****

Tecnologias de suporte ao conceito de criptomoeda

**Osman Torres Ximenes Junior**

Recife – 2013.1

Resumo

O conceito de criptomoeda, introduzido por Satoshi Nakamoto em 2008 [1] com a denominação de “bitcoin”, é um fenômeno das transações econômicas na Internet. Este trabalho tem como objetivo abordar as tecnologias de suporte ao sistema Bitcoin. Primeiramente, esta monografia provê uma visão geral de criptomoeda e especificamente da rede Bitcoin e seus componentes. Isto será feito a partir de um levantamento histórico e técnico. Os algoritmos de hash, de prova-de-trabalho e de mineração de criptomoedas serão detalhados no presente trabalho. Ao fazê-lo, definimos seus respectivos papéis nos processos do sistema de moeda digital.

Sumário

[1 – Introdução 1](#_Toc258323088)

[2 – Visão Geral 2](#_Toc258323089)

[3 – Sistema Bitcoin 5](#_Toc258323092)

[3.1 – Transferência de bitcoins 5](#_Toc258323093)

[3.2 – Verificação de Transações 8](#_Toc258323094)

[3.3 – Mineração 8](#_Toc258323095)

[4 – Conclusão 9](#_Toc258323097)

[Referências Bibliográficas 10](#_Toc258323098)

# **1 – Introdução**

As transações financeiras através da Internet utilizam o mesmo tipo de garantia do sistema financeiro tradicional. Ou seja, cada transação é regulada por órgãos do sistema ou instituições financeiras. Entretanto, o número de transações e seu tamanho prático são prejudicados por conta destes terceiros de confiança, que não conseguem deixar de mediar disputas entre as partes interessadas. Dessa forma, o custo das transações eletrônicas aumenta, o que representa uma fraqueza dos sistemas convencionais.

Bitcoin é uma "criptomoeda" elaborada inicialmente em 2008 por um indivíduo ou grupo de indivíduos usando o pseudônimo Satoshi Nakamoto. Diferente das moedas convencionais, a proposta era de uma versão peer-to-peer de dinheiro eletrônico, que permitiria pagamentos online de um nó a outro sem a presença de um terceiro nó regulador ou qualquer autoridade central. A criação da criptomoeda e suas transações são baseadas em um protocolo de criptografia de código aberto.

Bitcoins são facilmente transferíveis através de smartphones ou computadores e não dependem de qualquer órgão regulador financeiro ou gateway intermediário. Um bom número de criptomoedas já se encontra em operação, e uma relação de valores de mercado de cada uma delas se encontra em **Crypto-Currency Market Capitalizations** (http://coinmarketcap.com).

O uso expressivo do bitcoin e suas características que permitem realizar transações financeiras através da Internet, de forma rápida, barata e anônima tornam esta moeda digital uma forte candidata à moeda da nova era do mundo dos negócios, finanças e do comércio global.

# **2 – Visão Geral**

Apesar de o Bitcoin ser uma das primeiras implementações de um sistema de moeda digital baseado em criptografia para controlar a criação e transferência de dinheiro, o conceito de criptomoeda foi introduzido primeiramente por Wei Dai, em 1998. A ideia de criptomoeda baseava-se na noção de que o dinheiro é qualquer meio utilizado na troca e compra de bens e serviços.

O dinheiro do sistema Bitcoin são os bitcoins (frações dos bitcoins são conhecidas como satoshis). Como no sistema bancário, podemos possuir bitcoins e transferi-los a outra pessoa, porém de forma anônima e independente de órgãos reguladores para monitorar, verificar e aprovar as transações entre clientes e gerenciar a quantidade de dinheiro em circulação. Ao invés disso, sua garantia depende de uma rede de computadores peer-to-peer constituída por máquinas de usuários.

Desse modo, a rede é responsável basicamente por administrar a criação de novos bitcoins e as transferências entre usuários.

A criação de novos bitcoins é realizada por um processo chamado de mineração. Os usuários mineradores são recompensados com bitcoins pelos gastos com hardware para resolver problemas matemáticos bastante difíceis. A dificuldade dos problemas é regulada no sentido de manter o número de problemas resolvidos constante: a cada 10 minutos um problema é resolvido. Também foi estabelecido que o número máximo de bitcoins criados não ultrapasse a marca de 21 milhões bitcoins. Dessa forma evita-se a inflação caracterizada pela desvalorização das moedas em circulação em um sistema que não limita a oferta das mesmas.

O gráfico a seguir calcula o tempo em que o limite de bitcoins será alcançado, considerando o número de problemas resolvido por tempo constante.



Posteriormente será detalhada a ação dos usuários mineradores quanto a validação das transições.

Como já foi dito, a rede também é responsável por gerenciar as transições de bitcoins entre usuários. A segurança de cada transição é garantida pelo método de criptografia de chave pública que será destrinchado em seguida.

Nos últimos quatro anos, o valor do bitcoin oscilou, atingindo altas de até 266 dólares americanos e baixas de 7 dólares. Mas sempre se recuperando e ultrapassando valores anteriores.

O gráfico a seguir representa o preço do bitcoin em dólar americano nos últimos 12 meses.



O número de transações diárias no mesmo espaço de tempo pode ser observado no próximo gráfico.



Outras moedas diferem do sistema Bitcoin no uso das funções que adicionam dificuldade aos problemas dos usuários mineradores. Entre elas temos, Namecoin, Litecoin e PPCoin.

**3 – Sistema Bitcoin**

Dois tipos de objetos são transmitidos para todos os nós da rede Bitcoin: transações e blocos. Transações são as operações pelas quais o dinheiro é combinado, dividido e transmitido. Blocos registram as transações válidas [2]. Este capítulo abordará os principais processos do sistema: transferir bitcoin, verificar transações e mineração.

# **3.1 – Transferências de bitcoins**

#

# **3.2 – Verificação de Transações**

# **3.3 – Mineração**

**4 – Conclu****são**

# **Referências Bibliográficas**

[1] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System***.** 2008. Disponível em <http://bitcoin.org/bitcoin.pdf> (acesso em 29/06/2013)

[2] S. Barber, X. Boyen, E. Shi e E. Uzun. *Bitter to Better – How to Make Bitcoin a Better Currency.* Disponível em <http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf> (acesso em 29/06/2013)