ITI

Instituto Nacional de
Tecnologia da Informação

Blockchain - duas tecnologias, mesmas finalidades

INTRODUÇÃO – *Blockchain*

Blockchain é um arquivo de dados – *flat file,* cada registro é vinculado ao antecessor, por meio de resumo criptográfico – (*HASH*) .

Blockchain é uma tecnologia para múltiplos propósitos. Os registros são imutáveis e descentralizados. Em cripto moedas, há uma prova de trabalho a ser executada pelos mineradores, que tem validação por múltiplos outros.

O sistema provê o serviço de assinatura digital para acesso de usuários, garantindo integridade e não repúdio.

Blockchain - duas tecnologias, mesmas finalidades

Blockchain: HASH – sua importância

Uma função hash, Y = H(X), tem como característica:

(1) Dado Y, computacionalmente impossível determinar X

(2) Dado X e X', computacionalmente impossível encontrar HX) = H(X').

Baseado nesses princípios, utiliza-se a funções hash para o sistema de desafios.

ITI
Instituto Nacional de Tecnologia da Informação

Blockchain - duas tecnologias, mesmas finalidades

ESTRUTURA DE UM BLOCO: cabeçalho e lista de transações:

Tamanho do bloco:

04 bytes

Cabeçalho - em vários campos: *80 bytes*

Quantidade de transações:

1 a 9 bytes

Todas as transações:

quantidade [?]

tamanho médio de uma transação: *250 bytes*

do bloco:

> 500 transações

CABEÇALHO: *04 bytes:* *Versão software rastreamento*

32 bytes: hash do bloco

Blockchain - duas tecnologias, mesmas finalidades

CRIPTO MOEDAS VERSUS BLOCKCHAIN

No blockchain bitcoin o encadeamento das transações é tão bem formalizado que ataques de hackers na rede é praticamente impossível. Validações são realizadas por grupos de computadores, onde todos mantém sua cópia atualizada do blockchain.

Blockchain - duas tecnologias, mesmas finalidades

CRIPTO MOEDAS

Cripto moeda pode ser entendida como moeda atemporal, digital, com lastro permeado entre a confiança do usuário baseado: (i) na segurança do protocolo; (ii) falta de ingerência governamental; (iii) teoria técnica bem estabelecida; (iv) os registros do arquivo blockchain não são alterados ou apagados; (v) descentralização das validações.

As cripto moedas, conhecidas como *ICO'S – Initial Coin Offering*, podem ser entendidas como investimento a longo prazo; há os reticentes.

Blockchain - duas tecnologias, mesmas finalidades

"SUTILIZAS" do BLOCKCHAIN – prova de trabalho - I

Estabelecimento de dificuldade temporária para execução da validação de transações, é alterado de tal forma que um bloco deve ser validado em dez minutos.

A cada 2016 blocos essa dificuldade é reavaliada. Se o tempo de validação das transações ultrapassar, o esforço computacional, a *dificuldade de trabalho* diminui, ou vice versa.

Blockchain - duas tecnologias, mesmas finalidades

"SUTILIZAS" do BLOCKCHAIN – prova de trabalho - II

Para Cada validação há uma recompensa, para os mineradores. Inicialmente, cada bloco validado havia uma recompensa de 50 bitcoins.

A cada 4 anos (ou 210.000 blocos validados) a recompensa cai pela metade. Atualmente, é de 12.5 bitcoin. Presume-se que em 2056 a recompensa estará próxima a 0.01 bitcoin, e em 2140 próxima a 0.000000003 bitcoin .

Blockchain - duas tecnologias, mesmas finalidades

"SUTILIZAS" DO BLOCKCHAIN – prova de trabalho - III

O estabelecimento da prova de trabalho implica no cálculo de duplo hash – SHA256.

O nível de dificuldade está na quantidade de vezes de se ter que calcular hash até que as primeiras posições "k" sejam iguais a zero.

O grau de dificuldade é definido de tal forma que um bloco deve ser validado em dez minutos. Um "alvo" de dificuldade é estabelecido pelo sistema.

Blockchain - duas tecnologias, mesmas finalidades

"SUTILIZAS" DO BLOCKCHAIN – prova de trabalho - IV

Para o "alvo" igual a 0x1b0404cb, a dificuldade está em encontrar, a partir de uma entrada fixa e um 'nonce' aleatório, para cada minerador e incrementado passo a passo, de tal forma que seja menor do que 'DIFICULDADE':

DIFUCULDADE = 0x0404cb * 2**(8*(0x1b - 3)) = 0x00000000000404CB000000000000000000000000000000000000000000000000

Atualmente, o hash a ser encontrado deve ser iniciado com pouco mais de 60 bits iguais a zero, isso significa que a chance de se encontrar um hash 'imediatamente' com tantos zeros iniciais é mais do que um trilhão de vezes mais difícil que ganhar na Mega Sena: $2^{61}/2^{26}=2^{40}$

Blockchain - duas tecnologias, mesmas finalidades

"SUTILIZAS" DO BLOCKCHAIN – prova de trabalho - V

Suponha-se o cálculo do hash256 da expressão "Oi Certforum", acrescido de um 'nonce', até que se encontre um hash com início igual a "0x000", que equivale a "000000000000":

"Oi Certforum!3ac68be3af" => "1312af17...934c64"

"Oi Certforum!3ac68be3af+1" => "e9afc424...32a7d8"

"Oi Certforum!3ac68be3af+2" => "ae37343a...4266b7"

…

"Oi Certforum!3ac68be3af+4250" => "0000c3af...dcd4e9"

Blockchain - duas tecnologias, mesmas finalidades

ÁRVORES DE MERKLE

Cada bloco do *blockchain* contém um resumo de todas as transações baseadas na árvore de Merkle. Possibilita verificar de forma resumida e eficiente a integridade de grandes conjuntos de dados, por meio de *hashs* calculados de forma recursiva:

$\Rightarrow H_A = SHA256(SHA256(\text{Transação A}))$

$\Rightarrow H_B = SHA256(SHA256(\text{Transação B}))$

$\Rightarrow H_{AB} = SHA256(SHA256(H_A \,||\, H_B))$

$\Rightarrow H_C = SHA256(SHA256(\text{Transação C}))$

$\Rightarrow H_D = SHA256(SHA256(\text{Transação D}))$

$\Rightarrow H_{CD} =$

Blockchain - duas tecnologias, mesmas finalidades

ÁRVORE DE MERKLE E VERIFICAÇÃO DE PAGAMENTO SIMPLIFICADO (SPV)

Árvores de Merkle são extensivamente usadas em nós *SPV* – *Simplified Payment Verification*. Nós *SPV* não têm todas as transações. Nesses, baixam-se apenas os cabeçalhos, autenticam-se as transações utilizando-se filtros *Bloom*.

O nó *SPV* usa árvore de Merkle para vincular a transação ao bloco e o cabeçalho ao blockchain. A combinação dessas duas vinculações, entre transação e cabeçalho e blockchain prova que a transação está gravada no blockchain.

Blockchain - duas tecnologias, mesmas finalidades

"SUTILIZAS" DO BLOCKCHAIN – prova de trabalho - V

Sobre mineração, custos de um hardware x desempenho:

Plataforma ASIC: calcula 14 MH/s custa U$ 2,400;

FPGA: calcula 25.2 GH/s

custa U$ 15,295

calcula 800 MH/s

custa U$ 800

No bitcoin a prova de trabalho inclui a Árvore (de hashs) de Merkle, o que torna mais complexo.

O Hashcash-Scrypt usa algo como uma derivação de chaves, não é PoW.

Há pretensão/ possibilidade de se alterar o duplo cálculo do Sha256 para o cálculo simples do Sha3.

Blockchain - duas tecnologias, mesmas finalidades

NEGÓCIOS E INVESTIMENTO em CRIPTO MOEDAS

Uma parte sensível de protocolos de cripto moedas é o extravio ou roubo de chaves ou Carteira, o que torna irreversível a perda do montante investido.

Há dificuldade de se antever a inovação, blockchain pode ser algo inovador ou provocar algo ainda de maior impacto.

Blockchain - duas tecnologias, mesmas finalidades

Quesitos importantes para uso de solução tipo blockchain pelo Governo, em transações e acesso de documentos pelo servidor público e pelo cidadão:

(i) Conhecer a tecnologia a ser adquirida

(ii) Receber os códigos-fonte do protocolo e sistema

(iii) Ter o direito de alterar a criptografia de sigilo

(iv) Utilizar Assinatura Digital padrão ICP-Brasil

(v) Ter domínio exclusivo das chaves utilizadas pelo sistema

(vi) Todos os direitos tecnológicos reservados ao Governo

Blockchain - duas tecnologias, mesmas finalidades

PROPOSTA DO ITI

Prover aplicação e apoio técnico baseados na tecnologia *blockchain* para gerenciamento e armazenamento de documentos do Estado brasileiro com certificados digitais padrão ICP-Brasil.

José Carrijo

Assessor

(61) 3424-3934

Jose.carrijo@iti.gov.br