MarteXcoin

WHITEPAPER V 1.0

SUMÁRIO

1.	MARTEXCOIN	4
2.	REDE MASTERNODE	6
2.1	PROGRAMA DE RECOMPENSA DA MASTERNODE - CUSTOS E PAGAMENTOS	6
2.2	DETERMINAÇÃO DE ORDENAÇÃO	7
2.3	QUÓRUNS INCONFESSÁVEIS	7
2.4	FUNÇÕES E PROVA DE SERVIÇO	8
2.5	PROTOCOLO DO MASTERNODE	9
2.6	PROPAGAÇÃO DA LISTA DOS MASTERNODES	10
2.7	PAGAMENTOS VIA MINERAÇÃO E FISCALIZAÇÃO	10
3.	ANONSEND	11
4.	TRANSAÇÕES INSTANTÂNEAS VIA FASTTX	12
5.	PROVA DE PARTICIPAÇÃO (PROOF OF STAKE)	13
5.1	MELHORIAS ADICIONAIS	14
5.2	VANTAGENS DO X13	14
6.	BLOCOS ADAPTÁVEIS	15
7.	MENSAGENS CRIPTOGRAFADAS	16
8.	DETALHES TÉCNICOS	16
9.	CONCLUSÃO	17
10.	REFERÊNCIAS	17

APRESENTAÇÃO

MarteXcoin é uma moeda criptografada baseada no Bitcoin, resultado do trabalho de Satoshi Nakamoto, porém, com várias melhorias. Ela apresenta uma rede de dois níveis, conhecida como rede Masternode. Além disso, estão incluídos outros aprimoramentos, como o AnonSend, para aumentar a fungibilidade e o FastTX, que permite a confirmação instantânea de transações sem uma autoridade centralizada.

1. MARTEXCOIN

O sistema financeiro atual, que apresenta vários pontos e aspectos negativos é, em sua grande maioria, controlado pelo governo, o qual sempre salva os bancos da falência. Um fato que ficou claro às pessoas dos Estados Unidos, onde os bancos enganam seus clientes e no final, o próprio governo livrou eles da falência, afirmando que não podiam permitir a falência dessas empresas, pois, causaria um caos econômico avassalador. O que acabou resultando no seguinte: os chamados “contribuintes” (vulgos pagadores de impostos), pagaram a sobrevivência dos bancos por meio de seus impostos.

Filmes que explicam muito bem como isso aconteceu e sua consequência as: The Big Short (2015), Up In The Air (2009), Inside Job (2010).

Essas são falácias usadas por diversos governos para salvar corporações, empresas, amigos do governo; enfim, todos aqueles que o livre-mercado não deseja ou não se adequam às tendências do mercado. Essa mesma falácia aconteceu no Brasil; as empresas amigas do governo foram salvas, o maior exemplo são as empresas de Eike Batista.

Outro ponto negativo do mundo financeiro atual é o simples fato de ele escolher quais pessoas podem participar dele. Não é todo mundo que pode criar uma conta bancária. Outra desvantagem é, os bancos não honram com o

contrato que fazem com o usuário; os bancos são super protegidos pelo Estado (reveja a novela que foi para realizar o fechamento do banco Pan Americano).

Sabendo-se de tudo isso o Bitcoin foi criado. O Bitcoin é uma criptomoeda que surgiu como meio de troca popular. Ela é considerada a primeira moeda digital a sobreviver e ser largamente adota, e tem atraído a cada dia um número substancial de usuários. Desde a sua criação, no ano de 2009, o Bitcoin tem crescido rapidamente na adoção *mainstream* e no uso por comerciantes. Porém, um dos principais problemas na aceitação do Bitcoin é o tempo necessário para confirmar a validação da transação, por esse motivo várias organizações têm criado alternativas de pagamento, através de métodos que permitem aos fornecedores realizarem transações de confirmação zero. Ainda assim, essas soluções utilizam uma contraparte (*escrow*) confiável, que mede a transação fora do protocolo.

O Bitcoin apresenta transações em pseudônimo por meio de um livro público, que possui uma relação de um para um entre remetente e destinatário. Isso fornece um registro permanente de todas as transações que já aconteceram na rede. O Bitcoin é conhecido nos círculos acadêmicos por fornecer um baixo nível de privacidade. Embora com tal limitação muitas pessoas ainda confiam sua história financeira à *blockchain.*

A MarteXcoin surgiu com base no Bitcoin. Ela é uma moeda criptografada, cujo foco está na privacidade, com base no trabalho de Satoshi Nakamoto. Assim, o presente *whitepaper* propõe uma série de melhorias no Bitcoin, resultando em uma criptografia descentralizada e anônima, com transações instantâneas a prova de adulteração e uma rede P2P secundária de incentivos que fornece serviços para a rede MarteXcoin.

A moeda, cuja sigla é MXT, foi criada pelo brasileiro Marciano Valverde e é conhecida como uma das mais antigas e estabelecidas criptomoedas brasileiras. A mesma foi lançada no ano de 2014, e segue em dia com os passos estabelecidos pelo seu *wordmap.*

Ela é uma moeda completa: simples, rápida e segura que busca acompanhar as reais necessidades de um mundo que é cada dia mais digital e conectado. Durante o primeiro semestre de 2018 a moeda foi patrocinadora

oficial do Clube Atlético Bragantino de futebol, um time tradicional do interior paulista.

Atualmente a moeda conta com as seguintes tecnologias, as quais serão abordadas posteriormente de uma forma mais aprofundada:

- A*nonsend* - Possibilita o envio anônimo de **MXT**.
- *FastTX* - Transações instantâneas.
- *Adaptive Block Size (ABS)* - A rede se adapta ao número de transações correntes, podendo assim lidar confortavelmente com uma grade quantidade de tráfego simultâneo.
- *Velocity* - Parâmetro que faz a conferência e validação do tempo padrão entre os blocos.
- *Masternode* - Uma carteira comum com saldo de 5000 **MXT** e devidamente configurada. Seu papel é o de viabilizar os recursos de envio (*Anonsend* e *FastTX*). Requer atividade 24h.
- *Proof of Work (PoW)* - Prova de Trabalho, consenso responsável por processar novos blocos na rede, onde quem executa o *software* para essa função é chamado de “minerador”.
- *Proof of Stake (PoS)* - Prova de Participação, o usuário que mantenha saldo superior à 5 **MXT** e carteira aberta em seu computador passa a receber passivamente de acordo com seu saldo.

2. REDE MASTERNODE

Nós completos são servidores em execução em uma rede P2P, os quais permitem que os usuários os usem para receber atualizações sobre os eventos na rede. Esses *nós* exigem quantidades significativas de tráfego dentre outros recursos que carregam custos substanciais. Como resultado, na rede Bitcoin, uma diminuição constante na quantidade desses *nós* foi observada por algum tempo e, como resultado, a propagação de blocos foi superior a 40 segundos.

Esses *nós* são muito importantes para o bom funcionamento da rede. Os mesmos fornecem aos clientes a capacidade de sincronizar e propagar rapidamente mensagens por toda a rede. Propomos adicionar uma rede secundária, conhecida como a rede MarteXcoin Masternode. Onde os *nós* terão alta disponibilidade e fornecerão um nível de serviço necessário para a rede, a fim de participar do Programa de Recompensa da Masternode.

Para investidores, tanto os que possuem pouco conhecimento em programação a até os mais experientes, existe a *MarteXnodes*, uma plataforma que viabiliza investimentos em *masternodes* compartilhados, para quem não possui a quantia total requisitada ou para quem busca diversificar suas aplicações, suporte direto via *Telegram* em português e inglês.

2.1 PROGRAMA DE RECOMPENSA DA MASTERNODE - CUSTOS E PAGAMENTOS

Grande parte da razão para a diminuição de *nós* completos na rede Bitcoin, é a falta de incentivos para executa-los. Com o tempo, o custo de execução de um *nó* completo aumenta na medida que a rede é mais utilizada, o que cria maior largura de banda e necessita de um investimento maior do operador. À medida que o custo aumenta, as operadoras consolidam seus serviços para serem mais baratos de rodar ou executar um cliente leve, o que não ajuda a rede.

Masternodes são *nós* completos, assim como na rede Bitcoin, com exceção de que eles devem fornecer um nível de serviço para a rede e ter um vínculo de garantia para participar da mesma. A garantia nunca é perdida e é segura enquanto o Masternode está operando. Isso permite que os investidores prestem um serviço à rede, ganhem juros sobre seus investimentos e reduzam a volatilidade da moeda.

Para executar um Masternode, o *nó* deve armazenar 5.000(MXT). Quando ativos, os mesmos fornecem serviços à clientes na rede e, em troca, são pagos na forma de um dividendo. Esse fator permite que os usuários paguem pelos serviços e obtenham um retorno sobre o investimento. Masternodes são pagos a partir do mesmo bloco, 50% de prêmios dos blocos PoS(Proof Of Stake) e PoW(Proof Of Work) é dedicado a este programa.

Devido ao fato de que o programa de recompensas dos Masternodes é uma porcentagem fixa e os *nós* da rede da Masternode são flutuantes, as

recompensas esperadas do Masternode variam de acordo com a contagem total atual de Masternodes ativos.

O custo associado à execução de um Masternode cria um limite rígido e flexível de *nós* ativos na rede. Atualmente com 2,935 milhões de MXT em circulação, apenas 587 *nós* poderiam estar rodando na rede. O limite flexível é imposto pelo preço que custa para adquirir um *nó*, e pela liquidez limitada nas trocas devido ao uso da MarteXcoin como uma moeda e não apenas como um investimento.

2.2 DETERMINAÇÃO DE ORDENAÇÃO

Um algoritmo determinístico especial é usado para criar uma ordenação pseudo aleatória dos Masternodes. Usando o hash da prova de trabalho (PoW) para cada bloco, a segurança desta funcionalidade será fornecida pela rede de mineração.

2.3 QUÓRUNS INCONFESSÁVEIS

Atualmente, a rede da MarteXcoin tem 50 Masternodes ativos. Ao exigir a garantia de 5,000MXT para se tornar um Masternode, criamos um sistema no qual ninguém pode controlar toda a rede da Masternodes. Por exemplo, se alguém quiser controlar 50% da rede, deverá comprar 250.000 de MXT no mercado aberto. Isso aumentaria substancialmente o preço e se tornaria impossível adquirir o MXT necessário.

Com a adição da rede Masternode e os requisitos de garantia, podemos usar essa rede secundária para realizar tarefas altamente confidenciais de uma maneira infalível, onde nenhuma entidade única pode controlar o resultado. Selecionando N pseudo aleatórios Masternodes do total da *pool* para executar a mesma tarefa, esses *nós* podem atuar como um oráculo, sem que toda a rede faça a tarefa.

Por exemplo, a implementação de um *quorum* sem confiança (ver AnonSend), que usa quóruns para aprovar transações e bloquear as

entradas ou a implementação de prova de serviço.

Outro exemplo de uso para quóruns confiáveis pode incluir a utilização da rede da Masternode como um oráculo descentralizado para os mercados financeiros, tornando possível a obtenção de contratos descentralizados seguros. Como por exemplo, se a Apple Stock (AAPL) for superior a $300 em 31 de dezembro de 2016, pague a chave pública A, caso contrário, pague a chave pública B.

2.4 FUNÇÕES E PROVA DE SERVIÇO

A rede Masternode pode fornecer um grande número de serviços extras para a rede. Como prova de conceito, nossa primeira implementação incluiu o AnonSend e o FastTX. Ao utilizar o que chamamos de prova de serviço, podemos exigir que esses *nós* estejam online, respondendo e até mesmo na altura correta do bloco.

Os agentes nocivos também podem executar o Masternodes, porém, não fornecem nenhum serviço de qualidade exigido pelo restante da rede. Para reduzir a possibilidade de as pessoas usarem o sistema a seu favor, os nós devem fazer ping no restante da rede para garantir que permaneçam ativos. Este trabalho é feito pela rede Masternode, selecionando 2 quóruns por bloco. O quórum A verifica o serviço do Quórum B em cada bloco. O quorum A é o nó mais próximo do hash do bloco atual, enquanto o quorum B é o nó mais distante do referido hash.

Masternode A (1) verifica o Masternode B (rank 5123)
O Masternode A (2) verifica o Masternode B (rank 5122) O
Masternode A (3) verifica o Masternode B (rank 5121)

Todo o trabalho feito para verificar a rede para provar que os nós estão ativos é feito pela própria rede da Masternode. Aproximadamente 1% da rede será verificada em cada bloco. Isso resulta em toda a rede sendo verificada cerca de seis vezes por dia. Para manter esse sistema seguro e

confiável, selecionamos os nós aleatoriamente por meio do sistema Quorum, e também exigimos um mínimo de seis violações para desativar um nó.

2.5 PROTOCOLO DO MASTERNODE

Os Masternodes são propagados pela rede usando uma série de extensões de protocolo, incluindo uma mensagem de anúncio da Masternode e uma mensagem de ping da Masternode. Essas duas mensagens são tudo o que é necessário para tornar um nó ativo na rede, além dessas existem outras mensagens para executar uma solicitação de prova de serviço, AnonSend e FastTX.

Os Masternodes são originalmente formados enviando 5.000MXT para um endereço específico em uma carteira que “ativará” o nó, tornando-o capaz de ser propagado pela rede. Uma chave privada secundária é criada e usada para assinar todas as outras mensagens. A última chave permite que a carteira seja completamente bloqueada quando executada em modo autônomo.

Um modo frio é possível utilizando a chave privada secundária em duas máquinas separadas. O principal cliente "quente" assina a entrada 5.000MXT, incluindo a chave privada de assinatura secundária na mensagem. Logo após o cliente “frio” vê uma mensagem incluindo sua chave secundária e ativa como um Masternode. Isso permite que o cliente "quente" seja desativado (cliente desligado) e não deixa a possibilidade de um invasor obter acesso ao 5.000MXT, obtendo acesso ao Masternode após a ativação.

Ao iniciar, um Masternode envia uma mensagem “Masternode Announce” para a rede, contendo:

Mensagem: (Entrada 5K MXT, Endereço IP Acessível, Assinatura, Hora da Assinatura, Chave Pública do 5K MXT, Chave Pública Secundária, Chave Pública de Doação, Porcentagem de Doação)

A cada 15 minutos, uma mensagem de ping é enviada, provando que o nó ainda está ativo.

Mensagem: (5K MXT Input, Signature (usando chave secundária), Signature Time, Stop)

Depois que um tempo de vida tiver expirado, a rede removerá um nó inativo da rede, fazendo com que o nó não seja usado pelos clientes nem seja pago. Os nós também podem fazer um ping a rede constantemente, mas se eles não tiverem suas portas abertas, eles eventualmente serão sinalizados como inativos e não serão pagos.

2.6 PROPAGAÇÃO DA LISTA DOS MASTERNODES

Novos clientes que entram na rede do MarteXcoin devem estar cientes dos Masternodes atualmente ativos na rede para poder utilizar seus serviços. Assim que eles se conectam à rede da MarteXcoin, um comando é enviado para seus pares solicitando a lista conhecida de Masternodes. Um objeto de cache é usado pelos clientes para registrar os Masternodes e seu status atual, portanto, quando os clientes forem reiniciados, eles simplesmente carregarão esse arquivo em vez de solicitar a lista completa de Masternodes.

2.7 PAGAMENTOS VIA MINERAÇÃO E FISCALIZAÇÃO

Para garantir que cada Masternode seja pago, com uma parte justa da recompensa em blocos, a rede deve impor que os blocos paguem o Masternode correto. Se um minerador não estiver em conformidade, seus blocos devem ser rejeitados pela rede, caso contrário, a trapaça será incentivada.

Propomos uma estratégia em que a Masternodes forma quóruns, seleciona um Masternode vencedor e transmite sua mensagem. Depois que N mensagens forem transmitidas para selecionar o mesmo destinatário, um consenso será formado e esse bloco em questão será obrigado a pagar esse

Masternode.

Ao minerar na rede, o software pool (sites que mesclam os esforços de mineradores individuais) usam a interface da API RPC para obter informações sobre como fazer um bloqueio. Para pagar os Masternodes, essa interface deve ser estendida adicionando um beneficiário secundário ao GetBlockTemplate. Os pools então propagam seus blocos minerados com sucesso, com um pagamento dividido entre eles e um Masternode.

3. ANONSEND

Acreditamos que é importante ter uma implementação padrão com confiança para melhorar a privacidade de seus usuários no cliente de referência que fornece um alto grau de privacidade. Outros clientes, como o Electrum, o Android e o iPhone, também terão a mesma camada de anonimato implementada diretamente e utilizarão as extensões do protocolo. Isso permite aos usuários uma experiência comum de anonimato de fundos usando um sistema bem compreendido.

O AnonSend é uma versão aprimorada e estendida do CoinJoin. Além do conceito central da CoinJoin, empregamos uma série de melhorias, como descentralização, forte anonimato usando uma abordagem de encadeamento, denominações e mixagem passiva em tempo útil.

O maior desafio ao melhorar a privacidade e a fungibilidade de uma moeda criptografada é fazê-lo de uma maneira que não obscureça todo o blockchain. Em moedas de criptografia baseadas em Bitcoin, pode-se dizer quais saídas são gastas e quais não são, comumente chamadas de UTXO, que significa saída de transação não gasta. Isso resulta em um registro público que permite que qualquer usuário atue como garantidor da integridade das transações. O protocolo Bitcoin é projetado para funcionar sem a participação de contrapartes confiáveis, na sua ausência, é fundamental que as capacidades de auditoria permaneçam prontamente acessíveis aos usuários através do blockchain público. Nosso objetivo é

melhorar a privacidade e a fungibilidade sem perder esses elementos chaves que acreditamos ser atributos de uma moeda de sucesso.

Ao ter um serviço de mistura descentralizado dentro da moeda, ganhamos a capacidade de manter a moeda em si perfeitamente fungível. A fungibilidade é um atributo do dinheiro, que determina que todas as unidades de uma moeda permaneçam iguais. Quando você recebe pagamentos em uma moeda, ele não deve vir com nenhum histórico dos usuários anteriores da moeda ou os usuários devem ter uma maneira fácil de se desassociar desse histórico, mantendo assim todas as moedas iguais. Ao mesmo tempo, qualquer usuário deve ser capaz de atuar como auditor para garantir a integridade financeira do livro público sem comprometer a privacidade de outras pessoas.

Para melhorar a fungibilidade e manter a integridade do blockchain público, propomos o uso de uma estratégia de mistura (mixing) confiável e descentralizada. Para ser eficaz em manter a moeda fungível, este serviço é diretamente embutido na moeda, fácil de usar e seguro para o usuário médio.

4. TRANSAÇÕES INSTANTÂNEAS VIA FASTTX

Ao utilizar os quóruns da Masternode, os usuários podem enviar e receber transações irreversíveis e instantâneas. Uma vez que um quorum tenha sido formado, as entradas da transação são bloqueadas para somente serem gastas em uma transação específica, um bloqueio de transação leva cerca de dois a cinco segundos para ser definido atualmente na rede. Se o consenso for atingido em um bloqueio pela rede da Masternode, todas as transações conflitantes ou blocos conflitantes serão rejeitados a partir de então, a menos que eles correspondam à identificação exata da transação do bloqueio em vigor.

Isso permitirá que os fornecedores usem dispositivos móveis no lugar dos sistemas tradicionais de PDV para o comércio no mundo real e que os usuários resolvam rapidamente transações não comerciais face a face, como acontece com o dinheiro tradicional. Isso é feito sem uma autoridade central.

5. PROVA DE PARTICIPAÇÃO (PROOF OF STAKE)

MarteXcoin procura resolver um grande problema que ocorre na mineração do Bitcoin: Minerar Bitcoins requer um grande poder computacional e uma grande quantidade de energia elétrica, e os mineiros precisam de hardware de processamento avançado para contribuir. MarteXcoin usa a tecnologia blockchain e os mesmos mecanismos de mineração que o Bitcoin, mas também permite que os proprietários de MarteXcoin gerem mais MarteXcoins através de um processo eficiente de energia, uma cunhagem econômica (do inglês *minting*) que chamarei de *participação* neste whitepaper. Depois de períodos de tempo designados, os usuários podem empregar um algoritmo de prova de participação, que mantém o controle de quanto tempo você tem a posse sobre uma determinada MarteXcoin, para acumular mais MarteXcoin. Basicamente, a participação permite ganhar uma recompensa em MarteXcoin a fim de manter a rede robusta - 50% ao ano para todos os usuários. Funções de *participação* para mineração protegem a rede e tem como custo uma fração de energia - a participação pode ser feito em qualquer computador e sem hardware avançado. Este modelo de "prova-de-participação" distingue a MarteXcoin de outras moedas digitais, mas como ele ainda é jovem, mineração continua sendo a fonte predominante de suas moedas - benefícios significativos de participação só serão obtidos depois que a quantidade de moedas suficientes tenham sido adquiridas ao longo do tempo.

5.1 MELHORIAS ADICIONAIS

Algoritmo de hash x13.

x13 é um algoritmo de hash amplamente utilizado, que usa uma abordagem diferente, conhecida como encadeamento de algoritmos. x13 consiste em 13 algoritmos, cada hash é calculado e então submetido ao

próximo algoritmo na cadeia. Ao utilizar vários algoritmos, a probabilidade de que um ASIC seja criado para a moeda é mínima até uma parte posterior do seu ciclo de vida.

No ciclo de vida do Bitcoin, a mineração começou com amadores que usavam Unidades de Processamento Central (CPUs) para extrair a moeda, logo depois que o software para Graphics Processing Units (GPUs) foi criado, as CPUs foram rapidamente substituídas. Anos após o ciclo das GPUs, foram criados ASICs ou Circuitos Integrados Específicos da Aplicação, que rapidamente substituíram as GPUs.

Devido à complexidade e ao tamanho do molde necessários para criar um ASIC para mineração x13, esperamos que ele demore consideravelmente mais do que no Bitcoin, permitindo que os amadores participem da mineração por um período mais longo. Acreditamos que isso é altamente importante para uma boa distribuição e crescimento de uma criptomoeda.

Outro benefício da abordagem de hashing em encadeamento é que as CPUs de ponta oferecem um retorno médio semelhante ao das GPUs. Também se informou que GPUs rodam 30-50% com menor aquecimento, e com menos potência do que outros algoritmos.

5.2 VANTAGENS DO X13

Maior confiança e segurança para moedas.

O aumento da complexidade e sofisticação do algoritmo encadeado oferece níveis aprimorados de segurança e menos incerteza para uma moeda digital, em comparação com soluções PoW de hash único que não são protegidas contra riscos de segurança, como SPOF (Single Point Of Failure). Por exemplo, um avanço de computação possível, mas não provável, que “quebra” o hash SHA256 poderia colocar em risco toda a rede Bitcoin até que a rede passasse por um fork rígido para outro hash criptográfico.

No caso de uma descoberta de computação semelhante, uma moeda digital usando o X13 PoW continuaria a funcionar com segurança, a menos

que todos os 13 hashes fossem quebrados simultaneamente. Mesmo se alguns dos 13 hashes se provassem não confiáveis, haveria um aviso adequado para uma moeda usando o X13 para tomar medidas e substituir os hashes problemáticos por outros algoritmos hash mais confiáveis.

Dada a natureza especulativa das moedas digitais e suas incertezas inerentes como um novo campo, o algoritmo X13 pode fornecer maior confiança para seus usuários e potenciais investidores que as abordagens single-hash não podem. Soluções de hashing encadeadas, como o X13, proporcionam maior segurança e longevidade para fins de armazenamento de riqueza, diversificação de investimentos e proteção contra riscos associados a moedas com hashing único afetadas por SPOF (Single Point Of Failure - Ponto Único de Falha).

6. BLOCOS ADAPTÁVEIS

O Bitcoin tem um grande problema no quesito tamanho de bloco, pois isso trava o aumento do número de transações, pois está limitado a apenas 1MB.

Na sua criação em 2009 talvez fosse um bom tamanho, mas nos dias de hoje 1MB é muito pouco e isso causa um atraso significativo nas transações, que teoricamente teriam que levar algo em torno de 60 minutos no máximo já que cada bloco tem seu tempo médio de 10 minutos.

E ainda tem a taxa da rede (fee), que o padrão é de 0.00001BTC (mil satoshis), que em cada transação é priorizada pelo quanto que foi pago a taxa, se a taxa for a padrão provavelmente demorarão mais tempo do que alguém colocar uma taxa maior e priorizando a transação para o próximo bloco.

A MarteXcoin tem o sistema de blocos adaptáveis implementado, quanto as taxas da rede isso já não é problema na MarteXcoin, isso significa que qualquer transação independente do tamanho ou taxa paga sempre caberá no bloco corrente. Em outras palavras nunca haverá atraso em confirmações de transações, pois sempre em no máximo 3 minutos a

transação está liberada para uso (isso numa transação normal sem usar o recurso FastTX).

7. MENSAGENS CRIPTOGRAFADAS

A MarteXcoin tem um sistema de mensagens integrado na própria carteira, que é impossível de se rastrear, a mensagem não se propaga dentro do blockchain e sim numa camada específica que cria uma conexão única entre o remetente e o destinatário da mensagem. Garantindo anonimato e rapidez de ponta a ponta.

8. DETALHES TÉCNICOS

Ticker: **MXT**
Distribuição: **POW** / **POS** / *Masternodes*
Hash: Algoritmo **X13** (13 camadas de encriptação)
Emissão total: 11.600.000 (**POW** / **POS**) - *premine* de 2%
Taxa mínima de transação por bloco: 0.0001 **MXT** (pago aos mineradores)
Confirmações em carteira: 3 para transferências e 152 para novos blocos
Tempo para geração de novos blocos: 1 minuto
Recompensa do bloco **POW**: 0.066 **MXT**
Divisão do bloco **POW**: 0.05 **MXT** Miner / 0.01 **MXT MN** / 10% Fundação MarteXcoin
Recompensa do bloco **POS**: 50% anual com base no valor em carteira.
Divisão do bloco **POS**: 40% *Staking* / 50% **MN** / 10% Fundação *Martexcoin.*
Dificuldade: recalibrada a cada bloco pelo *Dark Gravity Wave*.
MN *COLLATERAL* : 5000 **MXT** (*standard*, sem algoritmo de alteração de *collateral*)
P2P *PORT* : 51315
Open souce code (Código livre)
GitHub (Desenvolvedores): 2
GitHub Stars: 26

Repositório *GitHub* : https://github.com/martexcoin/martexcoin

9. CONCLUSÃO

O presente Whitepaper apresenta vários conceitos e melhorias implementados na MarteXcoin, resultando em maior privacidade, escalabilidade e fungibilidade para o usuário médio, menor volatilidade de preços e propagação mais rápida de mensagens em toda a rede. Tudo isso é realizado utilizando um modelo de dois níveis incentivos, em vez do modelo de camada única existente em outras moedas criptográficas, como o Bitcoin. Ao utilizar este projeto de rede alternativa, torna-se possível adicionar muitos tipos de serviços, como a mistura descentralizada de moedas, transações instantâneas e oráculos descentralizados, usando quóruns dos Masternodes.

10. REFERÊNCIAS

http://en.wikipedia.org/wiki/NIST_hash_function_competition#Finalists

http://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.pdf

http://research.microsoft.com/pubs/156072/bitcoin.pdf

http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf

http://www0.cs.ucl.ac.uk/staff/s.meiklejohn/files/imc13.pdf

https://bitcoin.org/bitcoin.pdf

https://en.bitcoin.it/wiki/CoinJoin

https://en.bitcoinwiki.org/wiki/X13

https://forum.martexcoin.org/d/38-configura-o-masternode

https://gist.github.com/GeertJohan/b28da8105babf0553f21

https://github.com/martexcoin/martexcoin

https://masternodes.online/currencies/MXT

https://medium.com/@spair/a-simple-adaptive-block-size-limit-748f7cbcfb75

https://medium.com/zapchain-magazine/why-don-t-people-run-bitcoin-nodes-anymore-d4da0b45aae5

https://pt.wikipedia.org/wiki/Prova_de_participa%C3%A7%C3%A3o
https://pt.wikipedia.org/wiki/Prova_de_trabalho
https://queroficarrico.com/blog/entenda-o-caso-banco-panamericano/
https://www.criptomoedasfacil.com/entenda-o-que-e-masternode-e-quais-suas-vantagens/
https://www.cryptocoinsnews.com/3-solutions-instant-bitcoin-confirmations/