Desmistificando Blockchain: Conceitos e Aplicações

Chapter · August 2018

CITATIONS
0

READS
12,231

6 authors, including:

Paulo Henrique Cardoso Alves
Pontifícia Universidade Católica do Rio de Janeiro
15 PUBLICATIONS **20** CITATIONS
SEE PROFILE

Rodrigo Laigner
University of Copenhagen
17 PUBLICATIONS **57** CITATIONS
SEE PROFILE

Rafael Nasser
Pontifícia Universidade Católica do Rio de Janeiro
18 PUBLICATIONS **123** CITATIONS
SEE PROFILE

Gustavo Robichez de Carvalho
Pontifícia Universidade Católica do Rio de Janeiro
28 PUBLICATIONS **50** CITATIONS
SEE PROFILE

Desmistificando Blockchain: Conceitos e Aplicações

Paulo Henrique Alves, Rodrigo Laigner, Rafael Nasser,
Gustavo Robichez, Hélio Lopes, Marcos Kalinowski

Departamento de Informática
Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)
Rio de Janeiro, RJ, Brasil

Versão dos autores para distribuição.
Referência para citação da versão definitiva:
P.H. Alves, R. Laigner, R. Nasser, G. Robichez, H. Lopes, M. Kalinowski,
"Desmistificando Blockchain: Conceitos e Aplicações", Em: C. Maciel, J. Viterbo (Orgs).
"Computação e Sociedade", Sociedade Brasileira de Computação.

1. Introdução

O ano de 2017 trouxe ao conhecimento popular um modelo de transações financeiras criado em 2008 (Nakamoto, 2008), que extingue a necessidade de uma entidade central para transações de valores. Seguindo este modelo, a criptomoeda Bitcoin experimentou uma rápida valorização e passou a atrair grande atenção de investidores do mercado financeiro, da mídia e de organizações que regulamentam o mercado. No final de Julho de 2018 as 100 principais criptomoedas possuíam valor de mercado acima de 250 bilhões de dólares[1]. Fazendo um paralelo, se a distribuição dos investimentos fosse uniforme, é como se cada ser humano do planeta tivesse em torno de 40 dólares em criptomoedas.

Uma característica das criptomoedas como o Bitcoin é a realização de transações sem um agente intermediador/central, como um banco, por exemplo. Por isso, dizemos que se utilizam de um controle descentralizado. Nesse tipo de controle, a confiabilidade e auditabilidade na operação são garantidas por um processo onde nós em uma rede compartilham a responsabilidade em uma transação. Entretanto, antes de nos aventurarmos nas nuances de como as criptomoedas se utilizam de um controle descentralizado para garantir suas transações, é interessante entender de forma resumida a evolução dos modelos de processamento de transações em larga escala.

Nos anos 60 e 70, com a necessidade de armazenar grandes quantidades de dados pelas organizações, como registros bancários e transações, a IBM lança na indústria o primeiro computador para armazenamento e processamento intensivo de dados. Os mainframes, por meio de uma arquitetura centralizada, permitiam o acesso e interação por meio de um terminal. Entretanto, algumas limitações, como a grande dependência da capacidade do sistema operacional, criaram a necessidade de um outro modelo de processamento.

Na década 80, juntamente com proliferação e evolução dos computadores pessoais, surge o chamado modelo cliente/servidor. Neste modelo o processo deixa de estar limitado a um

[1] www.coinmarketcap.com

único ator (o mainframe) e os papéis em uma transação tornam-se divididos. O modelo cliente/servidor, ao contrário do modelo de processamento baseado em mainframes, abriu a possibilidade de uma transação ser realizada de forma remota. Isto é, não dependente de um terminal de acesso direto a um mainframe.

Entretanto, neste modelo o servidor é normalmente responsável por prover acesso aos dados e realizar as operações de recebimento e processamento de dados. Assim, o modelo cliente/servidor pode envolver riscos de segurança ao confiar em um servidor central como autoridade sobre os dados. Não é difícil imaginar que uma modificação não desejada em dados possa ser causada por um agente externo caso este obtenha o controle sobre os dados, podendo trazer impactos significativos.

Nesse contexto, surge a tecnologia utilizada pelas criptomoedas e que representa o tema central deste capítulo, blockchain. A blockchain provê uma forma singular de proteger os dados sobre a rede, utilizando um controle descentralizado para garantir a segurança em suas transações. De forma resumida podemos definir Blockchain como segue.

Definição: Blockchain

Blockchain é uma tecnologia que faz uso de uma arquitetura distribuída e descentralizada para registrar transações de maneira que um registro não possa ser alterado retroativamente, tornando este registro imutável.

A definição acima é premeditadamente introdutória e esclarece mais o propósito do que os detalhes e as aplicações da tecnologia. Detalhes sobre os conceitos básicos de blockchain, sua arquitetura e características, como transparência e estrutura de dados, são providos na Seção 2. Além disso, os diferentes tipos de blockchain e implementações de validação de transações são analisados para prover uma contextualização adequada sobre o tema.

Atualmente, as aplicações da tecnologia blockchain transcendem questões ligadas à segurança e a tecnologia tem sido considerada para criar soluções inovadoras e disruptivas em diversas áreas de negócios. Desta forma, é fundamental que profissionais envolvidos na área de computação tenham também uma compreensão básica de aplicações da tecnologia que lhes permita refletir sobre seus potenciais impactos na sociedade. Exemplos dessas aplicações que podem servir para subsidiar essa reflexão são descritos na Seção 3. Por fim, as considerações finais, incluindo uma discussão a respeito de benefícios, limitações e tendências, são providas na Seção 4.

2. Conceitos Básicos

2.1. Arquitetura

A tecnologia blockchain pode ser compreendida como um livro público, mantido pela cooperação e interação de nós em uma rede. Este livro é responsável por armazenar todas

as transações ocorridas em um sistema. Dessa forma, diferentemente de sistemas bancários, não há uma autoridade central em que se confia o processamento de transações.

Uma vez que uma transação é escrita neste livro público, a mesma não pode ser alterada. Ou seja, a inserção de novas transações é permitida, entretanto, a alteração ou exclusão de qualquer transação existente é uma operação não suportada. Ou seja, blockchain envolve necessariamente um armazenamento imutável de dados.

Toda a rede, por meio de seus nós, chega a um acordo antes que uma transação seja incluída no livro público. Os mecanismos para se chegar a um acordo serão tratados mais adiante. Para que haja uma concordância entre os nós, uma arquitetura de rede conhecida como *peer-to-peer* é tipicamente empregada.

Definição: Redes *peer-to-peer*

Segundo Tanenbaum (2010), em uma rede *peer-to-peer*, os nós agem como clientes e servidores para os outros nós da rede. Quando comparado ao modelo cliente/servidor, onde só há um servidor recebendo e processando requisições, no modelo *peer-to-peer* os nós compartilham responsabilidades de servir a outros nós. Assim, não há um ponto de controle único. É importante notar que para essa troca de informações ocorra, os nós têm de concordar com um conjunto de regras previamente definidas para a comunicação.

A Figura 1 ilustra a diferença na comunicação em um rede baseada na arquitetura cliente/servidor, onde o servidor exerce papel central, e uma rede *peer-to-peer*, onde os nós trocam informações entre si para atingir um objetivo.

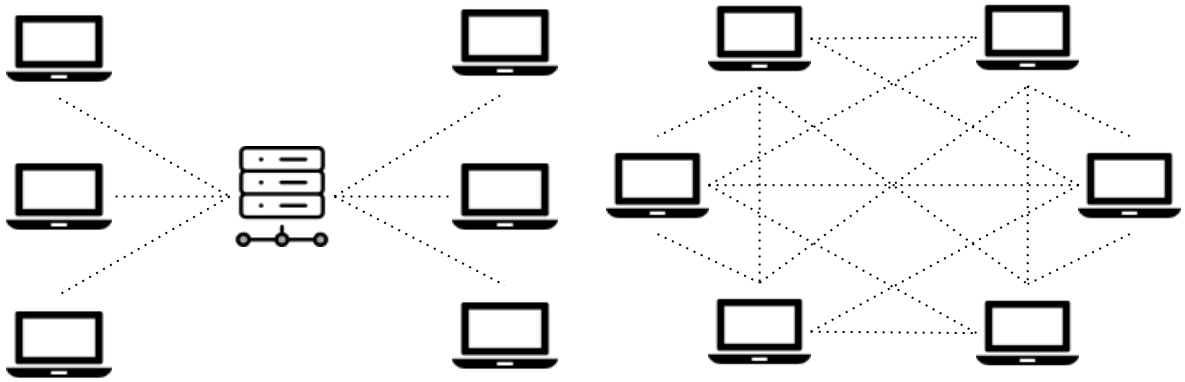

Figura 1. Arquitetura cliente-servidor e arquitetura *peer-to-peer*.

Assim, como ponto de partida, podemos caracterizar a tecnologia blockchain como um um paradigma de computação distribuída que envolve uma arquitetura descentralizada. Na próxima seção iremos ampliar a compreensão da tecnologia provendo mais informações sobre os componentes básicos de uma rede blockchain, os blocos.

2.2. Blocos

Um bloco é a unidade básica de dados de uma rede blockchain. Se caracteriza por ser uma estrutura de dados responsável por armazenar informações sobre um conjunto de transações.

Segundo Xu *et al.* (2016), uma rede blockchain é uma lista ordenada de blocos que tem por objetivo armazenar e reunir informações sobre as transações ocorridas. Uma transação em um bloco é tipicamente composta por informações sobre a data, o proprietário, e, no contexto específico de criptomoedas, o valor monetário transferido. Além disso, cada bloco possui um identificador único (ou impressão digital). Isso garante sua unicidade em toda a rede blockchain e permite que todo bloco seja identificável.

Para que as transações possam ser rastreadas de maneira histórica, um bloco deve possuir o identificador de seu bloco anterior, formando assim uma cadeia de blocos ("*Block chain*" em inglês). Uma outra propriedade importante de um bloco é o timestamp. O timestamp basicamente é uma instância de tempo com informações sobre a data e hora. Essa propriedade torna mais difícil para um atacante manipular a rede blockchain, uma vez que, além de um identificador único, um bloco também possui essa propriedade que varia bloco a bloco.

A Figura 2 apresenta uma representação de como blocos são encadeados em uma rede blockchain, compostos por uma *hash* que o identifica de forma única na rede, a identificação do bloco anterior e o identificador da transação correspondente.

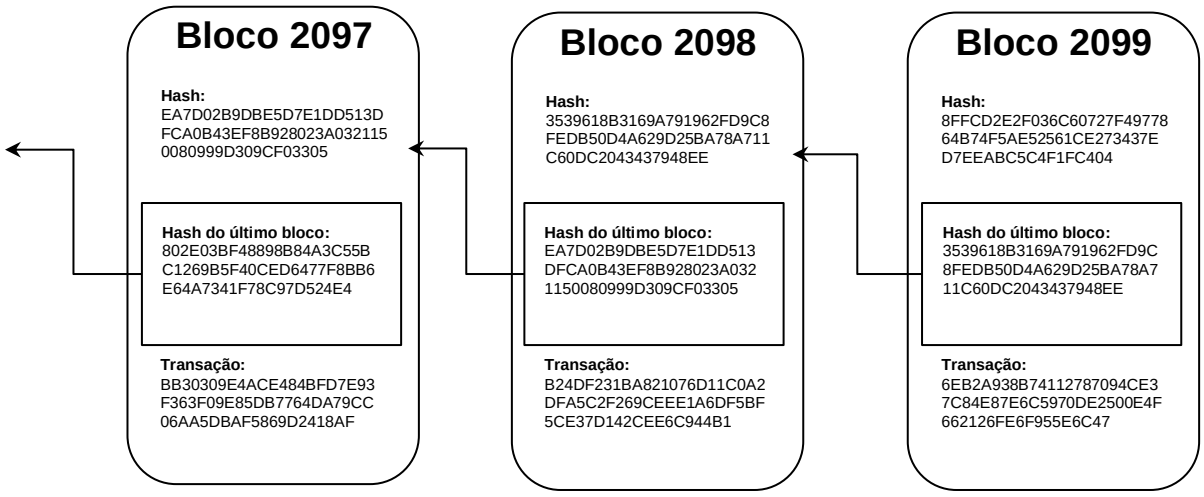

Figura 2: Cadeia de blocos em uma rede Blockchain

Na próxima seção veremos os detalhes de como o registro de todas as transações é compartilhado entre todos os participantes na rede blockchain, mas por ora, podemos afirmar que essa característica é crucial para garantir que um bloco não seja modificado ou inserido entre blocos pré-existentes.

2.3. Descentralização

Como esclarecido na seção sobre Arquitetura, uma rede blockchain tem por premissa não depender de uma autoridade central, sendo os nós na rede responsáveis por validar as transações ocorridas. Entretanto, do início de uma transação ao seu término, dados são compartilhados em toda a rede blockchain. Para isso, um importante conceito em redes de computadores é empregado: *flooding*.

Definição: *Flooding*

Flooding é uma técnica utilizada por roteadores para obter conhecimento sobre os nós da rede, uma vez que se inunda a rede com pacotes marcados como "flooding" por meio das interfaces de saída (para cada pacote recebido em uma interface de entrada, pacotes são enviados por meio das interfaces de saída)

Flooding se torna particularmente importante em uma rede blockchain, pois garante que as requisições sejam entregues a todo nó na rede. Em alguns cenários, isso pode causar um efeito desastroso em performance. Contudo, como veremos na próxima seção, particularmente em uma rede blockchain, a técnica se torna efetiva por garantir transparência, visto que todos os nós recebem informações das transações ocorridas.

Xu *et al*. (2016) sintetizam as etapas desde o início de uma transação até o reconhecimento da mesma por todos os nós na rede da seguinte forma:

"Uma vez criada, uma transação é assinada com a assinatura do iniciante da transação [e também recebe um identificador único, como o bloco a qual pertence], que identifica a autorização para o gasto do valor monetário [(no caso de transações envolvendo criptomoedas)] … A transação é então enviada para um nó da rede blockchain que sabe como validar a transação … [Este, por sua vez,] propaga a transação a um conjunto de nós conectados que [também] irão validar a transação e enviá-las a seus pares de nós até que se alcance todos os nós na rede."

É possível, após a descrição acima, notar a interdependência entre diversos nós e como a cooperação entre eles ocorre para a validação descentralizada de transações. Na próxima seção, abordamos outro conceito fundamental em redes blockchain, integridade.

2.4. Integridade

A integridade dos dados em um sistema é de fundamental importância para a realização de transações. Em bancos de dados tradicionais, ao longo de décadas de pesquisa, diversos mecanismos e técnicas foram desenvolvidos para garantir que, no tocante a uma transação, todas as operações por ela desencadeadas sejam concluídas. Ou seja, no caso de uma operação não concluída, todas as operações anteriores são revertidas e as posteriores são canceladas.

No contexto de uma rede blockchain, uma transação não representa um conjunto de operações, mas sim a mudança de um estado, como por exemplo o débito ou crédito de recursos (criptomoeda) entre contas.

Na seção anterior foi exposto que um conjunto de nós é responsável por verificar as transações na rede de forma descentralizada. Tais nós são conhecidos como nós mineradores. Uma vez verificada por um nó minerador, a transação é então propagada na rede novamente para que mais de um nó minerador possa verificar a validade da transação.

O conjunto de regras pelo qual se define se uma transação é válida ou não, é dependente da implementação da rede blockchain. Exemplos típicos dessas regras encontram-se abaixo:

- O identificador único do bloco está de acordo com a regra de criação
- O timestamp do bloco não pode ser maior que um período pré definido
- O bloco não pode estar duplicado
- O tamanho em bytes atende o número máximo de bytes permitido

Regras de bloco para o Bitcoin

O Bitcoin, por exemplo, define que cada bloco deve ter um timestamp baseado no Unix time. O timestamp é válido somente se a seguinte condição for atendida: o timestamp deve ser maior que a mediana dos timestamps dos últimos 11 blocos e menor que o “tempo ajustado” da rede + 2 horas. O “tempo ajustado” da rede se refere a mediana dos timestamps retornados por todos os nós conectados. Fonte: (Bitcoin Wiki, 2018)

2.5. Transparência

Na seção de arquitetura definimos que a ideia básica de uma rede blockchain é centrada na existência de um livro público. No ato de uma transação, sabemos que a mesma é propagada nó a nó na rede. Este mecanismo é de fundamental importância no processo de verificação da validade de uma transação, como vimos na seção anterior.

Entretanto, para que possamos questionar cada nó sobre seu histórico de registros, é necessário que cada nó, de forma redundante, armazene o livro razão da rede blockchain. Ou seja, cada nó serve como um backup da rede, armazenando cada nova transação. A transparência se refere à possibilidade de visualizar toda e qualquer transação na rede blockchain por qualquer nó pertencente à rede. A seguinte trata com maiores detalhes como diferentes tipos de redes blockchain abordam a transparência.

2.6. Tipos de Blockchain

Uma blockchain pode ser categorizado de três formas: blockchain pública, privada ou híbrida. Uma blockchain pública, como o próprio nome sugere, é uma rede blockchain que tem suas informações abertas ao público e permite a participação de qualquer usuário como nó no processo de consenso. Os usuários que disponibilizam poder computacional para auxiliar

nesse processo recebem uma gratificação caso resolvam um problema matemático, necessário para inserir um bloco na cadeia no caso do *proof of work*. Detalharemos mais esse conceito nas próximas seções.

Entretanto, essa gratificação paga não é obrigatória, os desenvolvedores podem remunerar ou não os nós do sistema, essa questão fica à critério de cada tecnologia de blockchain. Além disso, todos os nós mantém localmente uma cópia da blockchain e o mecanismo de consenso distribuído é então usado para alcançar uma decisão sobre o estado da blockchain, indicando o que será incluído no bloco.

Já uma blockchain privada pode ser acessada somente pelo grupo que criou a blockchain, nesse caso a participação de um nó é definida por esse grupo. Esse tipo de blockchain pode ser útil, por exemplo, em um cenário onde é necessário inserir informações sensíveis ou críticas ao negócio, de forma a não ser interessante ter essas informações expostas à qualquer pessoa. Entretanto, esse tipo de blockchain desvia da ideia de descentralização, pois essa característica, na maioria dos casos, está limitada à quantidade de nós na rede, enquanto uma blockchain pública tende a ter uma maior colaboração da comunidade de desenvolvedores e interessados nessa tecnologia.

Já uma blockchain híbrida, também chamada de consórcio blockchain, pode ser acessada somente por um grupo de indivíduos ou organizações que tenham decidido por compartilhar informações entre si, nesse caso a participação de um nó é definida por um grupo ou uma organização. Esse tipo de blockchain pode ser útil, por exemplo, em um cenário onde diferentes empresas se unem para construir uma blockchain própria, onde apenas as empresas participantes detêm a blockchain propriamente dita, já o direito de leitura e escrita pode ser, ou não, disponibilizado ao público.

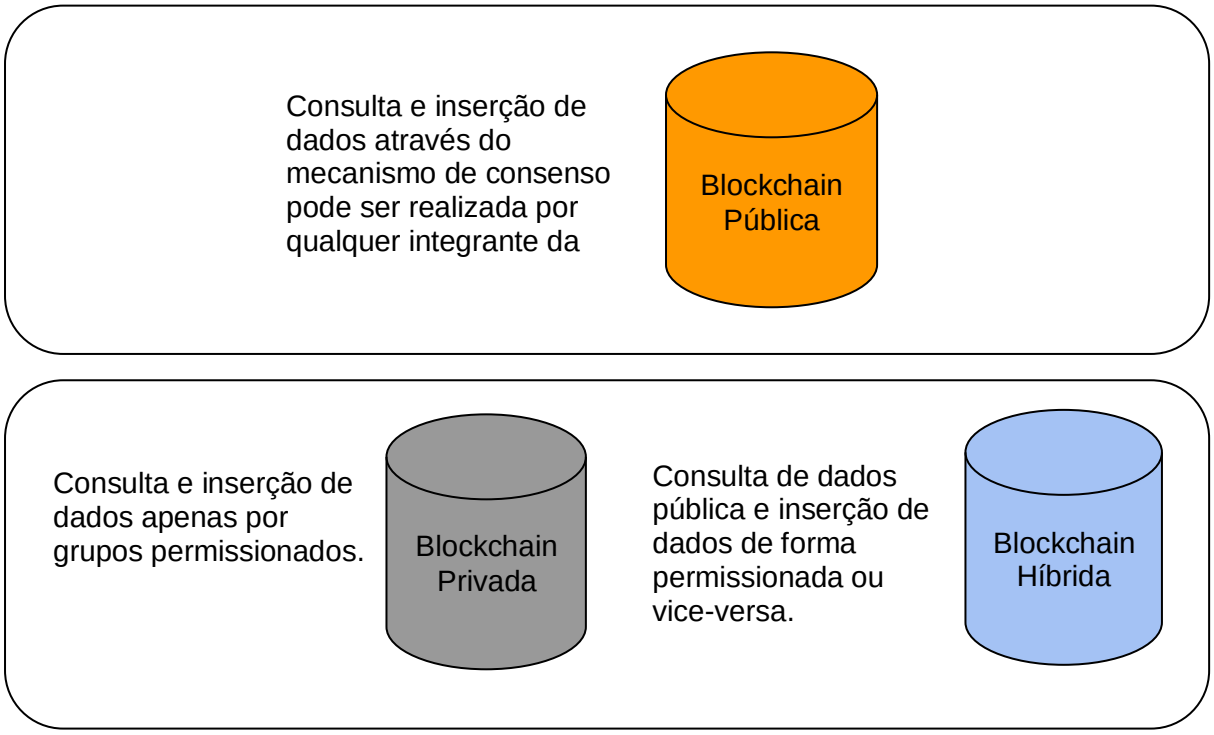

Figura 3: Tipos de Blockchain.

A Figura 3 resume as principais características dos diferentes tipos de blockchain. É interessante fazer a analogia da tecnologia blockchain com o surgimento da Internet em 1990, uma vez que informações trafegam livremente por toda a rede habilitando o desenvolvimento de aplicações, agora sobre essas camadas a Internet e a rede Blockchain sobre a mesma. Alguns autores caracterizam o blockchain como a nova geração da Internet.

2.7. Blockchain e Segurança

A definição sobre qual bloco será inserido na cadeia de blocos é feita de acordo com o mecanismo de consenso adotado por cada projeto. Existem diversos mecanismos diferentes. Dois comumente utilizados são *Proof of Work (*PoW*)* e *Proof of Stake (*PoS*)*. Entender estes mecanismos é fundamental para compreender a maneira que a segurança é alcançada em uma blockchain.

Definição: Mecanismo de Consenso

O mecanismo de consenso é basicamente um conceito de computação distribuída usado na blockchain para prover um acordo na definição de uma versão única do bloco que será enviada para todos os nós da rede sem a necessidade de uma autoridade central.

2.7.1. *Proof of Work* e *Proof of Stake*

O tipo de mecanismo *Proof of Work (*PoW*)* é baseado na resolução de problemas matemáticos, o pool de mineração que encontrar primeiro a resposta para o problema matemático atual ganha uma recompensa pelo poder computacional gasto no processo de resolução do problema. A dificuldade do problema pode ser definida de forma dinâmica, que pode variar de acordo com o uso da rede e da quantidade de blocos por minuto estipulado por cada projeto.

Definição: Pool de mineração

Os pools de mineração são grupos de mineradores que cooperam entre si e que concordam em dividir recompensas de bloco em proporção ao seu poder de hashing de mineração contribuído.

O PoW é utilizado na rede Bitcoin, onde cada nó da rede calcula um valor de dispersão (valor *hash*) que é constantemente alterado (Nakamoto, 2008). Quando nos referimos à um valor *hash*, este é o resultado de uma função *hash*. A função *hash* é um algoritmo que mapeia dados de entrada de comprimento variável para dados de comprimento fixo. Blockchains fazem uso de funções *hash* criptográficas (*one-way hash functions*), onde recriar o valor de entrada utilizando o valor *hash* é praticamente impossível.

Definição: Função *hash* criptográfica

Uma função de dispersão criptográfica ou função *hash* criptográfica (*one-way hash function*) é uma função *hash* considerada praticamente impossível de inverter, isto é, de recriar o valor de entrada utilizando somente o valor de dispersão. Uma função de dispersão criptográfica deve possuir as seguintes propriedades (Schneier, 2015):

- Deve ser fácil computar o valor de dispersão para os valores de entrada
- Deve ser difícil gerar um valor de entrada a partir de seu *hash*
- Deve ser difícil encontrar dois valores de entrada diferentes com o mesmo *hash*.

Os nós que calculam essas funções *hash* são chamados de mineradores e esse processo é chamado de mineração. A Figura 4 exibe o processo de mineração, dividido em três etapas. Em resumo, os mineradores precisam encontrar um valor que gere uma *hash* com determinadas características (por exemplo, um determinado número de zeros).

Além disso, o gasto energético está diretamente associado ao uso do poder computacional, o que torna esse mecanismo um dos mais onerosos sob essa ótica, pois as tentativas de resolução do problema computacional são feitas utilizando a técnica de força bruta, também conhecida por busca exaustiva. Dessa forma, números são testados de forma aleatória até que se chegue em no resultado esperado.

A Figura 4 mostra o funcionamento do PoW, onde os mineradores (ou um pool de mineração) buscam por uma prova de trabalho e recebem uma recompensa pelo esforço computacional empenhado. Como há uma recompensa envolvida, diferentes mineradores e pools de mineração competem entre si para encontrar a solução para esse problema matemático, para então receber a recompensa prometida na definição do projeto.

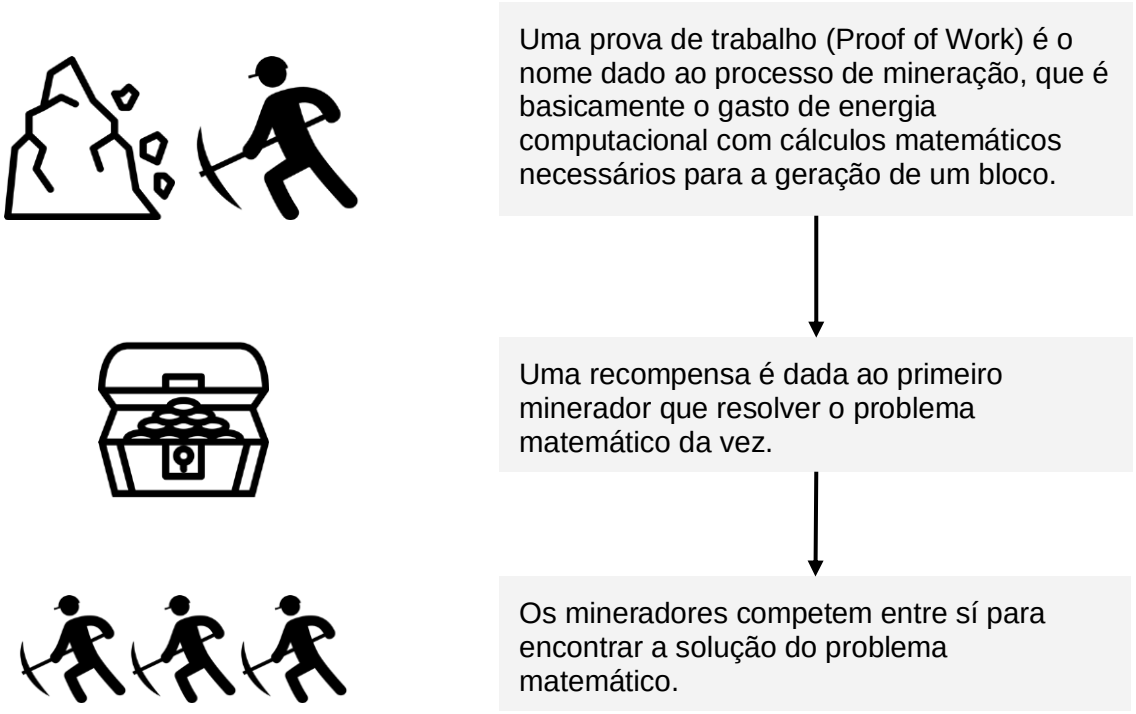

Figura 4: O funcionamento do PoW no processo de mineração.

No caso do Bitcoin foi estipulado que os mineradores receberão uma recompensa de 50 BTC no ato da descoberta de um novo bloco, mais as taxas de transação oferecidas por quem está solicitando a inclusão da transação na blockchain. Esse valor de recompensa é ajustado a cada 210.000 blocos, reduzindo-o em 50%. Esse ajuste é dado em média a cada 4 anos, uma vez que ocorre aproximadamente a mineração de um bloco a cada 10 minutos. Atualmente o valor da recompensa está em 12,5 BTC. O valor da taxa de transação é definido por quem está solicitando a inclusão da transação na blockchain e é utilizado pelos mineradores como critério para definir qual transação terá prioridade de inserção na blockchain. Naturalmente, caso seja necessário realizar uma transação em um momento de congestionamento na rede (muitas transações a serem inseridas no blockchain em um curto espaço de tempo), é natural que um valor de taxa de transação maior seja necessário para que a inserção tenha prioridade. Isso acontece pelo fato dos mineradores selecionam a transações com as maiores taxas de transação, já que eles serão recompensados caso consigam inseri-las na blockchain. Consequentemente, as transações que oferecem taxas com menor valor têm uma baixa prioridade para os mineradores.

Por outro lado, o mecanismo *Proof of Stake (PoS)* é definido de forma que cada nó que possui um *stake* no sistema pode delegar a validação de uma transação a outros nós através de uma votação. Esse algoritmo é uma alternativa ao excessivo gasto de energia realizado pelo PoW (Zheng *et al.*, 2016).

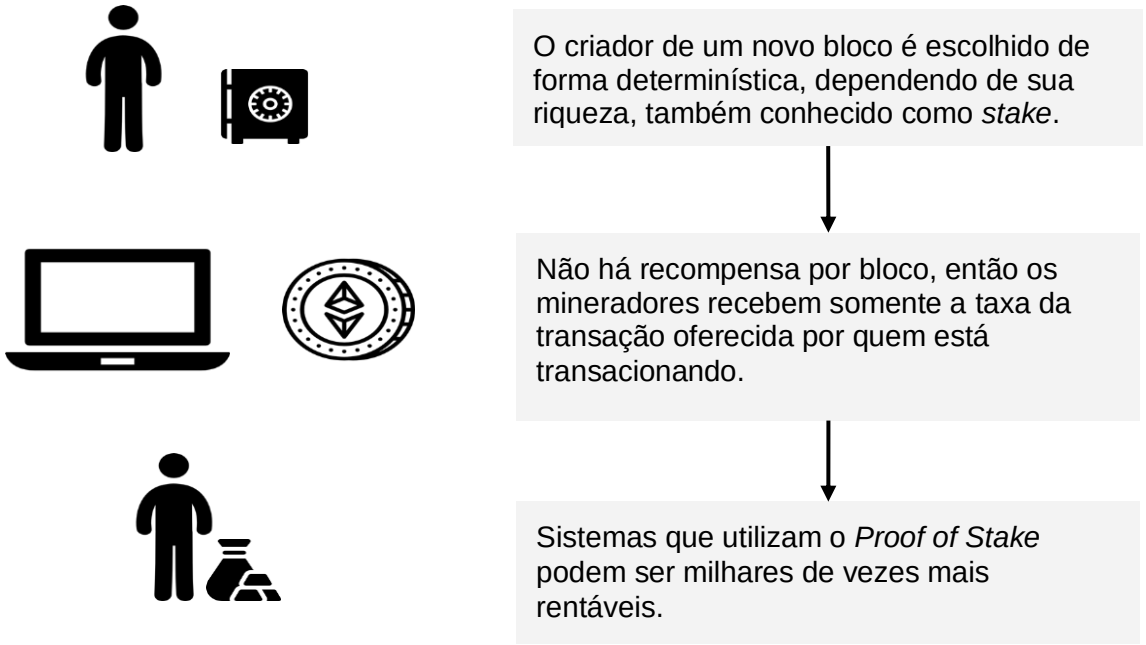

Figura 5: Funcionamento do PoS.

A Figura 5 ilustra como é o funcionamento do PoS, que começa com a definição de forma determinística de um criador de um novo bloco baseado no seu *stake*. Neste mecanismo não há recompensa por um problema matemático resolvido, então os mineradores recebem somente a taxa de transação cobrada no ato das operações de transferência. Com isso há uma enorme redução de esforço computacional gasto, pois não há problemas matemáticos envolvidos que exijam um alto gasto energético.

2.7.2. Segurança

Blockchain, como tecnologia, auxilia no reforço da segurança referente à imutabilidade dos dados e à transparência de transações. Conforme apresentado anteriormente, a blockchain armazena um conjunto de informações descrevendo as mudanças de um estado. Cada bloco inserido na blockchain contém uma *hash* gerada a partir dos dados do bloco anterior. Dessa forma, para realizar a alteração de um bloco já inserido é necessário modificar todos os blocos posteriores, já que a sua *hash* terá sido modificada.

A modificação de um bloco anterior ao bloco atual pode ser efetuada inicialmente sobre a ótica de melhoria ou correção de código. Por exemplo, imagine que um grupo de desenvolvedores de um projeto identificou uma falha no código. Caso todos os desenvolvedores concordem com corrigir esta falha, eles podem optar por voltar para uma outra versão e desconsiderar os blocos posteriores. No caso em que apenas uma parte dos desenvolvedores concorda com a ação de voltar alguns blocos e desconsiderar as transações posteriores, é realizado um *fork* da blockchain, o ramo que continha a falha continua existindo, e um novo ramo é criado a partir de um ponto antes da identificação da falha. A Figura 6 ilustra uma situação de um *hard fork*, onde há nós que rejeitaram as novas regras estipuladas por uma parte da comunidade. Este cenário reforça a relevância da aplicação de testes no desenvolvimento das aplicações que utilizam essa tecnologia (Porru *et al.*, 2017). Já em um *soft fork* uma alteração é sugerida e os membros do projeto de forma conjunta optam por implementar a alteração em questão, dessa forma a cadeia continua sendo única, diferentemente do *hard fork* onde uma outra cadeia é gerada.

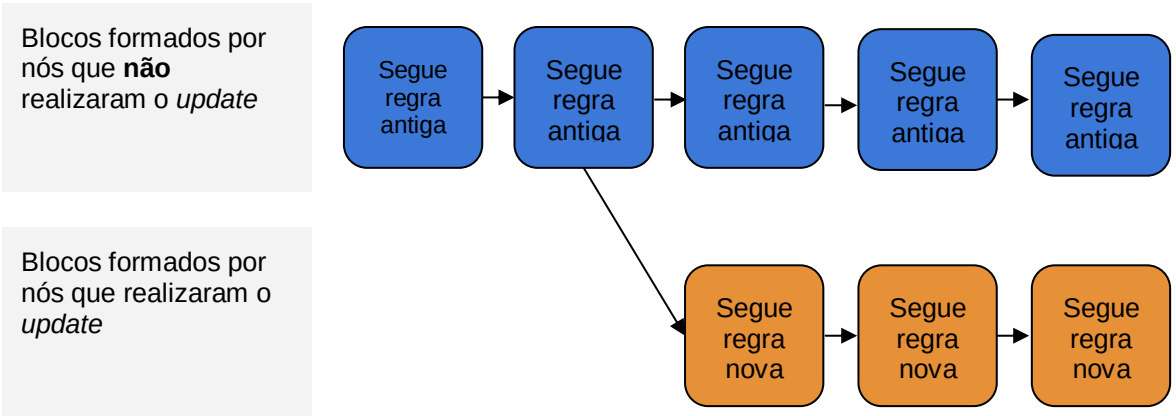

Figura 6: Exemplo de *hard fork*.

Sobre um outro aspecto de segurança, para que uma transação seja inserida em uma blockchain, onde o mecanismo de consenso é o PoW, é preciso que pelo menos 51% dos nós da rede confirmem a transação. Consequentemente, o mecanismo PoW, anteriormente explicado, está sujeito ao ataque de 51%. Isso significa que transações fraudulentas podem ser inseridas/alteradas por alguém que tiver posse de 51% do poder computacional, pois este poderá aprovar as próprias transações, inclusive reescrevendo os blocos na blockchain. Por outro lado, para alguém inserir esse tipo de transação fraudulenta é preciso ter sob controle a maior parte do poder computacional empregado na rede, o que atualmente é praticamente impossível. Além disso, do ponto de vista de retorno financeiro individual de cada minerador, ser honesto é mais vantajoso do que articular um ataque na rede, o que torna ainda mais improvável um ataque desta natureza em redes com inúmeros mineradores. Adicionalmente,

cabe considerar que o próprio valor obtido com a fraude automaticamente se desvalorizaria em função do próprio ataque, o que torna ainda menos atrativo para um minerador agir de forma desonesta.

2.7.3. Outros mecanismos

Como informado anteriormente, existem outros mecanismos de consenso que são utilizados em projetos sobre blockchain e aqui citaremos alguns deles.

O *Proof of Importance* apresenta o conceito de que uma prova de importância não depende somente do saldo de moedas que um usuário tem no sistema, mas também da sua reputação sobre operações anteriores e da quantidade de transações consideradas válidas. Um projeto que utiliza esse tipo de mecanismo é o projeto NEM[2] (https://nem.io).

Já o *Ripple*[3] utiliza um algoritmo de consenso que faz uso da confiança coletiva entre sub-redes e a rede principal. Na rede, os nós são divididos em dois tipos: (i) tipo servidor onde o nó será usado na participação no processo de consenso e (ii) tipo cliente que apenas realiza transferência de valores. O processo é iniciado através dos servidores que realizam a coleta de todas as transações não concluídas e então formam uma lista única - *Unique Node List* (UNL) de candidatos à terem as suas transações efetivadas. Após a criação da UNL os servidores votam sobre a veracidade das transações e as que receberem o número maior que o mínimo estipulado na rede deverão seguir para a próxima etapa, enquanto as transações que não conseguiram alcançar tal número deverão ser descartadas ou enviadas para um novo livro-razão para serem analisadas posteriormente.

Um outro mecanismo é o chamado *Delegate Proof of Stake (DPOS).* Ele foi criado pela organização Bitshares[4] e nesse mecanismo os *stakeholders* podem eleger representantes para gerar blocos. Cada conta recebe um voto por ação por representante e os N principais representantes são capazes de gerar blocos. Quando um representante gera um bloqueio, ou seja, quando for identificada alguma irregularidade, ele recebe uma recompensa pelo serviço prestado. Na maioria dos casos, o representante compartilhará sua recompensa com as pessoas que votaram para elegê-lo. O projeto Lisk[5], por exemplo, permite que os 101 representantes mais votados gerem blocos. Cada representante tem 10 segundos para gerar um bloco, porém, caso ele não o faça, o trabalho será redirecionado para o próximo representante. Além disso, o representante que não puder gerar blocos tem grande chance de perder a sua classificação no ranking.

Esse são apenas alguns mecanismos de consenso, a qualquer momento um novo mecanismo pode surgir com uma proposta diferente das demais já existentes, diferenciados pelo consumo energético, ou pela metodologia aplicada para eleger algum representante, ou por qualquer outro fator que seja considerado relevante. Na seção seguinte serão tratados algumas aplicações que utilizam a tecnologia blockchain.

---

[2] https://nem.io
[3] https://ripple.com
[4] https://bitshares.org
[5] https://lisk.io

3. Aplicações

3.1. Introdução

Como descrito anteriormente, a arquitetura da tecnologia blockchain habilita uma transparência centrada no conceito de um livro razão público. Quando pensamos em transações financeiras, podemos facilmente associar o acesso ao livro razão como uma forma de compreender e auditar todas as mudanças de estado ocorridas. De fato, criptomoedas e serviços financeiros estão entre as principais aplicações da tecnologia. Transações financeiras comumente são atividades fim de uma troca comercial anterior ou de acordos firmados entre as partes. Neste contexto a tecnologia pode apoiar a expressar acordos imutáveis entre as partes na forma de contratos inteligentes. As criptomoedas e os contratos inteligentes serão abordados nas Seções 3.2 e 3.3, respectivamente.

No cenário nacional, uma instituição que se posicionou na vanguarda do uso da tecnologia foi o BNDES, que tem experimentado utilizar a tecnologia para apoiar processos de financiamento, monitoração e avaliação de projetos de desenvolvimento (Moreno *et al.*, 2018). De fato, este pode ser visto como um exemplo de uma gama de aplicações possíveis da tecnologia e do seu potencial de agregar valor a diferentes áreas de negócio.

As possibilidades de aplicação da tecnologia blockchain, com soluções comumente envolvendo conceitos como segurança, privacidade, identidade e eficiência operacional de maneira geral, são plurais e multidisciplinares. O Departamento de Informática da PUC-Rio, na ideologia da universidade como o local onde empresas e acadêmicos se reúnem com o objetivo de compartilhar conhecimento e experimentar ideias, se posicionou de maneira pioneira na discussão de soluções envolvendo a aplicação da tecnologia. Blockchain tem sido pauta frequente da iniciativa ECOA PUC-Rio[6] onde se discutem, em parceria com empresas e focando em suas reais necessidades, soluções disruptivas para diversas áreas de negócio. Os vídeos disponíveis na *playlist* de blockchain[7] da iniciativa permitem facilmente observar o envolvimento e interesse dos grandes atores do mercado. Empresas chave de diversos segmentos, como óleo e gás, mídia e comunicações, financeiro, telecomunicações e seguros, entre outros, tem participado ativamente das discussões a respeito de aplicações da tecnologia. Diversas empresas têm estabelecido parcerias com o Laboratório de Engenharia de Software[8] (LES) para explorar e desenvolver soluções inovadoras utilizando a tecnologia.

Visando fornecer uma compreensão de algumas possíveis categorias de aplicações, além das criptomoedas (Seção 3.2) e dos contratos inteligentes (Seção 3.3), o restante deste capítulo discorre a respeito de algumas outras aplicações típicas da tecnologia blockchain, tais como Gestão da Identidade e Proveniência (Seção 3.4) e Transparência Pública (Seção 3.5). Uma visão dinâmica envolvendo soluções específicas aplicadas em diferentes áreas de negócio pode ser consultada através da iniciativa ECOA PUC-Rio[5].

[6] http://www.puc-rio.br/ecoa
[7] https://goo.gl/NxZJAE
[8] http://les.inf.puc-rio.br

3.2. Criptomoedas e Serviços Financeiros

A primeira aplicação de uma blockchain foi em 2008, quando Satoshi Nakamoto descreveu em seu White Paper o funcionamento da criptomoeda Bitcoin (Nakamoto, 2008). O conceito da tecnologia blockchain veio embutido na definição do Bitcoin, como uma arquitetura que torna a aplicação dos conceitos de alta disponibilidade, imutabilidade, transparência e ausência de entidade centralizadora possíveis em uma única estrutura concatenada de blocos. O Bitcoin foi a criptomoeda pioneira. Diversos outros projetos com caráter financeiro foram desenvolvidos baseados no Bitcoin, muitos deles são projetos derivados do Bitcoin com algumas alterações.

As moedas digitais têm despertado interesse de cidadãos de diferentes lugares ao redor do mundo, dentre os principais motivadores para esse aumento na procura sobre o assunto estão:

- A liberdade para o envio de valores entre diferentes países com taxas consideravelmente mais baixas que as dos bancos tradicionais.
- A não existência de uma entidade central, como um banco por exemplo, que regula as transações
- Serem moedas tipicamente deflacionárias. No caso do Bitcoin, apenas 21 milhões de moedas podem ser mineradas, impossibilitando a emissão de novas moedas.
- A alta dificuldade para realizar uma fraude. No caso do Bitcoin, que utiliza o mecanismo de consenso PoW, para isso seria necessário ter o controle de pelo menos 51% do poder computacional de toda a rede, como discutido anteriormente.
- A possibilidade, dependendo da moeda, de participar como nó na resolução dos problemas matemáticos, podendo ser recompensado financeiramente por isso, recebendo o valor das taxas pagas pelos usuários e a recompensa por ter resolvido um problema matemático.

Segundo o *CoinMarketCap*[1], portal utilizado para verificar a distribuição de moedas e *token*s pelo mercado digital, dentre os projetos com maior valor de mercado, no momento da escrita deste capítulo, estão: Bitcoin, Ethereum, Ripple, BitcoinCash e EOS. Popularmente os projetos em blockchain envolvendo criptomoedas são divididos em dois grupos, o Bitcoin e as AltCoins, que engloba todos os projetos, exceto o Bitcoin.

Na essência, as criptomoedas são um ativo digital, mas não são os únicos. Outro conceito importante no mundo de criptomoedas é o de ICO (*Initial Coin Offer*), onde pode ser feita uma analogia ao mercado financeiro tradicional com o IPO (*Initial Public Offering*). Dessa forma, o ICO é o nome dado ao início da geração de valor para um determinado projeto/empresa, onde serão oferecidos ativos digitais, chamados de *token*s, para quem participar dessa etapa inicial. Entretanto, por não ter uma regulamentação definida como temos no mercado de ações com todos os requisitos para poder realizar um IPO, o ICO pode ser feito por qualquer pessoa em qualquer etapa do projeto, em alguns casos o ICO é feito mesmo sem o projeto estar minimamente funcional. Essa falta de regulamentação traz um alto risco de investimento para quem quiser participar, pois existe o risco de um projeto ser uma fraude e o investidor perder toda a quantia aplicada.

Esses *token*s nada mais são que uma representação quantitativa de algo que dentro de um contexto tem valor, por exemplo, dentro das relações regidas por um contrato inteligente. Normalmente esses *tokens* podem ser divididos em três categorias em função dos direitos que concedem aos seus titulares:

- *Security Token*: concede o direito à participação nos dividendos do emissor (assemelha-se a uma ação preferencial no mercado de ações na bolsa de valores);
- *Equity Token*: confere o direito a voto, além da participação nos dividendos do emissor (assemelha-se a uma ação ordinária no mercado de ações na bolsa de valores);
- *Utility Token* (são sinônimos *User Tokens* e *App Tokens*): confere o direito a uma recompensa em serviços ou produtos do emissor (assemelha-se aos vouchers de crowdfunding).

Como exemplo, vamos supor que exista um projeto específico relacionado ao armazenamento de dados em uma rede distribuída. Um *utility token* poderia ser utilizado para permitir o uso de K megabytes do serviço por um determinado tempo e este serviço poderia ter um valor associado. Cabe observar que, em última leitura, podemos entender que o Bitcoin e outras AltCoins são *tokens* que representam um determinado poder de consumo.

3.3. Contratos Inteligentes

Nick Szabo, cientista da computação, em 1994 apresentou o conceito de contrato inteligente como uma forma de reduzir ambiguidade e automatizar relações jurídicas. Essas ideias foram a base para Vitalik Buterin em 2014, na época estudante na universidade de Waterloo no Canadá, levar esse conceito para um novo patamar ao publicar o *White Paper* "*A Next-Generation Smart Contract and Decentralized Application Platform*" e implementá-lo em um projeto de blockchain chamado Ethereum (Buterin, 2014).

Um contrato inteligente pode ser entendido como um agente autônomo armazenado em uma blockchain, onde o contrato é enviado da mesma forma que uma transação. Assim, ele deve ser aprovado pelos nós da rede de acordo com o seu mecanismo de consenso. Uma vez criado, o contrato inteligente é identificado por um endereço para que possa ser chamado por outros sistemas, usuários e até mesmo por outros contratos inteligentes.
Esses contratos são caracterizados não só por sua imutabilidade, descentralização e transparência, que são características de um blockchain, mas também pela ausência de ambiguidade, uma vez que precisam ser interpretados pela máquina, característica que geralmente pode ser encontrada e explorada em contratos tradicionais. O contrato inteligente é um código como outro qualquer, que será executado exatamente da forma em que foi programado. Normalmente este código é do tipo: se (condição satisfeita) então (ação).

Assim, uma vez disponível na rede, o contrato não pode ser modificado, ou sofrer qualquer intervenção em sua execução, a única opção possível é de parar o contrato caso uma função *kill* tenha sido programada, dessa forma o contrato deixará de existir assim que essa função for chamada. Assim, contratos inteligentes não podem ser alterados depois de serem enviados para uma plataforma, garantindo que nenhuma cláusula do contrato seja alterada. Com base nisso, torna-se extremamente necessário realizar testes antes de enviar um

contrato para uma plataforma, pois todos os casos possíveis devem ser cobertos por testes para que não ocorra nenhum problema ou desvio de valores durante a sua execução.

A partir do momento em que um contrato está disponível na rede, qualquer pessoa poderá utilizá-lo. Entretanto, como a manutenção da blockchain pode demandar alto poder computacional, normalmente há um custo para enviar e executar os contratos a fim de cobrir os gastos energéticos requeridos pela plataforma distribuída. Esse custo de execução recai sobre quem chama um contrato inteligente e é baseado na complexidade do contrato. Um contrato com baixa complexidade tem o seu custo de execução mais baixo e normalmente é mais fácil de ser interpretado por outros desenvolvedores, ou até mesmo por pessoas que não são da área técnica, favorecendo a transparência do ponto de vista do entendimento do que é executado no contrato. Por outro lado, um contrato de alta complexidade proporcionará um alto custo a quem for executá-lo e poderá dificultar o entendimento de sua execução. Além disso, tomando a blockchain do Ethereum para um entendimento mais profundo, essa é basicamente uma máquina de estados Turing completa baseada em transações. Uma máquina de estados é definida como algo que através de um conjunto de entradas e transições irá se transformar em um novo estado, conforme é mostrado na Figura 7.

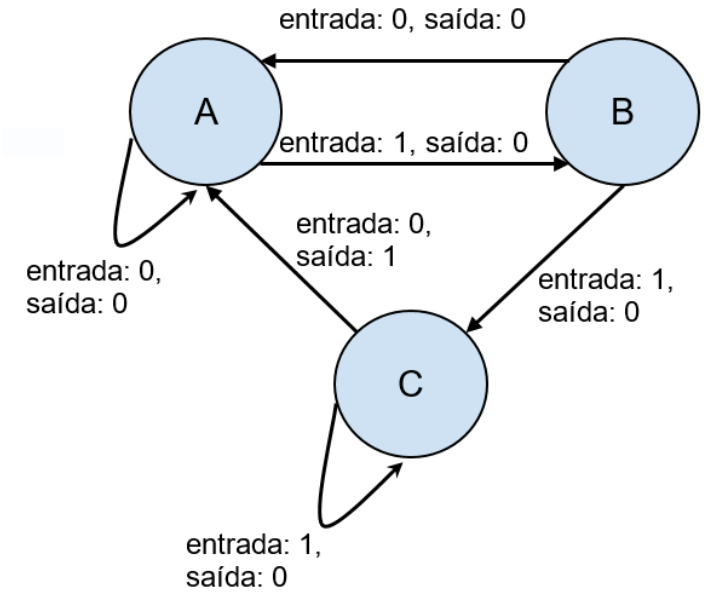

Figura 7: Exemplo de máquina de estados.

Na representação de uma máquina de estados do Ethereum o primeiro estado é chamado de "estado genesis", ou marco zero, estado anterior à execução qualquer transação. Ao executar uma transação, esse marco zero sofre uma transição para algum estado final e esse estado final sempre representará o estado atual do Ethereum, conforme ilustrado na Figura 8.

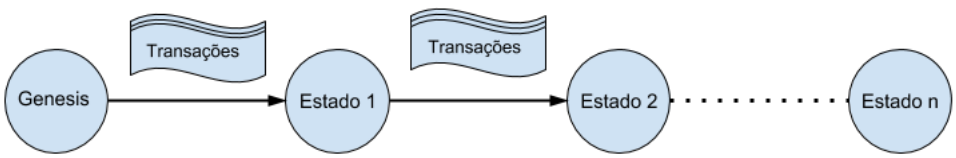

Figura 8: Exemplo de máquina de estados no Ethereum.

Dessa forma, o domínio dos conceitos de engenharia de software e análise de algoritmos são essenciais para a construção de contratos com menos falhas e mensuração do valor de execução de forma justa conforme a complexidade exigida pelo domínio da aplicação (Destefanis *et al.*, 2018).

A Figura 9 ilustra o acordo entre duas partes em forma de contrato inteligente, onde o contrato executa suas funções, como por exemplo o disparo de pagamento em uma data pré-determinada contida em uma cláusula do contrato. Nesse caso as partes podem utilizar um contrato inteligente já instanciado na plataforma Ethereum ou um deles pode criar um novo contrato e enviá-lo para a plataforma, para o exemplo em questão assumimos que um novo contrato foi criado.

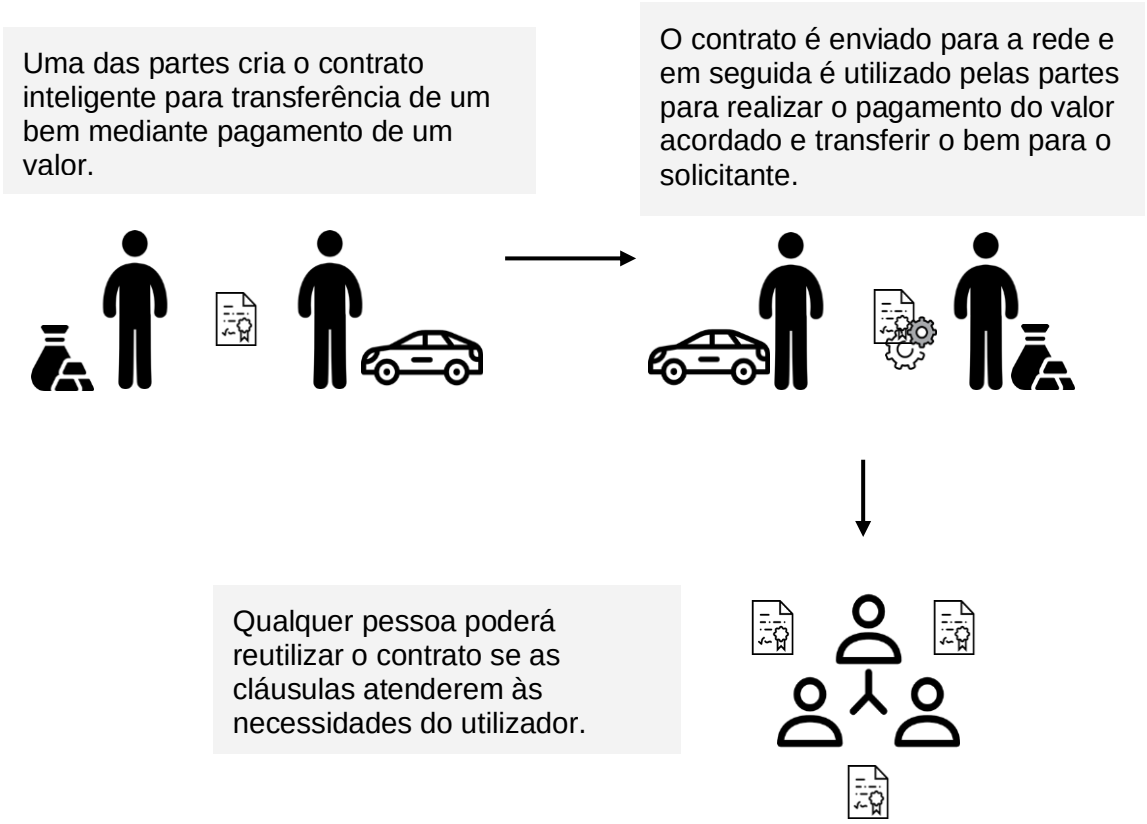

Figura 9: Exemplo de aplicação de um contrato inteligente.

Em relação à segurança, a segurança trazida pelo mecanismo de consenso é baseada na suposição de que mineradores honestos sejam racionais, ou seja, que é mais fácil seguir o protocolo estipulado pelo mecanismo de consenso do que tentar realizar um ataque (Atzei *et al.*, 2017).

Existem algumas plataformas para implementar contratos inteligentes, entre elas: Ethereum, Hyperledger, EOS e NEO. Por ser uma tecnologia ainda muito recente, muitos aspectos políticos, como a regulamentação e o reconhecimento por parte das principais organizações mundiais, e também técnicos ainda tem espaço para evolução.

3.4. Gestão de Identidade e Proveniência

A tecnologia blockchain pode trazer benefícios também do ponto de vista de gestão de identidade. Por exemplo, em relação à colaboração internacional, onde uma base única de dados poderia disponibilizar informações criptografadas dos cidadãos. Algo análogo ao passaporte, onde a utilização dessa informação apenas será possível caso a chave privada do usuário seja informada. Imagine o cenário onde passaportes, documentos de identidade, carteiras de motorista sejam substituídos por um simples *QR Code* onde a validação é feita através de uma chave privada. Não seria mais importante carregar ou se preocupar com esses documentos físicos. A Figura 10 exemplifica o uso do *QR Code* juntamente à chave privada, resultando no documento descriptografado.

Figura 10: Exemplo de uso de identidade.

No cenário atual é difícil listar com exatidão quais empresas tem nossas informações à disposição como lojas online, bancos, hospitais e outras empresas de prestação de serviço. Com isso, quando um dado confidencial é vazado, é difícil dizer com exatidão qual a fonte de dados foi responsável pelo ocorrido. Outro ponto importante a ser destacado sobre o assunto é a centralização dos dados, cada serviço armazena os dados da forma que considerar melhor, portanto o nível de exposição dos dados é bastante elevado a depender da quantidade de serviços online utilizados. Por outro lado, com a descentralização oferecida intrinsecamente pela tecnologia blockchain, esse grau de exposição e de vulnerabilidade é diminuído, visto que o ataque a uma rede descentralizada exige uma maior coordenação e um maior poder computacional como visto nas seções anteriores.

Definição: *QR Code*

QR Code (sigla do inglês *Quick Response* - resposta rápida em português) é um código de barras bidimensional que pode ser facilmente escaneado usando a maioria dos telefones celulares equipados com câmera. Esse código é convertido em texto, podendo conter, por exemplo, um endereço URI, um número de telefone, uma localização georeferenciada ou um e-mail.

Já sobre a ótica de proveniência, o projeto *Everledger Diamonds Platform*[9] exemplifica o assunto de forma simples. O projeto foi criado com o intuito de identificar todas as etapas da produção de diamantes, desde a extração até a chegada ao consumidor final. Dessa forma, todos os passos da cadeia produtiva são armazenados em uma blockchain para que o consumidor final tenha a garantia de que ele está comprando um produto que não foi falsificado ou até mesmo roubado, pois todas as transações do produto estão armazenados de forma imutável na blockchain do projeto.

[9] https://diamonds.everledger.io

É fácil imaginar um processo similar sendo aplicado a outros produtos que são passíveis de falsificação e/ou para os quais se queira informações de proveniência que permitam entender como foram realizadas as etapas do seu processo de produção. No caso de vinhos, por exemplo, poderia se saber com exatidão a partir do rótulo informações da colheita ao engarrafamento.

3.5. Transparência Pública

A sociedade demanda cada vez mais por transparência. A sanção da lei da transparência no Brasil, em 2010, é prova de um esforço contínuo de cidadãos preocupados com o destino de impostos e recursos públicos e sua posterior aplicação por agentes do governo. No contexto brasileiro, os esforços em transparência se tornam mais prementes pelo desencadeamento de diversos escândalos de corrupção ao longo dos anos e pela frequentemente distorcida distribuição de recursos públicos, nem sempre priorizando os reais interesses da população.

A tecnologia blockchain pode ser empregada para o monitoramento de gastos na gestão pública, habilitando, por exemplo, a visualização de toda a cadeia de transações desencadeada desde o pagamento de um imposto até sua aplicação. De fato, a tecnologia blockchain já tem sido utilizada na gestão pública. O governo sueco, por exemplo, experimenta blockchain como um meio para alcançar agilidade no processo de registro de terrenos[10]. Utilizando uma rede blockchain privada, envolvendo apenas nós autorizados, cópias de registros são compartilhados por bancos e agentes imobiliários. Assim, cada passo no processo de compra de uma propriedade pode ser auditado na rede blockchain, onde o acesso aos registros pode ser feito por qualquer nó. Com base na transparência provida pela blockchain, o objetivo do governo é reduzir o risco de fraudes.

4. Considerações Finais

A tecnologia blockchain se caracteriza por prover a imutabilidade dos dados, descentralização, alta disponibilidade, transparência e segurança. Assim, o uso dessa tecnologia permite desenvolver aplicações com as características supracitadas. Como vimos, a tecnologia tem sido utilizada para criar soluções disruptivas que beneficiam diferentes áreas de negócio. Moedas digitais que transcendem barreiras físicas entre países, investimento em projetos além das fronteiras com *tokens* que podem ser aproveitados como crédito para a utilização de um determinado serviço, transparência na gestão pública, rastreamento de proveniência, seguros regulados por objetos conectados. Nesse tema é possível dar asas à imaginação.

Essas aplicações podem empregar a tecnologia de forma customizada de acordo com o uso pretendido. Essas customizações podem envolver, por exemplo, a definição do tipo de blockchain (público, privado ou híbrido) e do tipo de mecanismo de consenso a ser utilizado (PoW, PoS, entre outros). É importante ressaltar que a performance das aplicações criadas

[10] "Sweden Trials Blockchain for Land Registry Management." Disponível em http://www.computerweekly.com/news/450421958/Sweden-trials-blockchain-for-land-registry-management (último acesso em 27/07/2018)

na tecnologia é fortemente dependente do mecanismo de consenso adotado. A estimativa de gasto energético da rede do bitcoin, que utiliza o algoritmo *proof of work* é de 14 gigawatts até 2020. Tendo isso em vista, as pesquisas sobre outros mecanismos mais econômicos estão ganhando cada vez mais espaço nos projetos que utilizam a tecnologia blockchain.

Ainda em relação às aplicações, Bashir (2017) de forma otimista relata algumas tendências que poderão se tornar realidade entre os anos 2020 e 2050:

- A internet das coisas (IoT) será executada em blockchains e aumentará a economia gerada de máquina para máquina.
- O compartilhamento de dados médicos será feito de forma segura preservando a privacidade dos pacientes em blockchains híbridos formados por grandes entidades renomadas da área.
- Eleições serão feitas através de sistemas web distribuídos baseados em uma blockchain, de forma transparente e segura.
- Instituições financeiras terão blockchains privadas e compartilharão dados entre os participantes para um processo interno de seleção de clientes e projetos.
- Atividades de imigração e controle de fronteira serão armazenadas em uma blockchain e o controle de passaportes será conduzido via compartilhamento de dados de uma blockchain entre diferentes entidades ao redor do mundo.
- Os investimentos em criptomoedas crescerão e um novo modelo de economia surgirá.

Cabe ressaltar que a tecnologia blockchain ainda não é madura o suficiente para que seja integrada de forma simples aos sistemas existentes. Mesmo com os padrões de tecnologia existentes e aplicados atualmente, duas redes blockchain não se comunicam de forma trivial. Recentemente algumas iniciativas têm surgido visando padronização. A mais notável é a criação do comitê técnico da ISO, ISO/TC 307[11] (*Blockchain and distributed ledger technologies technical committee*), com o objetivo de desenvolver padrões para a tecnologia blockchain. O objetivo principal desse comitê é viabilizar o aumento de interoperabilidade e troca de dados entre usuários, aplicações e sistemas.

Além disso, a tecnologia blockchain pode ser considerada como uma *Distributed Ledger Technology* (DLT), ou seja, uma tecnologia baseada em um livro razão distribuído. Portanto, blockchain é apenas uma DLT e diversas tecnologias podem surgir baseadas nesse conceito, preservando a essência de conter as características de uma aplicação imutável, transparente e distribuída, mas não necessariamente implementada como uma cadeia de blocos. De forma geral podemos organizar essas tecnologias de acordo com a Figura 11, onde é mostrado que os contratos inteligentes estão contidos no grupo de aplicações blockchain, que por sua vez estão contidos na classificação de aplicações DLT.

[11] https://www.iso.org/committee/6266604.html

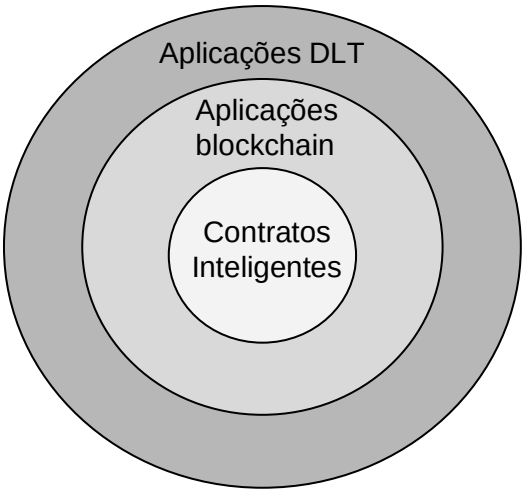

Figura 11: Classificação das tecnologias.

Outro aspecto relevante é a necessidade de evolução de métodos de engenharia de software, incluindo boas práticas de testes e segurança, para adaptá-las de forma mais séria as características únicas de blockchains (Chakraborty *et al*., 2018). De maneira geral, acreditamos que a tecnologia fornece um frutífero terreno para pesquisas em diferentes áreas da computação, como engenharia de software, redes de computadores e sistemas de informação.

5. Leituras Recomendadas

Bitcoin Wiki (Bitcoin Wiki, 2018). A wiki do Bitcoin apresenta conceitos fundamentais e regras implementadas na rede blockchain utilizadas para o processamento de transações na criptomoeda bitcoin. A wiki é mantida pela comunidade Bitcoin e é constantemente atualizada, servindo como referência para mudanças implementadas na rede.

ECOA PUC-Rio (disponível em http://www.puc-rio.br/ecoa). Blockchain tem sido pauta frequente da iniciativa ECOA PUC-Rio onde se discutem, em parceria com empresas e focando em suas reais necessidades, soluções disruptivas para diversas áreas de negócio. Diversos vídeos da iniciativa, de acesso gratuito, abordam a tecnologia e suas aplicações.

IBM Blockchain for Dummies (Gupta, 2017). O livro apresenta conceitos introdutórios sobre blockchain, processamento de transações e mecanismos de consenso. Voltado para profissionais que buscam um primeiro contato com a tecnologia blockchain, pode servir como um primeiro passo de estudo no assunto.

Mastering Blockchain (Bashir, 2017). O livro aborda os conceitos de blockchain e contratos inteligentes e serve como uma referência adicional a respeito destes assuntos.

6. Lista de Atividades

Conceitos Básicos

1. Com base na leitura do capítulo, defina blockchain.

2. Recapitule os conceitos básicos de Blockchain apresentados no capítulo (arquitetura, bloco, descentralização, integridade e transparência).

3. Qual a diferença entre uma blockchain pública, privada e híbrida? Em que situações faria uso de cada uma?

4. O que é um mecanismo de consenso blockchain? Como este conceito está relacionado com a segurança? E com o consumo de energia e sustentabilidade? Responda refletindo ao menos sobre o funcionamento dos mecanismos *Proof of Work* e *Proof of Stake*.

5. O que é um contrato inteligente? Para que são utilizados (cite exemplos de aplicação)? Quais são suas características?

Aplicações e Impacto Social

6. Pesquise a respeito de aplicações da tecnologia blockchain para cada uma das seguintes áreas de negócio: agricultura, cidades inteligentes, finanças, gestão pública e saúde. Busque compreender os benefícios e as implicações que blockchain oferece para as aplicações encontradas. Registre as aplicações, os benefícios e as implicações para subsidiar a discussão dos resultados.

7. Utilize sua criatividade e pense em aplicações da tecnologia blockchain que possam trazer potenciais benefícios para a sociedade. Pense tanto no benefício social quanto na razão pela qual blockchain seria uma escolha adequada para alcançar o benefício pretendido e as implicações. Registre as aplicações, os benefícios e as implicações para subsidiar a discussão dos resultados.

8. Considerando que o modelo econômico baseado em criptomoedas prospere, transações (eventualmente anônimas) e descentralizadas, sem o envolvimento de entidades governamentais, poderiam dificultar a arrecadação de impostos. Pense em soluções alternativas para permitir que este modelo não afete os serviços básicos oferecidos à população (como saúde, educação, transporte público, saneamento básico e aposentadoria). Registre as soluções para subsidiar a discussão dos resultados.

Observação: As atividades 6 a 8 podem ser realizadas em grupos de até 5 pessoas, idealmente no contexto de uma sessão de *brainstorm*, em que cada grupo registra seus resultados em *post-its*. Um roteiro exemplo para a realização deste tipo de dinâmica segue.

Preparação (~5 a 10 min):

- Explicar como funcionará a sessão (instrutor);
- Ler o enunciado da atividade (instrutor) e motivar a temática;
- Distribuir *post-its* (instrutor);

Sessão de Brainstorming (~15 a 30 min):

- Registrar resultados no post-it e colar no quadro da sessão (cada um dos grupos);
- Gerar quantas ideias for possível (cada um dos grupos);
    - Deixar a imaginação livre;
    - Não admitir críticas;

Ajuste dos Resultados (~10 a 20 min):

- Leitura e agrupamento de resultados próximos (instrutor junto com os grupos);
- Consenso dos resultados finais da sessão (um possível método para alcançar o consenso é a votação).

7. Referências

N. Atzei, M. Bartoletti, T. Cimoli, “A survey of attacks on ethereum smart contracts (sok)”, In: Principles of Security and Trust (pp. 164-186), 2017.

I. Bashir, “Mastering Blockchain - Distributed ledgers, decentralization and smart contracts explained”, Packt Publishing, 2017.

Bitcoin Wiki, “The Bitcoin Wiki”, mantido pela comunidade Bitcoin, 2018. Disponível em https://en.bitcoin.it/ (último acesso em 27/07/2018).

V. Buterin, “A next-generation smart contract and decentralized application platform”, *White paper*, 2014.

P. Chakraborty, R. Shahriyar, A. Iqbal, A. Bosu, “Understanding the Software Development Practices of Blockchain Projects: A Survey”, ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Oulu, Finland, 2018.

G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, R.M. Hierons, “Smart contracts vulnerabilities: a call for blockchain software engineering?”, International Workshop on Blockchain Oriented Software Engineering, Campobasso, Italy, 2018.

M. Gupta, “Blockchain for dummies”, IBM Limited Edition, John Wiley & Sons, 2017.

S.M.B.M. Moreno; G.M. Arantes-Jr; J.N. Almeida-Jr; M.T. Onodera; V.R.S. Almeida, “Improving the Process of Lending, Monitoring and Evaluating through Blockchain Technologies”, IEEE International Conference on Blockchain (Blockchain 2018), Halifax, Canada, 2018.

S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, artigo original de Satoshi Nakamoto sobre Bitcoin, 2008. Disponível em https://bitcoin.org/en/bitcoin-paper (último acesso em 27/07/2018)

S. Porru, A. Pinna, M. Marchesi, R. Tonelli, “Blockchain-oriented Software Engineering: Challenges and New Directions”, International Conference on Software Engineering (Companion Volume), 169–171, Buenos Aires, Argentina, 2017.

B. Schneier, “Applied cryptography: protocols, algorithms, and source code in C”, 20th Anniversary edition, Wiley, 2015.

A.S. Tanenbaum, “Computer Networks”, 5th Edition, Pearson Education, 2010.

X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, “The Blockchain as a Software Connector.” 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, Italy, 2016. DOI:10.1109/wicsa.2016.21.

Z. Zheng, S. Xie, H.N. Dai, H. Wang, “Blockchain challenges and opportunities: A survey”, International Journal of Web and Grid Services (*in press*), 2016.