
VERGE
A moeda cripto mais confidencial
BLACKPAPER

1.0 Introdução

Bitcoin foi desenvolvido e lançado em 2009 em resposta a uma falha inerente na forma como as transações eram processadas na Internet. Em seu whitepaper Nakamoto explica que "o Comércio na Internet passou a confiar quase que exclusivamente em instituições financeiras as quais servem como terceiros confiáveis para processar pagamentos eletrônicos. Embora o sistema funcione bem o suficiente para a maioria das transações, ele ainda sofre com as fraquezas inerentes ao modelo baseado em confiança "[1]. Desde sua concepção em 2009, o Bitcoin foi rapidamente adotado nos modernos mercados atuais. O problema principal com a rápida adoção do Bitcoin é o aumento da demanda no blockchain original para lidar com grande volume de transações. Devido à ao crescimento na demanda, aumentaram os períodos de espera transacionais e isso resultou em taxas de transação mais altas nas tentativas de tentar acelerar os tempos de confirmação destas transações.

A inovação central por trás do Bitcoin é sua estrutura descentralizada. Ao contrário das moedas fiduciárias tradicionais, emitidas pelo governo, o Bitcoin não tem controle central, depósito central de informações, gerenciamento central ou ponto central de falha. No entanto, um dos desafios que o Bitcoin enfrenta é que a maioria dos e-serviços e e-negócios construídos em torno do ecossistema Bitcoin são centralizados. Devido à natureza centralizada do sistema atual, o comércio eletrônico é administrado por indivíduos em locais específicos, que utilizam sistemas informáticos vulneráveis e que são suscetíveis a complicações legais. O Verge é uma das únicas moedas verdadeiramente descentralizadas disponíveis no mercado hoje devido ao seu compromisso permanente na construção em cima dos conceitos fundamentais do Bitcoin, ao mesmo tempo em que traz uma camada totalmente nova de anonimato.

2.0 Integração Tor

Tor, derivado de uma sigla para o projeto de software "The Onion Router" ("O roteador cebola"), é um serviço de ofuscação de IP que permite a comunicação anônima através de uma rede baseada em camadas de circuitos. O Tor direciona o tráfego na internet através de uma rede mundial gratuita de overlays, formado por mais de sete mil relays, para impedir a localização e utilização de qualquer vigilância de rede ou análise de tráfego. As camadas de informações de endereço criptografadas, usadas para anonimizar pacotes de dados enviados através da rede Tor, lembram os de uma cebola, daí a origem de seu nome. Dessa forma, o caminho de um pacote de dados através da rede Tor não pode ser totalmente rastreado. O uso do Tor destina-se a proteger a privacidade dos usuários, bem como a liberdade e capacidade de comunicação confidencial, mantendo suas atividades na internet livres de serem monitoradas.

O roteamento Onion é implementado por criptografia na camada de aplicação de uma pilha de protocolo de comunicação, aninhados como as camadas de uma cebola. O Tor criptografa os dados, incluindo o próximo IP do destino do nó, várias vezes e o envia através de um circuito virtual que inclui sucessivos relays Tor selecionados aleatoriamente. Cada relay descriptografa apenas o suficiente do pacote de dados para saber sua origem e para qual relay enviar depois. O relay então insere os dados em um novo pacote e o envia novamente. O relay final descriptografa a camada mais interna de criptografia e envia os dados originais para o destino sem revelar, ou mesmo saber, o endereço IP de origem.

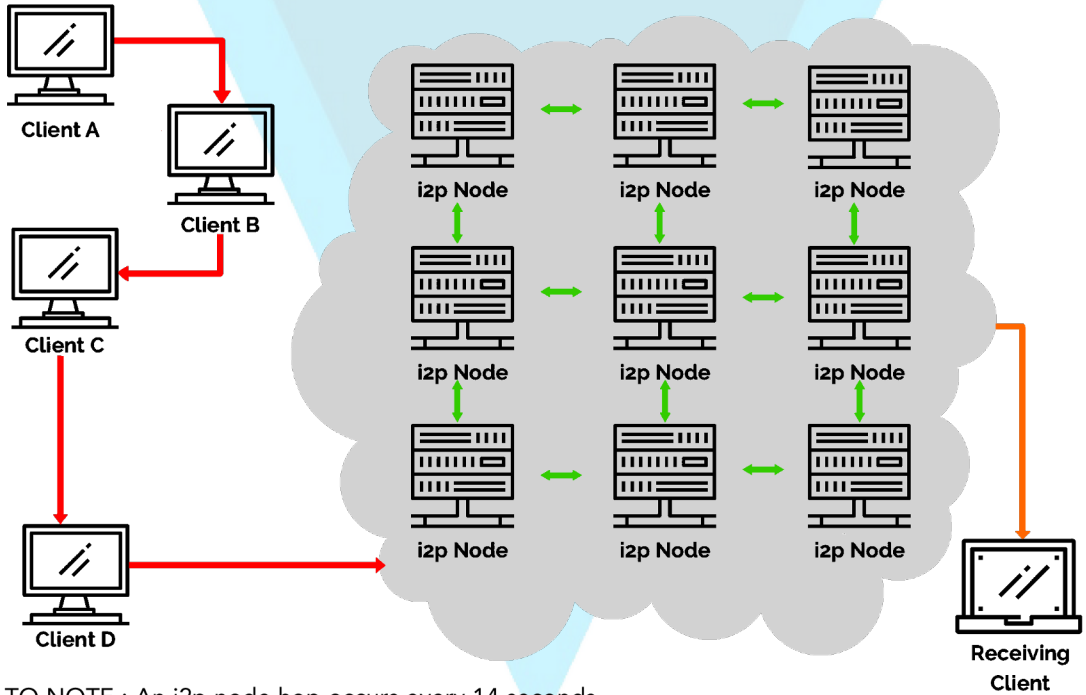
2.1 Integração Tor

Como o roteamento da comunicação está parcialmente escondido em cada salto do circuito Tor, este método elimina qualquer ponto no qual os pares de comunicação possam ser determinados por meio de vigilância de rede que depende do conhecimento de sua origem e destino.

3.0 Integração I2P

O i2P foi originalmente criado para fornecer serviços ocultos que permitem às pessoas hospedar servidores em locais desconhecidos. O i2P fornece muitos dos benefícios da rede Tor; ambos permitem o acesso anônimo ao conteúdo on-line, fazem uso de uma estrutura de roteamento de estilo P2P e operam usando criptografia em camadas. No entanto, o i2P foi concebido para ser uma "rede na internet" (ver figura 2.1), com o tráfego permanecendo contido em suas fronteiras. O i2P executa o roteamento baseado em pacotes, ao contrário do roteamento baseado em circuito da rede Tor. Esta vantagem permite ao i2P rotear dinamicamente o congestionamento e as interrupções de serviço de forma semelhante ao roteamento IP da internet, proporcionando um nível maior de confiabilidade e redundância para a própria rede.

Figure 2.1
How an i2p Transaction Occurs



TO NOTE : An i2p node hop occurs every 14 seconds.

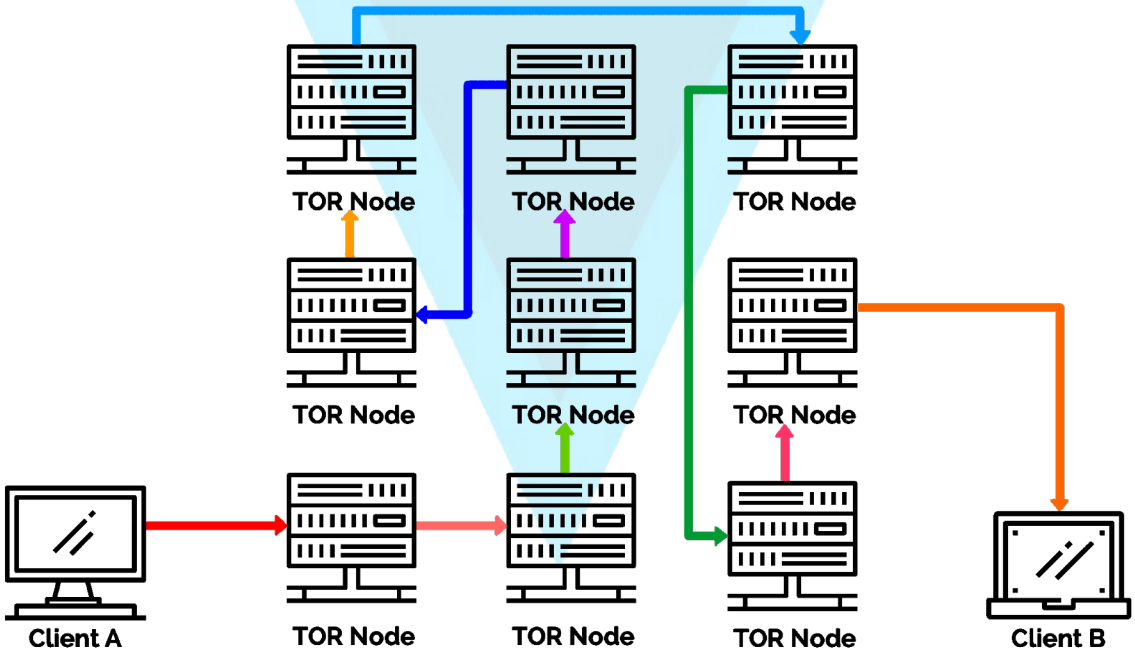
A primeira vez que um cliente quer entrar em contato com outro, eles fazem uma consulta no "banco de dados de rede" totalmente distribuído - uma customizada tabela de hash distribuída (THD) baseada no algoritmo Kademlia [2]. Isso é feito para encontrar os túneis de entrada do outro cliente de forma eficiente e, geralmente, estão incluídas informações adicionais para que não sejam necessárias mais pesquisas no banco de dados de rede.

3.1 Integração I2P

i2P é um serviço de tunelamento, utilizando ipv6, que torna anônimo todos os dados do Verge enviados pela rede. Cada aplicativo cliente possui o "roteador" do i2P construído em vários "túneis" de entrada e saída - uma seqüência de pares que passam dados em uma direção (para e do cliente, respectivamente) [2]. Desta forma, quando um cliente deseja enviar dados do Verge para outro cliente, o aplicativo passa a mensagem através de um dos seus túneis de saída visando um dos túneis de entrada do cliente, para finalmente chegar ao seu destino.

A rede i2P, ao invés de confiar em um conjunto centralizado de servidores de diretório, como o Tor, utiliza duas tabelas hash distribuídas para coordenar o estado da rede. Estas "Tabelas de Hash Distribuídas", ou THDs, são um mecanismo distribuído, e muitas vezes descentralizado, para associar valores de hash ao conteúdo. A principal vantagem das THDs é sua escalabilidade. Uma rede P2P descentralizada bem-sucedida requer uma boa escalabilidade de seus serviços para garantir que o tamanho do conteúdo ou o compartilhamento de transações possam continuar a crescer conforme necessário. Além disso, o i2P não depende de um serviço de diretório confiável para obter informações de rota. Em vez disso, as rotas de rede são formadas e atualizadas de forma constante e dinamicamente, com cada roteador avaliando outros roteadores. Por fim, o i2P estabelece dois túneis simples para que o tráfego percorra a rede de origem e destino para cada host, diferente da rede Tor, formado de um único circuito duplex (veja a figura 1.1).

Figure 1.1
How a TOR Transaction Occurs



TO NOTE: A TOR nod hop occurs every 10 minutes.

4.0 Electrum

A força do Electrum é sua velocidade e simplicidade com baixo consumo de recursos. Ela usa servidores remotos seguros que lidam com as partes mais complexas da rede Verge e também permite que os usuários recuperem suas carteiras com uma frase semente secreta. Adicionalmente, Electrum oferece uma solução de cold storage simples e fácil de utilizar permitindo aos usuários o armazenamento da totalidade, ou parte de suas moedas, de maneira off-line. Além disso, Electrum é uma das únicas carteiras à fornecer apoio nativo à rede Tor e i2P. Ao integrar Electrum com Tor e i2P é possível se manter anônimo enquanto utiliza a carteira desktop ou celular. Em ambos, o endereço IP e as informações da transação estão protegidas e não vazam para os servidores de conexão, aumentando a privacidade do usuário.

As transações padrão na rede Verge podem ser chamadas de "transações de assinatura única" [4] pois as transferências requerem apenas uma assinatura: a do proprietário da chave privada associada ao endereço Verge. Porém, Electrum também suporta transações de múltiplas assinaturas, o que exige mais de uma chave para autorizar uma transação eletrônica. Uma transação Electrum com suporte a assinatura múltipla exige as assinaturas de várias pessoas antes que as moedas possam ser transferidas. O Verge, em seguida, solicita vários endereços diferentes para fazer qualquer coisa com elas.

Aqui está um exemplo:

> "Uma carteira Electrum está em seu computador principal, a outra em seu smartphone - as moedas não podem ser gastas sem a assinatura de ambos os dispositivos. Assim, um invasor deve ter acesso a ambos os dispositivos para roubar suas moedas"

As principais características da carteira Electrum a se destacar:

a geração de chaves determinística

Se você perder sua carteira, você pode recuperá-lo a partir de sua frase semente. Você está protegido contra seus próprios erros.

Instantaneamente conectado

o cliente não necessita baixar o blockchain, ele solicita informações do blockchain de um servidor. Sem atrasos e sempre atualizado.

Transações assinadas localmente

Suas chaves privadas não são compartilhadas com o servidor. Você não precisa confiar suas moedas no servidor.

Liberdade e Privacidade

O servidor Electrum não armazena contas de usuário. Você não está vinculado a um servidor específico, e este não precisa conhecê-lo. Na verdade, os servidores Verge e i2P Electrum não recebem um endereço IP do cliente. Você também pode exportar suas chaves privadas, o que significa que VOCÊ detém seu endereço.

5.0 Suporte Multi-Algoritimo

Verge é uma criptomoeda de algoritmos múltiplos projetada para permitir que pessoas com diferentes tipos de dispositivos de mineração tenham igual acesso para ganhar moedas. É uma das únicas criptomoedas com suporte a 5 funções hash combinadas em uma única cadeia de blocos. Isso resulta em maior segurança e uma gama mais ampla de pessoas e dispositivos com possibilidade de minerar Verge, desta forma, uma distribuição igual é garantida para todos.

A oferta total de Verge é de 16,5 bilhões de moedas. O que faz Verge se destacar de outras criptomoedas são os 5 algoritmos de "proof-of-work" que funcionam em seu blockchain: Scrypt, X17, Lyra2rev2, myr-groestl e blake2s. Todos os 5 algoritmos possuem 30 segundos de block-time de destino e a dificuldade é influenciada apenas pela taxa de hash do algoritmo. Isso permite maior segurança e proteção contra ataques do tipo 51%.

6.0 Android Tor + I2P

Verge fica na vanguarda da inovação no espaço de criptografia móvel. Fomos pioneiros e desenvolvemos duas carteiras de Android totalmente inovadoras e únicas. Uma dos quais opera exclusivamente na rede Tor (The Onion Router Network) e o outro que opera exclusivamente no rede I2P (The Invisible Internet Project). As carteiras Verge Tor e I2p são construídas em torno da premissa de anonimato. As carteiras não possuem habilidade interna para se conectar ou transmitir informações do usuário na clearnet. As transações são completadas através da VPS (Verificação de Pagamento Simples), uma técnica descrita no documento de Satoshi Nakamoto que permite que a carteira verifique as transações através de prova de inclusão; um método para verificar se uma transação específica está incluída em um bloco sem necessidade de baixar o bloco inteiro (semelhante à forma como funciona uma carteira Electrum).

A VPS permite confirmações de pagamento quase instantâneas porque atua como um cliente leve que só precisa baixar os cabeçalhos dos blocos, e estes são drasticamente menores que os blocos completos. As carteiras Verge Tor e i2P também têm recursos de segurança incorporados, como um código PIN de 4 dígitos e opção de bloqueio biométrico, para uma camada adicional de segurança física. Além disso, as carteiras Verge Tor e i2P são capazes de lidar com transações de varredura de código QR P2P com verificação instantânea. Os clientes também podem importar códigos QR de carteiras de papel para extrair os saldos da cold wallet, se necessário.

7.0 Desenvolvimento Futuro: RSK

Rootstock, ou RSK, como é comumente referido, é uma cadeia lateral de dois sentidos que insere funcionalidade de contrato inteligente na rede de Verge. Ele também introduz um protocolo fora da cadeia para pagamentos quase instantâneos. RSK é uma cadeia de blocos independente que não possui seu próprio token, ao invés vez disso, depende de tokens existentes (como o Verge). A RSK pode fazer isso pegando (ou combinando) seu token inteligente com o Verge, de modo que o valor de um token RSK seja exatamente ao de um token Verge. Os usuários têm a capacidade de mover livremente seus tokens entre as duas cadeias.

Um contrato inteligente funciona ao colocar o Verge de um usuário em um tipo de reserva onde ele está trancado e usado para suportar o token RSK, conhecido como smartXVG. Pense nisso como colocar seu Verge em uma conta corrente e usar a rede RSK para gastar esse dinheiro. É importante notar que foram estabelecidos contratos simples para o Bitcoin, que permitem que os usuários criem contratos, como mutlisig, que exigem que dois ou mais usuários assinem um pagamento antes que ele possa ser liberado. Com a implementação da RSK no Verge os contratos simples e inteligentes são levados a um nível totalmente novo, com capacidades de contrato inteligentes e duradouros que vão de encontro com o oferecido pela Ethereum.

Um outro benefício adicional da RSK é a sua escalabilidade. Atualmente, a RSK atinge 400 transações de pagamento por segundo, o que representa um salto enorme em relação à nossa taxa de transação atual de cerca de 100 pagamentos por segundo. A equipe de desenvolvimento da RSK afirmou que o objetivo final é superar esse limite com metas futuras para suportar 2.000 transações por segundo utilizando uma tecnologia de segunda camada chamada Lumino. Conforme indicado no white paper LCTP, a Lumino Network é um sistema de pagamento fora da cadeia que depende de um protocolo conhecido como "Lumino Transaction Compress Protocol". O LTCP pode ser comparado à "Lightning Network", uma solução de dimensionamento originalmente projetada para Bitcoin que atualmente está sendo testada no Litecoin.

8.0 Desenvolvimento Futuro: Discord & Telegram P2P

O suporte de transações Peer-to-Peer (P2P) para Telegram e Discord está atualmente em desenvolvimento e programado para ser divulgado ao público no mês de agosto. O Telegram é um serviço gratuito de mensagens instantâneas baseado na nuvem com suporte a Android, iOS, Windows Phone, Windows NT, MacOS e Linux. O Telegram utiliza um método de criptografia simétrico chamado MTProto, desenvolvido pela Nikolai Durov e outros desenvolvedores do Telegram, e baseia-se na criptografia simétrica AES de 256 bits, criptografia RSA 2048 e troca de chaves Diffie-Hellman. O Discord é uma aplicação proprietária freeware de VoIP bastante adotada pela comunidade de criptomoedas. Assim como o Telegram, o Discord possui versões para Windows, MacOS, Android, iOS e um cliente web acessível por navegador. A implementação de recursos do Verge P2P nessas plataformas permite que os usuários enviem e recebam fundos na hora, independentemente de onde eles estão (independentemente de ter uma carteira real instalada ou não).

P2P é uma tecnologia que permite aos usuários transferir moedas através da internet ou dispositivo móvel. Para fazer isso, os consumidores utilizam um aplicativo, neste caso um bot, para designar o destinatário e a quantidade de moedas a serem transferidas. O destinatário é designado apenas pelo nome do usuário e, uma vez que a transferência foi iniciada pelo remetente, o destinatário recebe uma notificação de que recebeu um pagamento em um endereço de depósito recentemente criado. O destinatário pode então twittar ou enviar um comando simples ao bot, tal como "!sacar" e, então, é apresentado para ele um conjunto de instruções sobre como receber seus recém recebidos Verges. Este serviço não requer nenhuma informação adicional além do valor e para quem deseja enviar. Nenhuma informação de privacidade, como endereço IP, localização ou nome é mantida durante este processo. Sua identidade de antes do início da transação permanece completamente anônima.

Verge é uma das únicas criptomoedas a oferecer soluções P2P para Twitter, Reddit, IRC (Internet Relay Chat), Slack e Steam. Essas ofertas P2P permitem aos usuários transferir Verge para qualquer pessoa que estejam na mesma plataforma social.

9.0 Referências

[1] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] I2P: A scalable framework for anonymous communication - I2P. (n.d.). Retrieved from https://geti2p.net/en/docs/how/tech-intro

[3] Multisignature - Bitcoin Wiki. (n.d.). Retrieved August 8, 2017, from https://en.bitcoin.it/wiki/Multisignature

[4] Voegtlin, T. (n.d.). Welcome to the Electrum Documentation! — Electrum 2.5 documentation. Retrieved August 8, 2017, from http://docs.electrum.org/en/latest/

Additional References:

Gribble, S., Brewer, E., Hellerstein, J., & Culler, D. (2000, October 23). Scalable, Distributed Data Structures for Internet Service Construction. Retrieved from https://www.usenix.org/legacy/events/osdi2000/full_papers/gribble/gribble_html/index.html

Anonymity and the Block Chain • IHB News™. (2014, November 18). Retrieved August 08, 2017, from https://ihb.io/2014-11-17/news/anonymity-block-chain-13570

Holden, E. (2017, July 18). An Introduction to Tor vs I2P. Retrieved August 08, 2017, from https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

Distributed hash table. (n.d.). Retrieved August 08, 2017, from http://infoanarchy.org/Distributed_hash_table

Scharr, J. (2013, October 23). What Is Tor - How Does Tor Work - How to Use Tor. Retrieved August 08, 2017, from https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

Durumeric, Z., Wustrow, E., & Halderman, J. (2013). ZMap: Fast Internet-Wide Scanning and its Security Applications. Retrieved from https://zmap.io/paper.pdf

Voegtlin, T. (2015). Simple Payment Verification — Electrum 2.5 documentation. Retrieved from http://docs.electrum.org/en/latest/spv.html

SPV, Simplified Payment Verification - Bitcoin Glossary. (2017). Retrieved from https://bitcoin.org/en/glossary/simplified-payment-verification

https://atlas.torproject.org/#search/flag:authority

http://torstatus.blutmagie.de/

10.0 Contribuidores

Como um projeto open-source, consideramos muito importante agradecer aos contribuidores que nos ajudaram a chegar onde estamos hoje.

Por conta disso tudo, dizemos

Obrigado

Traduzido por

T. Sawamura

The Author

CryptoRekt

O.G Verge Development Team

Sunerok

Gfranko

CryptoRekt

Contribuidores

Equipe de marketing

@Spookykid
@CryptoRekt
@gfranko
@Crypto_K1NG
@JtheLizzard
@lucklight
@Cryptonator92
@feyziozsahin
@Slemicek
@Trilla6six6
@Dabbie USA
@Cyrus7at
@Thehunter9 Netherlands
@GGWeLost
@Jeanralphio69
@Crypth
@deheerlen
@Twomanytimes
@ScagFX
@TraderNILW

Contribuidores no GitHub

Sunerok
Gfranko
CryptoRekt
Mkinney
badbrainIRC
Grinfax
Swat69
NeosStore
Koenwoortman
Hellokarma
Kirillseva
Fuzzbawls
Buzztiaan
Spiralmann666
stshort
alcy0ne
chisustation
ShapeShifter499
Infernoman
pallas1
bearsylla
2Dai
31percent
Racoooon
ceasarpolar
enewnanwebdev
giovanni1186
labelmeagod

Informação de Contato

Twitter Telegram Slack Facebook IRC Reddit Steam Verge Discord Discussão BitCoin Estação de Rádio