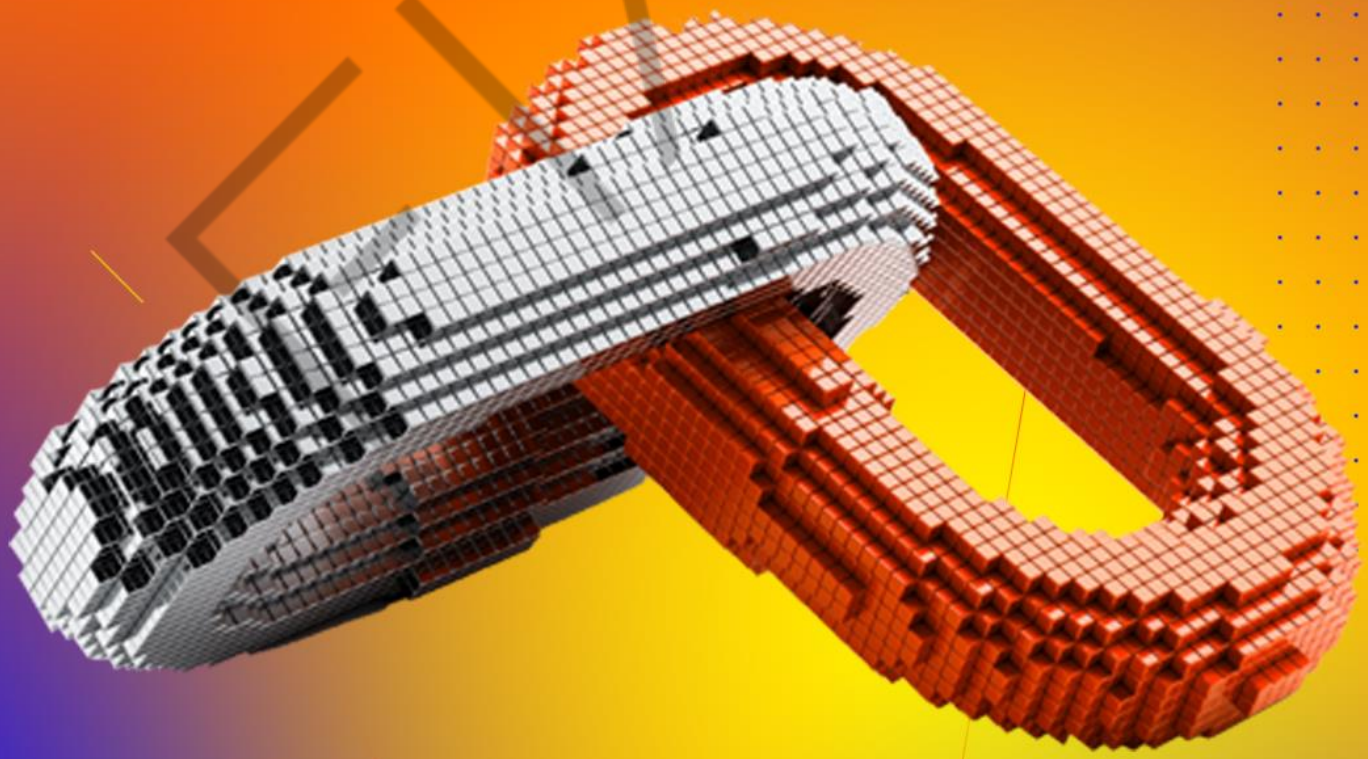
FIAP ON

BLOCKCHAIN ADVANCED

FUNCIONAMENTO DA PLATAFORMA BLOCKCHAIN

FABIO MAÇOLI



3

LISTA DE FIGURAS

SUMÁRIO

3 FUNCIONAMENTO DA PLATAFORMA BLOCKCHAIN

3.1 Recordando definições

Para darmos início a este capítulo, funcionamento *Blockchain*, e podermos compreender com exatidão todo o contexto técnico que conta, é muito interessante relembrarmos alguns conceitos básicos que foram tratados no capítulo anterior:

- **CRIPTOGRAFIA**: técnicas que promovem o embaralhamento, codificação das palavras, para que não permitam sua leitura, caso sejam interceptadas.
- **FUNÇÃO HASH**: permite que, através de uma string de qualquer tamanho, seja calculado um identificador digital de tamanho fixo, chamado de valor hash.
- **CERTIFICADO DIGITAL**: identidade digital da pessoa física e jurídica no meio eletrônico.
- **REDE P2P**: são denominadas redes P2P ou redes ponto a ponto, estrutura de redes de computadores e Internet em que não há um servidor definido para armazenamento e compartilhamento das informações, ou seja, todas as estações (computadores) que participam da estrutura exercem o papel de cliente e servidores.

3.2 Blockchain e sua cadeia de blocos

O termo *blockchain* tem origem pelo fato da plataforma armazenar as transações em blocos que estão interligados entre si, formando uma cadeia. Sendo que à medida que os números de transações ocorrem, vão sendo processados os blocos, interligando cada bloco processado. Desta forma, cada bloco gera um *hash* (identificação exclusiva do bloco), sendo que este também é baseado no bloco processado anteriormente, assim, sucessivamente, cada bloco processado gera um *hash* próprio, que também se encontra baseado no bloco anterior, gerando uma cadeia de processamento.

A geração desta cadeia de processamento em blocos evita que algum bloco seja alterado, conforme vários blocos são processados, vão fortalecendo em mais os blocos anteriores.

O referido método torna a alteração da cadeia inviolável, emprestando-lhe o atributo de chave de imutabilidade.

CHAVE DE IMUTABILIDADE ➔ A **imutabilidade** do nome civil é um **princípio** de ordem pública, em razão de que sua definitividade é de interesse de toda a sociedade, constituindo garantia segura e eficaz das relações de direitos e obrigações correlatas

Desta forma, o *Blockchain* gera uma cadeia de registros imutáveis, distribuídos e públicos.

- Cadeia, pois os registros processados no *blockchain* encontram-se encadeados uns aos outros.
- Imutáveis, uma vez que o registro é inserido em uma cadeia o mesmo não pode ser alterado.
- Público, pois encontra-se disponível na Internet.
- Distribuidos, por tratar-se de uma rede P2P que se trata de uma estrutura distribuída sem um servidor central.

3.2.1 Funcionamento da cadeia de blocos

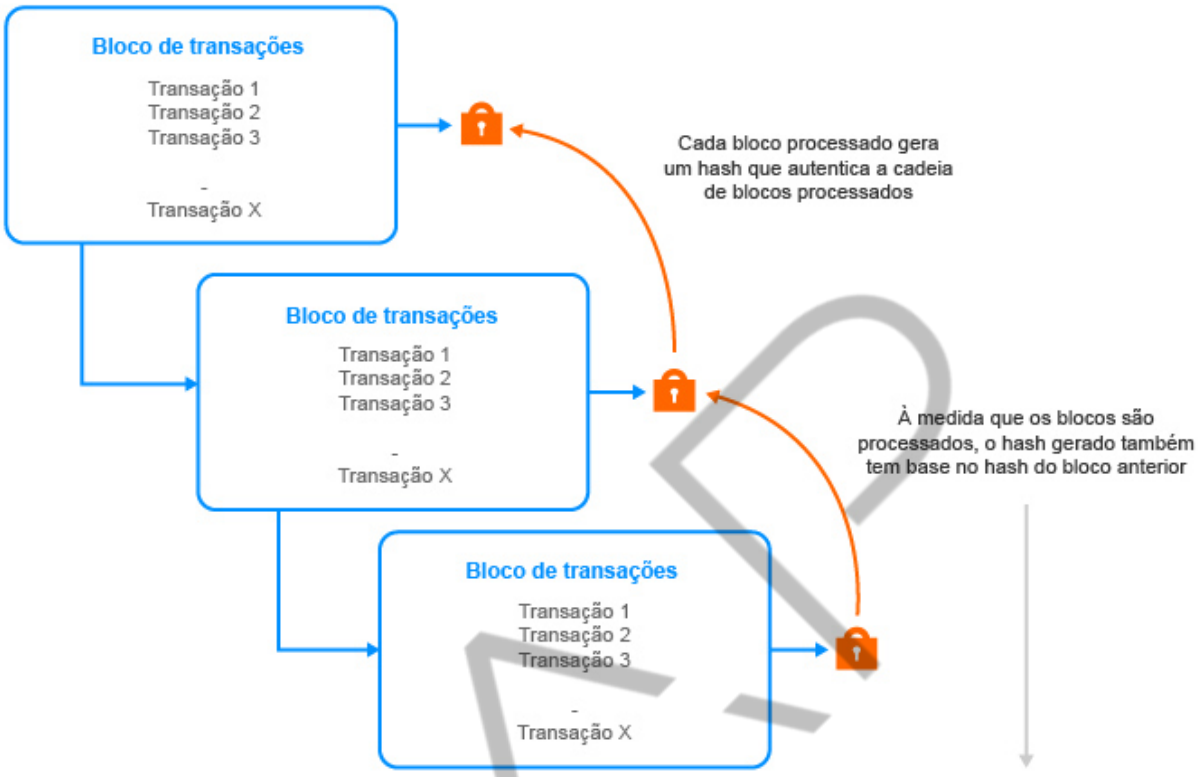


Figura 3.1 - Funcionamento da Cadeia de Blocos
Fonte: Elaborado pelo autor (2020)

3.2.2 Estrutura dos blocos blockchain

Cada bloco que compõe a estrutura do *blockchain* possui uma área destinada às transações que são feitas nele e uma outra área que é destinada ao armazenamento do cabeçalho, que por sua vez possui o *hash* do bloco anterior e a raiz da árvore de Merkle das transações presentes no bloco.

Segundo o site Unionpedia, em criptografia e ciência da computação, árvores de dispersão ou árvores de Merkle são um tipo de estrutura de dados que contém uma árvore de informações resumidas sobre um pedaço maior de dados, por exemplo, um arquivo, usado para verificar seu conteúdo.

ÁRVORE DE MERKLE: também denominada Merkle Root, trata-se de *hash* raiz de uma estrutura de dados.

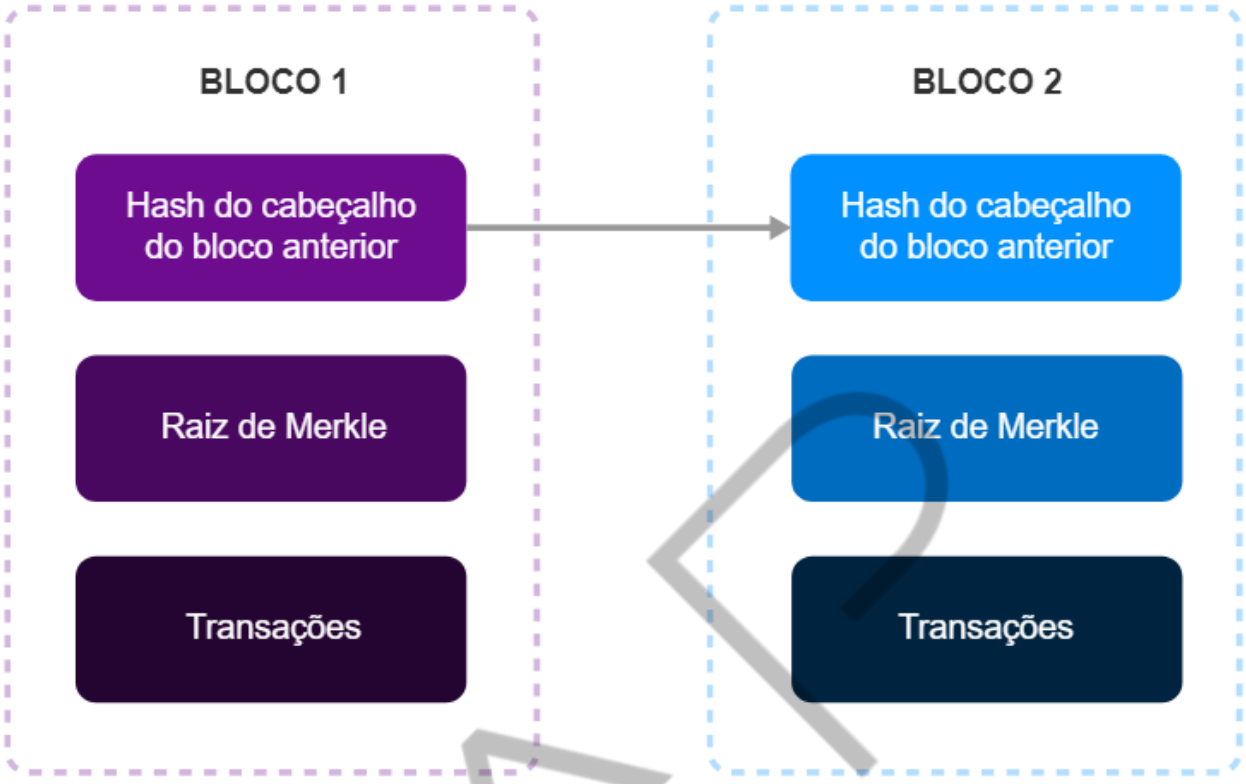


Figura 3.2 - Estrutura dos Blocos
Fonte: Okupski (2014) adaptado pelo autor (2020)

CURIOSIDADE BLOCKCHAIN X BITCOIN
O primeiro bloco da blockchain do bitcoin é o bloco 0 chamado de bloco gênesis. Este é o bloco minerado por Satoshi Nakamoto que serve como ponto de partida comum a todas as implementações do bitcoin e é escrito diretamente no código referência para este fim. Ele contém a famosa frase escolhida por Satoshi Nakamoto:
The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Uma vez que existente o conceito de imutabilidade e tendo em vista que parte da segurança *blockchain* está garantida no encadeamento dos blocos, para promover algum tipo de alteração, é necessário alterar todos os blocos que compõem a cadeia.

3.3 Pilares da tecnologia blockchain

A tecnologia *blockchain* está baseada em quatro pilares:

- Segurança das operações realizadas.
- Descentralização do armazenamento.
- Integridade de dados.

- Imutabilidade de transações.

Desta forma, a referida tecnologia é denominada *"ledger of facts"* ou livro de fatos, sendo que:

- O Ledger pode ser denominado o livro de registro digital, e uma vez validado um registro inserido neste livro, ele não poderá ser mais removido.
- O Fact (fato) denomina as transações que ocorrem dentro da plataforma.
- Os nós são os membros/integrantes da rede *blockchain*, que neste caso podem ser anônimos ou não.
- Bloco que constitui um conjunto de fatos.
- Cadeia de blocos que por sua vez trata-se de um conjunto de blocos encadeados.

Com base nos itens acima podemos concluir que toda transação/operação que ocorre dentro da plataforma é protegida pelas tecnologias que compõem a plataforma (criptografia, assinatura digital, certificado digital, *hash*, redes P2P).

3.4 Topologias de redes blockchain

As redes *blockchain* são divididas em dois modelos de topologia, sendo:

- **Redes privadas (permissioned):**

As redes *blockchain* denominadas privadas são plataformas fechadas, ou seja, atendem à demanda de um grupo, para participar do bloco, precisa ser convidado ou ter permissão para ter acesso a ele. São plataformas auditadas e controladas, desta forma eliminando possíveis riscos de segurança e vulnerabilidade.

Em se tratando de atualização dos blocos, por tratar-se de uma estrutura privada, é mais rápida e ágil, uma vez que existe um número limitado de participantes que concorrem ao fechamento e atualização dos blocos.

Suas principais aplicações são voltadas a ambientes corporativos e fechados.

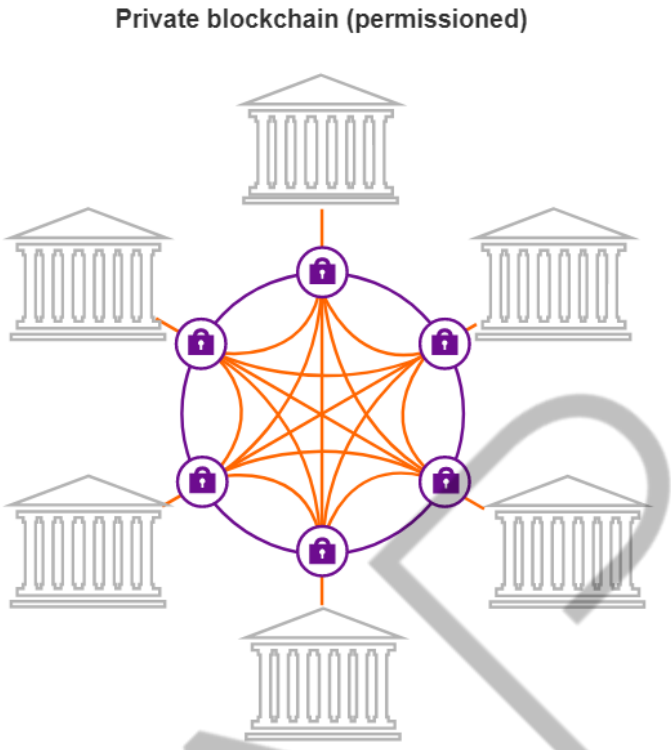


Figura 3.3 – Exemplo de rede privada
Fonte: E27 (2016)

- **Redes públicas (permissionless):**

As redes *blockchain* denominadas públicas são plataformas abertas, ou seja, qualquer pessoa pode se tornar membro e armazenar, enviar e receber dados, após baixar o software compatível. Trata-se de uma estrutura completamente descentralizada, muito recomendado para transações e modelos de negócios tradicionais, dentro da mesma empresa ou promovendo a interligação de um grupo de empresas, todas estas controladas e auditadas.

Desta forma, as redes públicas são mais vulneráveis, promovendo dificuldade em auditorias e controles de transações, pois por serem públicas, ninguém se conhece dentro de sua base de dados.

Nesse cenário, a atualização dos blocos é mais lenta, uma vez que, trata-se de uma plataforma com muitos integrantes e maior risco de vulnerabilidade. Suas principais aplicações são transações de *cryptomoedas (Bitcoin/Ethereum).*

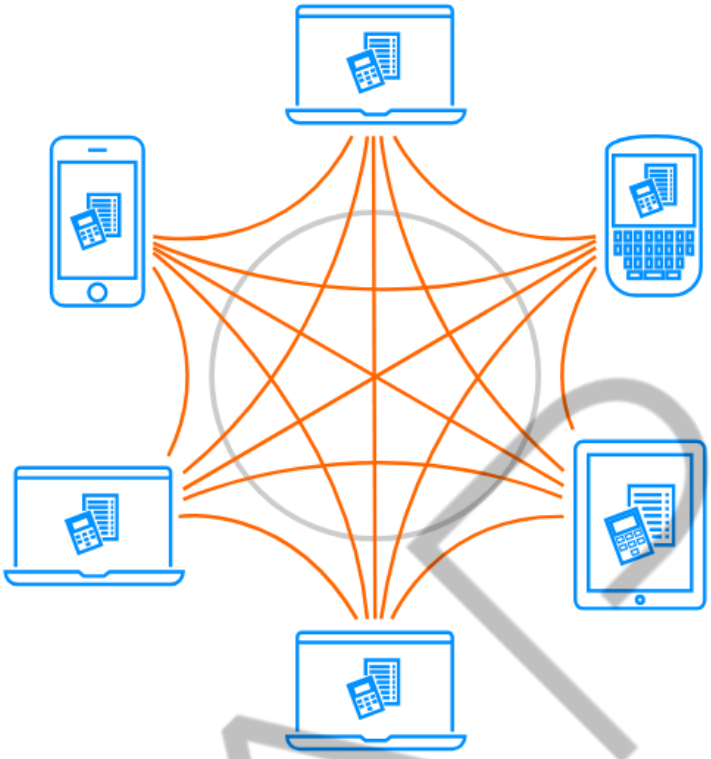


Figura 3.4 – Exemplo de rede publica
Fonte: E27 (2016)

3.5 Algoritmo de Consenso

Segundo Professor Henriques: “Um mecanismo de consenso é um algoritmo que serve para criar um novo bloco num ambiente descentralizado de forma consensual entre os nós da rede P2P. É uma nova solução ao Problema dos Generais Bizantinos (PGB) que consiste no dilema de atingir um consenso entre os usuários que neste caso chamaremos como generais com um objetivo comum. Entre eles podem existir generais traidores com objetivos opostos que tentam atrapalhar o processo. A ideia é que os generais leais atinjam o objetivo comum e os traidores não consigam interrompe-los.”

Por tratar-se de uma plataforma P2P, onde todos os nós que participam do *blockchain* compartilham a mesma base de dados, quando uma nova transação é efetuada, precisa ser validada e sincronizada com os demais nós que participam da estrutura, para que isso ocorra dentro da plataforma, deve-se eleger um líder, ou seja, um dos nós que atualizará o “*ledger*” (base de dados/registro das transações). Desta forma, o restante dos nós acompanharam o líder. Podemos dizer que o algoritmo de

consenso é um dos pilares da atualização *blockchain*, pois é ele que promoverá a decisão de quem será o “líder” para cadeia de blocos.

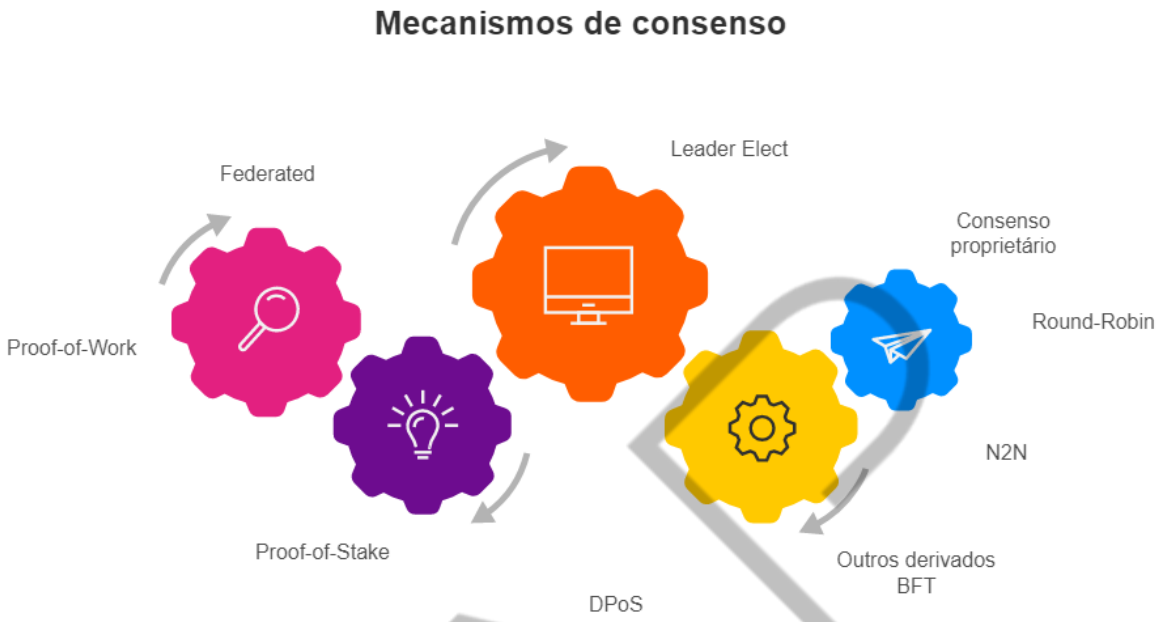


Figura 3.5 – Exemplo de algoritmos de consenso
Fonte: Irib (2017)

3.6 Questão dos Generais Bizantinos

Trata-se de uma metáfora utilizada nas áreas da Ciência da Computação, criada a aproximadamente há 30 anos, visando explicar a questão de consenso entre redes distribuídas, que elucida a tomada de decisão de invasão em uma guerra para que todos tomem à mesma ação, bem como para verificar a existência de traidores em seu meio. Em suma, trata-se de uma forma de um sistema distribuído chegar a um consenso, garantindo todas as transações decorrentes dentro dela.

Figura 3.6 – Generais Bizantinos
Fonte: Youtube / Block By Block (2017)

A questão do consenso está presente em vários locais em nossa rotina, trata-se de um grupo de pessoas, equipamentos, plataformas, precisando encontrar-se em consenso único, ou seja, todos estão de acordo com uma transação e estão cientes dela.

O consenso significa que boa parte dos envolvidos está de acordo com a transação, e este acordo é feito por meio de algoritmos que permitem que os envolvidos tenham conhecimento de todas as transações decorrentes.

Mecanismos de consenso buscam principalmente:

- Descentralização.
- Integridade.
- Confiabilidade.
- Verificação de origem.
- Privacidade.
- Regras predefinidas.
- Autenticação.
- Verificação de origem.
- Tolerância a falhas.
- Performance.

No caso do *blockchain*, o mecanismo de consenso é utilizado, principalmente por tratar-se de uma rede distribuída P2P, e pelo grande fato do encadeamento dos blocos, ou seja, como o processamento dos blocos é feito de tempos em tempos, torna-se necessário um dos nós pertencentes ao *blockchain* tornar-se o líder que enviará um broadcast a todos os outros nós que fazem parte da estrutura.

3.7 Exemplo de mecanismos de consenso

3.7.1 Prova de trabalho (Proof of Work – Pow)

O *Pow* foi o primeiro mecanismo de consenso distribuído, criado justamente para tratar as questões de segurança e estrutura do *Bitcoin* desenvolvido pelo então Satoshi Nakamoto que teoricamente foi o criador do *Bitcoin*, teoricamente, pois até hoje não se conhece a sua identidade, é claro que além deste algoritmo de consenso existem outros.

Neste mecanismo é lançado um enigma, *hash,* para a rede *blockchain*, uma espécie de quebra-cabeça e o computador que conseguir resolver a questão em menor tempo será eleito o líder da cadeia, sendo que este nó, enviará a atualização aos demais nós que se encontram conectados na plataforma *blockchain*. No caso particular do *Bitcoin* que se utiliza da plataforma *blockchain,* o nó que conseguir resolver a questão e ser eleito o líder da cadeia, este por sua vez recebe *bitcoins* de prêmio. Cabe salientar que muitas *criptomoedas* utilizam-se deste mecanismo.

A este poder de processamento de resolver o “enigma” ou resolver o quebra-cabeça damos o nome de mineração.

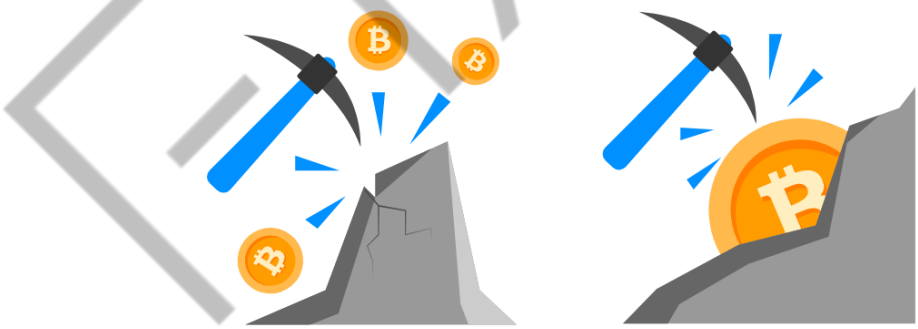


Figura 3.7 – Mineração de Dados
Fonte: Youtube / Block By Block (2017)

3.7.2 Outros exemplos de mecanismos de consenso

- Prova de participação (Proof os stake – Pos).
- Prova de participação locada (leased Poroof of stake – LpoS).
- Prova de participação delegada (delegated proof stake – Dpos).

- Prova de importância (Proof os importance – Pol).
- Prática Bizantina de tolerância a falhas (Practical Byzantine fault tolerance) PBFT.
- Ripple.

3.7.3 Mineração de Dados

No contexto da plataforma *blockchain,* mais especificamente em se tratando do *bitcoin,* mineração de dados diz respeito promover a verificação, validação e atualização de todas as transações decorrentes da estrutura *blockchain,* ou seja, promover o consenso das informações imputadas na plataforma.

As principais funções da mineração de dados são:

- Confirmar as transações.
- Validar as transações.
- Montar os blocos *blockchain.*
- Atualizar as transações efetuadas.

Cada momento que uma transação é efetuada cabe aos mineradores validarem, autenticarem - validarem se a referida transação é autentica -, sendo que o bloco é atualizado a cada 10 minutos, ou seja, de tempos em tempos à corrente de blocos do *blockchain* é acrescida de novas transações, sendo que cada bloco processado é baseado no bloco anterior (*hash* de validação), formando assim a cadeia de blocos.

3.8 Transações Blockchain

- Transação ➔ Duas partes, emissor e receptor, trocam informações/dados, que podem ser de qualquer tipo (dinheiro/contratos/registros), ou seja, qualquer tipo de transação.

- Verificação ➔ A transação é verificada e convertida em um registro seguro, dentro da plataforma *blockchain*. Nesse momento, os nós da rede, através de algoritmos de consenso, verificam se a transação é valida.
- Estrutura ➔ Cada block constituído é identificado por um código alfanumérico de 256 bits (hash), elaborado a partir de um algoritimo. Este bloco possui um cabeçalho, que por sua vez define a sequência de dados.
- Validação ➔ Os blocos criados são validados para fazer parte da cadeia de blocos. Neste momento é que ocorrer a prova de consenso.
- Mineração ➔ Os nós eleito mineiros, solucionam o enigma, e nesse momento, são capazes de autenticar a operação, que por sua vez não pode ser mais alterada.
- Cadeia ➔ Após ter sido validada pelos mineiros, a transação é distribuída pelos outros nós da rede. A partir desse momento, a transação torna-se imutável e passível a auditoria.
- Segurança ➔ Após todo esse procedimento, é impossível modificar a transação, pois qualquer tipo de tentativa de alteração conflitará com os blocos processados, desta forma a alteração é rejeitada.

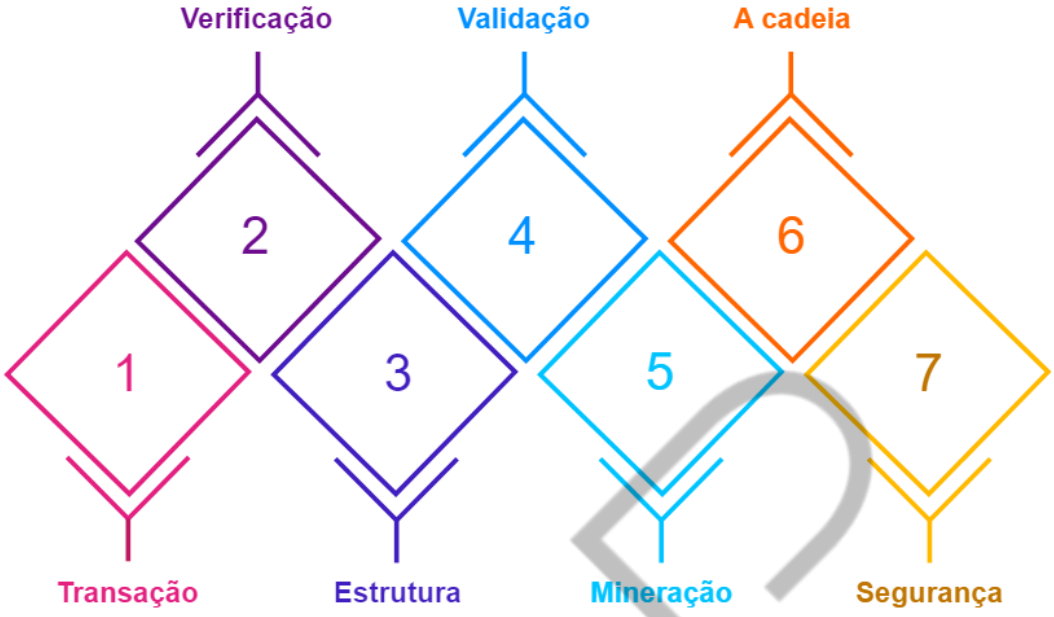


Figura 3.8 – Funcionamento blockchain
Fonte: Simply (2016)

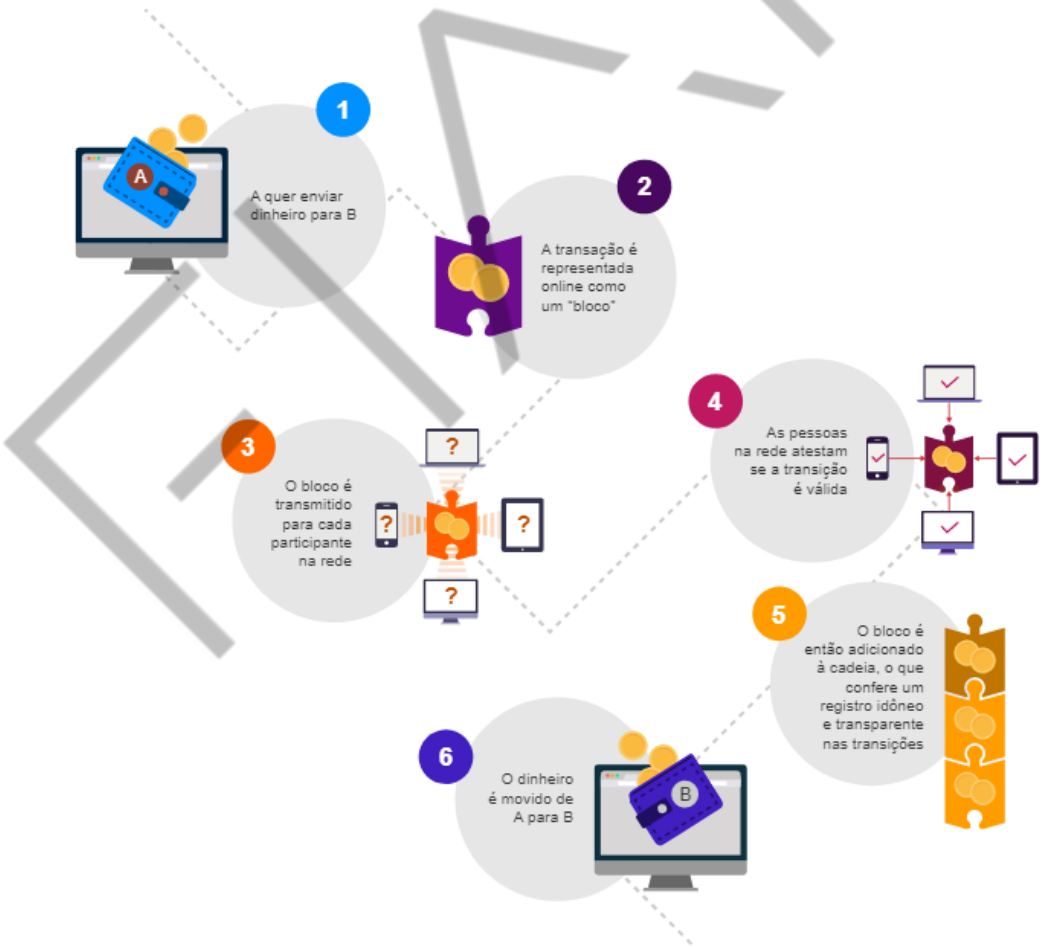


Figura 3.9 – Funcionamento blockchain
Fonte: Blog MJV (2016)

CONSIDERAÇÕES FINAIS

Conforme Tapscot, iniciando seu livro *Blockchain Tevolution*: “Parece que, mais uma vez, o gênio da tecnologia foi libertado de sua garrafa. Invocado em algum momento por um ou alguns desconhecidos com motivações desconhecidas, o gênio está agora a nosso serviço para mais uma oportunidade de impactar nossa vida – transformar a base do nosso sistema econômico e a antiga ordem das relações humanas para melhor”. Já para o blog Rivendel, o interesse pela tecnologia *Blockchain* chegou ao *mainstream.* De acordo com o Gartner, “em fevereiro de 2017, o ‘*blockchain*’ foi o segundo termo mais pesquisado no Gartner.com, um aumento de 400% nos últimos 12 meses. Entre 2015 e 2016, o número de consultas de clientes Gartner cresceram mais de 600%.”

Com base nas definições acima e com base a outras dezenas de referências bibliográficas, podemos concluir que a tecnologia *blockchain* surge para modificar as relações da Internet, bem como para promover profundas mudanças culturais na participação de intermediários de uma forma geral para a execução de todas as relações humanas.

É notório que o ponta pé inicial a esta mudança é a utilização do blockchain para o bitcoin, mas estamos notando o aquecimento da tecnologia para utilização de outros fins, tais como:

- Elaboração de contratos.
- Transações hospitalares.
- Serviços cartorários.
- Transações na área do Direito.
- Eleições.
- Disseminação de cryptomoedas.
- Mercado financeiro.
- Armazenamento de documentos
- Rastreamento de transações.
- Rastreamento de ativos.

De acordo com o blog Cedro Technologies, o *Bitcoin* é a porta de entrada para um futuro digital em que tudo que tem valor pode e, provavelmente, será trocado pela via digital. Os bancos centrais se espelharão na experiência do *Bitcoin* para construir ativos digitais lastreados/garantidos pelos bancos centrais.

Do ponto de vista corporativo, é possível aprender do *Bitcoin* e aplicar tal conhecimento em outros usos, por exemplo, na análise da cadeia de suprimentos de sua empresa, utilizando a tecnologia *blockchain* para rastrear a procedência dos produtos. Você pode fixar uma etiqueta/identificador aos itens ao longo da cadeia de suprimentos e registrar cada movimento diretamente no *blockchain.*

Creio que teremos *blockchains* privados ligados a *blockchains* públicos, similar à forma que pensamos a relação internet e intranet. Se voltarmos à época do lançamento da internet, muitas empresas tomaram um caminho similar: “a internet parece interessante. Na verdade, estamos interessados na intranet. Queremos essa conectividade interna.”

Figura 3.10 – Futuro do Blockchain
Fonte: Google Imagens (2020)

De 2012 a 2019 aumentou exponencialmente o investimento em startups voltadas à utilização da tecnologia *blockchain,* conforme demonstra o gráfico abaixo.

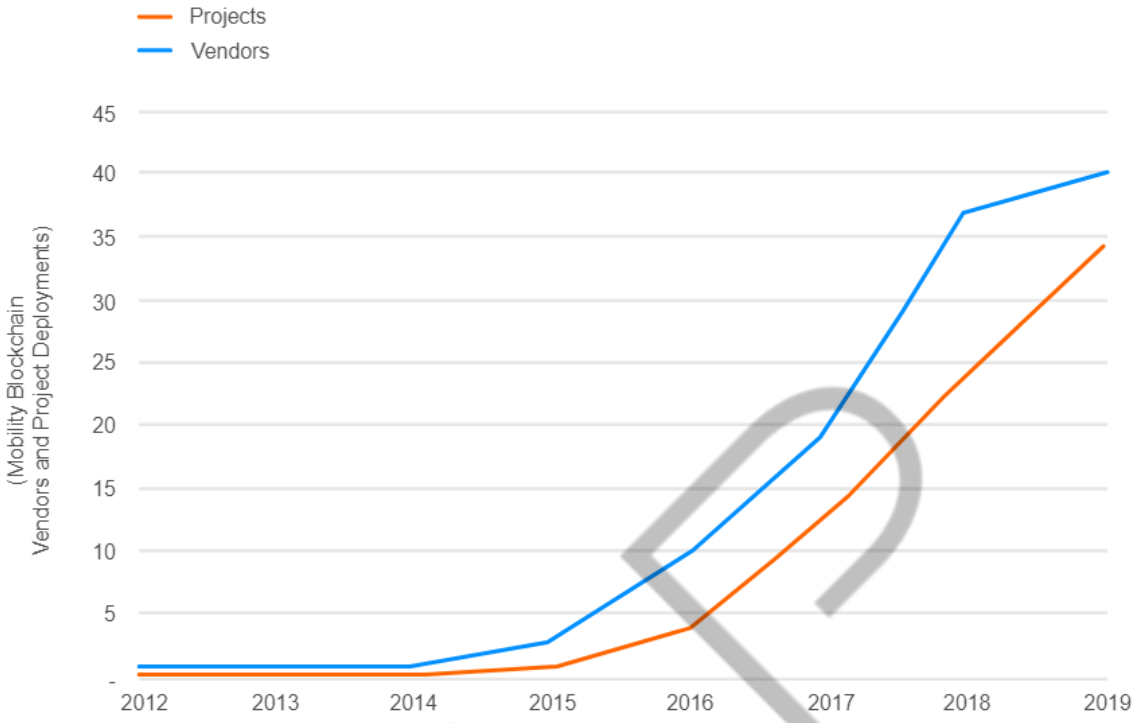


Figura 3.11 – Fornecedores de blockchain
Fonte: automotiveworld.com (2020)

Previsões Blockchain

1. Mercado financeiro adotará o blockchain primeiro
2. Mais casos de uso envolvendo o blockchain devem surgir
3. Países estão considerando regularizar o blockchain
4. Investidores continuarão a financiar startups de blockchain
5. Ethereum crescerá em importância
6. Empresas e organizações reguladoras impulsionarão a interoperabilidade do blockchain
7. A nova tecnologia tornará o blockchain mais rápido e escalável
8. A demanda por talentos em blockchain vai disparar
9. O blockchain pode tornar-se particularmente importante em mercados emergentes

REFERÊNCIAS

AGNER, Marco. **Bitcoin para programadores**. Disponível em: <https://itsriodejaneiro.gitbooks.io/bitcoin-para programadores/content/blockchain.html>. Acesso em: 20 jul. 2020.

BLOG CEDRO TECHNOLOGIES. **Qual é o futuro do blockchain?**. Disponível em: <http://blog.cedrotech.com/o-futuro-do-blockchain/>. Acesso em: 20 jul. 2020.

BRAGA, Alexandre Melo. **Tecnologia Blockchain**: Fundamentos, Tecnologias de Segurança e Desenvolvimento de Software. 2016. Disponível em: <https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper_blockchain_fundamentos_tecnologias_de_seguranca_e_desenvolvimento_de_softwar_FINAL.pdf>. Acesso em: 20 jul. 2020.

COMPUTER WORLD. **Blockchain: o que é e como funciona**. Disponível em: <http://computerworld.com.br/blockchain-o-que-e-e-como-funciona>. Acesso em: 20 jul. 2020.

GAVIÃO, Fausto Carpegeani de Moura. **Do Princípio da Imutabilidade do Nome**. Disponível em: <https://lfg.jusbrasil.com.br/noticias/1068463/do-principio-da-imutabilidade-do-nome-fausto-carpegeani-de-moura-gaviao>. Acesso em: 20 jul. 2020.

GUPTA, Manav. **Blockchain for dummies**: IBM Limited Edition. 2017. Disponível em: <https://bertrandszoghy.files.wordpress.com/2017/05/ibm-blockchain-for-dummies.pdf>. Acesso em: 20 jul. 2020.

JUNIOR, Edilson Osório. **Blockchain e Aplicações Descentralizadas**. Disponível em: <http://irib.org.br/files/palestra/blockchain-02.pdf>. Acesso em: 20 jul. 2020.

LOENERT, Laura. **O futuro do Blockchain: 9 Previsões**. Disponível em: <http://blog.rivendel.com.br/2017/07/24/o-futuro-do-blockchain-9-previsoes>. Acesso em: 20 jul. 2020.

PAPO BITCOIN. **Bitcoin para novatos e iniciados**. Disponível em: <https://www.youtube.com/watch?v=2PQGBwBW1pQ>. Acesso em: 20 jul. 2020.

PIRES, Timoteo Pimenta. **Tecnologia Blockchain e suas aplicações para provimento de transparência em transações eletrônicas**. Disponível em: <http://bdm.unb.br/bitstream/10483/16252/1/2016_TimoteoPimentaPires_tcc.pdf>. Acesso em: 20 jul. 2020.

STELER, Fernando Wosniak; CERQUEIRA, Aurimar Harry. **Cinco princípios básicos do Blockchain**. Disponível em: <http://cio.com.br/tecnologia/2017/03/06/cinco-principios-basicos-do-blockchain/>. Acesso em: 20 jul. 2020.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**: Como a Tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: Senai-SP, 2016.

UNIONPEDIA. **Árvores de Merkle**. Disponível em: <http://pt.unionpedia.org/i/%C3%81rvores_de_Merkle>. Acesso em: 20 jul. 2020.

VAAS, Lisa. **Mensagens baseado em Bitcoin poderia escorregar últimos censores**. 2014. Disponível em: <https://nakedsecurity.sophos.com/pt/2014/12/19/bitcoin-based-messaging-could-slip-past-censors/>. Acesso em: 20 jul. 2020.

VILLIER, Johnathon. **Driving blockchain forward: new innovations and business models to transform mobility**. Disponível em: <https://www.automotiveworld.com/articles/driving-blockchain-forward-new-innovations-and-business-models-to-transform-mobility/>. Acesso em: 20 jul. 2020.