bcd77bd29fcbdb009a21c8693ee9ad490352c93d
Raiz de Merkle	49dc5cb50d90f054d1fb0dbf5dce893b9d8d23a1544ef8235f0692d557223d21

Fonte:BLOCKCHAIN

INFO

<[blockchaininfo/pt/block/00000000000000000000c342e73ca0a4ebc85753461611f5c08ca6dba345ed8d6a](http://blockchaininfo.pt/block/00000000000000000000c342e73ca0a4ebc85753461611f5c08ca6dba345ed8d6a)> acessado em: 19 de novembro, 2017.

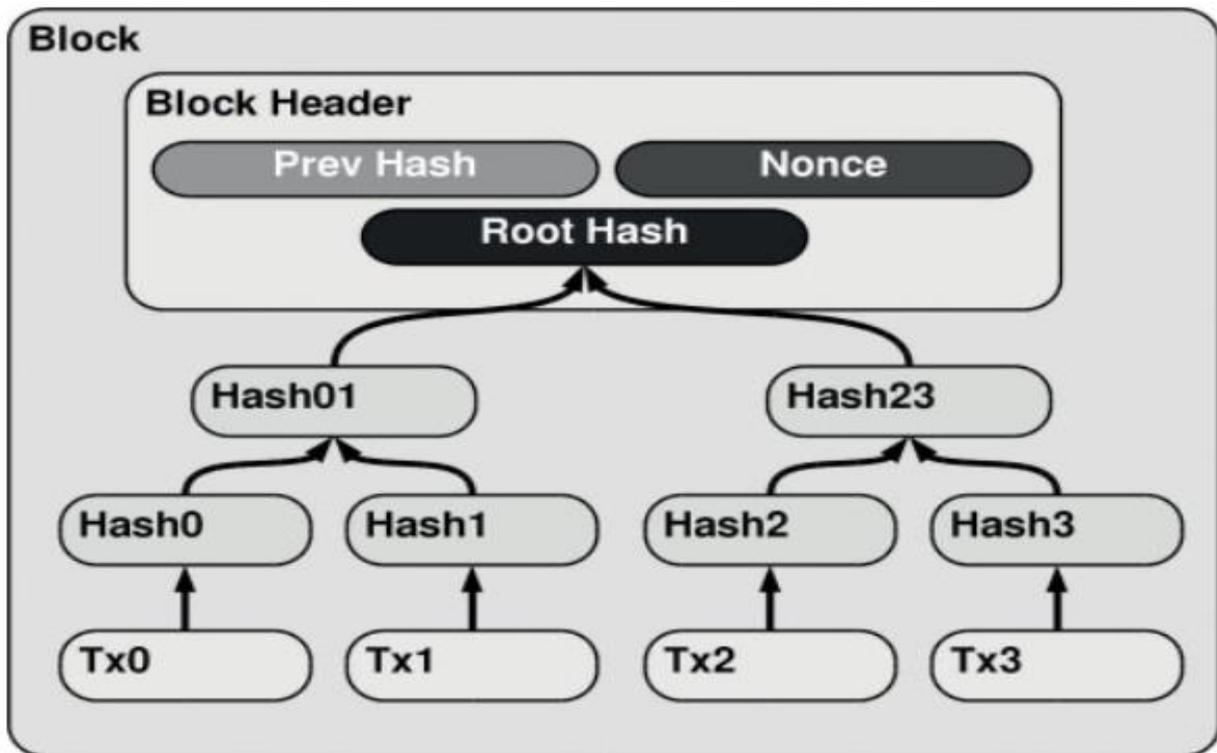
2.5 Arvore de merkle

Resumidamente, a utilização da árvore de merkle, é como se fosse um resumo de todas as informações das transações implantadas naquele bloco específico, esta função resulta em uma maneira eficaz em averiguar a totalidade da enorme quantidade de dados. (ANTONOPOULOS, 2014, p. 170. Minha tradução)

A maneira em que é formada o *hash* do bloco é utilizando a árvore de Merkle, ou *hash tree*. Primeiramente, é criado uma árvore binária, que em ciência da computação, o uso da palavra “árvore” é uma ordenação de dados de forma dividida, em que a “raiz” fica no topo e suas ramificações são as “folhas” que fazendo uma analogia seria algo semelhante a uma “árvore genealógica (ANTONOPOULOS, 2014, p. 170. Minha tradução).

A estrutura é formada por *hashes* de maneira característica de cada transação, elas são as “folhas” de nossa “árvore”, estes itens serão representados na Figura 05 por *hash0*, ... *hash3*. Na representação a seguir, a soma de duas “folhas” é a forma derivada de uma única informação, assim, dois dados se tornam uma única referência. A função usada para calcular o *hash* é também o SHA-256, resultando no tamanho correto para adicionar ao cabeçalho do bloco, demonstrado na tabela 02. (FRANCO,2015, p. 117-118. Minha tradução)

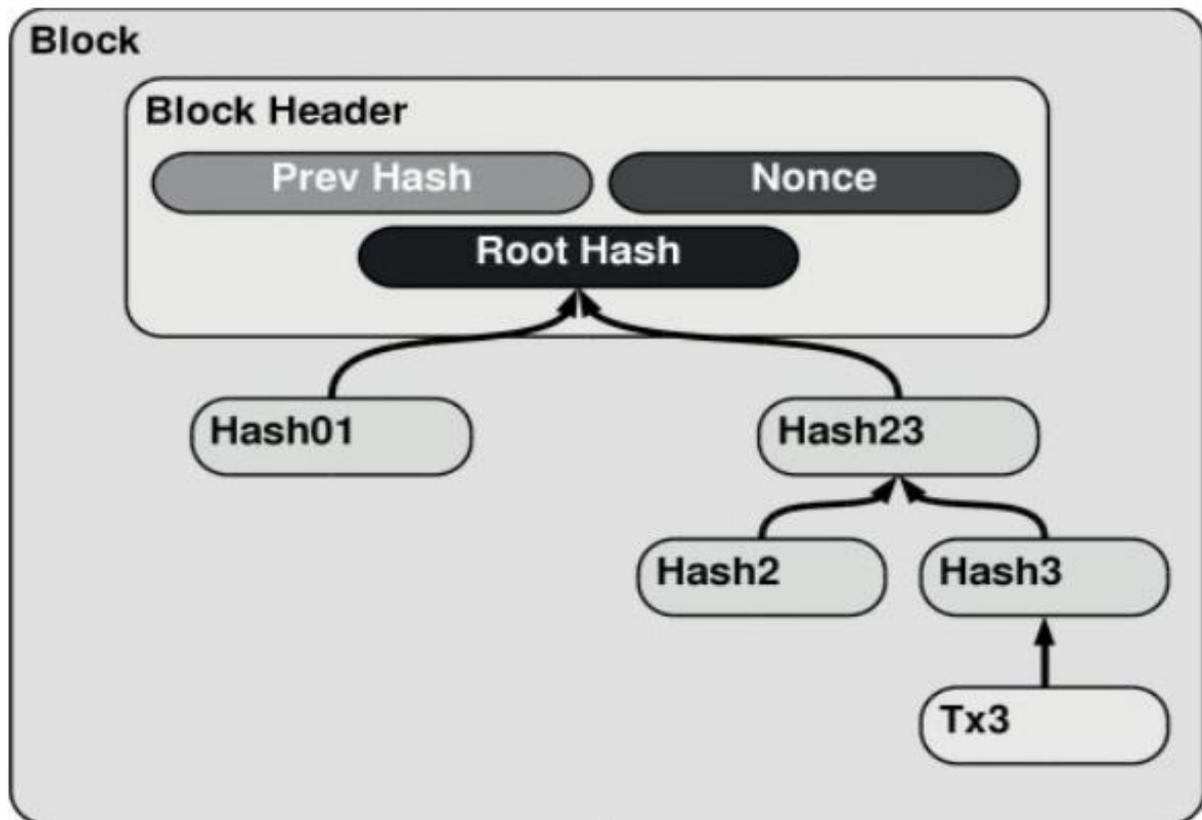
Figura 6 - Representação da Árvore de Merkle.



Fonte: FRANCO, Understating *Bitcoin*, p. 118. 2015.

Inicialmente, temos o bloco como um todo, em seguida separando algumas informações, possuímos o cabeçalho do bloco, que é chamado de *Block Header* na Figura 05, resultando em uma forma derivada o conjunto de transações com seus respectivos *hash*, portanto, a grande vantagem do uso desta estrutura de dados, é a fácil manipulação das informações. Imaginemos que algum usuário da rede queira verificar a operação Tx3 e se ela pertence ao bloco da Figura 05, então, para averiguar o item desejado o *nó* necessariamente passara no “galho” *Hash23*, que se deriva do *Hash2* + *Hash3*, e em seguida encontra a transação constatando que aquela informação composta é verdadeira, como demonstrado na Figura 06. (FRANCO, 2016, p 118. Minha tradução)

Figura 07 – Encontrado uma transação na árvore de Merkle.



Fonte: FRANCO, Understating *Bitcoin*, p. 118. 2015.

2.6 Mineradores

Em resumo, os *nós* da rede são o coração do sistema, sem eles não há possibilidade de fazer o *blockchain* funcionar, devido, ao termo utilizado para representar o que os *nós* executam na rede. Eles são responsáveis por toda validação e adição dos novos blocos e das transações.

Os pontos que compõe o funcionamento da rede *Bitcoin*, são chamados de “mineradores”, eles ganham uma recompensa determinada ao adicionar um novo bloco na rede e também uma porcentagem em taxas em relação as validações das transações efetuadas.

Satoshi estabeleceu uma recompensa dada ao se adicionar um novo bloco que resulta em 50 BTC, isso iria reduzir gradualmente após a criação de 210 mil blocos que dá entorno de quatro anos, pois a forma que é disponibilizado um novo bloco na rede, é de maneira periódica de dez em dez minutos em média disponibilizado um bloco novo nestes intervalos, portanto, entre 2008 até 2012, o

valor dado ao adicionar um novo item ao encadeamento era de 50 BTC, em 2012 até 2016, reduzira pela metade o valor, garantindo 25 BTC por bloco, e assim sucessivamente, agora em 2017, a retribuição é de 12,5 BTC, resultando em um valor aproximado de \$100.000,00 USD ao se implementar um novo bloco na pilha. (CARNUT,2016).

Satoshi também julgou que a quantidade de *bitcoins* no mundo deveria ser finita totalizando 21 milhões de moedas, para que conseqüentemente, as pessoas utilizassem o dinheiro para trocar com serviços e mercadorias, da mesma forma em que o dinheiro funciona nos dias de hoje (CARNUT,2016).

O minerador só irá ganhar a sua recompensa de adição de bloco ou taxa de transação, resolvendo o problema matemático descrito como *proof of work*, apresentando no capítulo 2.4 e 2.4.1, assim, provando que ele gastou um determinado tempo de poder computacional, para encontrar o *hash* criptográfico da solução matemática, desta forma, ganha o direito de validar uma operação e também de adicionar um novo bloco ao encadeamento e por fim, resultando em uma recompensa dada em *bitcoin* (ANTONOPOULOS,2014,p 177).

3. IOTA

A Criptomoeda *IOTA* foi apresentada ao público pela primeira vez em 2014, ela surgiu com uma proposta de ser tornar o *backbone* para internet das coisas, ou seja, seria o sistema que funciona por trás de todos os equipamentos de *IoT*, resultando em uma rede segura para todos os acessórios. Resumidamente, a internet das coisas, é uma forma representativa onde qualquer coisa que utilizamos no dia a dia estaria conectado na internet, como carros, geladeiras, painéis solares entre outros milhares de equipamentos(LAUNG,2017).

Da mesma maneira em que as outras criptomoedas se derivaram do *blockchain*, a *IOTA* não foi diferente, ela se baseou nos mesmos princípios, entretanto, em vez de utilizar o próprio *blockchain* e visando um alvo específico como “internet das coisas”, a *IOTA* apenas usou os conceitos do núcleo do *Bitcoin*, criando uma nova evolução chamada de *Tangle*. As principais características desta nova *altcoin*, é que não há mineradores, portanto, não há taxas possibilitando micro transações, estrutura dos dados leve para a *IoT*, escalabilidade enorme e velocidade, tudo graças a nova tecnologia chamada também de “rede flash” (LAUNG,2017)

3.1 Gráfico acíclico direto (GAD)

A inovação por trás da *IOTA* é que ela não utiliza blocos gerados periodicamente como o *Bitcoin*, em vez disso, ela usa vários pontos ligados de forma direta, diferente do *blockchain* que usa o empilhamento de informações de maneira aglomerada. A *Tangle* ou “rede flash” opera com um gráfico acíclico direto para executar o funcionamento da rede.

Toda transação realizada na *IOTA*, resulta em algo semelhante ao *Bitcoin*, mas ao mesmo tempo é de maneira diferente. Quando é executado uma transação que também é chamada de “*site*”, todos os *sites* na rede *IOTA* referenciam uma ou mais *sites*, resultando em um emaranhado de ligações, Serguei Popov explica em seu *white paper*, sobre o *tangle*, como ele lida com as validações e o surgimento de uma transação.

Quando uma nova transação aparece, ela deve aprovar duas transações anteriores. Estas aprovações são representadas por uma “borda direta”, como mostrado na Figura 1². Se não há uma “borda direta” entre a transação A e a transação B, mas, existe um caminho que leve as transações A e B, nós dizemos que A aprova B de forma indireta. (Popov, 2017, p. 2. Minha tradução).

Ou seja, como não há mineradores, quem garante a veracidade da transação na rede? A resposta é simples, a própria pessoa ou se preferir o *nó* da rede.

Ao se efetuar uma operação na *Tangle*, ela deve validar duas transações anteriores para que valide a sua, A *IOTA* se baseia em algo similar ao *proof of work* do *Bitcoin*, entretanto, a dificuldade do *proof of work* da rede flash, é muito mais simples ao se resolver a questão matemática do *hash*, devido, ao foco para IoT. Desta forma a própria pessoa se torna tecnicamente um minerador na rede, porém, ela não ganha qualquer tipo de taxa ao se validar as duas transações anteriores, e por fim Serguei descreve em um pequeno trecho do *white paper*, a solução do gasto duplo. (LEUNG; POPOV, 2017, p. 3)

Conforme a transação vai recebendo mais aprovação através da validação, ela se torna mais aceita pelo sistema com um grau alto de confiança, em outras palavras será muito difícil para o sistema aceitar uma transação de gasto duplo (Popov,2017, p. 3. Minha tradução).

4. Análise Comparativa

No decorrer deste trabalho, exploramos o funcionamento dos sistemas por trás das criptomoedas *Bitcoin* e *IOTA*, com suas respectivas tecnologias *blockchain* e *tangle*.

Analisando os dois, lado a lado, podemos perceber que o *blockchain* necessita dos mineradores para que seu sistema opere, eles fazem uma parte crucial executando as adições de blocos e validando as transações, sendo recompensando em forma de *bitcoin* com o esforço computacional do *proof of work*.

Já a *IOTA* não possui mineradores, o próprio *nó* da rede se torna tecnicamente o “minerador”, ou seja, o usuário que executa a operação, valida duas anteriores, para que torne a sua verídica, desta forma, a *IOTA* possibilita transações com zero de taxas, onde não há qualquer tipo de recompensa a não ser o seu próprio registro na rede, desta forma, quanto mais *nós* criando transações, mais o sistema ficará seguro e seu fluxo crescerá junto a demanda de forma exponencial.

4.1 Escalabilidade

Uma das grandes críticas ao sistema *blockchain*, é que ele não consegue lidar com escala em relação a taxa crescente de transações, em comparação a maioria dos outros sistemas de processo de transação (FRANCO, 2014, p. 120).

Um bloco é composto por 2.000 transações em média, se o bloco é gerado por volta de dez minutos, resulta em uma taxa lenta de adições de transações. Desta forma, o *Bitcoin* realiza $2.000 / (60 \cdot 10) = 3,3$ transações confirmadas por segundo, comparando o sistema com outros meios de pagamentos, o *Paypal* aprova por volta de 113 operações e por final a grande Visa, consegue operar com a quantidade de 4.000 transações por segundo. (LAUNG, 2017)

Desta forma, podemos demonstrar que se o *Bitcoin* se tornar o novo meio universal do uso do dinheiro, ele instantaneamente teria problemas com o seu fluxo, onde não suportaria a grande demanda. Além disso, a quantidade de espaço em disco, que os mineradores teriam que ter para manter uma cópia da *blockchain*, iria

aumentar de forma considerável, onde Franco descreve em seu livro *understaing bitcoin*, na seguinte forma.

As transações ocupam por volta de 0,5 kB de espaço, a utilização do espaço em disco, pode aumentar de forma escalada se houver uma grande quantidade de transação feitas a cada segundo, por exemplo, se a frequência for de 2.000 transações por segundo gerando por volta de 1 MB de dados por secundo, resultaria em 30 TB de informação a cada ano[...] (Franco, 2014, p 121 minha tradução)

Assim, podemos verificar que o *Bitcoin* ainda precisa sofrer algumas mudanças, enquanto ainda está na fase de crescimento em questão de uso, entretanto, já existem algumas propostas para resolver a questão de escalabilidade do *Bitcoin*, como a *Segwit2x* alterando o tamanho do bloco que resultaria em inúmeras mudanças, e a *Lightning Netwrok* com sua *blockchain* privada. (CHAWLA; THOMPSON, 2017).

Como o *Bitcoin* é um sistema distribuído, onde não existe algum órgão regulamentador ou dono, aplicar alterações é uma tarefa difícil, desta forma, só haverá alteração se a comunidade concordar com um grande grau de aceitação, assim, dificulta qualquer tipo de atualização resultando em muitas alterações.

Em comparação de escalabilidade da moeda *IOTA*, ela não sofre esse problema, pois, quanto mais transações são feitas na *Tangle*, resulta em segurança e escalabilidade de forma exponencial em relação as transações.

4.1.1 Análise de fluxo

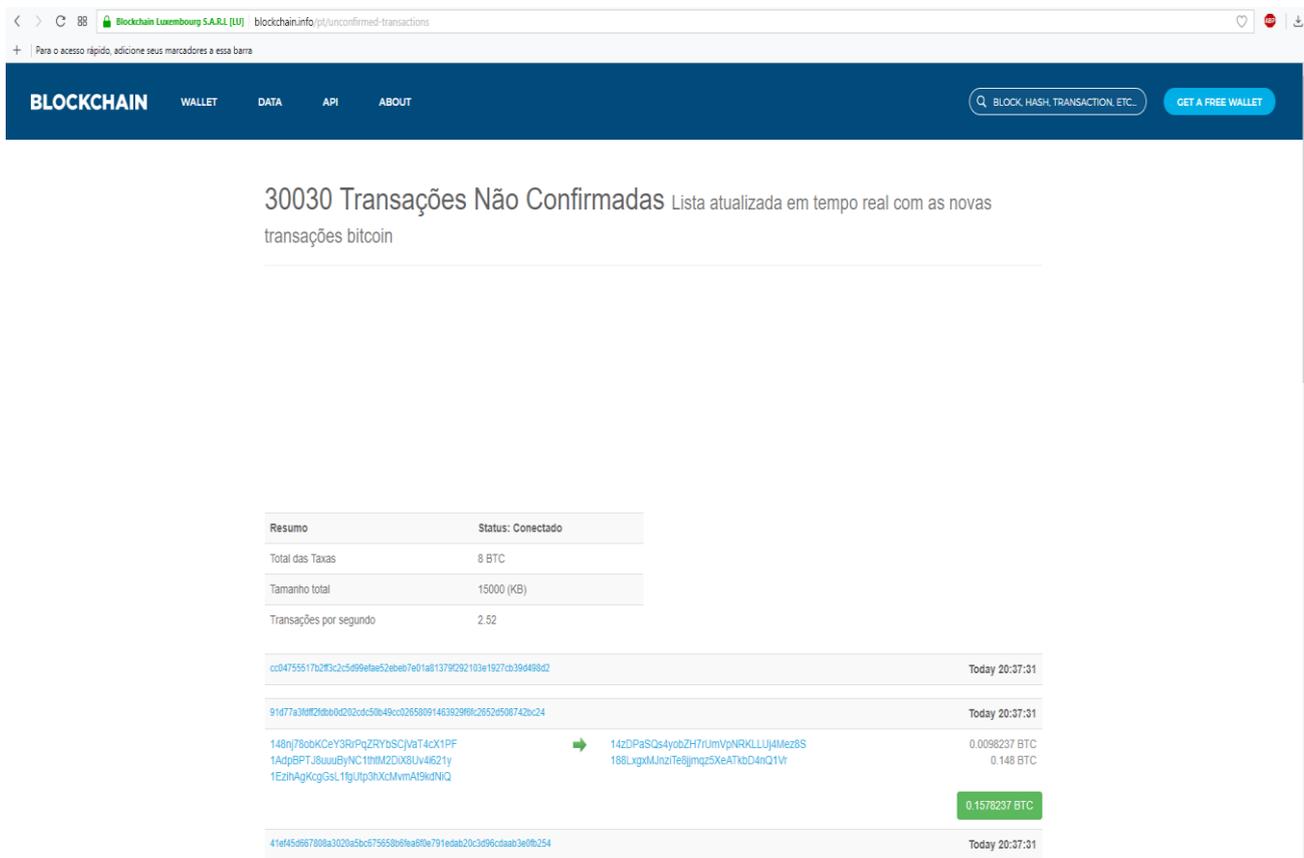
Todos os dados retirados, foram adquiridos do site oficial do *blockchain*, nele é demonstrado em tempo real o seu funcionamento mostrando informações sobre mercado, blocos, mineração e atividade da rede.

Em uma análise mais contemporânea, onde houve uma enorme valorização no mercado *Bitcoin*, por volta do início do mês de outubro em 2017, resultou em grandes fluxos de transações, criando uma grande parte de operações aguardando validação e registro nos blocos. Desta forma, uma quantidade crescente de transações diariamente apareceu.

Os dados foram adquiridos durante os dias 26 de outubro, até o dia 12 de novembro, que após esta data iniciou seu declínio definitivo. No dia 26 de outubro foi

visto que havia 14.000 transações em espera chegando ao pico de 30.000 no mesmo dia, portanto, com a valorização crescente a cada dia que passava, havia um novo topo sendo ultrapassado em relação as transações e valor do dinheiro, até que no dia 12 de novembro, houve um gargalo na rede, resultando em um total de 178.000 transações em espera, onde as taxas das transações se fixaram por volta de 25 dólares até 100 dólares, como descrito em uma notícia de uma carteira chamada *Exodus*. Substancialmente, uma carteira nas criptomoedas, é uma forma de se guardar um conjunto de criptomoedas em um único lugar de maneira segura.

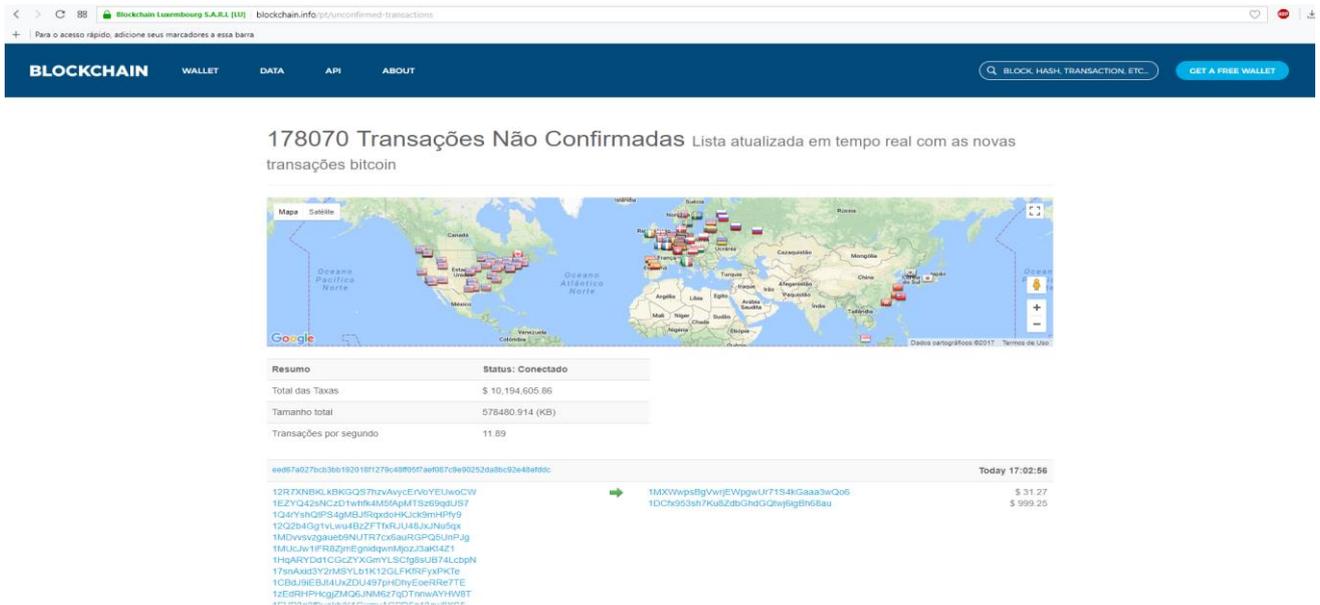
Figura 8 – Transações não confirmadas do dia 26 de outubro, 2017.



Fonte: BLOCKCHAIN INFO <blockchain.info/pt/unconfirmed-transactions> 2017.

A figura 9 demonstra claramente o problema de escalabilidade em relação as transações executadas na rede *Bitcoin*, desta forma, podemos comprovar em um fato que a moeda precisa solucionar o seu fluxo de operações quando houver uma grande demanda pelos usuários.

Figura 9 – Transações não confirmadas do dia 12 de novembro, 2017.



Fonte: BLOCKCHAIN INFO <blockchain.info/pt/unconfirmed-transactions> 2017.

A carteira *Exodus* relata em seu site, o resultado da enorme fila de espera das transações, esclarecendo os altos valores de taxas cobrados pelos mineradores da rede *Bitcoin*.

A Figura 10 diz o seguinte: “ALERTA: As taxas das transações são as mais altas vistas até agora na história do *Bitcoin*. Estas taxas são pagas diretamente a rede *Bitcoin*, em relação ao processamento das transações. *Exodus* não ganha qualquer tipo de taxa da rede *Bitcoin*. Acreditamos que as taxas fiquem entre 25 dólares até 100 dólares. O que faz essencialmente a rede inútil.

Para que fique claro, este fato só afeta as transações *Bitcoin*. Ela não afeta outras moedas como *Bitcoin Cash*, *Ethereum*, *Ethereum Classic*, *Litecoin* ou outras moedas que são usadas na *Exodus*.

Nosso conselho é que se você não tem que usar *bitcoin* hoje, apenas espere até a “tempestade se acalmar”. No passado já presenciamos estes tipos de eventos na rede, elas vão se normalizando durante a semana.”

Figura 10 - Comunicado da carteira *Exodus*.

Exodus Current Status

Below we detail any problems with Exodus or asset networks...

WARNING: Bitcoin transaction fees are the highest we have ever seen in the history of Bitcoin. These fees are paid directly to the Bitcoin network to process your transaction. Exodus does not keep ANY of the network fees. We are currently seeing Bitcoin fees range from \$25 USD up to \$100 USD. Many times this essentially makes using the Bitcoin network worthless.

For clarity, this only impacts Bitcoin transactions. This does not impact Bitcoin Cash, Ethereum, Ethereum Classic, Litecoin or any other Exodus assets.

Our best advice is if you do not have to use Bitcoin today just wait until this storm calms down. In the past we have seen these network events calm in a week's time.

Fonte: EXODUS <<https://www.exodus.io/status/>> acessado em: 12 de novembro, 2017.

Com a figura 11 podemos analisar a grande valorização da moeda no mercado que se iniciou no ano de 2016, até o fim de outubro de 2017, evidenciando o problema de escalabilidade citado anteriormente com a quantidade de transações feitas, criando uma ligação quando houver um enorme aumento monetário.

Figura 11 – Gráfico da valorização da moeda *bitcoin* em dólares.



Fonte:FOXBIT <<https://foxbit.com.br/grafico-bitcoin>> acessado em: 26 de novembro,2017.

Como pode-se notar nas imagens 8,9,10 e 11, com o decorrer dos meses de 2017, a valorização da moeda *bitcoin* não parou, assim podendo causando um grande atraso nas transações e aumento nas taxas quando houve uma enorme demanda na rede, causando problemas de escalabilidade em associação ao uso do sistema, portanto, o *Bitcoin*, precisa aplicar algumas mudanças caso queira conquistar o mercado de forma global.

5. CONCLUSÃO

O trabalho permitiu compreender o funcionamento do núcleo do *Bitcoin* com a utilização do *hash*, *timestamp*, *proof of work*, árvore de merkle e criptografia, é por meio destas funções em que o bloco funciona no sistema. A *IOTA* se baseando nestes processos criou algo paralelo onde não se utiliza mais blocos, em vez disso, usa o *tangle* com um gráfico ligado de forma direta e que não possui ciclo, assim, garantindo a mesma funcionalidade de maneira diferente e melhorada ao seu antecessor.

Por meio da análise comparativa entre o *Bitcoin* e a *IOTA*, podemos notar que o *Bitcoin* não consegue lidar com uma quantidade excessiva de operações sendo feitas a cada segundo, visando esta dificuldade a criptomoeda *IOTA* já soluciona este problema com o uso de seu GAD, assim, evitando o problema de escalabilidade em relação à grande demanda transações.

A pesquisa apresentada com os dados do *blockchain* em tempo real, reforçam a ideia de que o *Bitcoin* necessita aplicar certas mudanças em suas linhas de código melhorando sua escalabilidade de transações, onde tivemos um registro de um total de 178.000 mil operações em espera, conseqüentemente resultou em altas taxas, horas ou até mesmo dias para concretização de uma transferência na rede, por fim transformou o sistema praticamente inutilizável.

O sistema *blockchain* com seus poucos anos de lançamento, já disponibiliza uma grande confiabilidade em relação ao uso do dinheiro, o conceito de seu sistema ainda está em fase de exploração, onde podemos perceber que a *IOTA* evoluiu ainda mais sua base, portanto, podemos concluir que muitos progressos ainda estão por vir com essa tecnologia inovadora.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ALEX FERREIRA, **Explicando o *White Paper* do *Bitcoin***. Disponível em: <<https://moneytimes.com.br/explicando-o-white-paper-do-bitcoin>> **Acessado em 18 de Novembro, 2017.**

ANTONOPOULOS, Andreas M. **Mastering *Bitcoin***. 1 ed. Sebastopol: *O'Reilly Media Inc.* Dezembro, 2014.

ÁTILA LAMARINO, **Criptomoedas, *blockchain* e *Altcoins* | Nerdologia Tech 13. Setembro, 2017.** Disponível em: <<https://youtu.be/PQQONpwqMIg>> **Acessado em: 13 de Novembro. 2017.**

ERIC HUGHES. **A Cypherpunk's Manifesto. 9 de março, 1993.** Disponível em : <<https://www.activism.net/cypherpunk/manifesto.html>> **Acessado em: 12 de Novembro, 2017.**

FRANCO, P. **Understanding *Bitcoin***. 1 ed. United Kindom: *John Wiley & Sons Ltd*, 2015.

GUILHERME HAAS. **Cypherpunk: o ativismo do futuro. Tecmundo, 5 de julho, 2013.** Disponível em: <<https://m.tecmundo.com.br/criptografia/41665-cypherpunk-o-ativismo-do-futuro.htm>> **Acessado em: 12 de Novembro. 2017.**

GUILHERME VILLELA, **Fatos históricos: Plano Collor confiscou a poupança, e Brasil mergulhou na hiperinflação.** Disponível em <<http://acervo.oglobo.globo.com/fatos-historicos/plano-collor-confiscou-poupanca-brasil-mergulhou-na-hiperinflacao-15610534>> **Acessado em: 12 de Novembro. 2017.**

MARCOS CARNUT, **Marco Carnut - Tempest - Introdução ao *Blockchain* e à Rede *Bitcoin***. Disponível em: <<https://youtu.be/kQIQHGUEDv8>> **Acessado em: 18 de Outubro. 2017.**

NATHAN LAUNG, ***IOTA* BREAKDOWN: The *Tangle* Vs. *Blockchain* Explained.** Disponível em: <https://youtu.be/l_jNH9BIEEo> **Acessado em: 21 de Outubro. 2017.**

PATRICK THOMPSON, **Lightning Must Strike Soon, *Bitcoin* Facing backlogs as Scalability Solution Awaited.** Disponível em: <<https://cointelegraph.com/news/lightning-must-strike-soon-bitcoin-facing-backlogs-as-scalability-solution-awaited>> **Acessado em: 23 de Novembro, 2017.**

SATOSHI NAKAMOTO, ***Bitcoin: A Peer-to-Peer Electronic Cash System***. 31 de outubro, 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>> **Acessado em: 17 de Novembro, 2017.**

SEAN AU, **If you understand *Hash* Functions, you'll understand *Blockchain***. Disponível em: <<https://decentralize.today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d>> **Acessado em: 18 de Novembro. 2017.**

SHIVAM CHAWLA, **Why *Bitcoin* Developers are Against The Block Size Increase.** Disponível em: < <https://blockchaind.net/bitcoin-developers-block-size-increase/> > Acessado em: 23 de Novembro, 2017.

SIRIUS, R. U. **Cypherpunk rising: WikiLeaks, encryption, and the coming surveillance dystopia.** Disponível em:< <https://www.theverge.com/2013/3/7/4036040/cypherpunks-julian-assange-wikileaks-encryption-surveillance-dystopia>> Acessado em 12 de novembro. 2017.

ULRICH, F. ***Bitcoin* – a moeda na era digital.** Disponível em. 1. ed. São Paulo: Mises Brasil, 2014.