

BLOCKCHAIN, REDE DISTRIBUÍDA E A SEGURANÇA DA INFORMAÇÃO

BLOCKCHAIN, DISTRIBUTED NETWORK AND INFORMATION SECURITY

Alessandro Moreno Barbosa

Graduando em Tecnologia em Redes de Computadores pela FATEC-campus Bauru

E-mail: alessandro.barbosa3@fatec.sp.gov.br

Mickael Christianini Barbosa

Graduando em Tecnologia em Redes de Computadores pela FATEC-campus Bauru

E-mail: mickael.barbosa@fatec.sp.gov.br

Kelton Augusto Pontara da Costa

Docente na FATEC-campus Bauru

E-mail: kelton.costa@fatec.sp.gov.br

RESUMO:

A presente pesquisa pauta suas bases na segurança da informação, mas também no modelo topológico de rede distribuída. É importante compreender a tecnologia da cadeia de blocos, ou simplesmente *Blockchain*, bem como sua proposta de mudança no conceito de relação com a internet. O objetivo desse estudo é entender a segurança da informação, suas aplicações e os processos que envolvem a transição para esse novo modelo de Internet que precisa encontrar um caminho de interoperabilidade entre as diversas redes distribuídas, porém é de suma importância compreender seu impacto na segurança da informação. O que se demonstra por meio de simulação através de códigos de programação exibidos em um navegador web, a fim de recriar os mecanismos de estrutura algorítmica de segurança, testar e entender suas bases teóricas de forma visual. O resultado alcançado, revela que essa tecnologia possui um futuro promissor na relação com ativos na internet quanto a confiabilidade nos mecanismos de segurança. Com isso se percebe que o caminho para sua utilização será testado pela necessidade de um modelo de transações de ativos culturalmente diferente, que deverá passar pelo processo evolutivo através de discussões e inovações propostas a esse modelo de rede.

Palavras-chave: algoritmo; *blockchain*; encriptação; rede distribuída; segurança.

ABSTRACT:

The present research bases its bases on information security, but also on the topological model of a distributed network. It is important to understand the blockchain technology, or simply Blockchain, as well as its proposal to change the concept of relationship with the internet. The objective of this study is to understand information security, its applications and the processes that involve the transition to this new Internet model that needs to find a way of interoperability between the various distributed networks, but it is extremely important to understand its impact on the security of the information. What is demonstrated by means of simulation through programming codes displayed in a web browser, in order to recreate the mechanisms of algorithmic security structure, test and understand its theoretical bases in a visual way. The result achieved

reveals that this technology has a promising future in the relationship with assets on the internet in terms of reliability in security mechanisms. With this, the path to its use will be tested by the need for a culturally different asset transaction model, which must go through the evolutionary process through discussions and proposed innovations to this network model.

Keywords: *algorithm; blockchain; encryption; distributed network; security.*

1 INTRODUÇÃO

Essa pesquisa está pautada na segurança da informação de um modelo topológico em rede distribuída. É possível detectar um obstáculo a ser quebrado no que se refere a transição para esse novo modelo de Internet. A *Blockchain* ou cadeia de blocos, necessita encontrar um caminho de interoperabilidade entre as diversas redes distribuídas, porém é de suma importância compreender seu impacto na segurança da informação com a realização de comparativos com os modelos topológicos: centralizado e descentralizado.

O desenvolvimento dessa pesquisa se justifica pela necessidade de compreender mais a respeito da *Blockchain*, e com isso se espera entender melhor a tendência da rede mundial de computadores em se distanciar dos grandes e poderosos data centers, deixar para traz padrões topológicos centralizados e descentralizados, para cada vez mais se aproximar de modelos de Internet pautados em rede distribuída, bem como entender a segurança da informação no contexto da tecnologia da *Blockchain*.

Relacionar o caminho evolutivo da tecnologia *Blockchain* em um modelo de rede distribuída. Compreender o conceito dessa nova tecnologia e sua aplicação principalmente no que se refere a segurança da informação. Avaliar seu impacto e transformação no ambiente virtual. Analisar o futuro da internet diante dessa nova realidade e o efeito no cotidiano das pessoas.

2 FUNDAMENTAÇÃO TEÓRICA

Entender as urgências de nosso tempo sempre foi uma necessidade humana. Em todas as épocas da história se observa as expectativas intrínsecas em relação as tendências sociais, e se nota que tudo o que se faz ou se busca é na direção de uma máxima, a de se produzir mais e melhor em um tempo cada vez menor.

Ao mesmo passo que se busca aproximar pessoas e reduzir distâncias, dar agilidade aos processos e melhorar a qualidade de vida do indivíduo e do coletivo, novos desafios são impostos como meta ao desenvolvimento humano e tecnológico.

Uma análise feita por Gandham (2020) a COINTELEGRAPH Brasil, diz que um dos acontecimentos mais importantes na história recente da humanidade nessa busca, foi o surgimento da rede mundial de computadores ou simplesmente a Internet, que em pouco mais de 30 anos modificou profundamente a maneira de se olhar o mundo a volta.

A Internet adentrou quase todos os aspectos da existência humana. Sustenta praticamente tudo o que se faz, e é até difícil imaginar a vida sem ela. A marcha da tecnologia continua, e uma evolução tecnológica que provavelmente terá um impacto semelhante na vida das pessoas é a tecnologia *Blockchain*, conforme defendem diversos especialistas no assunto atualmente.

2.1 Blockchain – A arquitetura disruptiva

De acordo com Pitz (2017), tudo começou em outubro de 2008 quando alguém com o pseudônimo de Satoshi Nakamoto publicou uma tese com o título “*The Cryptography Mailing*” que descrevia uma nova arquitetura com o intuito de criar uma moeda digital, e assim em 2009 nasceu o Bitcoin, mas é necessário esclarecer a relação entre a tecnologia *Blockchain* e a Criptomoeda. “*Blockchain* é a arquitetura na qual o Bitcoin funciona, enquanto o Bitcoin é uma moeda digital que funciona em cima da *Blockchain*”. Existem muitas redes *Blockchain* além da rede do Bitcoin. Todas funcionam paralelamente, e não se comunicam entre si. A tecnologia *Blockchain* possui características que formam uma rede P2P, o que permite compartilhar serviços e dados sem a necessidade de um servidor central. Na figura 01 que segue abaixo, se pode observar três tipos de topologia de rede: a centralizada, a descentralizada e a distribuída.

Figura 01 – Topologia de Rede Centralizado, descentralizado e Distribuído



Fonte: PITZ, R. IMasters (2017)

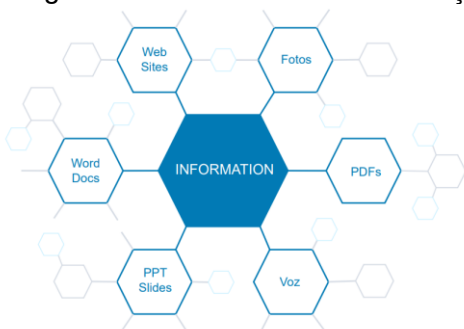
- a) Centralizado: um ótimo exemplo é o sistema bancário. Que é responsável por garantir cada transferência de uma pessoa para a outra, bem como garantir que o mesmo dinheiro não seja usado mais de uma vez;
- b) Descentralizado: ocorre se for possível acessar um servidor para se conectar a outros servidores com a finalidade de fornecer serviços a outros usuários;
- c) Distribuído: é a *Blockchain*, onde não existe um servidor central e nenhuma comunicação necessita passar por servidores intermediários. A comunicação ocorre diretamente de uma ponta a outra.

Segundo Pitz (2017), uma “rede *Blockchain* é composta por vários ‘nós’ em comunicação, e a partir do momento que eles recebem uma nova informação, automaticamente essa informação é propagada para toda a rede de forma encriptada”. No instante que os “nós” recebem a informação de uma transação, os indivíduos na rede validam a veracidade dessa transação por meio de uma assinatura e selecionam quais destas transações entrarão no próximo bloco, com isso todas as transações desse bloco são adicionadas na tabela pública.

De acordo com o artigo da Equipe DSA (2018), esse princípio usado na autenticação de transações financeiras pode ser aplicado na autenticação de todos os tipos de processos online. Tudo baseado no histórico de cada dado movimentado em uma rede de computadores distribuída, imune a fraudes, e capaz de dizer se uma transação é possível ou não, com base em criptografia SHA256 *hash function*, a fim de garantir a segurança. “A saída não pode ser descriptografada de volta para o texto original, pois é uma função *hash* criptográfica unidirecional. Independentemente do tamanho do texto, o comprimento da saída da função *hash* é o mesmo”.

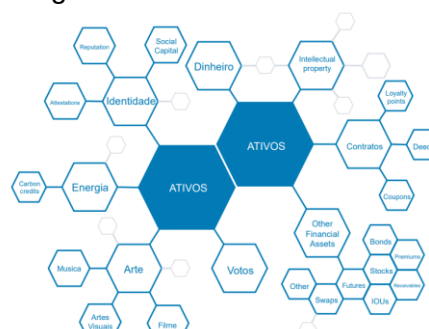
Em entrevista à Revista Cisco Live Magazine, Taspescott (2018) um dos fundadores da *Blockchain Research Institute*, declara que a *Blockchain* é uma segunda era da Internet como ilustra as figuras 02 e 03, pois ao invés de uma internet de informação, essa tecnologia cria uma internet de valor, e assim possui um enorme potencial disruptivo e transformador, que “além dos serviços bancários e financeiros, os setores de saúde, manufatura, varejo, energia, telecomunicações, governo e outras atividades serão impactadas”. Ele avalia ainda que: “qualquer indústria, empresa ou ação que atualmente exija um intermediário para estabelecer confiança entre duas partes, tem potencial para ser impactado pela *Blockchain*”.

Figura 02 – A Internet da Informação



Fonte: AGENDA BAHIA (2017)

Figura 03 – A Internet do Valor



Fonte: AGENDA BAHIA (2017)

2.2 *Blockchain* – Propriedades e características da tecnologia

De acordo com Lamounier (2019) em seu artigo para a plataforma 101 *Blockchains*, ele destaca as características chave da tecnologia *Blockchain* como algo que tem feito ela se tornar irresistível, ao passo em que ganha em popularidade.

2.2.1 Não pode ser corrompido

Em função de uma característica conhecida como imutabilidade, Lamounier (2019) defende que essa tecnologia não pode ser corrompida. Esse recurso garante que a rede permaneça inalterável por não depender de uma autoridade central, pois divide essa condição com um grupo de “nós” na rede, onde todos possuem uma cópia fiel do registro das transações que ocorrem em toda rede. Para que uma nova transação seja aceita, todos os “nós” precisam verificar sua validade, e se a maioria dos “nós” validarem essa transação, então ela será adicionada ao registro digital, e assim é atualizado todos os “nós” da rede com a nova transação. Caso ocorra que a maioria dos “nós” rejeitem essa transação, ninguém poderá adicionar o bloco ao registro da cadeia de blocos. Uma vez que um novo bloco é adicionado a cadeia de blocos, ninguém mais poderá alterar, seja por edição, exclusão, ou atualização de seu registro.

2.2.2 Tecnologia distribuída

Segundo Lamounier (2019), a tecnologia distribuída, diferentemente das redes centralizadas e descentralizadas, não possui uma autoridade centralizadora, mas um grupo de “nós” mantém a rede com uma topologia distribuída. Essa condição é que

permite acessar diretamente a rede e armazenar novos dados, desde criptomoedas, a documentos e contratos importantes, e até mesmo ativos digitais de valor, e é possível ter o controle e o acesso a eles por meio de uma chave privada. Suas características principais são por consequência de um algoritmo matemático preciso que elimina a interação humana em um ambiente altamente tolerante a falhas, e que permite o controle por parte do usuário sobre os seus ativos, e que é menos propenso a ações de *hackers*, pois atacar o sistema é mais caro e não é uma solução fácil, e por não haver ação de terceiros nenhum risco é adicionado, pois é um sistema executado por algoritmos, também é livre de fraudes devido sua característica distribuída que dá mais transparência a cada transação na rede, e ainda por se tratar de um único sistema de autenticação para todos, o que impede qualquer tentativa de sucesso em um eventual ataque *hacker*.

2.2.3 Segurança aprimorada

Devido as propriedades de uma rede distribuída, Lamounier (2019) afirma que não se pode alterar nenhuma característica da rede em seu próprio benefício, somado a isso se inclui uma criptografia que adiciona outra camada de proteção ao usuário, que é um algoritmo matemático muito complexo. Na *Blockchain*, toda informação é criptografada em *hash*, isso significa que a verdadeira natureza da informação fica oculta, pois qualquer dado que entra na rede passa obrigatoriamente por esse algoritmo matemático que resulta em um tipo diferente de valor, mas com um comprimento fixo, além disso todo registro no bloco tem um *hash* diferente, e contém o *hash* do bloco anterior, o que cria uma cadeia de blocos imutáveis. Além disso você precisará de uma chave privada para acessar os dados, e uma chave pública para realizar transações. Como característica o sistema é irreversível, pois o *hash*, além de complexo não pode ser alterado ou revertido, não se pode usar uma chave pública para inventar uma chave privada, uma pequena alteração no bloco gera um ID totalmente diferente, caso alguém queira corromper a rede distribuída, terá que modificar simultaneamente os dados em cada “nó” da rede, o que significa alterar milhões de “nós” que possuem a mesma cópia dos registros das transações realizadas na *Blockchain*, e assim seus ativos digitais estarão imunes contra ataques *hackers*.

2.2.4 Registros distribuídos

Como assegura Lamounier (2019), em um sistema de registro distribuído as informações sobre uma transação estarão visíveis aos olhos de todos, o motivo é que todos os usuários do sistema possuem o registro de transações de toda rede, o que garante partilhar o poder computacional de todos para obter um melhor resultado, e isso é uma característica da tecnologia *Blockchain*, um sistema contábil mais eficiente. Um sistema com recursos tão importantes garante uma rede livre de alterações maliciosas, e que pode responder rapidamente as atividades suspeitas, como adulterações de blocos de registro de transações, pois é inviável alterar um *hash*, e é muito fácil acompanhar o que ocorre com todos os “nós” na rede em função da manutenção do registro atualizado em tempo real das transações na rede distribuída. As propriedades de verificação também são uma das características desse modelo de registros, pois os “nós” da rede atuam como verificadores da cadeia de blocos, e assim no instante que alguém quiser adicionar um novo bloco na cadeia, terá que ser verificado por outro usuário, todos

precisam passar pelo mesmo processo, e só depois terá seus blocos adicionados na rede distribuída, para que isso funcione é fundamental que todos os “nós” da rede mantenham o registro e participem da validação de um novo bloco na rede, e isso possibilitará uma atualização dos registros de transações quase instantânea em toda rede *Blockchain*.

2.2.5 Consenso

O algoritmo de consenso conforme Lamounier (2019), é uma arquitetura inteligente projetada para fazer prosperar cada rede *Blockchain*, o que ajuda o sistema a tomar decisões. O consenso é um processo de tomada de decisões para o conjunto de “nós” que estão ativos na rede. Assim milhões de “nós” podem chegar a um consenso rapidamente, e validar uma transação. O consenso é extremamente necessário para que a rede funcione sem problemas. É como um processo de votação, onde a maioria vence e a minoria tem que apoiar a decisão. Algoritmos de consenso são a raiz que sustentam a tecnologia da rede *Blockchain*, pois o motivo de ser confiável é o consenso. Apesar de os “nós” não necessariamente confiarem uns nos outros, podem confiar nos algoritmos que são executados em seu núcleo, portanto todas as decisões dentro de uma rede *Blockchain* representam um cenário vitorioso para a rede como um todo. No mundo existem diversos algoritmos de consenso, e cada um toma decisões de maneira diferente, que aprimora sua arquitetura e cria um consenso de justiça na web. Contudo para se manter como uma rede distribuída, as redes *Blockchain* precisam ter seu algoritmo de consenso para não perderem sua principal característica.

2.3 Blockchain – Segurança da informação

Segundo Cabral (2018), a *Blockchain* é um mecanismo de segurança extremamente poderoso. A tecnologia é definida como registro de transação pública digital realizada, verificada e armazenada de forma permanente. Sua função principal é validar as transações criptografadas dentro dos blocos conectados de forma hierárquica a cadeia de blocos. Isso possibilita rastrear e verificar qualquer transação realizada, pois ela tem o registro de quem e do momento que foi concretizada. Sempre que houver consenso na rede o novo bloco gerado para nova transação será adicionado e sucederá o anterior e ficarão interligados, e assim aumentará a cadeia de blocos e fortalecerá sua segurança.

2.3.1 Contabilidade de tripla partida

Para começar entender a estrutura da segurança de um bloco gerado por uma transação é preciso conhecer o que é contabilidade de tripla partida (*triple entry accounting*). De acordo com Gabbardo (2018), os algoritmos avançados de encriptação levaram a outro nível a contabilidade com a criação da assinatura digital, o que permite adicionar uma terceira contrapartida de lançamentos para selar de vez a confiabilidade de uma transação.

Para entender na prática se deve observar o exemplo usado por Gabbardo (2018), que apresenta na figura 04 essa ocorrência, onde se pode ver 3 personagens: Alice, Bob e Ivan. Observe que primeiro ocorre no registro de única partida da tabela de Alice um débito de 5 unidades monetárias (U.M.). Em seguida se observa que o registro de única partida de Bob recebe um crédito de 5 (U.M.), então ao olhar para as tabelas de Alice e

Bob se observa o exemplo de um registro contábil de dupla partida. Agora entra um terceiro personagem chamado Ivan, que observa essa transação, verifica, e só então válida em sua tabela, que agora mantém o registro do débito de 5 (U.M.) na tabela de Alice, bem como o registro de 5 (U.M.) de crédito na tabela de Bob. Está formado então o que se chama de contabilidade de tripla partida. Ivan aqui representa os milhares de validadores da transação de uma rede *Blockchain*, que além de verificar as assinaturas digitais de cada uma das partes que realizaram a transação, também emitem um recibo digital deste evento, o que atesta que essa transação está correta, e que existia saldo na conta de Alice para ser transferido ao Bob.

Figura 04 – Exemplo de contabilidade de tripla partida

Alice		Bob	
Débitos	Créditos	Débitos	Créditos
5			5
	2	2	
	9	9	
1			1

Ivan	
Alice	Bob
-5	5
2	-2
9	-9
-1	1

Fonte: GABBARDO, M. Medium (2018)

Os registros de Ivan agora ganham *status* de registros públicos e podem ser auditados por todos os “nós” ativos da rede *Blockchain* que proporcionam imutabilidade dos lançamentos, pois uma vez realizados, auditados e validados pelos auditores nunca mais poderão ser alterados, isso elimina de vez qualquer possibilidade de fraude, além de ocorrer quase que instantaneamente conforme Gabbardo (2018).

2.3.2 Função *hash*

A tecnologia *Blockchain* se utiliza da função *hash* que segundo Vale (2020), é um algoritmo matemático de criptografia. Suas características principais são: uma saída de tamanho fixo (garante que o valor da saída possui a mesma quantidade de caractere não importa qual o valor de entrada), eficiência de operação (não pode ser complexa ao ponto de ter o desempenho comprometido) e determinística (um valor de entrada terá sempre a mesma saída). Suas propriedades são: unidirecional (é impossível aplicar a função inversa e obter os dados de entrada), resistência à segunda pré-imagem (não pode existir dois valores de entrada com a mesma saída) e resistência à colisão (uma redundância da propriedade anterior).

De acordo com Vale (2020), cada bloco recebe informações por um período aproximado de 10 minutos, e então é criptografado e ligado a um *hash* de outro bloco válido na rede que forma assim uma cadeia de blocos, onde o *hash* do bloco anterior é inserido no novo bloco que terá seu próprio *hash*, que por sua vez será inserido no bloco posterior e formará uma cadeia poderosa onde cada bloco possui seu próprio *hash*, mas

também o *hash* de seu antecessor. O *hash* mais usado nas redes *Blockchain* é o SHA256 devido suas características já descritas anteriormente.

2.3.3 Par de chave – Pública e privada

De acordo com Simmons (2019), se trata de criptografia assimétrica que é um algoritmo matemático pelo qual as chaves públicas e privadas são criadas e ligadas, e é possível afirmar que uma chave pública só pode ser criada a partir de uma chave privada, jamais o inverso. Em função dessa conexão matemática, informações criptografadas por uma chave pública só poderá ser descriptada por sua chave privada de origem. Na prática se pode afirmar que a chave privada serve para descriptar as transações encriptadas por, ou para uma chave pública equivalente.

2.3.4 Assinatura digital

De acordo com documentação publicada pela Equipe IBM (2020), uma assinatura digital é criada em duas etapas, e anexada a um documento com autenticação criptografada por uma chave pública. Essa assinatura estabelece a integridade e a identidade do autenticador da mensagem.

Na primeira etapa o conteúdo do documento é transformado em um número grande, que é o código de compilação. Esse código é criptografado, o que resulta na assinatura digital que é anexada ao documento do qual o código de compilação foi gerado. Esse processo é um *checksum* sofisticado. A mensagem não poderá ser restaurada a partir desse código, se alterada resultará em um código de compilação diferente.

Na segunda etapa da criação de uma assinatura digital o processo é superior ao de reversão de chave pública e privada, pois o código de compilação é computado no documento com a chave privada do emissor. Isso resulta na assinatura digital, e é anexada no final da mensagem. Então o destinatário recebe a mensagem, restaura o código de compilação e decodifica a assinatura com a chave pública do emissor, o que resultará no código de compilação original da mensagem, e se esse código corresponder a mensagem, então ela é legítima.

2.3.5 Token e wallets na Blockchain

Segundo Coquieri (2021), são os wallets que permitem a realização de transações, monitoramento e armazenamento de *tokens*. Os wallets são apenas interfaces que controlam o acesso aos criptoativos, e aos registros como: datas das transações, quem são os proprietários dos *tokens* e a quantidade que possuem, tudo registrado na *Blockchain*. Para acessar os *tokens* é necessário possuir a chave privada relacionada a eles, os wallets se comunicam com a rede *Blockchain*, e gerenciam os pares de chaves públicas e privadas correspondentes ao endereço na rede, cada *token* possui um endereço na *Blockchain* e o detentor da chave privada correspondente poderá acessar as informações, até mesmo as contidas no contrato inteligente. O investimento em *tokens* é seguro, os dados não podem ser alterados em função do processamento, organização e armazenamento distribuídos que impedem o roubo de informação, além disso a tecnologia dos contratos inteligentes garante a validação jurídica.

2.3.6 Transação na *Blockchain*

De acordo com Hack (2019), na *Blockchain* ao se usar as palavras bloco e cadeia, se faz referência as informações digitais armazenadas em um banco de dados público que consiste em informações digitais. Informações sobre transações como a data, hora e quantidade de sua última negociação, compra ou transferência, e armazena as informações sobre quem participa das transações, contudo em vez de usar seu nome real sua compra é gravada com uma assinatura digital única que é o seu endereço na rede *Blockchain*, e isso o diferencia de outros blocos. Cada bloco armazena um código único chamado *hash* que permite fazer distinção entre eles. Imagine que você fez uma compra, mas enquanto seu pedido está a caminho você decidiu que quer o produto uma segunda vez e pediu novamente, mesmo que os detalhes da nova transação sejam parecidos com sua compra anterior, ainda é possível distinguir os blocos com base em seus códigos únicos.

Um bloco na *Blockchain* pode armazenar até 1 MB de dados, diz Hack (2019). A depender do tamanho de uma transação um único bloco pode armazenar milhares de transações. No momento que um bloco armazena novos dados é adicionado a rede e forma uma cadeia de blocos. Para que um bloco seja adicionado a *Blockchain* uma transação deve ocorrer e ser verificada. Contudo na *Blockchain* essa verificação é deixada para uma rede com milhares de computadores espalhados por todo o mundo, esta rede de computadores é usada para verificar se suas transações estão em conformidade, inclusive nos detalhes da compra, o momento da transação, o valor e os participantes, além de sua assinatura digital e a do comerciante que ficarão armazenadas em um bloco após a confirmação, e então serão validadas por milhões de participantes da rede *Blockchain*. Depois que as transações pendentes forem verificadas e resumidas em um bloco, recebem uma designação única chamada de *hash*. Este bloco também contém o *hash* do último bloco adicionado na *Blockchain*. Após o *hashing* o bloco pode ser adicionado na rede *Blockchain*, e então esse novo bloco se torna disponível publicamente para todos os participantes da rede, que agora terão acesso aos dados de transações juntamente com as informações sobre em qual momento, onde e por quem o bloco foi adicionado à *Blockchain*. Segundo Hack (2019), registrar transações ajuda os usuários a entender o que foi pago e por quem. Todas as transações executadas são registradas em um arquivo chamado *Block*, que é a base da rede *Blockchain*. O bloco representa o presente, mas possui informações sobre seu passado e futuro, no instante que ele é concluído se torna parte do passado e dá lugar a um novo bloco na *Blockchain*. O bloco concluído é um registro permanente de transações no passado, portanto para novas transações serem registradas é necessário um novo bloco, e assim todo o sistema funciona em um ciclo e os dados são armazenados permanentemente. Um bloco conserva registros de transações recentes e faz referência ao bloco que o antecedeu, o que torna quase impossível a um usuário manipular dados de transações já validadas.

2.3.7 Mineração – Nonce

De acordo com Hack (2020), o nonce é a abreviação de um número usado apenas uma única vez, esse número é adicionado em um bloco criptografado na *Blockchain*. Esse número é difícil de ser encontrado, pois necessita que o minerador possua um grande poder computacional para resolver esse cálculo matemático. A função para se

criar um *hash* é determinista, pois apresenta o mesmo resultado sempre que for usada a mesma entrada, isso leva a mineração que é o processo pelo qual um novo bloco é inserido na cadeia de blocos. O processo começa no cabeçalho do bloco que contém o número da versão do bloco, um carimbo de data e hora, o *hash* usado no bloco anterior, o *hash* da raiz atual, o *nonce* e o *hash* alvo. Se o *hash* atender aos requisitos definidos no alvo, o bloco será adicionado na *Blockchain*. O *nonce*, também conhecido como a prova de trabalho do minerador permite que esse receba o valor pelo bloco minerado que por sua vez é pago em criptomoedas. Determinar qual string se deve usar como *nonce* exige uma grande quantidade de tentativas e erros por se tratar de uma sequência aleatória, onde o minerador precisa encontrar um *nonce*, acertar ao *hash* do cabeçalho atual, preparar o valor, e então comparar com o *hash* alvo. Se o valor de *hash* resultante atender aos requisitos a solução foi encontrada. Toda vez que um bloco é concluído, ele dá lugar ao próximo bloco na rede *Blockchain*. Um bloco é uma memória permanente de gravações escritas que não podem mais ser alteradas ou removidas, são arquivos nos quais os dados são gravados permanentemente.

2.3.8 Ataque dos 51%

Segundo Bastiani (2019), ataques de 51% ocorrem no instante que mineradores tentam assumir mais de 50% do poder computacional de uma rede *Blockchain*, e impedir a validação de novas transações. Esse tipo de ataque é muito raro, pois o invasor necessitaria de poder computacional para superar milhões de mineradores em toda a rede. Além disso se gastaria quantias financeiras exorbitantes para investir em hardware de mineração para suplantando o restante da rede, nem mesmo os mais poderosos computadores do mundo conseguiriam superar os milhares de outros computadores, e isso inviabilizaria a realização de um ataque com essa característica. O gasto com energia elétrica para levar a cabo esse ataque transformaria a operação em algo surreal, mas isso não significa que não exista outra forma de realizar o ataque de 51%. Um bug no código de uma rede *Blockchain* abriria possibilidade para um minerador explorar a falha e produzir blocos de maneira fraudulenta, burlar a rede e ficar em posição favorável para um ataque de 51%. Esse tipo de ataque é mais comum em uma rede *Blockchain* pequena com sistema de prova de trabalho (PoW), que não necessita de grande poder computacional para mineração, já as redes *Blockchain* de grande porte são mais robustas e possuem um poder de *hash* ativo que é mais difícil de ser comprometido.

2.4 Blockchain – Aplicações no ambiente virtual

Ainda de acordo com o mesmo artigo da Equipe DSA (2018) citado anteriormente, muito se tem falado sobre a aplicação mais óbvia da *Blockchain* que é a eliminação de intermediários em transações financeiras interbancárias. Mas a aplicação realmente disruptiva será algo que poderá tirar proveito dos pontos fortes fundamentais da *Blockchain*. Uma aplicação distribuída cujos participantes não necessariamente confiam uns nos outros, no entanto exige um registro preciso de todos os eventos que ocorrem. Se pode ver algumas aplicações para as quais a tecnologia *Blockchain* está em uso. Não se pode limitar a *Blockchain* apenas a uma tecnologia útil para questões financeiras. Se pode usar essa tecnologia em diversas outras aplicações como: contratos inteligentes, auditoria da cadeia de suprimentos, gerenciamento de dados, pagamentos e

transferências internacionais, proteção a direitos de propriedade intelectual, mercados imobiliários, detecção de medicamentos falsificados, gerenciamento de identidade, votação digital, distribuição de energia, saúde, educação, games, *internet of things* (IoT), no combate a *fake news*, e em outras aplicações que se atribua valor a informação.

3 MATERIAIS E MÉTODO

Com o propósito de demonstrar o conceito de segurança da informação em uma rede distribuída *Blockchain*, esse experimento usará um simulador de código fonte aberto desenvolvido por Anders Brownworth. Ele foi projetado para prover uma aplicação web que proporciona interação e pode demonstrar de forma visual conceitos fundamentais da *Blockchain*, bem como diversos processos relacionados à segurança da rede. A fim de explicar e simular visualmente essa tecnologia e suas prerrogativas de segurança em uma rede distribuída *Blockchain*, Brownworth (2019) disponibilizou não apenas sua plataforma web para simulação de estudos “*Blockchain Demo*”, como também o código fonte para realização de download via GitHub aos que desejarem executar localmente o simulador. É possível também executar a partir de uma máquina virtual através de uma distribuição Linux, ou mesmo se utilizar o Docker através do contêiner para apresentação.

Para realização prática desse experimento demonstrativo por opção de otimização dos processos se usará a apresentação web em duas partes com duas abas distintas do navegador de internet, que será executada preferencialmente no Sistema Operacional Windows 10 Pro 21H1, no Web Browser Microsoft Edge Versão 95.0.1020.44 (Compilação oficial) (64 bits) para emular os testes, bem como se utilizará conexão com a Internet para acessar via web o simulador “*Blockchain Demo*” na parte 01 e na parte 02 da simulação. O propósito é realizar as demonstrações de propriedades e características de uma rede *Blockchain* como: imutabilidade, função de criptografia *hash*, criptografia assimétrica, chaves públicas e privadas, assinatura digital, *nonce*, *tokens*, registro distribuído, validação de transações criptografadas na cadeia de blocos, rastreabilidade do registro das transações e contabilidade de tripla partida.

4 RESULTADOS E DISCUSSÃO

Conforme o experimento proposto de simulação web da interface “*Blockchain Demo*”, foi possível apresentar os conceitos fundamentais de segurança em uma rede distribuída que roda sobre arquitetura algorítmica de cadeia de blocos, com os seguintes resultados.

Abaixo se pode observar na figura 05 parte da janela de um navegador de internet com menu interativo para acessar as simulações da parte 01 com as seguintes opções: *Hash*, *Bloco*, *Blockchain*, *Distribuído*, *Tokens* e *Coinbase*.

Figura 05 – *Blockchain Demo*



Fonte: BROWNORTH, A. Anders Brownworth (2019)

Na “Aba Hash” é possível observar a entrada de informação de tamanho variável e a saída de um *hash* de tamanho fixo, isso porque o algoritmo mapeia o comprimento dos dados variáveis, e retorna dados de comprimento fixo, pois isso é uma função *hash*. A função SHA256 é utilizada para gerar esse código *hash*, e se espera que esses valores apresentem sempre um resultado diferente diante das variáveis de informação de entrada, a fim de evitar colisão de *hash*. A função *hash* está presente na *Blockchain* em várias informações, e é fundamental para segurança da rede distribuída.

Na “Aba Bloco” é possível observar dois novos campos: “Bloco” e “Nonce”. Também é possível observar um botão denominado “Minerar”. Com esses novos elementos se tem um “Bloco” simulado. Agora é possível ver um identificador do bloco, um número que permite a mineração do bloco que é o “Nonce”, o campo de “Dados”, e um “Hash” que possui uma particularidade, esse *hash* tem que iniciar com quatro zeros, isso é uma regra da rede para identificar se um bloco é válido em nosso simulador em particular. Ao clicar no botão “Minerar” é possível notar que qualquer mudança nos campos: Bloco, Nonce ou Data. Irá gerar um novo “Hash” que para identificar a validade do bloco sempre iniciará com os quatro números zero. A atividade de mineração na rede *Blockchain* contudo é realizada pelo poder computacional do minerador, que deve resolver o desafio matemático, e encontrar um “Hash” que atenda a regra estabelecida a partir do valor de todos os campos, e no final o nonce resultante será a prova de trabalho para que o minerador receba sua recompensa na rede.

Na “Aba Blockchain” é apresentado cinco blocos encadeados com um novo campo denominado “Prévio”. Esse campo também é um “Hash”, que no caso do primeiro seu valor é nulo, isso se deve ao fato de que o campo “Prévio” representa o *hash* do bloco anterior, e com isso se tem agora nossa cadeia de blocos delineada, ou a *Blockchain* propriamente dita. O propósito desse encadeamento é vincular o *hash* de um bloco ao seu sucessor no campo “Prévio” do bloco seguinte, ao passo que recebe em seu próprio campo “Prévio” o *hash* de seu antecessor. Isso cria uma cadeia de blocos com poderosa encriptação, que admite rastreabilidade, imutabilidade e confiabilidade, uma vez que não permite alteração de dados dentro de um bloco, mas apenas o acréscimo de dados através de um novo bloco.

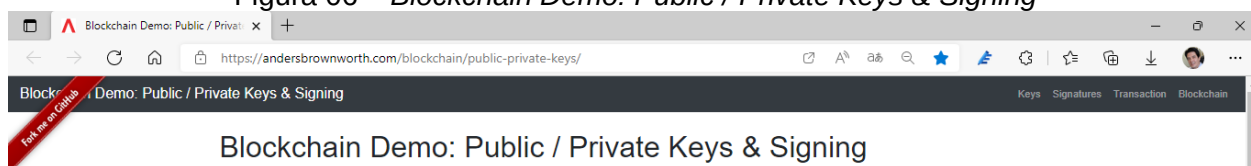
Na “Aba Distribuído” foi acrescido na rede outros dois “nós” semelhantes ao da “Aba Blockchain”, esse é o momento que se compreende o poder da rede distribuída. O objetivo de distribuição na *Blockchain* entre os diversos “nós” é impedir que as informações de um único “nó” se propaguem de forma divergente da maioria da rede. Se sabe que é possível acrescentar informações divergentes em um “nó” da rede, mas devido a sua arquitetura distribuída sobre os fundamentos de um algoritmo de consenso isso não tem possibilidade de prosperar, pois o consenso de 51% prevalecerá, e assim automaticamente a interferência do “nó” que possui adulteração na *Blockchain* será eliminada.

Na “Aba Tokens” se pode visualizar possíveis aplicações da *Blockchain*, mas nessa simulação se observa diversas transações que no campo de “Dados” chamado nessa aba de “Tx” representa um “Token”, que por sua vez possui diversos registros de envio de valores de uma pessoa para outra. Essa demonstração está representada aqui de forma bem simplista com apenas 3 campos, o que a princípio não seria suficiente para construir um sistema utilizável, que garanta o anonimato, e evite possíveis fraudes como a duplicidade de gastos.

Na “Aba Coinbase” se vê o conceito de transação gênese, nessa demonstração o desenvolvedor da cadeia de blocos cria para si um bloco gênese de identificador 1, esse bloco possui uma transação especial chamada de “Coinbase”, ela não pertence a ninguém. Esse é o valor que um minerador receberá como prêmio pela mineração do novo bloco. Nessa aba é possível verificar, se uma transação é válida ou não por meio da rastreabilidade das transações realizadas nos blocos anteriores. É claro que em situação real isso ocorre por meio de algoritmos de verificação, bem como por meio da contabilidade de tripla partida.

Abaixo se pode observar na figura 06 parte da janela de um navegador de internet com menu interativo para acessar as simulações da parte 02 com as seguintes opções: *Keys*, *Signatures*, *Transaction* e *Blockchain*.

Figura 06 – *Blockchain Demo: Public / Private Keys & Signing*



Fonte: BROWNORTH, A. Anders Brownworth (2019)

Na “Aba Keys” é possível observar o processo de criação de um par de chaves pública e privada. Se trata de criptografia assimétrica, e o processo ocorre sempre que uma chave privada gera uma chave pública. Na prática uma chave pública envia ou recebe uma transação que somente será descriptada por sua chave privada equivalente.

Na “Aba Signatures” é possível entender como ocorre o processo de assinatura digital de uma transação, e sua posterior validação. Na aba “Sign” no campo “Message” o conteúdo desse campo é assinado digitalmente ao usar a chave privada de quem originou a transação, e é possível observar no campo “Message Signature” a transação transformada em um grande código de compilação, que é criptografado e anexado a transação da qual foi gerado o código. Na aba “Verify” é possível verificar o campo “Message” ao usar a chave pública do emissor da transação, caso tenha alteração no campo “Message” essa verificação não validará a transação.

Na “Aba Transaction” se pode observar o mesmo processo que ocorreu na “Aba Signature”, com diferenças que se destacam no campo “Message”, onde aparece o local para inserir um valor monetário (\$), local para a chave pública do emissor (*From:*), e o local para a chave pública do destinatário (->). Os processos de assinatura digital e verificação da assinatura ocorrem como descrito na “Aba Signatures”.

Na “Aba Blockchain” se pode visualizar o processo da cadeia de blocos completo conforme detalhado nos itens apresentados das abas do navegador nas partes 01 e 02 do simulador “Blockchain Demo”. É possível destacar dessa aba que: ela se apresenta com três “nós” semelhantes, cada “nó” com cinco blocos encadeados, com destaque no primeiro bloco que é o “gênese”, o identificador do bloco “#”, o “Nonce” que é o número que serve como prova de trabalho do minerador na rede, o “Coinbase” que representa o valor a ser pago ao minerador pela solução *hash* do novo bloco validado, o “Tx” que representa o “Token” com o anonimato da origem e destino das transações enviadas e recebidas por meio de chave pública, bem como assinadas digitalmente pela chave

privada do emissor, e ainda o *hash* “Prévio” que pertence ao bloco anterior, e o “*Hash*” encontrado como solução matemática para validar o bloco na rede distribuída *Blockchain*.

5 CONSIDERAÇÕES FINAIS

Por meio do surgimento de diversas redes distribuídas que se utilizam da tecnologia algorítmica da cadeia de blocos, desde seus primórdios com o surgimento original voltado para as criptomoedas, e publicado em uma tese denominada “*The Cryptography Mailing*” no ano de 2008 pelo pseudônimo Satoshi Nakamoto, que literalmente significa a correspondência de criptografia, foi possível o surgimento do que hoje se conhece por “*Blockchain*”, que apesar de estar associada pela maioria das pessoas as criptomoedas, a cadeia de blocos é muito mais do que isso. O objetivo principal desse estudo foi elevar o entendimento das possibilidades da *Blockchain* quanto a segurança da informação e suas possíveis aplicações em um novo modelo de internet, onde a informação assume a forma de ativos na rede mundial de computadores. Foi possível observar os diversos dispositivos algorítmicos de segurança, mas também entender que o caminho para a verdadeira mudança e ampliação de sua utilização será testada pela necessidade de um modelo de transações de ativos culturalmente diferentes do modelo atual, e passará obrigatoriamente pelo processo evolutivo dessa tecnologia por meio de discussões e novas soluções propostas ao modelo de rede distribuída.

6 REFERÊNCIAS

AGENDA BAHIA - 2017. A Revolução *Blockchain*: Como essa tecnologia vai mudar os negócios, os governos e as pessoas. **Bahia: Blockchain Research Institute**, 2 out. 2017. Apresentação PDF. p. 3-4. Disponível em:

https://www.correio24horas.com.br/fileadmin/user_upload/correio24horas/Arquivos/especiais/agendabahia/docs/agenda-bahia-tempos-de-mudanca-carl-amorim.pdf. Acesso em: 4 jun. 2021.

BASTIANI, A. Entenda o que é um ataque de 51%. **CRIPTOFACIL**, 31 out. 2019. Disponível em: <https://www.criptofacil.com/entenda-o-que-e-um-ataque-de-51/>. Acesso em: 16 out. 2021.

BROWNORTH, A. *Technology and Disruption*. **Anders Brownworth**, 28 jun. 2019. Disponível em: <https://andersbrownworth.com/>. Acesso em: 14 out. 2021.

CABRAL, I. Cinco fatos sobre *blockchain* que você precisa saber. **TechTudo**, 03 ago. 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/08/cinco-fatos-sobre-blockchain-que-voce-precisa-saber.ghtml>. Acesso em: 13 out. 2021.

COQUIERI, D. Como a *blockchain* garante a segurança das suas transações? **COINTELEGRAPH Brasil**, 21 set. 2021. Disponível em: <https://cointelegraph.com.br/news/how-does-blockchain-guarantee-the-security-of-your-transactions>. Acesso em: 15 out. 2021.

EQUIPE DSA. Aplicações da Tecnologia *Blockchain*. **Data Science Academy**, 18 jul. 2018. Disponível em: <https://blog.dsacademy.com.br/aplicacoes-da-tecnologia-blockchain/>. Acesso em: 11 out. 2021.

EQUIPE IBM. Assinaturas Digitais. **IBM Integration Bus**, 10 jan. 2020. Disponível em: <https://www.ibm.com/docs/pt-br/integration-bus/10.0?topic=ssmkhh-10-0-0-com-ibm-etools-mft-doc-ac55190--htm>. Acesso em: 15 out. 2021.

GABBARDO, M. Partidas Triplas e o *Blockchain*. **Medium**, 29 mar. 2018. Disponível em: <https://medium.com/@marcosgabbardo/partidas-triplas-e-o-blockchain-79b627739aaf>. Acesso em: 14 out. 2021.

GANDHAM, I. V. O que a *blockchain* tem em comum com o surgimento da própria internet? **COINTELEGRAPH Brasil**, 13 jun. 2020. Disponível em: <https://cointelegraph.com.br/news/blockchain-is-evolving-like-the-internet-who-will-be-the-crypto-hotmail>. Acesso em: 11 out. 2021.

HACK, C. O *blockchain* – uma definição. **SATOSHI-SUSHI**, 9 nov. 2019. Disponível em: <https://satoshi-sushi.de/die-blockchain-eine-erklaerung/>. Acesso em: 16 out. 2021.

HACK, C. O que é Nonce (*Blockchain*) – Definição. **SATOSHI-SUSHI**, 19 jun. 2020. Disponível em: <https://satoshi-sushi.de/was-ist-nonce-blockchain-definition/>. Acesso em: 16 out. 2021.

LAMOUNIER, L. Conheça Os 6 Pilares Que Sustentam A *Blockchain*! **101 Blockchains**, 09 jan. 2019. Disponível em: <https://101blockchains.com/pt/caracteristicas-da-blockchain/>. Acesso em: 12 out. 2021.

PITZ, R. *Blockchain: A arquitetura disruptiva*. **IMasters** [S. l.], 7 set. 2017. Disponível em: <https://imasters.com.br/desenvolvimento/blockchain-arquitetura-disruptiva>. Acesso em: 4 jun. 2021.

SIMMONS, J. O que é a chave privada e a chave pública Bitcoin? **CRYPTO NEWS FLASH**, 16 out. 2019. Disponível em: <https://www.crypto-news-flash.com/pt-pt/bitcoin-chave-privada-chave-publica/>. Acesso em: 15 out. 2021.

TASPCOTT, D. Uma Revolução Chamada *Blockchain: Blockchain*. **Cisco Live Magazine**, São Paulo, ano 2018, n. 25, p. 14-16, 20 set. 2018. Disponível em: https://www.cisco.com/c/dam/global/pt_br/about/livemagazine/25-edition.pdf. Acesso em: 4 jun. 2021.

VALE, S. Definição, funcionamento e as aplicações do *hash*, a função popular da criptografia. **Voitto**, 27 jun. 2020. Disponível em: <https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona>. Acesso em: 14 out. 2021.