Síntese *Blockchain*

José Carrijo / ITI / CC / PR

Palavras-chave: Blockchain, cripto moeda, moeda digital, bitcoin, ethereum, Monero, prova de trabalho, curva elíptica, RSA

1. INTRODUÇÃO

Quanto mais se detalha *blockchain* ou cripto moeda, mais se tem consciência do quanto essa tecnologia é engenhosa, incita pensamento técnico, fomenta a curiosidade, ajuda internalizar conceitos, permite perceber que esta tecnologia pode mudar o modo de interação entre pessoas, órgãos do Governo, empresas públicas e privadas. Ao se ater às teorias matemáticas que possibilitaram o desenvolvimento de aplicações seguras e eficientes, não se percebe dificuldade no entendimento das provas matemáticas, vislumbra-se provocação à curiosidade. O ITI busca conhecimento técnico suficiente para dialogar no mesmo tom com técnicos que tem conhecimento aprofundado, propor soluções, analisar projetos, realizar parcerias com órgãos governamentais e com a iniciativa privada. Enfim, o ITI se empenha para contribuir tecnicamente, disseminar sentimento técnico e provocar uma entoada tecnológica, fomentando a pesquisa, objetivando prospecção tecnológica. Com conhecimento técnico sobre redes que contemplam *blockchain*, como exemplo redes de cripto moedas, percebe-se os porquês de sua beleza tecnológica, de sua sutiliza, aceitação e uso quase que desenfreado pela sociedade. O intrigante é que todo processo realizado de forma seriada, intermitente ou periódica pode ser registrado de forma encadeada em um *blockchain*, bastando para tanto mensurar a estratégia, relacionando interesse técnico e político, burocrático, estrutural e financeiro.

Blockchain é uma tecnologia promissora. É base de aplicações diversas, como as de cripto moedas e as de registro de documentos, dispostos em blocos encadeados e vinculados, em ambientes descentralizados. O encadeamento é feito de tal forma que é pouco provável que ocorram alterações em seus registros e que essas passem despercebidas ou desapercebidas.

É possível que diversas outras aplicações baseadas em *blockchain* ainda sejam criadas e, em pouco tempo, venham fazer diferença e consolidem-se como algo ainda maior, causando impacto social significativo, implicando em mudanças culturais e cotidianas irreversíveis. Com o usufruto dessa tecnologia, seja para comodidade do cidadão, seja para controle e transparência, como as cripto moedas que vêm revolucionando e mudando prognósticos e prospecções, sejam as aplicações para registro e encadeamento de documentos, sua concepção, internalização e culturalização poderão implicar em mudança comportamental relevante na população. Nesse caso, é importante considerar dois princípios: primeiro, se é o caso prover serviço cuja homologação ocorra de forma descentralizada; segundo, se transparência é o princípio a ser alcançado.

O fato é que *blockchain* é base dessa dicotomia, alicerce das aplicações de cripto moeda e registro de documentos de forma encadeada e vinculada. É comum ocorrer comentários sobre cripto moedas, ou registro de documentos encadeados, ressaltando a tecnologia e nomenclatura *blockchain*, por um lapso deixa-se de mencionar a aplicação. *Block*chain tornou-se uma marca, as aplicações embora as mais diversas quase que são esquecidas diante do princípio tecnológico: encadeamento de blocos com verificação descentralizada por meio de desafios. Há de se considerar que tornar-se-ia difícil de se consolidar sistemas com transações e verificações descentralizadas assinadas digitalmente,

exclusivamente, onde a origem estaria sendo contemplada, mas a vinculação do destino talvez não.

Aplicações que vinculam e encadeiam documentos são peculiares, talvez pouco diferenciadas comparando-se àquelas desenvolvidas para cripto moedas, tanto por motivo de seu uso quanto para quem os utiliza. Aplicações exclusivas para vinculação de documentos não têm o porquê de serem baseadas em 'provas de trabalho' – *PoW,* por meio de desafios, além de que os documentos ou as informações não necessariamente são gravados nos blocos de registros. Também, o desenvolvimento ou definição de uma aplicação para essa finalidade depende do interesse de empresa ou do Estado, porque demanda infraestrutura, interesse em transparência e disponibilização de documento e informação não necessariamente de acesso irrestrito.

Por sua vez, cripto moeda pertence a uma classe de aplicações bem mais difundida no 'mundo' *blockchai*n. Aplicações como as de cripto moedas são mais do que um sistema, são topologias em si porque são por demais complexas e, ao mesmo tempo, como se houvesse uma dicotomia de conceitos e pressupostos, são transparentes para os usuários. O intrigante é que o núcleo de poucas cripto moedas derivam centenas de outras.

Por enquanto, das aplicações de *blockchain* hoje existentes, a mais impactante, mais conhecida e até enigmática são as de cripto moedas. A ideia de cripto moedas, analisada como ideia somente, chega a ser excêntrica: a partir de um sistema, pessoas passam a comprar e vender moedas digitais, algo como um 'ativo digital', que se valoriza devido a demanda, não pelo 'produto material', que não existe. Quem as compra não recebe dividendos, tem lucro apenas em caso de haver demanda. Têm flutuações talvez pela falta de lastro, talvez por serem recentes, talvez porque não necessariamente tenham liquidez. Há centenas de moedas

disponíveis, que em sua maioria têm dificuldades em se estabelecer por serem menos conhecidas.

Para uma cripto moeda, inicialmente sem valor, são oferecidas certas quantidades para usuários quaisquer – por isso são nominadas como *Initial Coin Offering – ICO* - quando do lançamento da aplicação são repassadas gratuitamente. Depois, aguarda-se sua aceitação, disseminação e comercialização. Isso acontece sem um aparente lastro, sem comando centralizado, baseado na confiança depositada por usuários, investidores, que passam a acreditar e confiar na tecnologia, no processo e no sistema. Inclusive, quesitos como esses talvez são considerados, subjetivamente entendidos, como lastro de moedas digitais.

Entre outras peculiaridades de cripto moedas está a implementação e desenvolvimento das aplicações. Sua topologia é por demais complexa. Por exemplo, em sua criação fixa-se a quantidade máxima de moedas, o tempo aproximado para os mineradores formalizarem e homologarem cada transação, possibilita cobrança de taxa de serviço por parte das mineradoras cobradas dos usuários e, a ideia mais intrigante, recompensa o minerador que primeiro autorizar a transação como correta por meio de desafios baseados em “Força [computacional] de Trabalho” realizada pelo minerador. Os resultados são obtidos probabilisticamente, baseados em esforço computacional por meio de uma prova, Prova de Trabalho – *Poof of Work, PoW*. Para realização desses desafios, para as cripto moedas mais comuns, precisa-se de alguns minutos de execução computacional exaustiva, baseadas em hardwares e firmwares, em geral dedicados. Também, para algumas moedas digitais, há também a prova de participação (prova de consenso – *Proof of Stake, PoS*), nesse caso demoram em média menos tempo, um minuto ou menos.

A disponibilização de um montante de moedas entregues aos mineradores como recompensa após execução da Prova de Trabalho e

comprovação de que a transação é válida é singular; este é o momento de criação de moeda digital. Para o caso da cripto moeda *bitcoin*, esse montante perde pela metade por período de tempo pré-fixado. Esse esforço computacional é fixado baseado no tempo médio computacional necessário para comprovação da veracidade da transação, isso para que o tempo limite de “vida” da moeda seja devidamente contemplado. Dessa forma, o esforço computacional ora é maior, ora é menor, sempre privilegiando o tempo necessário para homologação da transação, independentemente da tecnologia utilizada para 'rastrear' a solução de interesse.

Como curiosidade dessas cripto moedas, seu início se dá tão somente por meio do desenvolvimento de uma aplicação, que pela sua maioria se baseia e utiliza-se da infraestrutura tecnológica de outras já bem estabelecidas, permitindo usuários comprar e vender algo exclusivo, nominado também como 'moeda digital' ou 'moeda virtual' ou ‘cripto moeda’. A operação de compra e venda chama-se transação, que precisa ser validada por terceiros nominados como mineradores, que são geralmente recompensados a cada validação pelo sistema.

Para os usuários, há possibilidade de entraves para que ocorra mineração. Por exemplo, o valor da transação é irrisório ou a cripto moeda que melhor gratificar, que tem melhor custo/benefício para o minerador, pode ter preferência para execução da mineração. Por sua vez, as mineradoras precisam realizar algum investimento de infraestrutura computacional e pagamento do consumo de energia elétrica. Assim, torna-se um comércio mesclado entre a confiança no sistema e na infraestrutura da mineração, com objetivo de lucro para as partes, entre mineradoras e usuários.

2. TEORIA E TECNOLOGIA

Blockchain tornou-se rapidamente uma expressão bastante conhecida, uma terminologia bem difundida, uma referência técnica para

múltiplas aplicações. De forma natural, e aos poucos, sua disseminação ocorreu intrinsecamente e concomitantemente com o uso massivo de algumas aplicações e a possibilidade de implementação nos mais diversos segmentos tecnológicos. Hoje, a tecnologia *blockchain* é entendida como síntese de sua própria fundamentação técnica.

A tecnologia *blockchain* é utilizada em aplicações que contemplam o encadeamento de blocos com registros de informações vinculados, rastreáveis e imutáveis. Possibilita ainda o acompanhamento e homologação descentralizados ou não, interligando cada bloco de registros - *flat file* - ao seu antecessor. Aplicações que utilizam *blockchain* com impacto significativo na sociedade são as de moedas digitais. Essas são concebidas objetivando homologação descentralizada de cada transação, com anotação dos registros em arquivos, possibilitando acompanhamento transparente das transações, não necessariamente dos usuários. Poucos anos foram suficientes para centenas de cripto moedas surgirem. As identidades dos usuários são preferencialmente anônimas e os registros das movimentações inalteráveis. É bastante comum a existência de comentários sobre a terminologia *blockchain* fazendo-se referência a cripto moeda, ou vice-versa.

As aplicações *blockchain* ao proverem serviços com homologação descentralizada e registros imutáveis provocaram em usuários mais ideológicos e entusiastas o sentimento de vislumbre. Esses passaram atribuir seu uso e disseminação como saída e exclusão quanto ao excesso de controle do Estado, como condição inequívoca para obtenção de transparência dos serviços prestados pelo Governo, instituições ou empresas. Por meio de posicionamentos dos mais diversos fica subentendido que a disponibilização de quaisquer serviços por parte de aplicações em *blockchain* têm que ter necessariamente seu controle e homologação exclusivamente descentralizados. Algo que não é premissa e nem proposta

determinante desta tecnologia. Além disso, esses usuários conservadores também defendem que em caso de adoção de aplicações com regras contrárias como a de homologação descentralizada necessariamente estar-se-ia subvertendo processos de transparência. Este pensamento é tão sintomático e enviesado que a mera possibilidade de se adquirir algo diferente, como a de homologação centralizada, gera-se automaticamente o sentimento como se fosse uma atitude retrógrada, como sendo um retrocesso à transparência, mal uso da tecnologia e também de má-fé. O que não é o caso, necessariamente.

Blockchain é um assunto que ao se discorrer se desmistifica sua complexidade técnica. Para provocar melhor entendimento da fundamentação da ideia, aqui é abordado com viés técnico, informativo e de contexto. Parte das observações pode ser redundante, meramente elucidativa ou tecnicamente mais conservadora. Expressões e terminologias técnicas ocorrerem apenas quando estritamente necessárias. Ao discorrer um pouco sobre técnicas desta tecnologia, pode se ter melhor compreensão e entendimento de muitos porquês de sua massificação que envolve e promove minimamente curiosidades.

Esses posicionamentos e observações sobre *blockchain* têm como base compilação e sequenciação de ideias expostas em diferentes fontes de estudo e pesquisa. Sobretudo, contemplam exposição de percepção tanto da parte tecnológica como de contexto. Algumas definições expostas de forma simplista têm como objetivo minimizar dúvidas quando citadas ao se comentar processos que envolvem *blockchain*.

2.1. HASH – RESUMO CRIPTOGRÁFICO

Primeiro, entende-se como 'sequência binária' o conteúdo digital armazenado em áreas de memória ou em arquivos digitais como documentos, imagens, áudios ou vídeos digitais.

Função Hash - Hash function - não tem tradução estabelecida para o português. Primeiramente, professores paulistas – Unicamp e USP – definiram essa expressão como “função resumo”. Por sua vez, também, definiram *hash*, correspondente unívoco de uma sequência binária, como “resumo criptográfico”. Este conceito é importante porque é base fundamental do encadeamento de blocos.

Tecnicamente, existem premissas de segurança para uma função resumo, que garante a unicidade dos resultados, e consequente segurança no encadeamento *blockchain*. Dadas as sequências binárias x e y, de comprimento |x| e |y| quaisquer:

- É impossível [computacionalmente] o resumo criptográfico ser o mesmo, digo, HASH(x) = HASH(y)

- Dado um resumo criptográfico h = HASH(x) é impossível recuperar a sequência binária x que o definiu.

Entende-se como quebra de uma função resumo quando um atacante consegue verificar que uma ou outra dessas duas premissas não é atendida; mesmo que parcialmente, porém de forma significativa. A terminologia “quebra” de uma função resumo é utilizada de forma diferente quando se trata de quebra de algoritmo de sigilo ou de assinatura. A quebra de uma função resumo acontece quando se encontram dois resumos criptográficos, com entradas quaisquer, com alto nível de colisão, a quantidade de *bits* dos resumos criptográficos coincidentes é significativamente acima de 50%. Sobre quebra de algoritmo de sigilo acontece quando se consegue recuperar a informação sob sigilo ou a chave. A quebra de um sistema de assinatura, algumas vezes comentado como quebra da assinatura, ocorre quando um atacante consegue assinar determinado documento se passando por um terceiro, adulterando ou não o documento.

Um função resumo segura tem como saída, dada uma sequência de *bits* de entrada de qualquer comprimento, uma sequência de *bits* estatisticamente bem distribuída. Assim, cada minerador ao receber os dados de uma transação, e um “nonce”, sequência de *bits* também bem distribuída, e mais um contador, executa operações exaustivas de cálculos de resumos criptográficos até que se obtenha um que tenha pelo menos “k” *bits* iguais a zero no início da sequência. Por isso, o desafio é justo, é imprevisível ter algum conhecimento a priori que determinado “nonce” poderá contribuir que uma menor ou maior quantidade de cálculos.

2.2. ASSINATURA DIGITAL

Com pretensão de melhor discorrer sobre *blockchain*, sem retornar a princípios técnicos criptográficos, é imprescindível abordar esquemas de assinatura digital. Princípio necessário para lisura e confiança de sistemas que se baseiam nesta metodologia de encadeamento de blocos, com registros assinados e verificados por pares de chaves pública e privada, ou por certificados digitais gerados em estruturas do tipo ICP.

Para aplicações *blockchain*, o ITI considera importante certificação digital baseada em Infraestrutura de Chaves Públicas – ICP, embora a maioria das aplicações hoje disponibilizadas utilizem pares de chaves pública e privada. O uso desses pares busca privilegiar o anonimato dos usuários, que as geram pela aplicação, tornando a chave pública base de seu endereço. O ITI entende como importante esses dois modelos de negócio, defende a possibilidade de certificados digitais padrão ICP-Brasil, por possuírem validade jurídica.

Processos de assinatura digital advém de técnicas e métodos criptográficos, protocolos específicos, a partir de primitivas criptográficas. Por sua vez, os esquemas mais conhecidos são os baseados no sistema RSA e os em curvas elípticas, utilizados em

aplicações baseadas em *blockchain*. Um certificado digital é basicamente a chave pública (do usuário) encapsulada em determinado formado com informações adicionais como nome do usuário e sua validade, com assatura de um órgão fiscalizador, homologador e de confiança, irrelevantes no processo matemático para determinação da assinatura, porém importantes para controle e credibilidade.

Cabe comentar que uma assinatura digital provê o serviço de não repúdio e integridade – o usuário não tem como negar determinada assinatura quando realizada por meio de sua chave privada. Por sua vez, o certificado digital do usuário, que inclui sua chave pública, realiza tal verificação.

2.3. PROVA DE TRABALHO (PoW)

A medida Prova de Trabalho compreende o cálculo de *hashs* repetidas vezes até que se obtenha um *hash* onde as primeiras “k” posições sejam iguais a zero.

O sistema define como “alvo” uma medida encaminhada para o minerador para que este determine um resumo criptográfico menor do que esta medida encaminha. Por exemplo, para o alvo 0xc7ea4f82, o resultado do hash de uma transação acrescido de um *nonce*, sequência aleatória para cada minerador, concatenado com um número que é incrementado passo a passo, corresponde a determinar um hash que seja menor do que:
PoW = 0xea4f82 * 2**(8*(0xc7 - 3)) =
0x0000000000ea4f820000000000000000000000000000000000000000000000000000

3. CENÁRIO

É importante o entendimento quanto a eficácia e credibilidade dos protocolos *blockchain*, por esses motivos em pouco tempo outros protocolos e aplicações serão disponibilizados.

Blockchain aparece no cenário mundial como uma ferramenta inovadora e promissora provocando por si só fomento à pesquisa e desenvolvimento em inúmeros cenários. As aplicações disponibilizam o serviço de geração de pares de chaves para os usuários que se auto-identificam. O ITI considera que para aplicações específicas, como para uso de Governo, essas podem utilizar certificados digitais padrão ICP-Brasil, que têm validade jurídica, em detrimento do uso de pares de chaves.

A tecnologia *Blockchain* personifica-se pelo encadeamento de blocos, homologação descentralizada, assinatura e verificação digitais. Como regra, os protocolos já propostos garantem não repúdio, mas não necessariamente sigilo da informação ou impossibilidade de rastreamento, nem validade jurídica.

O ITI entende como fundamental a construção de um pensamento alinhado para prover conhecimento técnico e contribuição efetiva em *blockchain* para fins de interesse do Governo. Neste contexto, o uso de certificação digital com validade jurídica é importante. Como citação de aplicações baseadas em *blockchain* são as de cripto moedas. Embora tenham sido propostas recentemente a partir de 2009, com apoio e investimento de empresas de grande porte, rapidamente avançaram tecnologicamente e no agrado dos usuários. Como consequência houve aparecimento de centenas de outras moedas, neste curto período de tempo.

As inúmeras propostas de protocolos baseados em *blockchain* requerem transposição de desafios quanto à privacidade, escalabilidade e falta de governança – controle de usuários e dos pares de chaves pública e privada geradas.

Escalabilidade é um entrave para algumas aplicações que utilizam ou podem fazer uso da tecnologia *blockchain. H*á aplicações que seus usuários têm que estar previamente cadastrados –

permissionados, há àquelas que não exigem – não permissionadas. Para essas aplicações, o desempenho das homologações é baixo, além de provocar falta de governança. Para as aplicações com usuários permissionados, o desempenho é mais eficiente, mas a quantidade de usuários é menor. Além disso, organizações ou empresas não necessariamente se comportam de forma democrática, requerem controle de seus sistemas, negócios e políticas, viés desta tecnologia é transparência.

4. APLICAÇÕES

Aplicações em *blockchain* baseiam-se em assinatura digital com curvas elípticas. Entre elas, comento sobre a peculiaridade da cripto moeda Monero, pela sutileza de seu protocolo: utiliza-se de um método de assinatura bastante eficiente e seguro baseado em curvas elípticas denominado Ed25519. Tem segurança equivalente à da curva elíptica do NIST P-225 e a do sistema RSA com 3000 *bits*; provê não rastreabilidade por meio de endereços de uso único e anonimato do usuário; baseia-se em esquema criptográfico homomórfico; impossibilita revogação de assinatura. Foi implementado o esquema proposto por Fujisaki et al, variação da proposta de Shamir et al, denominado *ring signature*: o usuário assina uma transação com sua chave privada; para verificação este usuário disponibiliza todas as chaves públicas de todos os usuários pertencentes ao anel – do grupo cadastrado; qualquer participante do grupo que verificar a assinatura constante na transação, estará convencido que o assinante faz parte do grupo mas não tem como saber quem a assinou; mantendo-se assim o anonimato. Se por um lado o protocolo *bitcoin* utiliza-se de um único par de chaves pública e privada, o protocolo Monero gera uma chave pública, usada uma única vez; esta é baseada no endereço de acesso do usuário; somente a origem [o nó] pode recuperar a chave privada única equivalente.

5. CONDICIONANTES

A tecnologia *blockchain* provê integridade dos dados, não repúdio e transparência – transações são encadeadas e rastreáveis, algumas não têm sigilo. Destaca-se significativamente em transações financeiras, seus usuários podem realizar consultas ou transações.

Há certa preocupação por parte das instituições e empresas para adoção da aplicação que melhor se ajusta, vinculando ao seu modelo de negócio premissas básicas como restrição para usuários permissionadas ou não, bases de dados centralizadas ou não.

Como exemplo, B*itcoin* e *Ethereum* são instâncias de *blockchain* para usuários não permissionados, com base de dados descentralizados. Quaisquer usuários podem entrar na rede para executar tarefas ou não, sem entidade que os administre.

Cripto moeda é apenas uma aplicação dessa invenção tecnológica, tem regras específicas para validação de transações de forma independente e descentralizada.

Cada bloco de transações é encadeado por meio do resumo criptográfico do bloco anterior de forma unívoca. Cada transação é assinada pelo usuário e os resumos criptográficos mais utilizados têm comprimento de 256 *bits*.

O fundamento técnico de protocolos baseados na tecnologia *blockchain* refere-se a recursos distribuídos que são públicos, impermutáveis e ordenados.

A tecnologia se desenvolve nos detalhes de cada uma de suas partes. Especificamente, o núcleo b*itcoin* inclui carteiras, quesitos para transação, validação de bloco e rede completa de nós - ponto a ponto. É um projeto aberto para quaisquer propósitos, tem comunidade de voluntários que o otimiza, com base em

documentos técnicos que descrevem cada serviço, característica ou funcionalidade.

Para melhor compreensão do núcleo *bicoin*, para aqueles que têm conhecimento de instalação de aplicações e sistemas operacionais, pode ser interessante a instalação do ambiente de desenvolvimento a partir da documentação técnica, observando as ferramentas, bibliotecas e suporte de *sofware* e as mais diversas diretivas.

6. CRIPTO MOEDA

Aplicações que vinculam e encadeiam documentos são diferenciadas se comparadas às de cripto moedas, tanto por motivo de uso quanto por quem os utiliza. Aplicações exclusivas para vinculação de documentos não têm o porque de serem baseadas em Provas de Trabalho – PoW (desafios). A demanda ocorre pela iniciativa privada, pelo Estado, ou pelo cidadão. Os primeiros objetivam interesse em transparência e disponibilização de documentação, o último em investimento e lucro.

Cada aplicação ao ser disponibilizada para usuários, cada moeda, tem definido o seu tempo de vida, tem fixado a quantidade máxima de moedas, o tempo aproximado para os mineradores validarem cada transação por meio de realização de desafios nominados como Prova [computacional] de Trabalho – Proof of Work, PoW, que é ajustado continuadamente, ou Prova de Consenso – Proof of Stake, PoS, e sua bonificação.

Cripto moeda pertence a uma classe de aplicações bem difundida na tecnologia *blockchai*n. Os sistemas de cripto moedas são topologias em si, são por demais complexas. Como se houvesse uma dicotomia de conceitos e pressupostos, são transparentes para os usuários. O intrigante é que o core de poucas cripto moedas derivam centenas de outras.

Das aplicações de *blockchain* hoje existentes as mais impactantes, mais conhecidas e até enigmáticas são as de cripto moedas. Analisadas somente como ideia, chega a ser excêntrica: a partir de um sistema, pessoas passam a comprar e vender moeda digital que se valoriza devido a demanda, não pelo 'produto material', que não existe. Quem as compra não recebe dividendos, tem lucro apenas em caso de haver mais demanda. Têm flutuações talvez pela falta de lastro, talvez por serem recentes, talvez porque não necessariamente tenham liquidez. Existem centenas de cripto moedas disponíveis, que em sua maioria têm dificuldades em se estabelecer por serem menos conhecidas.

7. SUTILIZAS DA CRIPTO MOEDA *BITCOIN*

a Criação de uma medida denominada “Prova de Trabalho”, para validação de transações é uma ideia minimamente engenhosa. No caso de *bitcoin*, a cada 2016 blocos esse esforço computacional é redimensionado. A validação de um bloco ocorre em média em alguns minutos. Se o tempo médio para homologação exceder ao previsto, o esforço computacional diminui, ou vice-versa. Essa métrica está diretamente ligada ao tempo estipulado para durabilidade da moeda. Com isso, independentemente de novas tecnologias de hardware e firmware, o sistema controla para que cada homologação ocorra conforme sua concepção.

Para Cada validação há uma recompensa. No caso de *bitcoin*, em 2009 era de 50 *bitcoins*. A cada 4 anos (ou 210.000 blocos validados) a recompensa cai pela metade. Atualmente é de 12.5 *bitcoins*, em 2056 será de 0.01 *bitcoin*, e em 2140 de 0.000000003 *bitcoin*. O fato de esse valor nominal de recompensa cair para a metade a cada período de tempo poderá ocasionar ajustes da tarifação estipulada pelas mineradoras.

A medida “Prova de Trabalho” compreende o cálculo de hashs repetidas vezes até que se obtenha um hash onde as primeiras “k” posições sejam iguais a zero.

O resultado do hash de uma transação acrescido de um 'nonce', sequência aleatória diferente para cada minerador e incrementado passo a passo, corresponde a determinar um hash que tenha pelo menos “k” *bits* iniciais iguais a zeros, em uma sequência de 256 *bits*. Atualmente, o hash a ser encontrado deve ter 60 *bits* iniciais iguais a zero, k=60. Isso significa que a chance de se encontrar um hash ao acaso com tantos zeros iniciais corresponde a pelo menos um trilhão de vezes mais difícil que ganhar na Mega Sena: $2^{61}/2^{26}=2^{40}$. Por esse motivo, é imprescindível escolha de função resumo segura, com sequência resultade bem distribuída estatisticamente.

8. CHAVES e ENDEREÇOS

Uma cripto moeda se estabelece em métodos, protocolos e algoritmos criptográficos provendo sigilo, autoria e integridade das transações; serviços críticos para a tecnologia *blockchain*. Chaves, endereços e esquemas de assinaturas digitais formam o cerne desse protocolo. Chaves públicas são usadas para definir os endereços dos usuários para recebimento de fundos, as chaves privadas são para assinaturas das transações. Os pares de chaves são criados pelos usuários e gravados em suas carteiras, os parâmetros de geração são gravados pelo sistema com o objetivo de se necessário gerar as respectivas chaves públicas a partir das chaves privadas. Cada usuário habilita vários serviços com atestado de propriedade, modelo de prova criptográfica de confiança e controle descentralizado.

O protocolo *bitcoin* utiliza a curva elíptica sec256k1, padrão NIST – National Institute of Standards and Technology ($Y^2 = X^3 +$

7 mod p, com p primo definido como p = $2^{256}+2^{32}+2^{9}+2^{8}+2^{7}+2^{6}+2^{4}-1$), com 256 *bits*. Para geração de chaves, utiliza-se também um ponto da curva G preestabelecido. A chave pública é um ponto na curva consistindo de um par de coordenadas (x,y), solução dessa equação. Para reduzir pela metade o espaço de armazenamento da chave pública, grava-se na Carteira apenas a varíavel “x”. Para manter a chave privada segura cifra-se essa com o algoritmo criptográfico padrão AES com uma senha do usuário e a grava cifrada na Carteira.

Uma Carteira pode ter uma coleção de pares de chaves, pública (K) e privada (k), codificadas na base 'Base58'. A chave privada é uma sequência binária com 256 *bits* gerada aleatoriamente, frequentemente representada em QR code. A partir da chave privada determina-se a chave pública correspondente. O endereço (A) desse usuário é gerado com as funções resumo SHA256 e RIPEMD160 e sua chave pública. Em cada carteira é gravado o terno (k , K , A).

9. CARTEIRA

A terminologia 'Carteira' para protocolos de cripto moedas pode ter significados e estruturas diferentes. Nas Carteiras não têm gravados os créditos dos usuários, porque esses permanecem na rede *blockchain*. Esta terminologia pode se referir à aplicação que interfaceia com o usuário, à disponibilização de serviço que impede acesso indevido, à administração de chaves e endereços, ao rastreamento e assinatura de transações. Essas aplicações provêm o cerne do processo, facilidade operacional, segurança e flexibilidade. 'Carteira' refere-se também à estrutura de dados – arquivos - usada para armazenar e gerenciar chaves, que podem ser determinísticas ou não. Essas são geradas a partir de sequências aleatórias e usadas uma a uma. Àquelas são geradas hierarquicamente, por meio de sementes em estrutura de árvore. Assim, podem ser regeradas e provém facilidade de uso e

portabilidade – migração para Carteira diferente. Na prática, flexibilizou-se a segurança em detrimento da facilidade do uso e portabilidade. Entendendo as chaves como uma estrutura em árvore, determinados ramos podem ter fins específicos, como o de pagamentos, recebimentos ou criação de sequência de chaves públicas sem ter que acessar as chaves privadas. Geradas a partir de sequências de palavras escritas em inglês, disponibilizadas pela aplicação, torna o processo de geração bastante amigável por ser algo mnemônico. A tecnologia *bitcoin* tem amadurecido, o que implicou na criação de padrões, tornando-se interoperável, de fácil uso, segura e flexível.

10. TRANSAÇÕES

Referência a uma ou outra técnica pode ser meio insossa ou enfadonha; conceitos, nomenclaturas ou definições expostos em breves comentários ocorrem quando necessários. Os sistemas de cripto moedas como o bitcoin têm melhorado em segurança e resiliência, tem potencial muito além do de transações com moeda digital, permite armazenamento de dados não relacionados à transferência de moeda digital. No entanto, esse viés é controverso porque vai de encontro com o escopo primário desse protocolo.

Transações são a parte mais importante dos protocolos de cripto moedas. Todo o sistema é projetado para assegurar transações validadas em estruturas de dados, com transferências de valores entre usuários, codificadas e registradas no *blockchain*, como se fosse uma entidade contábil. Porque *Blockchain* é uma tecnologia recente que avança e permite prospecção para criação de diversas outras aplicações, é importante entender o conteúdo de uma transação, o detalhamento de sua criação e modo de verificação, e como se tornam parte permanente de registros na estrutura *blockchain*.

A parte do bloco mais importante em uma transação é a saída, formada por partes indivisíveis, gravada no *blockchain*, organizada e validada na rede, rastreada por nós organizados de forma descentralizada.

Para a aplicação de cripto moeda, assinatura digital tem como propósito definir e garantir incondicionalmente a origem, a integridade e não repúdio da transação. Cada transação é assinada de forma independente, inclusive pode ter diferentes usuários, quando parte dos créditos são oriundos de outras transações. Como quesito, uma assinatura implica em um comprometimento entre o usuário que assina e a transação. Para tanto, depende da geração de sequências de números aleatórios, que deve ser diferente para cada assinatura. A reutilização de sequências pode provocar a quebra da assinatura e assim facilitar roubo de Carteira, e consequente desvios de cripto moeda.

11. CONSIDERAÇÕES

Conhecer a tecnologia *blockchain* implica em se conhecer a de cripto moedas, a mais bem difundia e conhecida. Sistemas que se utilizam da estrutura *blockchain* podem mudar a forma de o mundo se relacionar, comenta-se exaustivamente sobre cripto moedas, relacionando *blockchain*, e vice versa. O que mais surpreende é que sua aplicação pode ocorrer em processos quaisquer que resultam em procedimentos e resultados gerados de forma intermitente ou periódica. Para tanto, a dimensão do cenário a ser implementado é imprescindível, os resultados e impactos têm que ser mensurados.

12. REFERÊNCIAS para leitura:

1. AlTawy, Riham; ElSheikh, Muhammad; Youssef, Amr M.; Gong, Guang – Lelantos: A Blockchain-based Anonymous Physical Delivery System

2. Antonopoulos, Andreas M.: Mastering Bitcoin - Programming the Open Blockchain,
3. Chou, Tung – Sandy2x: New Curve 25519 Records
4. Kumar, Amrit; Fischer, Clément; Tople, Shruti; Shaxena, Prateek - A Traceability Analysis of Monero’s Blockchain
5. Li, Ming; Weng, Jian; Yang, Anjia; Lu, Wei – CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourincin
6. Li, Wenting; Sforzin, Alessandro; Fedorov, Sergey; Karame, Ghassan - Towards Scalable and Private Industrial Blockchains
7. Lin, Huijia; Tessaro, Stafano – Indistinguishability Obfuscation from Bilinear Maps and Block-Wise Local PRGs
8. Rivest, R. L; Shamir, A.; Tauman, Y. - How to leak a secret
9. Su, Borching - MathCoin: A Blockchain Proposal That Helps Verify Mathematical Theorems In Public
10. Wüst, Karl; Gervais, Arthur – Do you need a Blockchain?
11. https://eprint.iacr.org
12. https://monero.org
13. https://www.ethereum.org
14. https://bitcoin.org
15. https://www.rsa.com/