**Universidade Paulista - UNIP**

**Victor Sinesio dos Santos**

# ANÁLISE DE ESCALABILIDADE DO BLOCKCHAIN

**Limeira**

**2020**

**Universidade Paulista - UNIP**

**Victor Sinesio dos Santos**

# ANÁLISE DE ESCALABILIDADE DO BLOCKCHAIN

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. Sérgio Eduardo Nunes, Me. Antonio Mateus Locci e Me. Danilo Rodrigues Pereira.

**Limeira**

**2020**

**Victor Sinesio dos Santos**

# ANÁLISE DE ESCALABILIDADE DO BLOCKCHAIN

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. Sérgio Eduardo Nunes, Me. Antonio Mateus Locci e Me. Danilo Rodrigues Pereira.

Aprovada em 26 de novembro de 2020.

**BANCA EXAMINADORA**

_____

_____

_____

## DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, aos meus colegas, amigos, familiares e professores, os quais estavam ao meu lado dando apoio durante esta trajetória acadêmica.

*“O sucesso é ir de fracasso em fracasso sem perder o entusiasmo.”*

(Winston Churchill)

## RESUMO

Na última década, o *Blockchain* se tornou popular com sua utilização nas criptomoedas, onde não há envolvimento de terceiros em suas transações. Com o crescimento no número de usuários na rede blockchain, nos encontramos diante a uns grandes problemas de escalabilidade, que pode ser categorizado em taxa de transferência, custo e capacidade da rede. Neste trabalho iremos abordar o problema de escalabilidade com o *blockchain Bitcoin* e as promissoras propostas para solucionar essa questão, para que a solução seja a ideal seria necessária que ela alcançasse tal feito sem comprometer a descentralização e a segurança da rede. Com isso podemos verificar que tanto o *Bitcoin* como diversas criptomoedas que surgiram a partir do *blockchain* necessitam aperfeiçoar sua estrutura.



**Palavra-chave:** *Blockchain*; escalabilidade; solução; *bitcoin*; livro-razão

## ABSTRACT

In the last decade, Blockchain has become popular with its use in cryptocurrencies, where there is no third party involvement in the transactions. With the growth in the number of users on the blockchain network, we are faced with a major scalability problem, which can be categorized in throughput, cost and capacity of the network. In this work we will analyse the scalability problem with the Bitcoin blockchain and the promising proposals to solve this issue. So that the solution is ideal, it would be necessary for it to achieve this feat without compromising network decentralization and security. With this we can verify that both Bitcoin and several currencies that have emerged from the blockchain need to improve its structure.



**Keyword**: Blockchain; scalability; solution; Bitcoin; ledger

## LISTA DE FIGURAS

## LISTA DE ABREVIATURAS

| | |
|---|---|
| **BTC** | *Bitcoin*; |
| **P2P** | *Peer-to-Peer* ou Ponto a Ponto; |
| **SHA** | *Secure Hashing Algorithm* ou Algoritmo de Hash Seguro; |
| **MB** | *Megabyte*; |
| **USD** | *United States Dollar* ou Dólar dos Estados Unidos; |
| **US$** | Dólar; |
| **IBM** | *International Business Machines*; |
| **LN** | *Lightning Network;* |

**SUMÁRIO**

## 1. INTRODUÇÃO

Os pagamentos digitais estão cada vez mais acessíveis e populares para o público em geral, na década de 90, era possível observar diversos problemas, como por exemplo, *softwares* com interfaces pouco intuitivas, onde os bancos controlavam o mercado, ditando as tarifas, taxas, armazenando as informações de seus clientes e utilizando elas a favor deles. À medida que evoluímos ao longo dos anos, também evoluímos a maneira como trocamos bens e serviços. (MEDIUM, 2017).

No século 21, no entanto, obtivemos um grande avanço nos métodos de pagamentos, e agora os consumidores estão utilizando cada vez mais as carteiras digitais, que nos leva as famosas criptomoedas. A criptomoeda é uma forma de moeda virtual e descentralizada criada por sistemas computacionais que permite transações monetárias contínuas, assim como o real, mas são independentes de um Banco Central. As criptomoedas, como *Bitcoin* (BTC), utilizam tecnologia ponto a ponto (P2P) e *blockchain* para atuar como meio de troca.

Um dos desenvolvimentos mais relevantes para a economia mundial é a criptomoeda digital *Bitcoin*. Apesar do surgimento de vários tipos de criptomoedas estejam em operação, a mais popular é o *bitcoin*, que foi lançada e meados de 2009 por Satoshi Nakamoto. A revista Exame informou que em 2017, ano em que *bitcoin* ficou mundialmente conhecido, sua valorização aumentou 1.400%. (EXAME, 2017).

A arquitetura do blockchain é única, pois revoluciona a maneira como interagimos uns com os outros. O *blockchain* mostrou seu potencial com as moedas digitais fazendo com que suas transações sejam seguras e transparentes. Em seu nível mais básico, *blockchain* é literalmente apenas uma cadeia de blocos, quando dizemos as palavras “bloco” e “cadeia” neste contexto, estamos na verdade falando sobre informação digital (o “bloco”) armazenada em um banco de dados público (a “cadeia”). Descentralização de dados, transparência, segurança e imutabilidade são os princípios fundamentais da tecnologia.

Todos os nós que participam da rede devem processar as transações, o que requer um aumento no poder computacional podendo prejudicar seu princípio de descentralização. Os problemas de escalabilidade surgem devido ao tamanho do bloco limitado e o atual método de consenso em que cada nó da rede validar sequencialmente a transação antes de ser publicada no *blockchain*.

À medida que o *Bitcoin* amadurece, os engenheiros de *softwares* desenvolveram protocolos adicionais para melhorar a velocidade e a privacidade das transações *Bitcoin*. Diante deste cenário, a escalabilidade do *blockchain* se torna um problema para pesquisadores e programadores a ser solucionado, mostrando que a tecnologia ainda não tem capacidade para sua adoção global.

## 1.1. Objetivo

O objetivo deste trabalho é explicar os processos que levam uma transação ser registrada na criptomoeda *Bitcoin* com ênfase na estrutura de seu núcleo, o *blockchain*, após a compreensão de seu funcionamento, será realizado uma análise nos parâmetros e problemas relacionados a escalabilidade de fluxo, e também nas possíveis soluções para esse problema que fica cada vez mais em evidencia com o crescimento da rede.

## 1.2. Justificativa

O blockchain é a tecnologia por trás da estrutura das moedas digitais. Segundo Diniz (2017, p.47), “Ao operar como um livro de registros de transações on-line, o blockchain tem o potencial de revolucionar não apenas as finanças, mas toda a troca de informações em comunidades de negócios e grupos sociais.”. Para melhor compreendê-lo há a necessidade de um estudo abrangente de seu funcionamento, para então entender o que é de fato a “tecnologia blockchain” e sua relevância para o mundo.

Contudo, o blockchain ainda é uma tecnologia nova, e apesar de suas vantagens ainda possui “pontos” de preocupação para investidores e programadores da área, os quais necessitam ser melhorados para atingir a

eficiência ideal. E em meio a essa preocupação, esta pesquisa visa compreender o sistema por trás do *Bitcoin*. Além disso, analisar os parâmetros do *blockchain* e verificar os fatores que tornam a rede não escalável. E por fim, abordar os métodos que podem ser empregados para solucionar sua limitação.

## 1.3. Metodologia

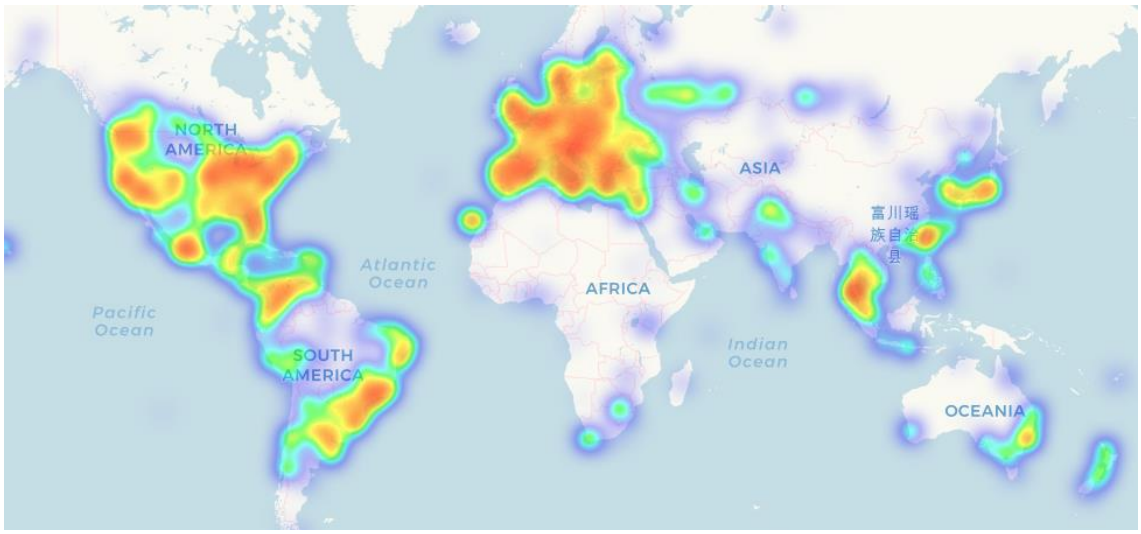
Inicialmente foi realizado um estudo onde consiste em explicar os processos que fazem uma transação ser registrada e validada nas criptomoedas *Bitcoin*, em seguida compreender o funcionamento do sistema distribuído *blockchain*, onde também será apresentada outras áreas para sua aplicação. Após compreensão do núcleo da tecnologia, será realizado um estudo dos parâmetros de escalabilidade com dados reais da carteira *blockchain*. Por fim, apresentar algumas soluções já empregadas no *Bitcoin* para tornar sua rede escalável.

## 2. CRIPTOMOEDAS

A origem do nome criptomoeda é bem evidente, sendo derivada de criptografia e moeda, ou seja, ela tem esse nome porque é uma moeda que utiliza vários algoritmos de criptografia e técnicas criptográficas para verificar as transações realizadas, também aumentando sua segurança as tornando mais difíceis de serem *hackeadas*. A criptomoeda é um sistema de pagamento descentralizado baseado na tecnologia do *blockchain*, onde qualquer pessoa poderá enviar ou receber pagamento sem a necessidade de um banco central, protegendo-as assim de manipulações por parte de terceiros, como do governo por exemplo. (INVESTOPEDI, 2020).

Com o crescente avanço em nossa tecnologia, empresas e consumidores tem dado preferencias para os pagamentos digitais, como *PicPay*, *Apple Pay* dentre outros, abrindo cada vez mais espaço para as criptomoedas, a figura 1 é um mapa de calor que nos apresenta a concentração dos estabelecimentos que aceitam a criptomoeda *Bitcoin*.

**Figura 1** - Estabelecimentos que aceitam Bitcoin




Fonte: *COIN MAP.* Disponível em: </coinmap.org/view/#/world/12.72608430/8.78906250/2>. Acesso em 9 out. 2020.

As criptomoedas enfrentam críticas por algumas razões, incluindo seu uso para atividades ilegais, volatilidade da taxa de câmbio e vulnerabilidades da infraestrutura. No entanto, eles também foram elogiados por sua portabilidade,

divisibilidade, resistência à inflação e transparência. A primeira e mais popular das criptomoedas baseadas no *blockchain* é o *Bitcoin*.

## 2.1. Bitcoin

O *Bitcoin* é uma moeda digital criada em janeiro de 2009 por um programador anônimo ou um grupo de programadores sob o pseudônimo de Satoshi Nakamoto, onde apresentaram o *Bitcoin* como um “sistema de caixa eletrônico ponto a ponto” e totalmente descentralizado. É a primeira rede de pagamento ponto a ponto descentralizada que é alimentada por seus usuários sem nenhuma autoridade central ou intermediários. (BITCOIN, 2020).

Antes do surgimento do *Bitcoin*, houve diversas tentativas de criar uma moeda digital, mas não obtiveram sucesso. Uma das primeiras moedas inventadas foi o *E-gold*, e os motivos de seu fracasso foram vários, como vulnerabilidade a fraudes e o problema de gasto duplo, onde resumidamente o usuário tenta utilizar o valor de uma transação mais de uma vez.

Uma moeda digital é aquela que pode ser facilmente armazenada e usada em um computador. Por essa definição, até mesmo dólares podem ser considerados uma moeda digital, uma vez que podem ser facilmente enviados a outras pessoas ou usados para fazer compras *online*, mas seu fornecimento é controlado por uma organização bancária centralizada. “(Conrad Barski and Chris Wilmer, 2015, p.1)

Ao longo dos anos, muitas pessoas afirmaram publicamente ser Satoshi, todas falhando em apoiar a declaração com fatos indiscutíveis, a verdadeira identidade ou identidades por trás de Satoshi permanece oculta.

Mas porque Nakamoto decidiu manter em anonimato com uma super invenção em suas mãos? Podemos entender que ao criar um protocolo sem ponto central falha, ele pode ter percebido que teria de tratar o último ponto de falha possível, a própria pessoa que o criou. Sem conhecer a entidade que a criou, a criptomoeda estará imune da influência e manipulação de interesses.

Por que alguém usaria *Bitcoin*? Uma das principais vantagens é a possibilidade de envio e recebimento de pagamentos em qualquer lugar do mundo de modo fácil, rápido e seguro, já que para um *hacker* roubar endereços de *Bitcoin* é completamente inútil porque para uma transação ser válida, ela deve ser assinada com sua chave privada associada, e o usuário não precisa compartilha-la para efetuar o pagamento.

“Graças a todos os seus benefícios, o *Bitcoin* continua a aumentar em popularidade; no entanto, qualquer pessoa familiarizada com o *Bitcoin* concordará que a tecnologia por trás dele é difícil de explicar e entender. À primeira vista, é difícil entender como os *bitcoins* são armazenados, como são usados ou mesmo de onde vêm. “(Conrad Barski and Chris Wilmer, 2015, p.3).

## 3. BLOCKCHAIN

O nome vem de sua estrutura, na qual os registros são chamados de blocos, e são vinculados em uma única lista chamada de cadeia. O *Blockchain* é utilizado atualmente para registrar transações feitas com criptomoedas, como o *Bitcoin*, dentre outras aplicações.

"O *blockchain* tem recebido muita atenção na discussão pública e na mídia. Alguns entusiastas afirmam que o *blockchain* é a maior invenção desde o surgimento da *Internet*." (DRESCHER, 2017, p.7)

Um *blockchain* é basicamente um livro-razão, nome que se dá para o principal agrupamento de registros contabilísticos de uma empresa, no caso do *blockchain* este livro é digital e replicado para toda a rede, cada transação adicionada é validada por vários computadores na *internet* e cada bloco da cadeia contém várias transações, sempre que ocorrer uma nova transação na cadeia de blocos, um registro dessa transação é adicionada ao livro-razão, dessa forma todos os participantes da rede trabalham juntos para garantir que cada transação seja válida antes de ser adicionada ao *blockchain*, vinculando-a nos blocos anteriores.

Isso significa que se um bloco na cadeia for alterado, seria imediatamente aparente para os demais participantes da rede essa alteração, dessa forma garante que a corrente nunca seja quebrada e que cada bloco seja registrado permanentemente tornando-o difícil ou impossível alterar, *hackear* ou trapacear o sistema, uma vez que todos os blocos subsequentes devem ser alterados primeiro. Se um *hacker* decidir corromper o sistema, teria que mudar pelo menos 51% da cadeia.

Resumidamente, antes de uma transação ser adicionada ao *blockchain*, ela deve ser autenticada e autorizada.

## 3.1. Autenticação:

O *blockchain* originalmente foi projetado para operar sem uma autoridade central, ou seja, não há a necessidade de um banco para controlar e validar as transações, mas elas ainda sim precisam ser autenticadas.

Isto é feito utilizando chaves criptográficas, cada usuário tem sua própria chave privada e pública que todos podem visualizar. O uso de ambos cria uma identidade digital segura para autenticar o usuário por meio de assinaturas digitais e para “desbloquear” a transação que deseja realizar.

### 3.1.1. Autorização:

Quando uma transação ocorre entre os usuários, ele precisa ser aprovada ou autorizada antes de ser adicionada a cadeia de blocos.

Para uma *blockchain* pública, a decisão de adicionar uma transação à cadeia é feita por consenso. Isso significa que a maioria dos “nós” ou computadores na rede devem concordar que a transação é válida. Os proprietários dos computadores da rede são incentivados a verificar as transações por meio de recompensas. Este processo é conhecido como prova de trabalho.

A razão pela qual o *blockchain* ganhou tanta admiração é:

• Não é propriedade de uma única entidade, portanto é descentralizado.

• Os dados são armazenados criptograficamente.

• O *blockchain* é imutável, então ninguém pode adulterar os dados que estão dentro do *blockchain*.

• O *blockchain* é transparente, os dados são visíveis a todos os integrantes da rede.

## 3.2. Os três pilares da tecnologia *Blockchain*.

As três principais propriedades da Tecnologia *Blockchain* que fizeram com que ganhasse tanto destaque são: Descentralização, transparência e imutabilidade. (BLOCKGEEK, 2020)

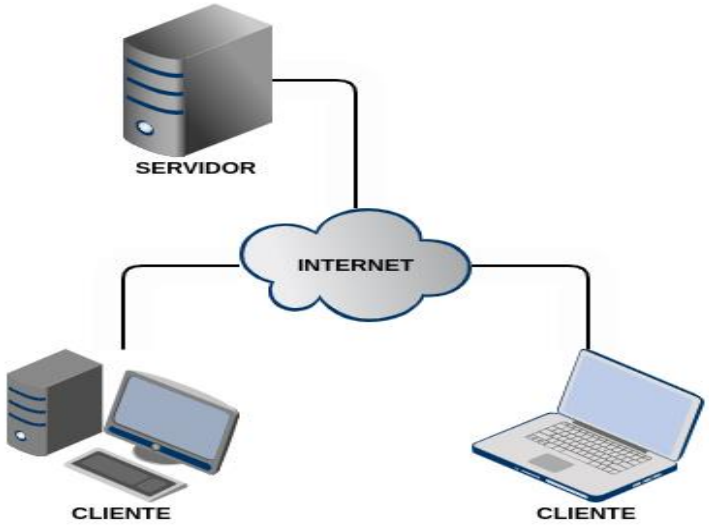
### 3.2.1. Descentralização

A descentralização se refere ao grau de diversificação da propriedade, influência e valor no *blockchain*. Em geral, as criptomoedas são “descentralizadas”, pois não há uma única entidade que possa controlar toda a rede.

Antes do surgimento das criptomoedas, a sociedade estava acostumada com os serviços centralizados, onde é tudo muito simples. Se tem uma entidade centralizada, por exemplo um banco central, que armazena todos os dados e seu dinheiro, deve-se interagir exclusivamente com essa entidade para obter as informações necessárias para se realizar as transações.

O modelo cliente-servidor tradicional apresentado na figura 2 é um exemplo perfeito. Quando realizamos uma pesquisa na internet, enviamos uma consulta ao servidor, que então nos responde com as informações solicitadas.

**Figura 2** – Exemplo simples de um modelo cliente-servidor




Fonte: Elaborado pelo autor.

Embora utilizemos os sistemas centralizados, pode-se notar diversos problemas com eles. Justamente por serem centralizados, todas as informações são armazenas em um único local, correndo um grande risco de perda de informação e se tornando um alvo visado pelos *hackers*.

E se a entidade central deixar de existir por algum motivo inesperado? Se isso acontecer todas as informações serão perdidas, pois estavam armazenadas por uma única entidade central.

Com a rede descentralizadas não temos esse risco, pois todos possuem as informações contidas na rede, essa é a uma das vantagens quando não se tem as informações armazenadas em um único local.

Com a rede descentralizada, caso queira realizar uma transferência de dinheiro para outro usuário, não será necessário a interação do banco nesta transação. Esta é a principal ideologia do *Bitcoin*.

### 3.2.2. Imutabilidade

Imutabilidade no *blockchain* significa que uma vez que a informação for transferida para a rede, não pode ser adulterada. A razão pela qual o *blockchain* obtém essa propriedade é a função *hash* criptográfica. Por causa da propriedade do *hash*, qualquer alteração realizada em algum bloco mudará drasticamente o *hash*.

### 3.2.3. Transparência

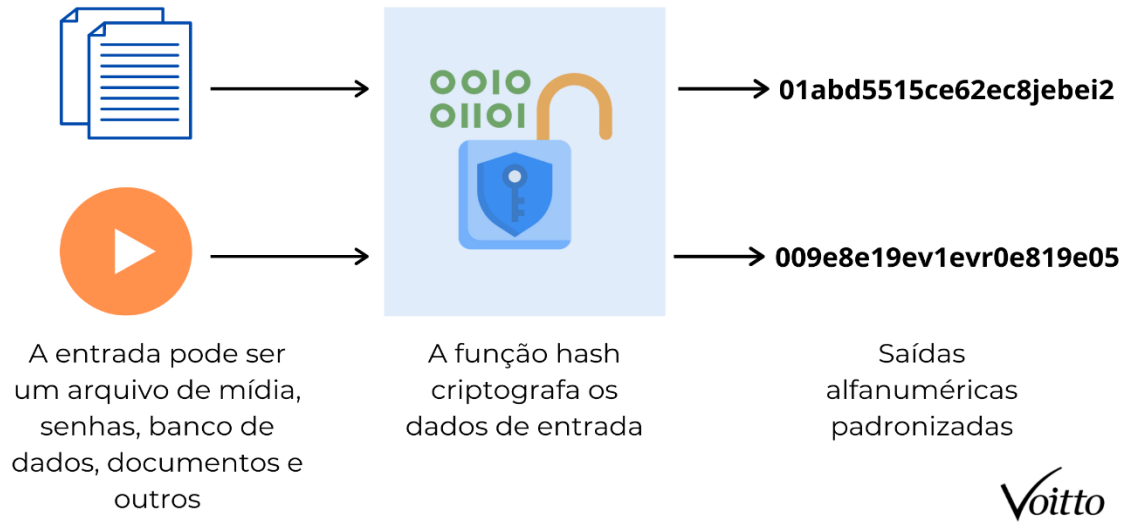
Outro conceito muito importante do *blockchain* é sua transparência. Conforme mencionado anteriormente, todas as transações são visíveis na rede. Ter os mesmos registros espalhados por uma grande rede para que todos vejam é a alma da transparência do *blockchain*, o que significa que ninguém pode tentar manipular, alterar ou remover qualquer um dos dados que foram armazenados, uma vez que tenham sido validados pela rede. Se a transação fosse alterada na rede, todos os outros blocos do sistema também precisariam ser alterados, o

que torna impossível todo o processo de alteração das transações. É também por isso que o *blockchain* é considerado resistente a *hackers*.

### 3.3. Hashes

*Hash* é uma sequência única de comprimento fixo de dígitos aleatórios escritos de forma hexadecimal, que pode ser criada a partir de dados de qualquer tamanho. Cada *hash* é criado com o auxílio de um algoritmo duplo-SHA-256 (*Secure Hashing Algorithm* -256 *bits*), que cria um número randômico de 512 *bits* (ou 64 *bytes*), sendo assim o *hash* não é uma criptografia qualquer, pois não podemos recuperar os dados originais descriptografando ele, portanto é uma criptografia unilateral. (BLOCKGEEK, 2020). Resumindo a explicação, o funcionamento do *hash* pode ser visualizado na figura 3:

**Figura 3** – Exemplo do funcionamento do *hash*



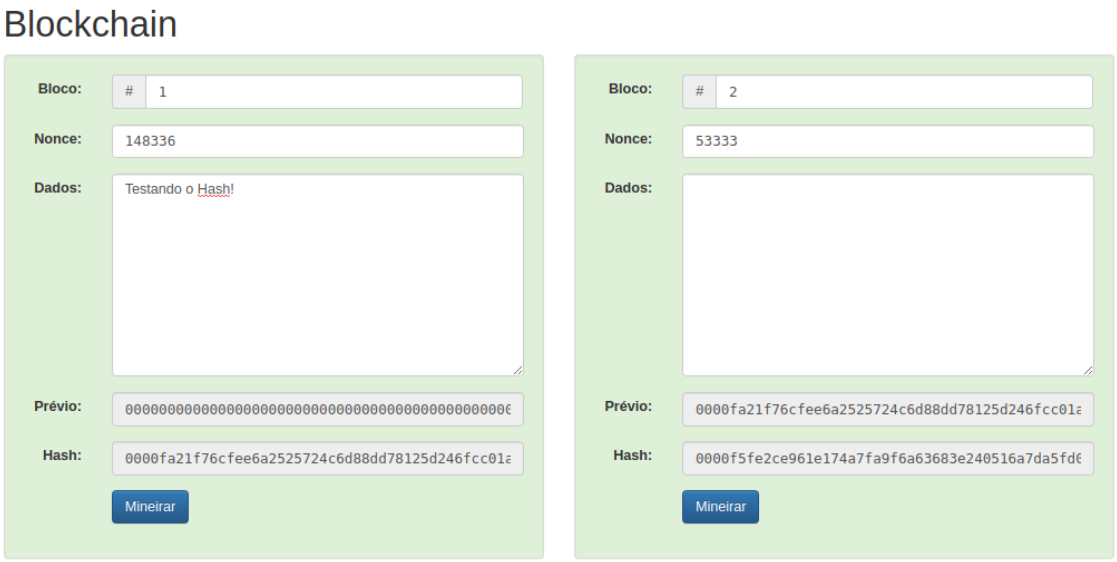

Fonte: Voitto. Disponível em: < https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona>. Acesso em 28 out. 2020

No *Blockchain*, cada bloco tem um *hash* do bloco anterior, o bloco anterior é chamado de bloco pai para o bloco atual, e o bloco atual será o pai do próximo contendo também seu *hash*. Quando alteramos qualquer dado no bloco atual, o *hash* do bloco será alterado, isso afetará o bloco anterior e de todos os blocos

subsequentes. Com isso o *hashing* é um dos fundamentos centrais para a integridade do *blockchain*, dado a ele a propriedade de imutabilidade, uma vez que os dados não podem ser alterados ele preserva a veracidade das informações armazenadas, sendo essencial para o gerenciamento do *blockchain* em criptomoedas.

Na figura 4 abaixo temos ilustrado o funcionamento do *hash*, o bloco um contêm os seguintes dados “Testando o *Hash*!”, por ser no bloco gênesis sua prévia não contém um valor de *hash*, pois ele é o primeiro de nossa cadeia, mas contêm seu próprio *Hash*. No segundo bloco não temos dados adicionados a ele, e pode-se verificar que nele contêm o valor de *hash* do bloco gênesis e seu próprio valor de *hash*.

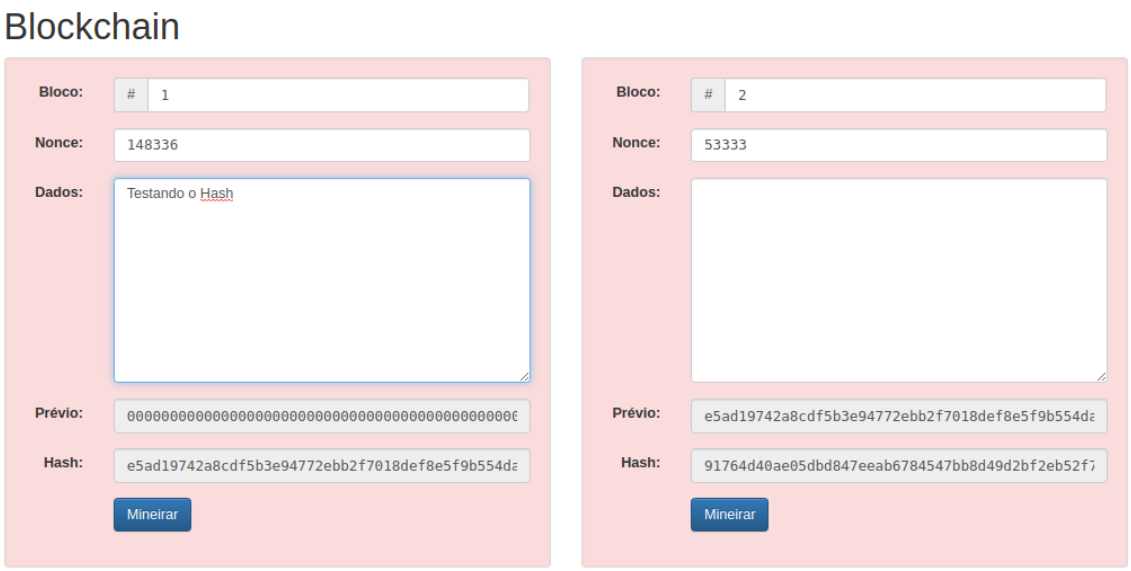
**Figura 4** – Representação de um bloco com dados inseridos




Fonte: *Demo* do *Blockchain.* Disponível em: </andersbrownworth.com/blockchain/blockchain>. Acesso em 10 out. 2020.

Em seguida podemos verificar o que acontece se alterarmos qualquer detalhe por menor que seja e aplicarmos a função *hash*. O *hash* resultante é totalmente diferente da entrada como podemos verificar na figura 5:

**Figura 5** – Alteração dos dados resulta em um *hash* diferente




Fonte: *Demo* do *Blockchain.* Disponível em: </andersbrownworth.com/blockchain/blockchain>. Acesso em 10 out. 2020

O valor resultante do *hash* após a alteração é completamente diferente do *hash* anterior e afetando os blocos subsequentes, apesar de haver uma pequena mudança nos dados de entrada, afetando também o bloco “filho”. Isso mudará completamente a cadeia, assim fica fácil identificar um arquivo alterado.

## 3.4. Mineradores

Com um *blockchain* público, os mineiros têm a liberdade de ir e vir. Há um incentivo econômico para que protejam a rede e contribuam para o consenso, em vez de tentar trapacear o sistema. O valor da unidade de conta da *blockchain* pública, no nosso caso *Bitcoin*, é o *driver* por trás do incentivo econômico. (CAETANO, 2015, p. 152).

Acontece que atrair uma forte rede de mineradores é realmente difícil, o que prova seu valor intrínseco. Com um forte incentivo econômico, como o *Bitcoin*, seria um desafio atrair uma rede pública de “nós” cujo interesse é proteger a rede. (CAETANO, 2015, p. 152).

A mineração é um processo de adicionar registros de transações ao livro-razão público do *Bitcoin* chamado *blockchain*. A mineração é realizada por

computadores de alta potência que resolvem os problemas matemáticos complexos que não podem ser resolvidos manualmente. O papel dos mineiros é proteger a rede e processar todas as transações.

O que atrai novos mineradores é a possibilidade de serem recompensados com a própria moeda *Bitcoin,* sem ter que pagar diretamente para obtê-la, pois cada tentativa de mineração consome poder de processamento, energia e consequentemente dinheiro, em Outubro de 2017, a recompensa era de 12,5 *Bitcoins* por bloco, e em maio de 2020 o valor foi reduzido à 6,25, o minerador recebe esse valor quando encontrar um *hash* válido.

Abaixo na figura 6 temos um gráfico que mostra a receita das mineradoras como porcentagem do volume de transações sendo evidente sua redução.

**Figura 6** – Porcentagem de custo de volume de transações


Fonte: Blockchain.com. Disponível em: <blockchain.com/charts/cost-per-transaction-percent>. Acesso em 12 out. 2020

## 3.5. Forks

Devido à sua natureza independente, a rede de “nós” pode consistir em “nós” honestos ou maliciosos. “Nós” honestos apenas aceitam transações válidas e rejeitam qualquer um que duplique o gasto ou tenha assinaturas inválidas. “Nós” maliciosos podem tentar aceitar uma transação corrompida ou rejeitar seletivamente as outras transações. (CAETANO, 2015, p. 93).

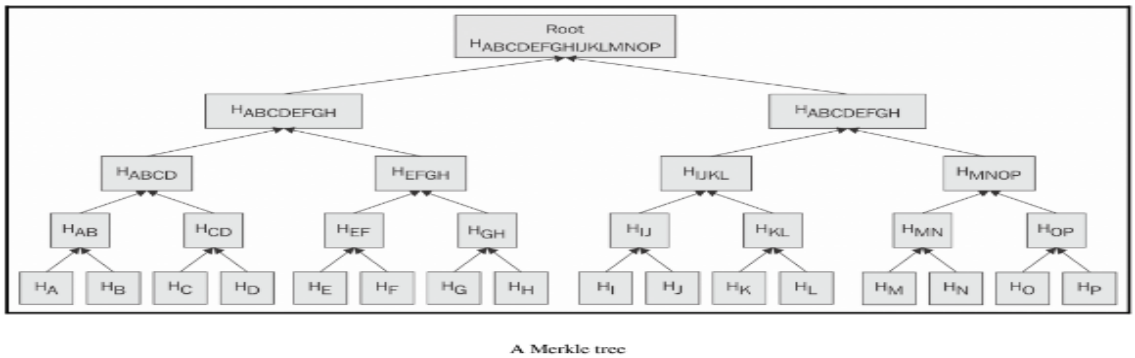
Para isolar e rejeitar os “nós” inválidos na rede, existe um consenso entre os “nós” sobre qual conjunto de regras aceitar. Esse consenso determina quais blocos são aceitos na rede. Desde o bloco de gênese, a grande maioria dos “nós” concordaram em "jogar limpo" ao invés de se corromper, devido à recompensa de ganhar novos *bitcoins*. Esse consenso forma uma cadeia mais longa e confiável. (CAETANO, 2015, p. 93)

## 3.6. Árvores de Merkle

O conceito de árvore Merkle foi introduzido por Ralph Merkle. Uma visualização da árvore Merkle é mostrado aqui, o que torna mais fácil de entender. Árvores Merkle permitem segurança e eficiência verificação de grandes conjuntos de dados. (BASHIR, 2017, p. 95)

É uma árvore binária na qual primeiro, as entradas são colocadas nas folhas (nó sem filhos), e então os valores dos pares de nós filhos são misturados para produzir um valor para o nó pai (nó interno) até que um único valor *hash* conhecido como raiz Merkle seja alcançado: (BASHIR, 2017, p. 95)

**Figura 7** - Uma árvore Merkle




A Merkle tree

Fonte: (BASHIR, 2017, p. 95. *Mastering Blockchain*)

## 3.7. Prova de Trabalho

Este tipo de mecanismo de consenso se baseia na prova de que recursos computacionais suficientes foram gastos antes de propor um valor para aceitação pela rede. Isso é usado em *bitcoin* e outras criptomoedas. Atualmente,

este é o único algoritmo que provou surpreendentemente bem-sucedido contra ataques de *Sybil*. (BASHIR, 2017, p. 28).

Resumidamente, em um ataque *Sybil* o invasor cria um grande número de identidades “fantasma” e as utiliza para obter uma grande influência sobre algum serviço. No caso do *blockchain*, utilizaria as identidades (nós) falsas para manipular as transações.

Os mineiros competem pela recompensa do *Bitcoin* enviando uma "prova de trabalho" para o rede. Gerar a prova de trabalho envolve o cálculo de um valor *hash* no bloco. O minerador está procurando o menor valor de *hash* possível. (CAETANO, 2015, p. 96)

O valor alvo, denominado dificuldade, é divulgado pela rede. Se o valor *hash* de o novo bloco é menor do que o valor de dificuldade publicado, então o minerador encontrou uma solução válida que é elegível como prova de trabalho. (CAETANO, 2015, p. 96)

Blocos são aceitos na rede conforme outros mineiros confirmam a prova de trabalho. (CAETANO, 2015, p. 96)

## 3.8. Mempool

O *Mempool* é uma “área de espera” para transações *Bitcoin*, onde elas aguardam para serem confirmadas pela rede *Bitcoin*. Ao verificar o tamanho do *mempool*, pode-se analisar quanto tempo terá o congestionamento de transferência na rede que resulta em tempos de confirmação mais lentos e aumento no valor das taxas. (BLOCKCHAIN, 2020).

As transações não confirmadas aguardam no mempool para serem compensadas. Normalmente, uma transação fica presa no mempool quando a taxa de transação incluída com a transação é muito baixa. (EXODUS, 2020).

Em termos mais simples, as transações no mempool são como compradores esperando para comprar um produto quando o preço estiver baixo o suficiente. (EXODUS, 2020).

Se a demanda diminuir, os preços cairão e essas confirmações do mempool começarão a ser incluídas nos blocos. Se a demanda aumentar, as taxas de transação de Bitcoin aumentam e consequentemente o número de transação no mempool também aumentará.

### 3.11.1. Algumas das possibilidades de aplicação do Blockchain

### 3.11.2. Transferência de dinheiro:

Provavelmente este seja o uso mais popular do *blockchain*, pois sua utilização no financeiro foi o que conceituou a tecnologia, como já mencionado, traz diversas vantagens para transferência de dinheiro, sem a necessidade de um banco central para validar a transação. Alguns bancos estão visando a utilização do *blockchain* em suas transações, como exemplo, temos o Santander que se uniu à Ripple, uma empresa de pagamentos em *blockchain* e criptomoeda, com o propósito de melhorar o processo de transações internacionais "podendo torná-las mais rápidas, baratas e transparentes.", disse Ed Metzger, CTO da One Pay FX em nota divulgada pela Ripple em 9 de julho.

### 3.11.3. Rede de alimentos:

*Blockchain* pode ser usado para gerenciar a cadeia de suprimentos de forma segura e transparente. Essa tecnologia já vem sendo utilizada pelo *Walmart*, em parceria com a IBM, e na prática, é aplicada para rastrear e controlar o caminho dos alimentos até os consumidores, assim gerando um controle excelente de qualidade, desde o local de origem até o varejo. (IBM, 2020).

### 3.11.4. Eleições e sistema público

A tecnologia pode revolucionar o setor público com mais transparência, visibilidade e segurança, diminuindo também a corrupção.

Permitindo eleições mais seguras, evitando fraudes e oferecendo a capacidade de votar digitalmente, em 3 de novembro de 2020 a agência de notícias *Associated Press* publicou os resultados das eleições presidenciais dos Estados Unidos nos blocos *Ethereum*, tornando assim o processo de divulgação mais seguro e dificilmente mutável, possibilitando também a visualização em tempo real dos votos.

### 3.11.5. *Backup* de dados imutáveis

Pode ser uma maneira eficiente para o uso da *blockchain*, aumentando ainda mais a segurança dos meios de *backups* que possuímos, mesmo com o armazenamento em nuvem sendo extremamente seguros, não estão imunes a ataques de *hackers* para alteração dos dados.

### 3.11.6. Rastreamento de medicamentos controlados

Além de armazenar os registros do paciente, o usuário que possui a chave para acessar esses registros digitais estaria no controle de quem tem acesso a esses dados na rede, podendo também ser útil no rastreamento de medicamentos de forma transparente e inibir a falsificação de receitas médicas. Merck KGaA é uma empresa alemã da indústria química e farmacêutica que está testando o sistema *blockchain* para devolução de medicamentos controlados.

### 3.11.7. IDs digitais:

É fato que hoje nossa identidade possui mias dados do que imaginamos, a *Microsoft* acredita que todas as pessoas têm o direito de possuir uma identidade digital própria, de modo que possamos guardar os dados de maneira mais segura, e isso será possível com a identidade descentralizada substituindo os identificadores, como o nomes de usuário, por IDs próprios e independentes utilizando a *blockchain*.

Embora o *blockchain* esteja longe de ser perfeita para sua utilização, ela certamente tem muitas aplicações para o mundo real além das citadas neste trabalho.

# 4. PARÂMETROS DE ESCALABILIDADE

## 4.1. Latência

A latência na computação se refere ao atraso de tempo entre uma entrada e a saída recebida. Latência na rede *blockchain* resumidamente é o tempo necessário para gerar o próximo bloco, pode ser considerado qualquer atraso na propagação dos blocos. Quanto menor o tempo de confirmação das transferências na rede, menor será a sua latência e consequentemente uma propagação mais rápida.

Latência também pode ser como "tempo de bloqueio", que é o tempo que o usuário espera para sua transação aparecer na *blockchain* após confirmar seu envio

## 4.2. Throughput

*Throughput* (taxa de transferência é a quantidade de dados transferidos de um lugar a outro) do sistema *blockchain* é definido em termos do número de transações confirmadas por segundo. O *Bitcoin* tem uma taxa de transferência de 7 transações por segundo.

## 4.3. Custo de transação

A custo por transação tem um impacto direto no tempo de confirmação, pois seu custo está diretamente associado a velocidade de banda, tamanho da rede e esforço dos mineradores, afetando assim a latência e consequentemente a escalabilidade da rede.

## 4.4. Tamanho do bloco

Atualmente o tamanho do bloco no Bitcoin é fixo em um 1Mb.

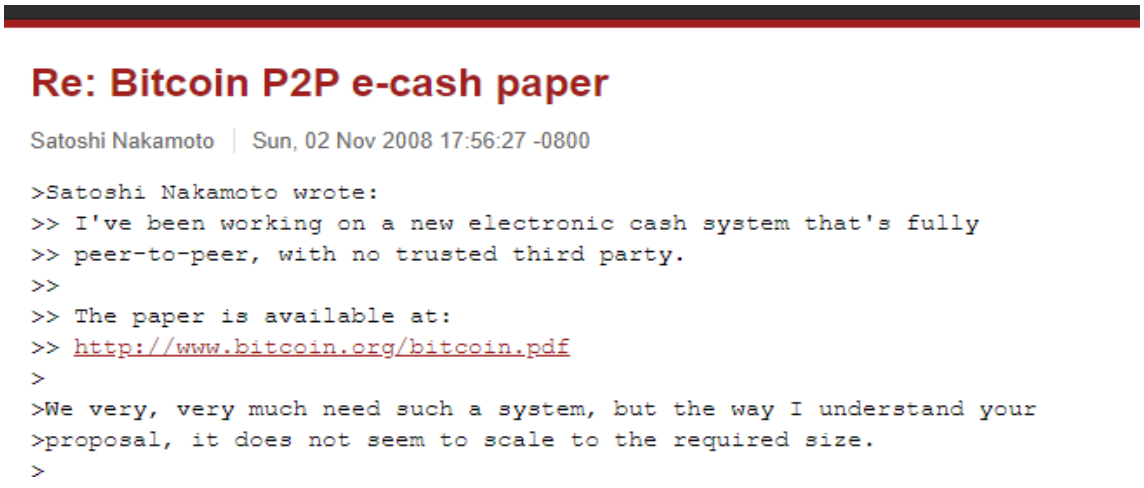
## 5. Escalabilidade

A escalabilidade é o maior problema do *blockchain* conforme seu crescimento nos últimos anos, se tornando o foco principal dos programadores e profissionais da área e investidores desde que o *Bitcoin* surgiu em 2009.

Escalabilidade é o quanto a tecnologia é capaz de crescer com o número de usuários, mas mantendo a qualidade do serviço sem aumentar seu custo, um exemplo atual de tecnologia escalável é a *internet*. Quando se trata de escalabilidade relacionada a *blockchain* falamos do aumento de sua capacidade de lidar com as transações sem aumentar seu custo por transação. O problema da escalabilidade surge devido ao tamanho limitado dos blocos que está diretamente relacionado com o número de transações, que é proporcional a queda na escalabilidade do *blockchain*. Como mencionado anteriormente, mais da metade dos nós na rede *Bitcoin* precisa concordar que uma transação é válida antes de ser adicionada ao *blockchain*. Quanto mais nós houver na rede, mais tempo levará para chegar a um acordo ou consenso.

Desde os primeiros e-mails de Nakamoto em 2008 apresentado na figura 8, já era mencionado o problema de escalabilidade do *Bitcoin*. “Precisamos muitíssimo desse sistema, mas pelo que entendo sua proposta, não parece escalar para o tamanho necessário.” Satoshi Nakamoto.

**Figura 8** – E-mail de Satoshi Nakamoto



**Re: Bitcoin P2P e-cash paper**

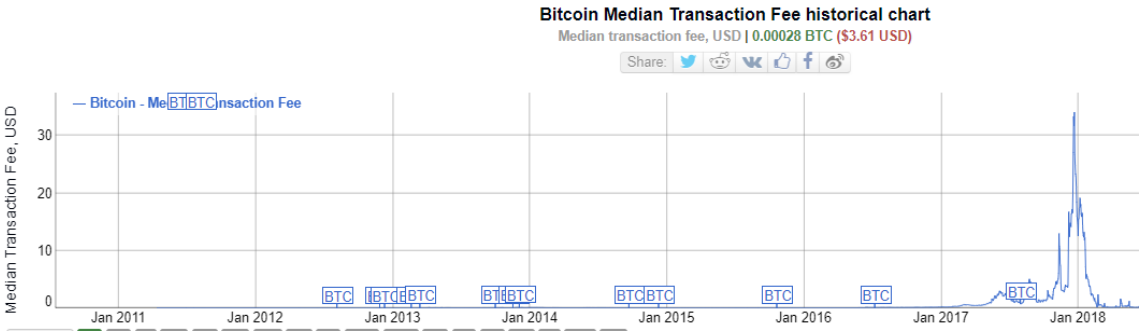
Satoshi Nakamoto | Sun, 02 Nov 2008 17:56:27 -0800

```
>Satoshi Nakamoto wrote:
>> I've been working on a new electronic cash system that's fully
>> peer-to-peer, with no trusted third party.
>>
>> The paper is available at:
>> http://www.bitcoin.org/bitcoin.pdf
>
>We very, very much need such a system, but the way I understand your
>proposal, it does not seem to scale to the required size.
>
```

Fonte: TheMailArchive. Disponível em: <mail-archive.com/cryptography@metzdowd.com/msg09964.html>. Acesso em 26 out. 2020

Mas apenas em 2018 o problema ficou evidente, onde as transações chegaram a um valor médio superior a 30 dólares.

**Figura 9** - Gráfico histórico da taxa de transação mediana de bitcoin




Fonte: BitInfoCharts. Disponível em: <bitinfocharts.com/comparison/bitcoin-median_transaction_fee.html>. Acesso em 27 out. 2020.

Os blocos do *Bitcoin* contêm as transações da rede, com um tempo médio de 10 minutos para a criação de um novo bloco com o tamanho de 1Mb. Isso, em conjunto, dificulta a taxa de transferência da rede. O ditado comum de que "*bitcoin* não é escalável" concentra-se principalmente em sua taxa de transferência, ou seja, é pelo fato dele conseguir lidar com apenas 7 transações por segundo, podemos considerar um tempo relativamente baixo se compararmos com outras carteiras digital como o *Paypal* por exemplo, onde a transferência geralmente leva alguns segundos ou minutos, mas podendo chegar a demorar trinta minutos ou até mesmo dois dias caso o pagamento entre em análise pela ferramenta.

E com essa questão os pesquisadores vem estudando inúmeras formas para solucionar o problema. As possíveis soluções que serão apresentadas a seguir são: *On-chain* (Na cadeia), *Off-chain* (Fora da cadeia), *Lightning Network, Side-chain* (Cadeia lateral), *SegWit* e *Sharding* (Fragmentação). Também será realizado a análise dessas propostas sobre a capacidade de solucionar o problema e destacar os pontos negativos se houver. Mas lembrando que pontos negativos podem surgir conforme os estudos com o passar dos anos.

## 5.1. Análise de Métricas de Escalabilidade

Vamos verificar alguns parâmetros do *blockchain* e realizar uma análise sobre eles para melhor compreensão. Os dados foram coletados do *blockchain*.info uma fonte confiável que nos apresenta informações gráficas do *blockchain*, sendo utilizado o filtro de 1 ano com média de 30 dias.

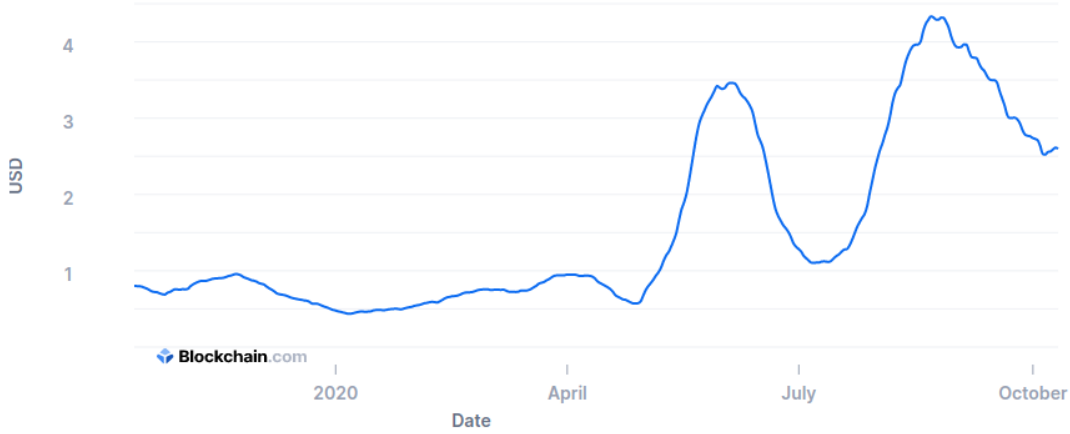
**Figura 10** – Média do tempo de confirmação


Fonte: Blockchain.com. Disponível em: <blockchain.com/charts/avg-confirmation-time>. Acesso em 12 out. 2020.

O gráfico acima na figura 10 mostra a média do tempo de confirmação para que uma transação seja incluída em um bloco minerado e adicionada na *blockchain*, podemos verificar oscilações expressivas durante o ano de 2020, onde do começo para o final do ano a média de tempo aumentou aproximadamente 5 vezes.

O gráfico a seguir na figura 11 nos mostra a taxa de transação em USD.

**Figura 11** – Taxas totais de transação




Fonte: Blockchain.com <blockchain.com/charts/transaction-fees>. Acesso em 12 out. 2020.

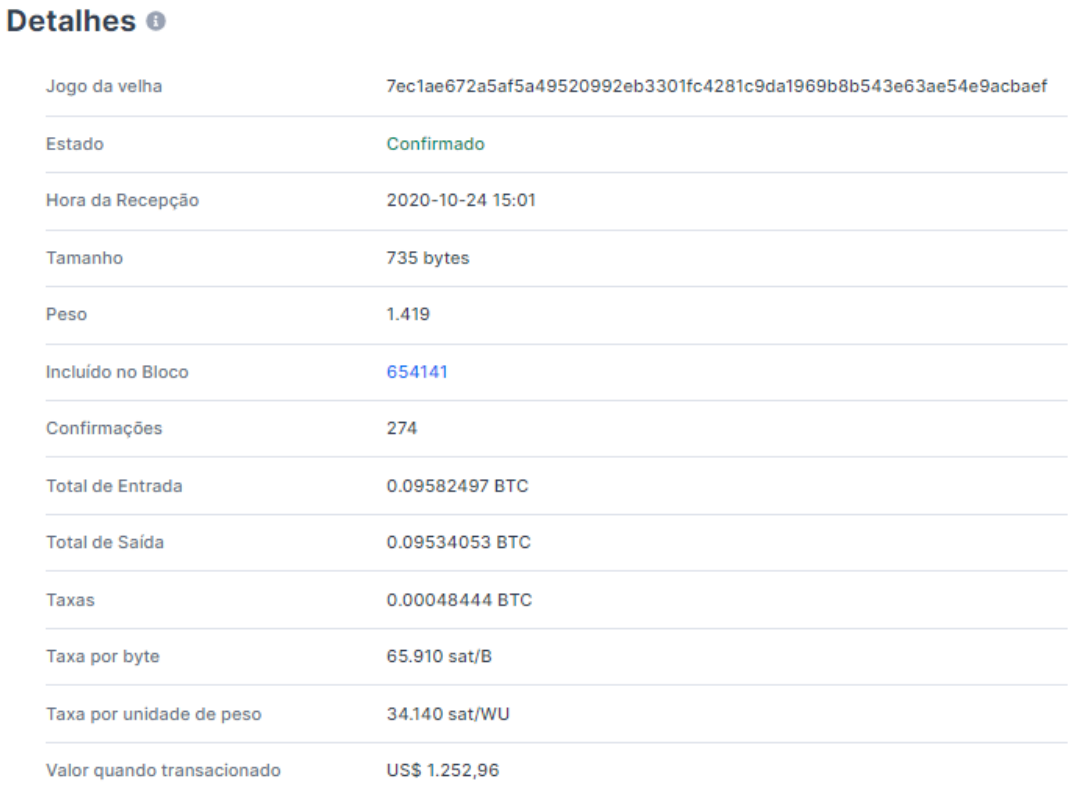
A taxa da transação desempenha um papel importante na decisão dos horários de confirmação de uma transação. É o único maior incentivo para um minerador minerar uma transação específica e incluí-la em um bloco.

Podemos ver com clareza semelhança em ambos os gráficos, os que nos leva a concluir:

- O valor cobrado por transação é diretamente proporcional ao tempo de confirmação. Como já mencionado anteriormente quanto maior o tempo de confirmação maior será o valor cobrado para que a transação seja concluída mais rapidamente, pode-se dizer que é a famosa lei da “oferta e demanda”.

A seguir temos um exemplo real da importância da escalabilidade em relação a taxa de transferência, vamos analisar a transação presente na figura 12 realizada no dia 24 de outubro de 2020.

**Figura 12** – Transação de Bitcoin



**Detalhes**

| | |
|---|---|
| Jogo da velha | 7ec1ae672a5af5a49520992eb3301fc4281c9da1969b8b543e63ae54e9acbaef |
| Estado | Confirmado |
| Hora da Recepção | 2020-10-24 15:01 |
| Tamanho | 735 bytes |
| Peso | 1.419 |
| Incluído no Bloco | 654141 |
| Confirmações | 274 |
| Total de Entrada | 0.09582497 BTC |
| Total de Saída | 0.09534053 BTC |
| Taxas | 0.00048444 BTC |
| Taxa por byte | 65.910 sat/B |
| Taxa por unidade de peso | 34.140 sat/WU |
| Valor quando transacionado | US$ 1.252,96 |

Fonte: Blockchain.com <blockchain.com/pt/btc/tx/7ec1ae672a5af5a49520992eb3301fc4281c9da1969b8b543e63ae54e9acbaef>. Acesso em 24 out. 2020

Para realizar a conversão do *bitcoin* para dólar vamos considerar o valor da criptomoeda no dia em que a transação ocorreu, obtendo a seguinte informação:

Total de Entrada: 0.09582497 BTC = US$ 1257,70

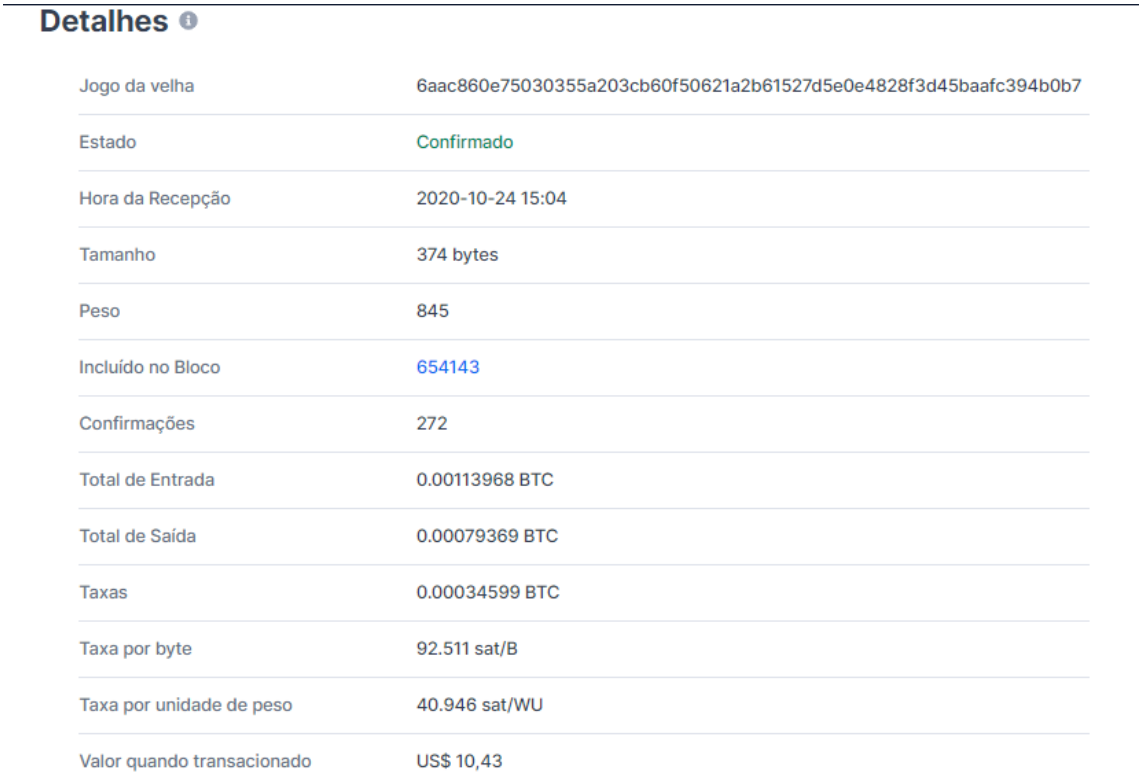
Total de Saída: 0.09534053 BTC = US$ 1251,34

Taxas: 0.00048444 BTC = US$ 6,36

Valor quando transacionado = US$ 1.252,96

A taxa de transferência foi de US$ 6,36, comparado com o valor transacionado essa taxa pode ser considerada em um valor “aceitável”. A figura 13 apresenta outra transferência realizada no mesmo dia e horário, mas com um valor transferido consideravelmente menor.

**Figura 13** – Transação de Bitcoin



**Detalhes**

| | |
|---|---|
| Jogo da velha | 6aac860e75030355a203cb60f50621a2b61527d5e0e4828f3d45baafc394b0b7 |
| Estado | Confirmado |
| Hora da Recepção | 2020-10-24 15:04 |
| Tamanho | 374 bytes |
| Peso | 845 |
| Incluído no Bloco | 654143 |
| Confirmações | 272 |
| Total de Entrada | 0.00113968 BTC |
| Total de Saída | 0.00079369 BTC |
| Taxas | 0.00034599 BTC |
| Taxa por byte | 92.511 sat/B |
| Taxa por unidade de peso | 40.946 sat/WU |
| Valor quando transacionado | US$ 10,43 |

Fonte: Blockchain.com. Disponível em: <blockchain.com/pt/btc/tx/6aac860e75030355a203cb60f50621a2b61527d5e0e4828f3d45baafc394b0b7>. Acesso em 24 out. 2020

Convertendo os valores de *Bitcoin* para dólar:

Total de Entrada: 0.00113968 BTC = US$ 14,96

Total de Saída: 0.00079369 BTC = US$ 10,42

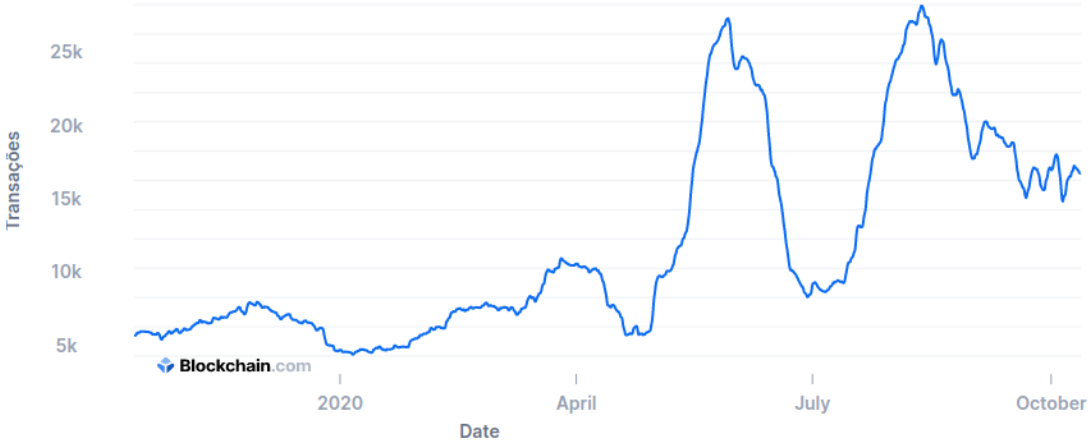
Taxas: 0.00034599 BTC = US$ 4,54

Valor quando transacionado = US$ 10,43

Como pode ser verificado o valor transacionado foi de 10,43 dólares, e sua taxa foi de 4,54 dólares, praticamente metade do valor transferido para outra carteira. Apesar de que na figura 12 o valor transacionado ser mais de cem vezes maior, a taxa de transferência é muito semelhante. Sendo questionável o uso da moeda para pequenas transações, como por exemplo, realizar compras em pequenos comércios ou até mesmo comprar aquele “cafezinho”, já que o valor da taxa pode ser superior ao da compra realizada.

Na figura 14 temos o gráfico que nos apresenta o número total de transações não confirmada no mempool e na figura 15 o tamanho médio do bloco durante o ano.

**Figura 14** – Contagem de transação no mempool




Fonte: Blockchain.com. Disponível em: <blockchain.com/charts/mempool-count>. Acesso em 12 out. 2020.

**Figura 15** – Tamanho médio do bloco


Fonte: Blockchain.com. Disponível em: <blockchain.com/charts/avg-block-size>. Acesso em 12 out. 2020.

## 5.2. Observação chave:

Com isso também podemos concluir mais um ponto destacado anteriormente, quanto mais transações no *mempool* que indica

congestionamento na rede, maior será o tempo de confirmação e custo por transação. A análise do *Mempool* como dito anteriormente, é uma métrica para se estimar quanto tempo pode durar o congestionamento da rede.

Como a escalabilidade depende não de um parâmetro, mas sim de um acumulo de parâmetros, outros fatores, como sobrecarga da rede, número de mineradores e taxa de transação, desempenham papel importante no tempo de confirmação de uma transação.

Por quanto tempo uma transação de *Bitcoin* pode permanecer sem confirmação? A resposta é bem simples, se olharmos o gráfico da figura 11, veremos que no período analisado, a taxa do Bitcoin em poucos momentos ficou abaixo de um dólar. Portanto, se um usuário enviou uma transação de Bitcoin com uma taxa de apenas 10 centavos de dólar, ela poderia ter ficado sem confirmação por dias ou semanas.

Se a transação de *Bitcoin* não for confirmada em algumas horas, há algo que o usuário pode fazer para resolver o problema. Ele pode concordar em pagar uma taxa mais alta para que a transação seja confirmada.

Simplificadamente, o que o usuário pode fazer é enviar uma segunda transação com uma taxa mais alta e essa transação pega a primeira para que ambas sejam compensadas. Uma analogia, é como mandar um caminhão buscar um carro quebrado, então o caminhão com o carro guinchado pode continuar pela rodovia.

# 6. SOLUÇÕES PARA ESCALABILIDADE

## 6.1. ON-CHAIN

Uma transação o*n-chain,* “em cadeia” ou “em rede” é nada mais nada menos que uma transferência de valor de um *token* de criptomoeda específico, mantendo-se todos os detalhes da transação nos blocos e transmitido para toda a rede da criptomoeda. Elas envolvem a participação de diversos usuários na verificação das transações e validação das assinaturas, tendo de haver um consenso para que a transação ocorra e conste no livro-razão público e seja considerado válida.

Embora os dados das transações fique registrando no *blockchain* público para inspeção, pode levar mais tempo de confirmação se comparado ao o*ff-chain*. Portanto pode acarretar um atraso se houver um grande volume de transações a serem confirmadas. Além disso irá fazer com que o custo de cada transação seja maior.

As transações o*n-chain* devem ocorrer em tempo real para manterem seguras, verificáveis, transparentes e instantâneas. Mas na realidade isso raramente acontece, e as transações em rede apresentam algumas desvantagens.

Como visto anteriormente a rede *blockchain* tem um número "limitado" de transações que podem ser processados. Se a rede se tornar muito grande os nós podem não acompanhar sua expansão, pois leva um tempo indeterminado para acumular o número de verificadores e autenticação dos participantes da rede antes de confirmar esta transação, fazendo com que todas as partes envolvidas esperem mais tempo no *mempool* e maior custo, pois será necessário também *hardwares* mais potentes para processá-las.

A solução *on-chain* refere-se a resolver o problema de escalabilidade adicionando ou modificando elementos diretamente dentro da *blockchain* como por exemplo aumentando o tamanho do bloco.

Blocos grandes são uma maneira de aumentar o rendimento da transação, aumentando o tamanho máximo do bloco para incluir mais transações em um bloco. Atualmente, o *Bitcoin* pode armazenar 1 MB de transações por bloco, portanto, se você executar muitas transações ao mesmo tempo, terá que esperar muito tempo para processar todas as transações.

"Aumentar o tamanho do bloco significará sincronizações mais longas da cadeia, menos nodes completos operando a partir de conexões domésticas à Internet e mais centralização geral.", disse Yocom-Piatt sobre uma transição para grandes blocos.

As transações *on-chain* também têm um custo, dependendo do volume de transações na rede essa taxa pode chegar a valores altíssimos, já que os mineiros cobram uma taxa por oferecer seus serviços de validação e autenticação para confirmar uma transação no *blockchain* no menor tempo possível. Aumentar o tamanho do bloco exigiria uma grande quantidade de recursos para lidar com a maior parte das transações e, consequentemente, minerá-las. Conforme disse Yocom-Piatt, o aumento do bloco nos leva a blocos mais pesados sendo transmitidos pela mesma largura de banda da rede anterior, o que leva a propagação em rede ser muito mais lenta

## 6.2. OFF – CHAIN

De acordo com um artigo da IBM, as transações fora da cadeia lidam com "valores que estão fora do *Blockchain* e podem ser concluídas usando vários métodos".

Como já mencionado solução do *off-chain* tem o objetivo de melhorar a escalabilidade processando a transação fora do *Blockchain*. Este protocolo empregado com transações fora da rede é semelhante ao que é usado em plataformas de pagamento como o *PayPal*.

Se as partes envolvidas optarem por um acordo fora do *Blockchain*, a próxima etapa poderá ou não envolver um terceiro, onde sua função será confirmar a transação e certificar que ela foi concluída com sucesso, tornando o

terceiro como uma espécie de fiador da transação. Outro método para transações fora da rede é usar um mecanismo de pagamento baseado em cupom, onde o participante compra cupons em troca das criptomoedas por exemplo e dá o código a outra parte que pode resgatá-los. O resgate é possível na mesma criptomoeda ou em diferentes, dependendo do provedor de serviço de cupom. Da maneira mais simples, duas partes podem até mesmo trocar suas chaves privadas envolvendo uma quantidade fixa de criptomoedas, dessa forma, as moedas nunca saem do endereço ou carteira, no entanto, a moeda irá receber um novo dono fora da rede.

### 6.2.1. Algumas das vantagens

Liquidação imediata, sendo executada instantaneamente. Ou seja, não temos o mesmo problema que ocorre na transação *on-chain*, onde dependendo da quantidade de nós a transação irá aguardar na fila para serem confirmadas.

Taxas mais baixas, geralmente inexistentes, já que nada irá ocorrer no *blockchain*. Como nenhum minerador irá validar a transação, não terá custo.

Maior anonimato se compararmos com as transações em cadeia, pois os dados da transação não ficarão visíveis publicamente. Em uma transação *on-chain* por exemplo, pode-se saber parcialmente a identidade de um dos participantes estudando os padrões de transação.

## 6.3. LIGHTNING NETWORK

Rede relâmpago é outra solução para o problema de escalabilidade que permite aos usuários estabelecer canais de pagamento para micropagamentos. Micropagamentos são transações não confirmadas que só se tornam válidas quando o canal de pagamento é fechado e o saldo total das transações é processado pela rede.

### 6.3.1. Exemplo do funcionamento da Lightning Network:

A *Lightning Network* consiste em uma rede de transferência *off-chain* que é construída em cima ou em paralelo à *blockchain* da *Bitcoin*. O sistema opera em um nível *peer-to-peer* (P2P) e seu uso baseia-se na criação do que chamamos de canais de pagamento bidirecionais, pelos quais os usuários podem fazer inúmeras transações de criptomoedas. (BINANCE, 2020).

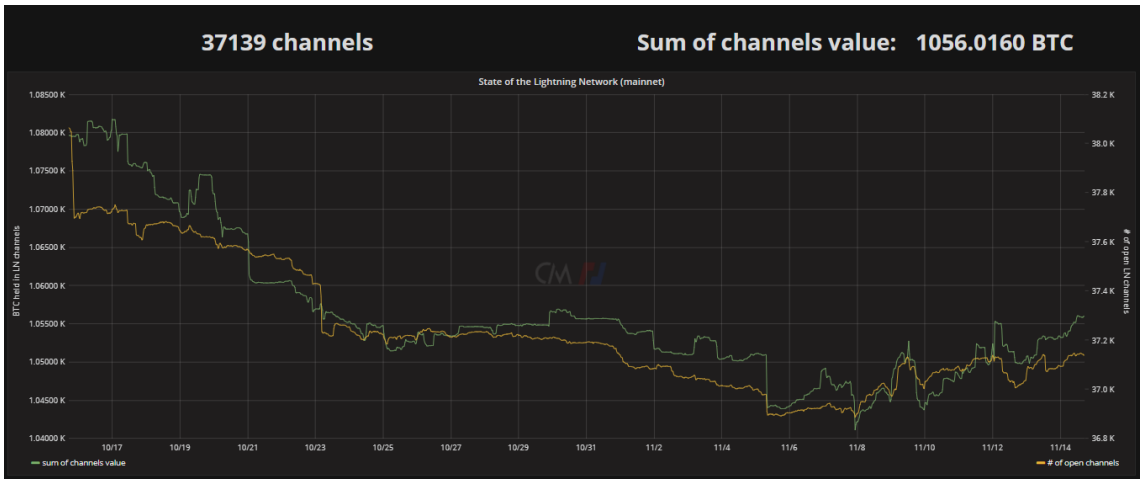
Maria trabalha para João, e ele efetua pagamentos para ela de *1 bitcoin* por dia. Em vez de processar a transação no *blockchain* principal, João e Maria configuram um canal de pagamento privado onde João pode enviar *bitcoin* diretamente para Maria. Ele envia a ela um micropagamento de 1BTC por dia, e cada pagamento deve ser assinado por João e Maria. Se Maria trabalhar para João por dez dias, ao final desse período, João e Maria podem fechar o canal de pagamento. Nesse momento, todos os micropagamentos são transmitidos para a rede como uma transação de 10BTC.

Mesmo que dois participantes não tenham um canal de pagamento direto, eles podem enviar e receber *Bitcoins* utilizando de canais de pagamento interconectados. Utilizando o exemplo acima, se João tiver um canal com Charlie e Charlie um canal com Maria, João pode enviar os pagamentos através de Charlie.

Resumindo, os participantes envolvidos só precisam interagir duas vezes com a *blockchain* da *Bitcoin*. Uma para abrir o canal de pagamento e outra para fechá-lo, o que significa que todas as outras transações, que são executadas dentro do canal *off-chain*.

Canais de pagamento como esses formam a base de uma rede relâmpago de milhares de micropagamentos ocorrendo fora do *blockchain* principal, e só serão adicionadas ao *blockchain* principal quando os usuários fecham o canal de pagamento. Conforme verificamos na figura 16 atualmente a *Lightning Network* possui mais de 37 mil canais de pagamentos.

**Figura 16** – Quantidade de canais de pagamento da LN




Fonte: *Lightning Network*. Disponível em: <https://txstats.com/dashboard/db/lightning-network?orgId=1>. Acesso em 14 nov. 2020

O trabalho coletivo dos nós e dos canais de pagamentos é o que torna o *Lightning Network* uma solução interessante para o problema de escalabilidade.

### 6.3.2. Vantagens da Lightning Network

A *Lightning Network* é um protocolo de "camada dois" para *Bitcoin*, projetado para pagamentos com menor custo, rápidos e privados. Como uma rede de sobreposição que consiste em canais de pagamento, os pagamentos *Lightning* não são registrados no *blockchain* do *Bitcoin*, apenas transações de fechamento de canal são registradas

Os protocolos da camada 2 enviam a maioria das transações para fora da cadeia, aliviando a carga da rede do *blockchain*. Portanto, outro pró é o fato de que as transações não são registradas no *blockchain*, isso significa que os usuários *Lightning* geralmente desfrutam da privacidade extra do *off-chain*. Como um canal de pagamento é apenas entre duas partes, quaisquer erros ou falhas dentro do canal afetam apenas os participantes e não a rede por completa.

### 6.3.3. Desvantagens da Lightning Network

Uma das principais desvantagens da LN é o fato de não estar totalmente operacional, então não é possível afirmar o quão bom ela será, e traz consigo o problema do aumento de centralização. Como a rede é formada por canais de pagamentos bidirecionais, os “nós” criam entre si contratos inteligentes, caso a qualquer momento uma das partes de baixa no canal ele será fechado e registrado no *blockchain*. “Uma interrupção do servidor pode causar interrupções em toda a rede e pode fazer com que muitos usuários tenha seus fundos congelados por dias.”, disse Dash.

No entanto, não há como dizer o que acontecerá se o pagamento tiver que seguir um caminho muito complicado, de fato a transação precisará passar por dezenas de canais, e isso aumentará o valor das taxas. Outra preocupação é com a formação de *hubs*, que são “nós” com capital alto, onde grande parte das transações irão passar, criando uma espécie de centralização na rede, porém não se pode afirmar que se esses nós conseguirão obter lucros em cima das transações. Muito depende de como os recursos e pesquisas da tecnologia serão desenvolvidos no futuro.

## 6.4. SIDECHAIN

Tal solução visando resolver o problema de escalabilidade fazendo com que certas tarefas sejam feitas fora do *blockchain* (*off-chain*) em questão, mas em um *blockchain* secundária (*sidechain*). Os *sidechains* rodam em paralelo com o *blockchain* principal, podendo estender suas funcionalidades, segurança, performance, escalabilidade e diminuir custos.

Em termos mais simples, as cadeias laterais permitem que os nós de um *blockchain* sejam usados com segurança em um *blockchain* separado e movidos de volta para o *blockchain* principal.

A *Sidechains* permitem que o *blockchain* seja escalonado, assim as informações certificadas de um *blockchain* podem ser utilizadas por outro,

derivando a segurança da cadeia principal, ampliando significativamente os casos de uso para *blockchains* mundiais além de criptomoedas.

Basicamente permite que você mova seus *bitcoins* para outro *blockchain* completamente independente, troque-os lá, e eles podem então ser movidos de volta para o *blockchain* principal de *bitcoin*, ou seja, um usuário na cadeia principal envia suas moedas para um endereço externo de saída, onde suas moedas irão ficar bloqueadas para que ele não possa gastá-las em outro lugar. Assim que a transação for concluída, sua confirmação é transmitida entre as cadeias. Após o valor ser liberado na *sidechain* o usuário pode acessar e gastar suas moedas. o inverso acontece para voltar da cadeia lateral para a principal.

### 6.4.1. Como a *Sidechain* funciona

Digamos que você tenha dez *Bitcoins* e queira trocar por 10 unidades da moeda do *sidechain*, neste exemplo vamos chamá-las de *sidecoins*. Como já mencionado a *sidechain* utiliza uma atrelagem bidirecional, ou seja, podemos transferir ativos do *blockchain* principal para a *sidechain* e vice-versa. Para obter seus *sidecoins*, você irá transferir os 10 Bitcoins para outro endereço, que pode ser o endereço de alguém que irá realizar a troca e enviar os *sidecoins* para seu endereço após receber seus *Bitcoins*.

Agora que temos convertido os *sidecoins*, pode se realizar a troca por *bitcoin* novamente quando quiser, enviando os *sidecoins* para um endereço e após esta transação ser confirmada os *bitcoins* equivalentes serão desbloqueadas e entregue no seu endereço dentro da cadeia principal. Uma vez dentro da *sidechain* pode se realizar transações na *blockchain* separada.

### 6.4.2. Segurança

Sidechains precisam de seus próprios mineiros, esses mineiros podem ser incentivados por meio de "mineração combinada", em que duas criptomoedas separadas, com base no mesmo algoritmo, são extraídas simultaneamente.

Uma grande vantagem das *sidechains* serem independentes, se ela for comprometida, não afetara a cadeia principal com seu dano. E se a cadeia principal for comprometida, a *sidechain* continuará operante, más perdera grande parte de seu valor. Se os mecanismos de segurança para *sidechains* puderem ser reforçados, a tecnologia *sidechain* promete uma escalabilidade massiva de *blockchain*.

## 6.5. SEGWIT

*SegWit*, abreviação de *Segregated Witness* que significa Testemunha Segregada, segregar significa separar, e Testemunhas são as assinaturas da transação. Consequentemente, Testemunha Segregada, em resumo, significa separar as assinaturas da transação. É um *upgrade* de protocolo que foi ativado no *bitcoin* em 23 de agosto de 2017. Esta proposta surgiu com o objetivo de resolver o problema da maleabilidade de transações e escalabilidade da rede, nosso foco com ele será em cima da escalabilidade, e para isso fez-se necessário mover os “dados da testemunha” para fora do *Blockchain*. (BITDEGREE, 2020).

Explicação rápida sobre a falha de maleabilidade da transação no código do *Bitcoin* permite que um dos envolvidos na transação altere os dados da testemunha. Por exemplo usuário 1 vai realizar um pagamento para o usuário 2, a falha permite que o usuário 2 altere os dados da testemunha do usuário 1 antes que a transação seja confirmada. Quando a transação alterada é confirmada pela rede, ela cancela a transação original. Agora o usuário 2 questionará o usuário 1 para reclamar que não recebeu seu pagamento, fazendo com que o usuário 1 efetue novamente o pagamento.

O usuário 1 e o resto da rede não tem como saber que isso está acontecendo. Uma vez que as transações são confirmadas e adicionadas ao *blockchain*, elas não podem ser alteradas ou excluídas.

Uma testemunha segregada cria um *sidechain* (cadeia lateral) onde os dados da testemunha são armazenados longe do *blockchain* principal. Isso evita

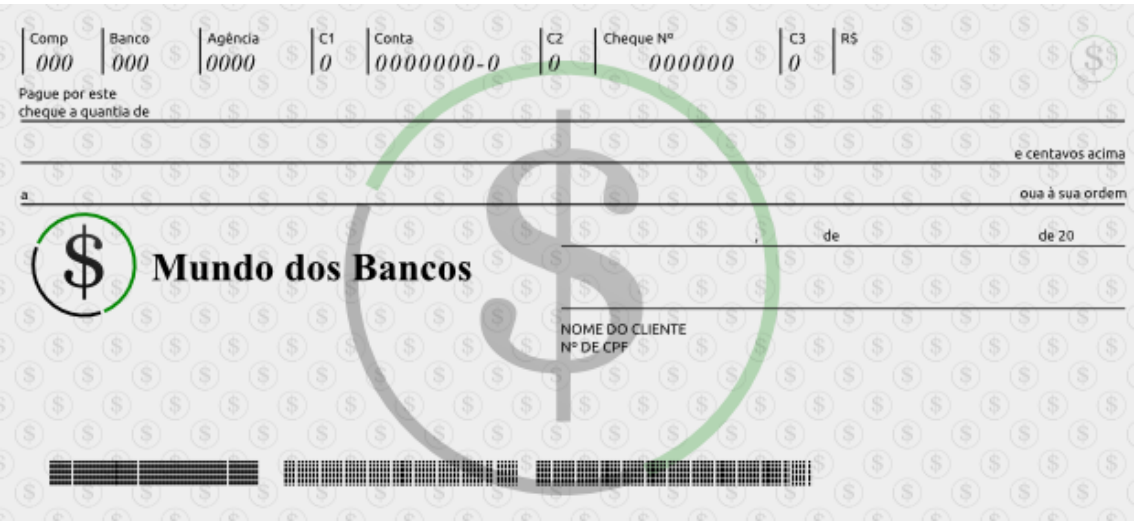
que os dados de uma transação sejam alterados por usuários desonestos como o usuário 2 do exemplo anterior.

Simplificadamente, a função do *SegWit* é separar os dados de assinatura digital de cada transação *Bitcoin*. Quando essa parte da transação é removida, mais espaço dentro de cada bloco fica disponível para ser preenchido por novas transações. Ou seja, *SegWit* é o processo pelo qual o limite de tamanho de bloco em um *blockchain* é aumentado removendo dados de assinatura de transações *Bitcoin*. Quando removemos parte de uma transação, liberamos espaço ou capacidade para adicionar mais transações na cadeia.

### 6.5.1. Como o *SEGWIT* funciona

Para explicar o *SegWit* de forma mais prática, vamos imaginar que uma transação em *Bitcoin* seja feita em cheque, como a imagem a seguir. Da mesma forma que um cheque, uma transação em *Bitcoin* contém o remetente, destinatário e a quantia que está sendo transferida. A figura 17 é o exemplo de cheque que utilizaremos.

**Figura 17** – Modelo de cheque

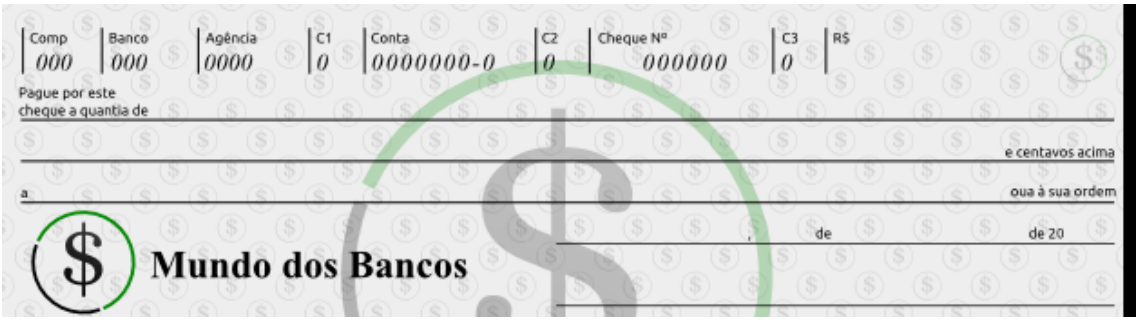



Fonte: MUNDO DOS BANCOS. Disponível em: </mundodosbancos.com/18/cheques/>. Acesso em 01 out. 2020.

No exemplo do *Bitcoin*, vamos supor que a assinatura ocupe cerca de 65% do espaço do bloco, então o *SegWit* basicamente irá removê-la. Então

teremos um cheque sem dados de assinatura conforme a figura 18, representando o que o *SegWit* faz com as transações de *Bitcoin*.

**Figura 18** – Modelo de cheque sem assinatura




Fonte: MUNDO DOS BANCOS. Disponível em: </mundodosbancos.com/18/cheques/>. Acesso em 01 out. 2020.

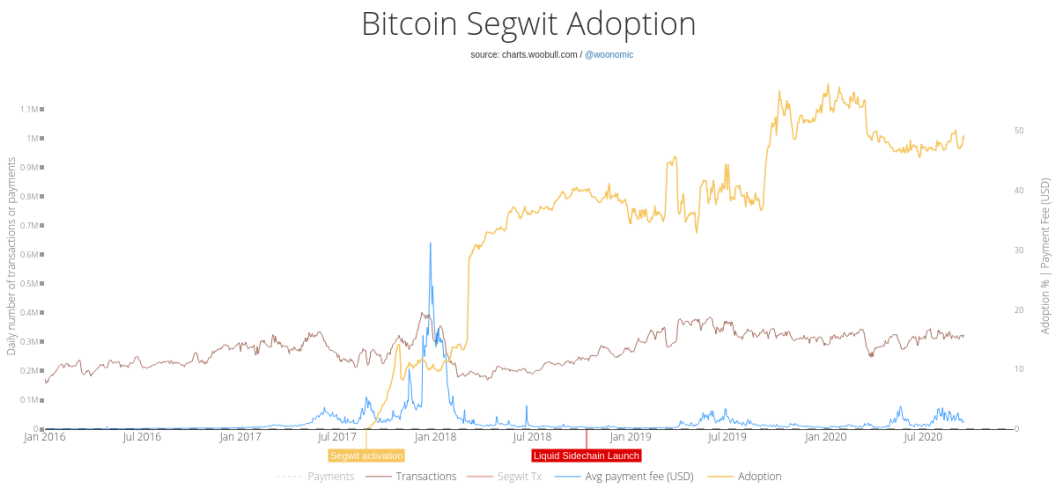
Ao remover dados de testemunhas, os blocos *SegWit Bitcoin* agora têm espaço para muito mais informações de transações.

O peso de um bloco é uma combinação de 1Mb de informações armazenadas no *blockchain* principal e os dados da testemunha armazenados em uma cadeia lateral. Uma testemunha segregada torna a rede mais leve e permite que ela processe mais transações sem alterar o tamanho geral do *blockchain* do *Bitcoin*.

### 6.5.2. Existem desvantagens para o *SegWit*?

Contudo, a solução *SegWit* tem um problema, que é a adoção. Nem todas as plataformas de troca possuem suporte para transações com *SegWit*, conforme a imagem 19 sua adoção é de apenas 50%, pois os mineiros terão lucros ainda mais baixos. A capacidade do *SegWit* de possibilitar mais transações em um bloco, baseia-se na ideia de manter alguns dados fora da cadeia principal. Então se precisamos lateralizar parte da transação, pode significar que o *blockchain* por si só não irá funcionar. (COINTELEGRAPH, 2019).

**Figura 19** – Adoção do SegWit



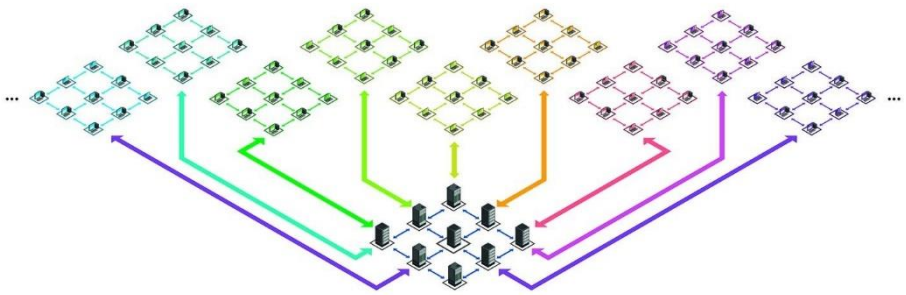

Fonte: *Woobull Charts*. Disponível em: < https://charts.woobull.com/bitcoin-segwit-adoption/>. Acesso em 15 nov. 2020.

## 6.6. SHARDING

A fragmentação é um método que foi utilizado em banco de dados para garantir que um banco opere com velocidade e eficiência ideal.

"*Sharding* é um conceito que se originou com o particionamento horizontal do banco de dados e está sendo adotado pela *Ethereum* ... e funciona de forma que nem todos os "nós" tenham que processar todas as transações, aumentando assim a escalabilidade.", disse Avivah Litan, vice-presidente do Gartner e conceituado analista. A figura 20 nos mostra um exemplo do seria a fragmentação.

**Figura 20** – Modelo de fragmentação



Fonte: *FOREX ACADEMY*. Disponível em: <forex.academy/is-sharding-the-future-of-blockchain-systems/>. Acesso em 10 out. 2020.

*Sharding* tem se mostrado como uma forma promissora de atingir altas taxas de escalabilidade no *blockchain*, dividir a rede em várias redes menores faz com que ela seja capaz de processar diversas transações simultaneamente, em vez de processar uma transação por toda rede. Podemos dizer que a fragmentação é uma forma de particionar com o propósito de dividir a carga de trabalho da rede, para que cada “nó” não seja responsável por toda carga transacional da rede. Por exemplo, se tivermos uma rede com 100 ‘nós”, e dividirmos ela em 10 fragmentos composto por 10 “nós”, no final teremos uma velocidade 10 vezes maior.

Atualmente, cada “nó” em uma rede *blockchain* armazena todos os estados. Isso significa que cada “nó” é responsável por armazenar informações críticas, como saldos de contas e histórico de transações. Embora nos dê mais segurança, como já vimos, armazenar todos os estados em todos os “nós” faz com que o processamento das transações se torne consideravelmente mais lento.

### 6.6.1. Problema de comunicação

Ao isolarmos a rede os fragmentos estarão separados do *blockchain* como uma rede própria de *blockchain* separada, os usuários não poderão se comunicar com os usuários de outro fragmento, sem a implantação de um mecanismo de comunicação.

### 6.6.2. Segurança

Sabendo como funciona a segurança de uma rede *blockchain*, se pensarmos no exemplo de fragmentação apresentado anteriormente, temos uma rede 10 vezes mais rápida e também 10 vezes menor, o que faz com que a segurança se torne uma preocupação, pois se torna mais fácil com que um

hacker assuma o controle de um fragmento. Então temos o principal problema relacionado a segurança:

- "Ataque de controle de um único fragmento". Onde se for um atacante assume a maioria dos agrupadores em um único fragmento, ele poderia manipulá-los para criar um fragmento malicioso e enviar transações maliciosas também.

A *Ethereum*, uma plataforma para aplicações descentralizadas que utiliza a tecnologia *blockchain*, propôs para solucionar este problema a amostragem aleatória, onde será atribuindo “nós” aleatoriamente a certos fragmentos e reatribuindo-os constantemente em intervalos aleatórios. Isso torna difícil para os *hackers* saber quando e onde corromper um fragmento.

**“**A fragmentação não é uma solução tão simples para escalabilidade", disse Husebuy. Podemos notar alguns detalhes a serem analisados, no entanto, implementá-lo em um *blockchain* público ainda é um desafio. Portanto, a natureza da descentralização e da transparência torna difícil manter a segurança. Além de ataques de fragmento único, os desenvolvedores enfrentam outros problemas, como comunicação entre fragmentos que é uma parte crucial antes de sua implementação, deixando o *blockchain* a poucos passos para sua adoção.

## CONCLUSÃO

Com a popularização do blockchain nos últimos anos sua aplicação em diferentes áreas que visam explorar seu potencial tem sido questionada, não apenas para a utilização da moeda digital, mas para outros aplicativos e serviços que podem ser construídos e cima de sua estrutura, e para isso o problema de escalabilidade deve ser resolvido.

Primeiramente, sobre o objetivo do projeto de apresentar o problema de escalabilidade do blockchain Bitcoin e a estrutura das possíveis soluções, fora realizado com êxito, porém a pontos importantes a se comentar dos resultados obtidos após o estudo das propostas.

Sobre a análise de escalabilidade vimos os parâmetros que devem ser analisados e tratados ao se criar uma aplicação na blockchain, demonstrando no cenário real da criptomoeda o quanto pode afetar a segurança e descentralização.

Com o grande aumento da utilização da tecnologia, nos apresenta um cenário que deve ser analisado cuidadosamente, pois o congestionamento da rede já ocorreu algumas vezes. Compra de mercadorias, micro transações, validação de receitas médicas entre outros é apenas o começo da era blockchain. E com isso vem surgindo diversas novas soluções conforme descritas neste trabalho visando solucionar o problema de desempenho do blockchain, principalmente sua escalabilidade, mostrando-se promissoras, com suas vantagens e desvantagens diante do objetivo e cenário atual.

Sobre as propostas de tornar a rede escalável, não podemos dizer ao certo em quanto tempo teremos a solução definitiva, ainda mais quando se trata de uma nova tecnologia que mudara por completo nosso contexto de segurança e confiabilidade nos serviços em que será utilizada. No entanto, é possível identificar alguns indícios que apontam para um provável cenário futuro, mesmo que ocorra daqui a 10 anos, ainda será um espaço de tempo pequeno devido aos benefícios e mudanças que trará para nossa tecnologia.

Por tanto, este trabalho com ênfase no problema de escalabilidade e analisando as possíveis soluções, nos traz uma perspectiva promissora para que

as redes se tornem escaláveis num futuro próximo, e espero poder inspirar ainda mais os estudos em expansão dedicados a melhorar a escalabilidade do blockchain.

## REFERÊNCIAS BIBLIOGRÁFICAS

ARE you still only detecting or are you already avoiding counterfeits. **Merck**, c2020. Disponível em: <https://www.merckgroup.com/en/research/innovation-center/highlights/blockchain.html>. Acesso em: 06 nov. 2020.

BARSKI, Conrad; WILMER, Conrad. **Bitcoin for the Befuddled**. 1 ed., São Francisco: No Starch Press, 2015.

BASHIR, Imran. **Mastering Blockchain - Distributed ledgers, decentralization and smart contracts explained**. 1 ed., Birmingham: Packt Publishing Ltd, 2017.

BITCOIN - Frequently Asked Questions. **Bitcoin**, c2020. Disponível em: <https://bitcoin.org/en/faq#what-is-bitcoin>. Acesso em: 06 nov. 2020.

CAETANO, Richard. **Learning Bitcoin**. 1 ed., Birmingham: Packt Publishing Ltd, 2015.

CRYPTOCURRENCY. **Investopedia**, 5 mai. 2020. Disponível em: <https://www.investopedia.com/terms/c/cryptocurrency.asp>. Acesso em: 06 nov. 2020.

DINIZ, Eduardo Henrique. **Emerge uma nova tecnologia disruptiva**. São Paulo: GV-Executivo, 2017.

DRESCHER, Daniel. **Blockchain Basics - A Non-Technical Introduction in 25 Steps**. New York: Springer Science, 2017.

FOXBIT: foxbit.com.br, c2019. O que é blockchain. Disponível em:< https://foxbit.com.br/o-que-e-blockchain/>. Acesso em: 08 out. 2020.

IBM Food Trust - Uma nova era para o fornecimento de alimentos mundial. **IBM**, c2020. Disponível em: <https://www.ibm.com/br-pt/blockchain/solutions/food-trust>. Acesso em: 07 nov. 2020.

KLEMENS, Sam. How Long Does a Bitcoin Transaction Take? And Sending Faster. **Exodus**, 03 jul. 2020. Disponível em: <https://www.exodus.io/blog/how-long-does-a-bitcoin-transaction-take/>. Acesso em: 07 nov. 2020.

LIGHTNING Network: A Solução de escalabilidade do Bitcoin. **Livecoins**, 21 jul. 2019. Disponível em: <https://livecoins.com.br/lightning-network-a-solucao-de-escalabilidade-do-bitcoin/>. Acesso em: 22 out. 2020.

MARTIN, Jack. Associated Press publica resultados das eleições presidenciais dos EUA em blockchains. **Cointelegraph**, 04 nov. 2020. Disponível em: <https://cointelegraph.com.br/news/ap-news-publishes-us-presidential-election-results-on-the-blockchain>. Acesso em: 04 nov. 2020.

NORMAN, A. T. **Blockchain Technology Explained: The Ultimate Beginner's Guide about Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts** 1. ed. CreateSpace Independent Publishing Platform, 2017.

PINTO, Rohan. On-Chain Versus Off-Chain: The Perpetual Blockchain Governance Debate. **Forbes**, 06 set. 2019. Disponível em: <https://www.forbes.com/sites/forbestechcouncil/2019/09/06/on-chain-versus-off-chain-the-perpetual-blockchain-governance-debate/?sh=5985065c1f5e>. Acessedo em: 06 nov. 2020.

ROSIC, Ameer. What is Blockchain Technology? A Step-by-Step Guide For Beginners. **Blockgeeks**, c2020. Disponível em: <https://blockgeeks.com/guides/what-is-blockchain-technology/>. Acesso em: 06 nov. 2020.

ROSIC, Ameer. What is Hashing? Step-by-Step Guide-Under Hood Of Blockchain. **Blockgeeks**, c2020. Disponível em: <https://blockgeeks.com/guides/what-is-hashing/>. Acesso em: 06 nov. 2020.

Sharding. **Investopedia**, 05 out. 2020. Disponível em: <https://www.investopedia.com/terms/s/sharding.asp>. Acesso em: 8 out. 2020.

THE Evolution of payment methods: past, present and future. **Medium**, 5 set. 2017. Disponível em: <https://medium.com/zeta-blog/the-evolution-of-payment-methods-past-present-and-future-ab0dfdac7069>. Acesso em: 06 nov. 2020.

THE Difference Between On-Chain and Off-Chain Transactions. **Vertexmarket**, 02 set. 2019. Disponível em: <https://vertexmarket.medium.com/the-difference-

between-on-chain-and-off-chain-transactions-6b5121da9d4c>. Acesso em: 06 nov. 2020.

THE Financial Network of the future. **Ripple**, c2020. Disponível em: <https://ripple.com/ripplenet>. Acesso em: 05 nov. 2020.

WHAT is SegWit and How it Works Explained. **BitDegree**, 11 set. 2020. Disponível em: <https://www.bitdegree.org/crypto/tutorials/what-is-segwit>. Acesso em: 15 out. 2020.