Monitoramento e Análise das Métricas da Blockchain do BTC

ANDRÉ VIEIRA DA SILVA

Monday 9th October, 2023

Resumo

PALAVRAS CHAVE: .

Abstract

KEYWORDS: A.

Sumário

1 Introdução

Ao usar a blockchain do Bitcoin (**BTC**) [1], uma rede descentralizada, é possível fazer transações financeiras sem a presença de intermediários. As métricas da blockchain, que são dados brutos da blockchain extraídos de APIs[1] que mostram as atividades da blockchain, são usadas para monitorar e analisar as métricas da blockchain do **BTC**.

Na avaliação de criptomoedas e blockchain, as quatro principais métricas são a taxa de hash, os endereços ativos, os valores de transação e as taxas. A taxa de hash de uma blockchain é o poder computacional que os mineradores de criptomoedas usam para fazer cálculos em uma blockchain de Prova de Trabalho (**PoW**) para criar novos blocos, ou minerar novos tokens. Em outras palavras, é a taxa de hash de uma blockchain.

A análise on-chain também inclui observar os movimentos da blockchain e dos usuários para obter informações, insights e indicadores sobre o preço de um criptoativo. Por exemplo, o **BTC**: Balanced Price, fornecido pela Glassnode, “representa a diferença entre o preço realizado e o preço transferido"do **BTC**.

O indicador fornece o valor nominal do btc e serve como uma guia para saber se o ativo está próximo ou não do seu “valor justo". A dominância do **BTC**, que calcula a proporção total de **BTC** em relação ao mercado de criptoativos, é outro indicador útil.

A métrica pode ser encontrada dividindo o valor da capitalização do **BTC** pela capitalização total das criptomoedas mais valiosas e multiplicando por 100. Um estudo recente realizado pelo MIT Sloan revelou que a realidade da rede **BTC** difere do modelo idealizado e descentralizado que os entusiastas de criptomoedas costumam apresentar. O estudo mostrou que grandes jogadores concentrados ainda dominam a rede e que an estrutura dos principais participantes é diferente do que se pensava.

Em resumo, a análise das métricas da blockchain do **BTC** é uma ferramenta útil para entender o comportamento da rede e dos usuários, bem como para avaliar o valor do **BTC** e outras criptomoedas. Para investidores e entusiastas de criptomoedas, as métricas de blockchain e an análise de blockchain de podem fornecer informações úteis. Nas próximas seções serão descritos os termos técnicos sobre blockchain.

2 O que é análise on-chain?

A análise on-chain é um método para examinar dados e extrair *insights* sobre as dados da blockchain, que é a tecnologia que sustenta o **BTC**. Em outras palavras, a blockchain é a livro contábil público onde as transações são registradas em uma database imutável.

[1] A interface de programação de aplicações, ou API, é a sigla em inglês para interface de programação de aplicações. As interfaces de programação de aplicativos (APIs) são uma coleção de ferramentas, protocolos e definições que são usadas para criar aplicações de software.

Utilizando métricas on-chain, esta base de dados é utilizada para avaliar o sentimento do mercado de criptomoedas.

A alteração da informação após a inclusão de um bloco na blockchain é extremamente difícil, se não impossível. Além disso, os dados da blockchain são armazenados de forma distribuída entre os participantes da rede, em vez de em um único local. Isso o distingue de uma database convencional. A explosão de novos tipos de negócios e serviços financeiros que antes não eram possíveis foi desencadeada por esse conceito fundamental de permitir a transferência e armazenamento de transactions de um local para outro.

As métricas on-chain que são construídas a partir da dados da blockchain, oferecem uma visão abrangente da rede do **BTC**. As principais métricas on-chain são citadas abaixo:

- As entradas e saídas de **BTC** das exchanges[2],
- Carteiras ativas de **BTC**,
- Balanço de **BTC** nas carteiras das Baleias,
- A dificuldade para minerar um bloco,
- Valor da recompensa para os mineradores em 24 horas,
- A oferta de **BTC** pode ser dividida em duas categorias principais: líquida e ilíquida.

Os mais populares provedores de dados on-chain, como o Glassnode[3] e Coin Metrics[4], oferecem muitas outras métricas. O objetivo principal da análise on-chain é examinar os dados são como um termômetro da rede **BTC** e do mercado, para determinar as tendências de preços do **BTC** atual e futuro usando métricas.

2.1 Os fundamentos da Blockchain

Para entender como funciona a tecnologia blockchain, você deve aprender as bases. Estas são as principais noções:

1. **Blocos**: Uma blockchain é uma estrutura de dados composta por cadeia de blocos. Cada bloco é composto por um conjunto de informações ou transações. Uma cadeia contínua é criada quando os blocos são conectados de forma cronológica.

[2] O mercado de criptomoedas é um espaço onde as pessoas podem comprar e vender diferentes tipos de moedas digitais, como Bitcoin, Ethereum e muitas outras. O termo "exchange" refere-se a uma plataforma online que permite que os indivíduos negociem essas criptomoedas entre si.

[3] https://glassnode.com/

[4] https://coinmetrics.io/

2. **Transações**: As transações são ações ou eventos que estão registrados na blockchain. Por exemplo, transferir bitcoins de um indivíduo para outro pode ser uma transação em uma blockchain de criptomoeda.

3. **Criptografia**: técnicas de criptografia são usadas na blockchain para garantir a segurança dos dados. Os algoritmos criptográficos protegem as transações e as informações em um bloco, tornando-as extremamente difíceis de alterar.

4. **Rede descentralizada**: A blockchain é distribuída em uma rede de computadores, também conhecidos como "nós", que são envolvidos na validação e armazenamento dos blocos. A rede não tem uma autoridade central; em vez disso, a comunidade local o administra.

5. **Consenso**: O processo pelo qual os nós da rede concordam sobre a validade das transações e como elas devem ser adicionadas à blockchain é conhecido como consenso. Os algoritmos de consenso Prova de trabalho (PoW) e 'Proof of Stake' (PoS) são usados em várias blockchains.

6. **Imutabilidade**: Uma transação é praticamente imutável quando é registrada em um bloco e adicionada à blockchain. Isso indica que alterar ou apagar uma transação após sua inclusão na blockchain é extremamente difícil ou impossível.

7. **Contratos inteligentes**: Algumas blockchains, como an Ethereum, permitem a criação de contratos inteligentes. Esses programas são executáveis por computador e têm a capacidade de automatizar a execução de contratos e acordos, eliminando a necessidade de intermediários.

8. **Chave pública e privada**: Duas chaves são usadas nas carteiras de criptomoeda: uma para receber fundos e outra para autorizar transações. Como permite que o proprietário use o dinheiro associado à chave pública, a chave privada deve ser mantida em segredo.

9. **Mineração (em PoW)**: Os mineradores usam poder computacional em blockchains PoW, como o Bitcoin, para resolver problemas matemáticos difíceis e adicionar novos blocos à blockchain. Eles recebem criptomoedas como recompensa por seu trabalho.

10. **Armazenamento distribuído**: Uma cópia completa da blockchain é armazenada em cada nó da rede blockchain. Isso aumenta a redundância e a segurança da informação.

Essas são as bases da tecnologia blockchain. Ela inclui aplicativos que vão além das criptomoedas, como contratos inteligentes e muito mais, oferecendo uma maneira transparente, segura e descentralizada de registrar transações e informações. A blockchain é a tecnologia fundamental por trás da criptomoeda **BTC**.

2.2 Bitcoin: Um Sistema de Dinheiro Eletrônico

Em 2008, um indivíduo ou grupo com o pseudônimo Satoshi Nakamoto sugeriu um sistema de pagamentos decentralizado para pessoas com outras pessoas. O principal obstáculo para digital payments é evitar que os mesmos bens sejam gastos dois vezes. De acordo com o bitcoin 'white paper', uma nova abordagem para validar transações por meio de criptografia resolve o problema conhecido como 'gasto duplo'. Esses e outros avanços para a tecnologia de um livro contábil distribuído constitui a base para ativos digitais.

2.3 História do Bitcoin e a importância de Satoshi Nakamoto

O artigo "Bitcoin: A Peer-to-Peer Electronic Cash System" foi o primeiro whitepaper que apresentou o Bitcoin. Foi publicado em outubro de 2008. Satoshi Nakamoto escreveu um whitepaper que apresentava uma ideia revolucionária de uma moeda digital que funcionaria em uma rede descentralizada, eliminando a necessidade de intermediários financeiros como bancos.

2.4 Blockchain: O Livro-Razão Público do Bitcoin

O fundamento sobre o qual o Bitcoin e muitas outras criptomoedas são construídas é o blockchain, que significa "cadeia de blocos" em português. Ele funciona como um registro público e descentralizado de todas as transações que ocorrem em uma rede de criptomoeda. O papel do blockchain no Bitcoin é essencial para garantir a segurança, transparência e integridade da rede.

2.4.1 Arquitetura da Blockchain

O blockchain é chamado de "cadeia de blocos" porque é composto por um conjunto de blocos que estão conectados de forma cronológica. Cada bloco contém um conjunto de transações que os mineradores da rede validaram. Aproximadamente a cada dez minutos, essas transações são organizadas em blocos.

Principais componentes de um bloco:

1. **O cabeçalho do bloco**: Contém informações importantes como o número do bloco, um registro da data e hora, um hash que identifica o bloco anterior (exceto no primeiro bloco, conhecido como "bloco gênesis") e um hash que representa o conteúdo do bloco atual.

2. **Transações**: Um conjunto de transações que detalham como transferir bitcoins de um endereço para outro é exibido em cada bloco. Para garantir a segurança e an autenticidade dessas transações, elas são criptografadas e assinadas digitalmente.

O blockchain do Bitcoin funciona em uma rede mundial de computadores descentralizados que trabalham em conjunto para validar e registrar essas transações. A "mineração" é o processo de validar e adicionar um novo bloco à cadeia.

Mineração e Consenso:

- Mineradores de Bitcoin lutam para resolver quebra-cabeças matemáticos complicados conhecidos como "prova de trabalho". O direito de adicionar um novo bloco ao blockchain pertence ao minerador que é o primeiro a resolver o quebra-cabeça.

- Os outros nós da rede verificam e aceitam as transações em um bloco a cada vez que é adicionado. Isso os leva a concordar sobre o estado atual do blockchain.

2.4.2 Segurança e Integridade

O blockchain do **BTC** é altamente seguro e resistente a manipulações devido a várias características:

- **Criptografia**: As transações no blockchain são protegidas por algoritmos criptográficos robustos.

- **Descentralização**: A rede é distribuída globalmente, tornando difícil para qualquer entidade controlar a maioria dos nós.

- **Imutabilidade**: Uma vez que um bloco é adicionado ao blockchain, é extremamente difícil (quase impossível) alterá-lo sem o consenso da maioria da rede.

2.4.3 Trilema das Blockchains

O "trilema das blockchains" no contexto do Bitcoin (**BTC**) refere-se aos três desafios fundamentais que a rede Bitcoin enfrenta ao tentar equilibrar três características principais:

- **Segurança**, (Segurity)
- **Descentralização**, (Decentralization)
- **Escalabilidade**. (Scalability)

- **Segurança**: A segurança do **BTC** deve ser priorizada. Isso significa que todos os dados e transações que estão no blockchain do Bitcoin devem ser inalteráveis e indetectáveis. As informações no blockchain não podem ser comprometidas por meio da criptografia e do protocolo de consenso à prova de trabalho.
- **Descentralização**: A descentralização é um pilar do **BTC**. Isso significa que, em vez de ser controlado por uma única entidade ou grupo, a rede deve ser operada e mantida por uma ampla rede de nós descentralizados. Isso fortalece a resistência à censura. Além disso, evita um único ponto de falha.
- **Escalabilidade**: A capacidade do **BTC** de lidar com uma quantidade significativa de transações sem comprometer sua descentralização e segurança é chamada de escalabilidade. Isso é essencial para atender à crescente demanda por transações e garantir que o Bitcoin seja uma moeda viável em larga escala.

Esses desafios são frequentemente descritos como um "trilema" porque é difícil atender completamente a todos eles simultaneamente na rede **BTC**. Aqui estão os componentes do trilema específicos para o **BTC**.

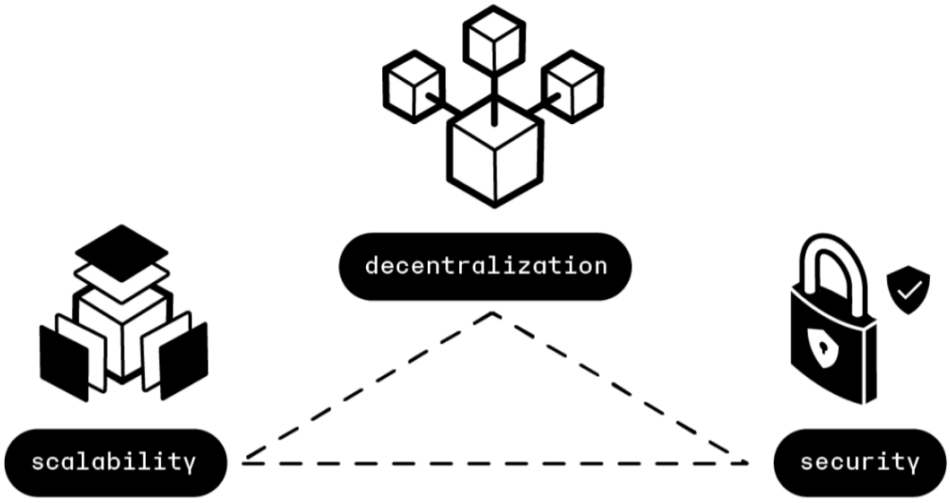

Figura 1: Trillema das Blockchains. Figura retirada do site What is Blockchain Trillema.

O problema com o trilema do **BTC** é que muitas vezes há um compromisso nos outros dois ao tentar melhorar um. Por exemplo, aumentar a escalabilidade pode exigir uma implementação de soluções de segunda camada, como a Lightning Network, que têm o potencial de impactar a descentralização. De forma semelhante, o foco na segurança máxima pode afetar a escalabilidade.

A evolução e o crescimento do **BTC** envolveram a busca de soluções para o trilema. Para equilibrar melhor os três fatores, podem ser incluídos atualizações de protocolo, otimizações de software, ajustes nas configurações e soluções de segunda camada. Manter o **BTC** seguro, descentralizado e escalável é um objetivo que os desenvolvedores e a comunidade estão continuamente trabalhando para resolver. É fundamental entender que o trilema é uma questão complicada e flutuante no desenvolvimento do **BTC**, e encontrar a maneira de equilibrar adequadamente esses três aspectos é fundamental para seu sucesso contínuo.

Referências

1. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review* (2008).