SEGURANÇA DA INFORMAÇÃO E O POTENCIAL IMPACTO DE TECNOLOGIAS BLOCKCHAIN NA SOCIEDADE

Rafael C. Ribeiro
rafael.ribeiro@coinmarketbrasil.com.br

Resumo

Este artigo considera os impactos da crescente adoção e usabilidade dos sistemas baseados em blockchain seus impactos no setor de segurança da informação e na crescente competitividade de dominantes na produção de tecnologias disruptivas. Com foco na análise e demonstrações do papel destas ferramentas para a melhora na qualidade de vida e gatilhos para avanços nos sistemas econômicos modernos, apresentando um conceito de perspectiva aos possíveis avanços ocasionados pela expansão da usabilidade e impactos em diversos setores importantes para a sociedade.

Palavras-chave: Blockchain, Segurança da Informação, Inovação, Economia.

1. Introdução

Para iniciarmos a discussão deste assunto em aspecto global, são utilizados alguns conceitos e estudos do economista Joseph A. Schumpeter, com suas contribuições para o campo de estudos da economia, inovação *"Teoria do desenvolvimento econômico (Die Theorie der Wirschaftlichen Entwicklung), de 1911, ciclos econômicos (Business cycles), de 1939."*, para observações de ciclos, e desenvolvimento econômicos em períodos atuais, o paper *"Bitcoin: A Peer-to-Peer Electronic Cash System"* de Satoshi Nakamoto, aplicadas neste artigo a observações de cenários, impactos e usabilidade e inovação empresarial, além de estudos sobre os potenciais impactos da computação quântica na sociedade.

A computação está diretamente ligada aos avanços econômicos da sociedade, desde a criação dos primeiros computadores com objetivos de executarem cálculos para tomadas de decisões estratégicas em campos de guerra, com o fim da segunda guerra os computadores continuaram a ser usados em diversas aplicações, até que chegamos ao momento que estamos hoje, onde a tecnologia, o processamento computacional é fundamental para praticamente todo campo econômico, seja processando grande volume de pagamentos em sistemas bancários, em pequenos sistemas comerciais ou em tratamento de dados para pesquisas científicas.

O surgimento de novas tecnologias é constante e muitas vezes seu surgimento deve-se a algum cenário socioeconômico, tendo como foco neste artigo algumas dessas tecnologias aplicando observações de seu impacto nos campos de economia. segurança e na organização da sociedade.

2. As particularidades da Blockchain: informações descentralizadas, autenticadas e imutáveis a custos mais baixos

A Blockchain é simplesmente um livro descentralizado ou distribuído (versus os centralizados mantidos por, digamos, bancos para registrar transações e manter o equilíbrio do cliente) de registros digitais confiáveis compartilhados por uma rede dos participantes. Como tal, expande a Internet tradicional de informação e comunicação (e-mails, enviando / recebendo / pesquisando informações, trocando arquivos, participando de mídias sociais etc.) para uma nova categoria que pode ser chamada de "Internet de Valor". Essa Internet inclui o envio / recebimento de dinheiro entre duas partes, sem a necessidade de intermediários financeiros, compra e venda de ações, manutenção / emissão de certificados, incluindo títulos imobiliários, criação / execução de contatos inteligentes, melhoria das cadeias de suprimentos etc. A singularidade do Blockchain vem dos quatro seguintes recursos:

Confiança: novas informações podem ser adicionadas somente quando a maioria dos computadores na rede aprova após uma prova satisfatória de que as informações transmitidas criptograficamente são verdadeiras. A autenticação das informações é feita em curtos intervalos de tempo e as informações atualizadas são armazenadas (anexadas) a todos os computadores da rede participantes.

Imutabilidade e transparência: as informações podem ser anexadas apenas às anteriores e, uma vez inseridas, não podem ser alteradas, modificadas ou perdidas, fornecendo um registro histórico permanente e incorruptível que permanece no sistema permanentemente. Além disso, as alterações nas blockchains públicas são visíveis por todas as partes na rede, resultando em transparência.

Desintermediação: o livro razão (banco de dados) não é mantido por nenhuma pessoa, empresa ou governo, mas por todos os computadores participantes localizados em todo o mundo. Isso significa que duas partes podem gerar uma troca sem a necessidade de um intermediário confiável para autenticar as transações ou verificar os registros.

Custos mais baixos: menores custos de transação e eficiência também são características dos aplicativos de blockchain, removendo o poder monopolista de intermediários poderosos (por exemplo, bancos) ou grandes líderes da indústria centralizados (por exemplo, Airbnb).

Por que o Blockchain é uma tecnologia disruptiva

O Blockchain fornece uma mudança fundamental tecnologia da informação / comunicações e para a internet de valores. A diferença entre os dois Internets é fundamental. O primeiro interrompeu os modelos de negócios na década de 2000 e criou os gostos da Amazon, Google, Facebook, Alibaba e Uber e Airbnb. Sua desvantagem é que as informações transmitidas podem ser copiadas, tornando impossível garantir sua confiabilidade sem a aprovação de um intermediário, por exemplo, um banco que verifica se o dinheiro transmitido está disponível. A maior vantagem da Internet de valor é o estabelecimento de confiança, através da aplicação da tecnologia blockchain, entre estranhos que agora podem confiar um no outro. Isso significa que os ativos podem ser trocados de maneira instantânea e eficiente sem a necessidade de intermediários que não são mais necessários, pois a confiança é incorporada ao sistema. Essa vantagem da Internet de valor está fadada a causar mudanças ainda mais profundas do que aquelas trazidas pela Internet de informações / comunicações. As transações ponto a ponto confiáveis incentivarão a formação de estruturas descentralizadas, diminuindo o poder monopolista de intermediários, como bancos ou empresas como Uber e Airbnb. Isso será feito através da criação de novos players que exporariam as plataformas baseadas em blockchain de redes descentralizadas com o potencial de reduzir drasticamente o poder monopolista dos atuais atores dominantes, democratizando a economia global e criando um sistema econômico mais eficiente e sustentável.

Amazon, Google, Facebook, Alibaba, Tencent, Netflix, Uber e Baidu (com um valor de mercado combinado superior a US $ 3,5 trilhões no final de 2017) foram criadas explorando as vantagens oferecidas pela internet em evolução no final dos anos 90 e nos anos 2000. Essas oito empresas interromperam o setor econômico e de negócios, revolucionando os hábitos de compra e visualização, a busca por informações e gastos com publicidade, entre outros, de maneiras que ninguém poderia prever no início dos anos 90, quando a Internet foi introduzida. Como o blockchain possui o potencial de interrupções iguais ou ainda maiores, principalmente quando combinadas à IA, mudanças revolucionárias de magnitude considerável cobrindo uma ampla gama de indústrias e produtos / serviços surgirão nos próximos vinte anos e novas empresas, correspondentes para os oito mencionados provavelmente surgirá. O grande desafio para os empreendedores é direcionar suas startups para explorar as tecnologias blockchain emergentes e desenvolver novos aplicativos e produtos / serviços inovadores a preços acessíveis para melhor atender às necessidades existentes e emergentes.

Abaixo está uma apresentação do que acreditamos serem os dez aplicativos blockchain existentes mais importantes, ou que serão introduzidos em breve, destacando seu uso e vantagens e mencionando as startups que foram formadas para desenvolvê-los e implementá-los. Esses aplicativos foram classificados em termos dos setores que estão sendo afetados e dos vários aplicativos que estão sendo executados. Não há dúvida de que muito mais aplicativos serão introduzidos no futuro,

alguns deles se tornando avanços bem-sucedidos, principalmente quando combinados com algoritmos de IA.

Setores:

1. **Bancário:** os aplicativos bancários do Blockchain podem reduzir custos em até US $ 20 bilhões, eliminando intermediários e aumentando a segurança e a eficiência das transações bancárias. Uma das startups líderes em campo é a ThoughtMachine, que desenvolveu o Vault OS, executado na nuvem, fornecendo sistemas bancários completos, seguros, rápidos e confiáveis, capazes de gerenciar usuários, contas, economias, empréstimos, hipotecas e produtos financeiros mais sofisticados (consulte https://www.thoughtmachine.net/). Um aplicativo bancário blockchain alternativo é o Corda, uma plataforma de contabilidade distribuída que é o resultado de mais de dois anos de intensa pesquisa e desenvolvimento pela startup R3 e 80 das maiores instituições financeiras do mundo. Ele atende aos mais altos padrões do setor bancário, mas é aplicável a qualquer cenário comercial. Usando Corda, os participantes podem realizar transações sem a necessidade de as autoridades centrais criarem um mundo de comércio sem atrito (consulte https://www.corda.net/). De acordo com o Business Insider, praticamente todos os principais bancos globais estão experimentando a tecnologia blockchain tentando reduzir custos e melhorar a eficiência operacional e de segurança e, ao mesmo tempo, certificando-se de que não serão deixados para trás startups que utilizam tecnologias blockchain para dominar o mercado.

2. **Pagamentos e transferências monetárias:** Ao evitar uma autoridade central para verificar pagamentos e transferências de dinheiro, os custos podem ser reduzidos substancialmente. Atualmente, há um bom número de serviços usando a tecnologia destinada principalmente àqueles sem contas bancárias ou que buscam economias importantes. Abaixo está uma breve descrição de seis serviços de blockchain localizados em várias partes do mundo o Abra (EUA) é um aplicativo móvel que permite transferências de dinheiro de pessoa para pessoa. O aplicativo pode ser baixado na Apple ou nas lojas do Google. o Allign Commerce (EUA) é um provedor de serviços de pagamento (PSP) que permite que as empresas enviem e recebam pagamentos em moedas locais o Bitspark (Hong-Kong) é uma plataforma de remessa de ponta a ponta para qualquer um dos seus mais de 100.000 locais em todo o mundo. o Rebit (Filipinas) é um serviço de transferência de dinheiro que oferece taxas significativamente mais baixas para muitos imigrantes filipinos que trabalham no exterior. o CoinRip (Singapura) é um serviço que oferece transferência de dinheiro rápida e segura, cobrando uma taxa fixa de 2%. o BitPesa (África) é um serviço de transferência de dinheiro barato e seguro, operando na África.

3. **Negociação de valores mobiliários:** as tecnologias Blockchain visam reduzir custos e acelerar as negociações, além de simplificar os processos de liquidação. Por esses motivos, seis bolsas estão considerando a introdução de blockchain em suas operações. A Bolsa de Londres, a Austráliana

   a Securities Exchange (ASX) e a Tokyo Stock Exchange já estão experimentando tecnologias de blockchain que deverão estar operacionais em um futuro próximo. Bancos e empresas financeiras também estão explorando aplicativos blockchain para negociação de segurança. T zero (consulte https://tzero.com/), uma startup dos EUA, afirma em seu site a primeira plataforma de negociação baseada em blockchain que integra ledgers distribuídos com criptografia segura com processos de mercado existentes para reduzir tempo e custos de liquidação, aumentar a transparência, eficiência e auditabilidade.

4. **Assistência médica:** Os custos com assistência médica aumentam rapidamente, estimados em cerca de 10% do PIB nos países desenvolvidos e superior a 17% (perto de US $ 3 trilhões) nos EUA. Isso significa que qualquer esforço para melhorar os serviços de saúde pode resultar em economias substanciais e as tecnologias blockchain são as principais candidatas a obter essas economias, melhorando a eficiência e provavelmente salvando vidas ao mesmo tempo. Existem aplicativos blockchain de curto prazo prontos para aplicar e ambiciosos, de longo prazo, destinados a revolucionar o setor de saúde.

   - **Segurança e confiança:** colete dados de saúde completos (relatórios médicos para cada paciente, histórico de doenças, resultados laboratoriais, raios-X) de maneira segura, usando um identificador exclusivo para cada pessoa e permita o compartilhamento desses dados apenas com o permissão do indivíduo envolvido. A tecnologia Blockchain eliminará as mais de 450 violações de dados de saúde, afetando mais de 27 milhões de pacientes, relatadas em 2016.
   - **Permutabilidade de informações:** as informações de saúde entre os vários atores não são comunicadas livremente, criando silos que impedem sua utilização efetiva para melhorar os cuidados de saúde. A tecnologia Blockchain pode melhorar tanto a permutabilidade de informações quanto sua qualidade, levando a benefícios significativos. o Liquidação de reclamações e
   - **Gerenciamento de contas:** Facilite a liquidação de reclamações, reduzindo a burocracia e introduza o gerenciamento de contas para reduzir fraudes e acelerar o pagamento. Isso pode ser alcançado com mais eficiência, criando consórcios de provedores e seguradoras de saúde. o Autenticação de medicamentos: garantir a integridade dos medicamentos, com base nas estimativas atuais da indústria, as empresas farmacêuticas incorrem em uma perda anual estimada de US $ 200 bilhões devido a medicamentos falsificados em todo o mundo, enquanto cerca de 30% dos medicamentos vendidos nos países em desenvolvimento são considerados imitações.

- **Ensaios clínicos e pesquisas médicas:** Estima-se que até 50% dos ensaios clínicos não são relatados e que os pesquisadores geralmente deixam de compartilhar os resultados de seus estudos. As tecnologias Blockchain podem resolver os problemas por meio de registros imutáveis e com registro de data e hora de ensaios clínicos. Mais importante ainda, a tecnologia poderia facilitar a colaboração entre participantes e pesquisadores e contribuir para melhorar a qualidade da pesquisa médica.

A Estônia implementou um aplicativo blockchain, eHealth, cobrindo todos os seus cidadãos. Além disso, existem várias startups como a GEM que alegam ter desenvolvido o primeiro aplicativo para alegações de saúde com base na tecnologia blockchain. Isso é feito através da introdução de transparência em tempo real e reduzindo substancialmente o tempo para as contas serem pagas pelo compartilhamento da mesma plataforma entre os envolvidos. Existem várias outras startups, algumas já em operação, outras

no caminho de se tornar funcional, como o Guardtime, operando na Estônia e sendo usado por pacientes, provedores, empresas privadas e de saúde pública e pelo governo para armazenar e acessar informações em seu sistema de eSaúde de maneira segura e eficiente. Funções semelhantes são fornecidas pela Brontech, uma startup australiana, oferecendo dados confiáveis de saúde para melhorar o processo de diagnóstico, entre outros; Health Co visa revolucionar a relação entre pesquisadores e usuários médicos; Factom, Stratumn e Tierion preocupam-se principalmente com a melhoria da qualidade dos dados de saúde, enquanto o objetivo do Blockpharma é combater a falsificação de medicamentos.

5. **Varejo:** a multinacional eBay é líder em comércio on-line entre vendas de consumidores a consumidores. O OpenBazaar, é uma nova startup que desafia o eBay, utilizando a tecnologia blockchain para descentralizar o comércio online de pessoa para pessoa. Ao executar um programa em seu computador, os usuários podem se conectar a outros usuários na rede OpenBazaar e negociar diretamente com eles. Essa rede não é controlada ou administrada por uma organização proprietária, mas é descentralizada e gratuita. Isso significa que não há taxas obrigatórias a serem pagas e que as negociações não são monitoradas por uma organização central (consulte https://www.cbinsights.com/company/openbazaar)

Aplicações:

6. **Contratos Inteligentes:** Os contratos inteligentes são provavelmente a tecnologia blockchain com o maior potencial de afetar, ou mesmo revolucionários, com poucas transações desde a execução de vontades até a Internet das Coisas (IoT). A principal inovação de contratos inteligentes é a eliminação de intermediários confiáveis. Considere, por exemplo, o executor de um testamento que aprova as diretrizes do falecido sobre como o dinheiro será gasto / alocado. Em vez de um executor, um contrato inteligente programável e juridicamente vinculativo pode atingir o mesmo objetivo, usando a tecnologia

blockchain, evitando o intermediário confiável, reduzindo custos e melhorando a eficiência. A startup "SmartContracts" permite conectar contratos inteligentes em várias redes a aplicativos existentes e dados externos, enviando pagamentos postulados no contrato inteligente para contas bancárias designadas e criando conectividade segura entre as cadeias entre o contrato inteligente e outra cadeia pública ou privada. Uma aplicação adicional de contratos inteligentes é com a IoT, facilitando o compartilhamento de serviços e recursos que levam à criação de um mercado de serviços entre dispositivos que permitiriam automatizar de maneira criptograficamente verificável vários fluxos de trabalho demorados existentes uma aplicação mais radical é fornecida pela startup Koinify, que visa acelerar a descentralização econômica por meio de blockchain e tecnologia de contrato inteligente. O mais importante é que essa tecnologia é o princípio central por trás do Ethereum (veja abaixo), uma nova extensão de tecnologias blockchain com foco na execução do código de programação de aplicativos de contrato inteligente descentralizados.

7. **Cadeia de suprimentos:** as operações da cadeia de suprimentos são dominadas por métodos baseados em papel que exigem cartas de crédito (de 1% a 3%) e fatoração (de 5% a 10%), aumentando os custos em cerca de um trilhão de dólares (Allison, 2016) e também transações de desaceleração. Tais custos podem ser reduzidos substancialmente, usando a tecnologia blockchain que eliminará os intermediários, estabelecendo a confiança entre compradores e vendedores. Existem várias startups, entre elas, Skuchain, visando sua tecnologia blockchain na interseção de pagamentos (carta de crédito ou transferência eletrônica), finanças (empréstimos comerciais e operacionais de curto prazo) e Proveniência, com foco no rastreamento da autenticidade e credenciais sociais e ambientais dos produtos desde a origem até o momento. o consumidor final. Além das startups, grandes empresas, como o Walmart, também têm como objetivo explorar as vantagens da tecnologia blockchain para melhorar a eficiência e reduzir os custos da cadeia de suprimentos (Lohade, 2017).

8. I**oT:** o Blockchain pode revolucionar a IoT se aplicado de forma segura aos estimados 8,5 a 20 bilhões de dispositivos IoT conectados que existem em 2017 e devem crescer para um trilhão em 2020. Explorar as informações geradas por dispositivos IoT de maneira inteligente pode transformar nossas casas e cidades, ter um efeito profundo na qualidade de nossas vidas, poupando energia. De acordo com Compton (Compton, 2017) "Como o blockchain é construído para controle descentralizado, um esquema de segurança baseado nele deve ser mais escalável do que o tradicional. E as fortes proteções da blockchain contra adulteração de dados ajudariam a impedir que um dispositivo não autorizado interrompa um sistema residencial, de fábrica ou de transporte transmitindo informações enganosas ". A Eciotify, uma startup especializada em aplicar blockchain à IoT, planeja implantar aplicativos utilizando a tecnologia blockchain para dispositivos IoT.

9. **Armazenamento em nuvem descentralizado:** o armazenamento em computador foi descentralizado em computadores individuais, até cerca de uma década atrás, quando o Dropbox foi fundado, fornecendo a primeira unidade de armazenamento em nuvem centralizada e moderna. Desde então, a computação em nuvem foi introduzida revolucionando aplicativos, incentivando as empresas a terceirizarem suas necessidades de armazenamento para empresas como Amazon, Google ou Microsoft Web Services. A vantagem de tais serviços foram custos mais baixos e maior confiabilidade. A tecnologia Blockchain visa re-descentralizar o armazenamento de computadores em computadores individuais em todo o mundo. Segundo especialistas, existem três razões principais para essa mudança. Primeiro, o custo da maioria dos serviços em nuvem é de cerca de US $ 25 por terabyte por mês, enquanto o correspondente de armazenamento em blockchain é doze vezes e meia mais barato, a US $ 2 por terabyte / mês. Segundo, há maior segurança à medida que os dados da blockchain são criptografados, o que significa que apenas os usuários que possuem as chaves apropriadas podem visualizá-las (os dados armazenados nos serviços comerciais em nuvem podem ser visualizados por terceiros). Por fim, o armazenamento em nuvem da blockchain é imutável, fornecendo um registro de todas as alterações históricas feitas nos dados.

10. **Certificação:** Uma das grandes promessas da tecnologia blockchain é que ela pode servir como uma alternativa de armazenamento descentralizada e permanentemente inalterável para todos os tipos de informações ou ativos, não apenas como moeda ou sistema de pagamento. Isso faz da tecnologia a ferramenta principal para certificar todos os tipos de informações, transações, documentos e registros. O que atraiu o maior interesse, no entanto, é a certificação de dados (com a startup Stampery sendo a líder) e a de identidades (com a startup ShoCard como líder). Existem muitas áreas adicionais nas quais a certificação usando a tecnologia blockchain pode ser aplicada, incluindo a emissão de IDs e a votação.

11. **Outras aplicações Blockchain:** Existem muitos aplicativos adicionais que exploram as tecnologias blockchain. Isso inclui verdadeiros serviços descentralizados de compartilhamento de viagens (Uber e Lyft são, na verdade, serviços de táxi centralizados), como os oferecidos por La'Zooz e Arcade City. Stratumn, uma plataforma com o objetivo de automatizar a auditoria, a Synereo, cujo objetivo é ajudar os usuários a criar conteúdo, publicar e distribuir on-line, a Docusign oferece a solução eSigniture e a Steem, uma plataforma de mídia social onde qualquer um pode ganhar recompensas, já que algumas dessas startups já estão operacionais enquanto outros ainda estão sendo desenvolvidos.

Empresas especializadas em blockchain VC e distribuição geográfica de fundos: De acordo com a Fintechnews, na Suíça, oito grandes empresas de capital de risco investiram mais de US $ 1,55 bilhão em startups de bitcoin e blockchain desde 2012. Em termos de país, os EUA dominam a corrida com 55% do total, seguido pelo Reino Unido com 6%, Cingapura com 3% e Japão, Coréia do Sul e China com 2% cada. À medida que o interesse nas tecnologias blockchain aumenta, espera-se que os investimentos em VC aumentem muito, acelerando o número de aplicativos disponíveis.

Ethereum: Ethereum, como o Bitcoin, é uma rede pública distribuída de blockchain (desenvolvida pela fundação suíça sem fins lucrativos com o mesmo nome) que mantém seus recursos exclusivos (Confiança, imutabilidade / transparência, desintermediação, baixo custo), mas com os três adicionais: Executar aplicativos exatamente como programado, sem possibilidade de inatividade, censura, fraude ou interferência de terceiros. Permitir que os desenvolvedores construam e implantem aplicativos descentralizados, atendendo a propósitos específicos que se tornam parte da rede blockchain e, como tal, não controlam por nenhuma entidade individual ou central que é o caso de aplicativos da Internet. Explorar a Ethereum Virtual Machine (EVM) para executar qualquer programa desejado, escrito em qualquer linguagem de programação, usando os desenvolvedores do EVM não precisa criar aplicativos de blockchain do zero, mas pode utilizar os milhares de aplicativos já disponíveis (um tipo desses aplicativos podem ser contratos inteligentes).

2.1 O potencial impacto na sociedade

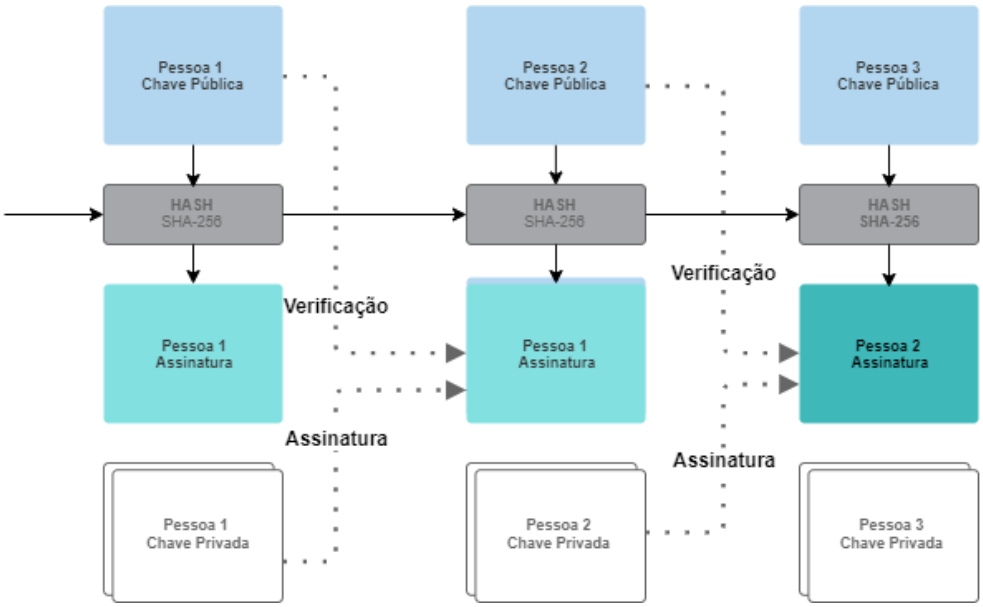
Com todos os aspectos e particularidades citadas anteriormente, é possível se conduzir pesquisas e parametrização com base na necessidade, usabilidade e demanda para tais aspectos, em um mundo amplamente globalizado e informatizado, a informação é cada dia mais valiosa e de manipulação delicada, sendo criados diversos mecanismos de padronizações internacionais para tratamento de dados e seu armazenamento além da atenção de governos a medidas contra monopólios e conflitos que o domínio dessas tecnologias e meios podem causar.

2.2 Transações com criptomoedas, e sua garantia de segurança e privacidade

No modelo de economia tradicional, as transações monetárias, são centralizadas em um órgão que controla a emissão, valida as transações com objetivo de evitar duplicações e fraudes, porém o sistema utilizado por estes órgãos não é nada econômico além de não permitir que a privacidade seja um ponto crucial nestas transações.

As transações com criptomoedas surgem como um escape a esta falta de privacidade e segurança que os sistemas proveem.

Com tudo a blockchain provê um sistema de auto validação que se mostra eficaz em diversos cenários, não há possibilidade de pessoas com credito ruim interferirem em transações e mercado, mesmo com sua grande volatilidade, que é comum e causada principalmente pelo fato de não haver um controle realizado por um órgão central deixando o mercado totalmente a critérios do próprio em sua livre negociação.



A imagem descreve o processo de uma transação com bitcoin, onde os hash são incrementados com as chaves públicas de cada pessoa transacionando o ativo sendo assinada pela chave privada verificando os hashs a serem validados por nodes em todo o mundo.

2.3 Definições do SHA-256

O padrão de criptografia SHA-256 utiliza-se de seis funções lógicas, cada uma dessas operando palavras de 32 bits e produz uma palavra de 32 bits como saída**.** Com cada função definida por pelo exemplo abaixo:

$$
\begin{aligned}
Ch(x, y, z) &= (x \wedge y) \oplus (\neg x \wedge z) \\
Maj(x, y, z) &= (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \\
\Sigma_0(x) &= S^2(x) \oplus S^{13}(x) \oplus S^{22}(x) \\
\Sigma_1(x) &= S^6(x) \oplus S^{11}(x) \oplus S^{25}(x) \\
\sigma_0(x) &= S^7(x) \oplus S^{18}(x) \oplus R^3(x) \\
\sigma_1(x) &= S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x)
\end{aligned}
$$

Onde os blocos de cada mensagem é calculado da seguinte forma:

$W_j = M_j^{(i)}$ for $j = 0, 1, \ldots, 15$, and
For $j = 16$ to 63
{

$$W_j \leftarrow \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$$

}

Retornando uma sequência de chaves constantes em HEX . $K_0, \ldots, K_{63}$ dados por:

```
428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1 923f82a4 ab1c5ed5
d807aa98 12835b01 243185be 550c7dc3 72be5d74 80deb1fe 9bdc06a7 c19bf174
e49b69c1 efbe4786 0fc19dc6 240ca1cc 2de92c6f 4a7484aa 5cb0a9dc 76f988da
983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147 06ca6351 14292967
27b70a85 2e1b2138 4d2c6dfc 53380d13 650a7354 766a0abb 81c2c92e 92722c85
a2bfe8a1 a81a664b c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070
19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3
748f82ee 78a5636f 84c87814 8cc70208 90befffa a4506ceb bef9a3f7 c67178f2
```

Estes são os primeiros trinta e dois bits das partes fracionárias das raízes cúbicas do primeiro sessenta e quatro primos.

2.3 Cálculo de Hash Amostrais

Dando como exemplo a mensagem “abc” em hexadecimal mostra-se como

61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018,

E o valor de seu hash é

ba7816bf 8f01cfea 414140de 5dae2223 b00361a3 96177a9c b410ff61 f20015ad.

Hash de “abc”

	a	b	c	d	e	f	g	h
init:	6a09e667	bb67ae85	3c6ef372	a54ff53a	510e527f	9b05688c	1f83d9ab	5be0cd19
t = 0	5d6aebcd	6a09e667	bb67ae85	3c6ef372	fa2a4622	510e527f	9b05688c	1f83d9ab
t = 1	5a6ad9ad	5d6aebcd	6a09e667	bb67ae85	78ce7989	fa2a4622	510e527f	9b05688c
t = 2	c8c347a7	5a6ad9ad	5d6aebcd	6a09e667	f92939eb	78ce7989	fa2a4622	510e527f
t = 3	d550f666	c8c347a7	5a6ad9ad	5d6aebcd	24e00850	f92939eb	78ce7989	fa2a4622
t = 4	04409a6a	d550f666	c8c347a7	5a6ad9ad	43ada245	24e00850	f92939eb	78ce7989
t = 5	2b4209f5	04409a6a	d550f666	c8c347a7	714260ad	43ada245	24e00850	f92939eb
t = 6	e5030380	2b4209f5	04409a6a	d550f666	9b27a401	714260ad	43ada245	24e00850
t = 7	85a07b5f	e5030380	2b4209f5	04409a6a	0c657a79	9b27a401	714260ad	43ada245
t = 8	8e04ecb9	85a07b5f	e5030380	2b4209f5	32ca2d8c	0c657a79	9b27a401	714260ad
t = 9	8c87346b	8e04ecb9	85a07b5f	e5030380	1cc92596	32ca2d8c	0c657a79	9b27a401
t = 10	4798a3f4	8c87346b	8e04ecb9	85a07b5f	436b23e8	1cc92596	32ca2d8c	0c657a79
t = 11	f71fc5a9	4798a3f4	8c87346b	8e04ecb9	816fd6e9	436b23e8	1cc92596	32ca2d8c
t = 12	87912990	f71fc5a9	4798a3f4	8c87346b	1e578218	816fd6e9	436b23e8	1cc92596
t = 13	d932eb16	87912990	f71fc5a9	4798a3f4	745a48de	1e578218	816fd6e9	436b23e8
t = 14	c0645fde	d932eb16	87912990	f71fc5a9	0b92f20c	745a48de	1e578218	816fd6e9
t = 15	b0fa238e	c0645fde	d932eb16	87912990	07590dcd	0b92f20c	745a48de	1e578218
t = 16	21da9a9b	b0fa238e	c0645fde	d932eb16	8034229c	07590dcd	0b92f20c	745a48de
t = 17	c2fbd9d1	21da9a9b	b0fa238e	c0645fde	846ee454	8034229c	07590dcd	0b92f20c
t = 18	fe777bbf	c2fbd9d1	21da9a9b	b0fa238e	cc899961	846ee454	8034229c	07590dcd
t = 19	e1f20c33	fe777bbf	c2fbd9d1	21da9a9b	b0638179	cc899961	846ee454	8034229c
t = 20	9dc68b63	e1f20c33	fe777bbf	c2fbd9d1	8ada8930	b0638179	cc899961	846ee454
t = 21	c2606d6d	9dc68b63	e1f20c33	fe777bbf	e1257970	8ada8930	b0638179	cc899961
t = 22	a7a3623f	c2606d6d	9dc68b63	e1f20c33	49f5114a	e1257970	8ada8930	b0638179
t = 23	c5d53d8d	a7a3623f	c2606d6d	9dc68b63	aa47c347	49f5114a	e1257970	8ada8930
t = 24	1c2c2838	c5d53d8d	a7a3623f	c2606d6d	2823ef91	aa47c347	49f5114a	e1257970
t = 25	cde8037d	1c2c2838	c5d53d8d	a7a3623f	14383d8e	2823ef91	aa47c347	49f5114a
t = 26	b62ec4bc	cde8037d	1c2c2838	c5d53d8d	c74c6516	14383d8e	2823ef91	aa47c347
t = 27	77d37528	b62ec4bc	cde8037d	1c2c2838	edffbff8	c74c6516	14383d8e	2823ef91
t = 28	363482c9	77d37528	b62ec4bc	cde8037d	6112a3b7	edffbff8	c74c6516	14383d8e
t = 29	a0060b30	363482c9	77d37528	b62ec4bc	ade79437	6112a3b7	edffbff8	c74c6516
t = 30	ea992a22	a0060b30	363482c9	77d37528	0109ab3a	ade79437	6112a3b7	edffbff8
t = 31	73b33bf5	ea992a22	a0060b30	363482c9	ba591112	0109ab3a	ade79437	6112a3b7

2.1 Fatores para baixas de valor de mercado

As criptomoedas são ativos muito voláteis, e atrelado muitas vezes a tecnologias projetadas para o futuro, sendo assim alguns ativos ficam em estagnação de preço, outras com crescimento constante e outras com desvalorização periódicas, além dessas moedas e tokens serem projetados para serem pareados com ativos ou projetos que estão em diferentes etapas de maturidade perante a demanda e mercado.

3 Aplicações da Computação Quântica

3.1 Impactos da computação quântica

A computação quântica poderá melhorar e ser útil em projetos de setores de grande importância ao sistema econômico com melhorias nos campos de ciência de materiais, engenharias indústrias, medicina, energia, controle de tráfego, logística e supply chain, agricultura, além da criptografia e diversos outros campos provendo uma grande melhoria nos campos de computação em nuvem e a inteligência artificial impactando diretamente na maneira em que os dados são armazenados e manipulados, além da forma em que os dados são disponibilizado e acessados, garantindo uma melhora no processo de desenvolvimento colaborativo.

3.2 Computação Quântica não acabará com a criptografia em redes blockchain

Referências

[1] Artificiallawyer.com (2017). ***OpenLaw Brings Legal Norms to Blockchain Token Transactions***. Disponível em: https://blog.agrello.org/how-to-make-smart-contracts-worthy-of-theirname-using-artificial-intelligence-3a90e4dd3c47. Acessado em 24, Out, 2018.

[2] BBC. (2017). ***China bans initial coin offerings calling them 'illegal fundraising'.*** Disponível em: http://www.bbc.com/news/business-41157249. Acessado em: 30, Dez, 2017.

[3**] Blockchain Data Analytics,** ***JOURNAL OF IEEE INTELLIGENT INFORMATICS****, VOL. 20, NO. 1, JANUARY 2019*, Disponível em: http://math.iit.edu/~mdixon7/block_chain_analytics.pdf, acessado em: 10, Jul, 2019.

[4] ***Descriptions of SHA-256, SHA-384, and SHA-512.****Disponível em: http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf,* acesso em: 12, Dez, 2019.

[5] Kocianski, S. (2017). **THE BLOCKCHAIN IN BANKING REPORT: The future of blockchain solutions and technologies.** Available: http://www.businessinsider.com/blockchain-in-banking-2017-3. Acessado em: 12, Jun, 2018.

[6] Lagarde, C. (2017). ***Central Banking and Fintech—A Brave New World?*****. Disponível em: https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintecha-brave-new-world**. Acessado em: 13, Dez, 2019.

[7] PALLOCK, Darryn Pollock. (2019). ***Can Afghanistan Catapult Its Healthcare Sector Forward with Blockchain?*** Disponível em: https://www.forbes.com/sites/darrynpollock/2019/12/09/can-afghanistan-catapult-its-healthcare-sector-forward-with-blockchain/#1589d47c28a3. Acessado em: 13, Dez, 2019.

[8] Qi, Bing & Qian, Li & Lo, Hoi-Kwong. (2010). ***A brief introduction of quantum cryptography for engineers.***

[9] *SCHUMPETER, Joseph A. Schumpeter,* ***Die Theorie der Wirschaftlichen Entwicklung****,* New York: Graw-Hill Book Company, 1911.

[10] SCHUMPETER, Joseph A. Schumpeter***, Business Cycles: A Theoretical, Historical, and Statistical Analysis of the Capitalist Process****,* New York: Graw-Hill Book Company, 1939.

[11] ***The Internet of Value: What It Means and How It Benefits Everyone****, Ripple Foundation, Disponível em: https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/,* acesso em: 22, Fev, 2018.

[12] ***The Limits of Quantum, Scott Aaronson, The University of Virginia, 2008****. Disponível em: https://www.cs.virginia.edu/~robins/The_Limits_of_Quantum_Computers.pdf,* acesso em: 13, Dez, 2017.

[13] Therlow Alan & Nash Richard & Cuomo Jerry & Pureswaran Veena, IBM (2017), ***Building Trust in Government: Exploring the Potential of Blockchain,*** Disponível em: <https://www.ibm.com/thought-leadership/institute-business-value/report/blockchain-for-government>, IBM Institute of Business Value and the Economist Intelligence Unit, London, acesso em: 13, Dez, 2019.

[14] *WOLF,* Ronald de Wolf, *The Potential Impact of Quantum Computers on Society*, 2017. Disponível em: https://arxiv.org/pdf/1712.05380.pdf, acesso em: 12, Dez, 2019.