ESPERS

Um projeto do time Cryptocoderz

Whitepaper

Escrito pelo time Cryptocoderz
20 de fevereiro 2018 (Version 1.0)

ESPERS

SUMÁRIO

ESPERS

RESUMO

Com o advento da tecnologia blockchain (cadeia de blocos) no começo dos anos 2000, o mundo está ansioso para acompanhar sua evolução. De uma maneira especial, o Bitcoin capturou a atenção de todos como sendo a moeda operacional dessa blockchain, levando outros projetos/comunidades a seguirem seus passos. Existe, ainda, uma grande carência por uma blockchain avançada que seja capaz de fornecer uma solução para as tarefas diárias, onde tanto o provedor do serviço como o usuário sejam beneficiados de forma garantida, segura e descentralizada que ainda não foram totalmente supridas. Mesmo aqueles que atualmente apresentam características especiais, geralmente têm uma mentalidade de "lobo solitário" que faz com que os projetos lutem entre si e se fragmentem, isso faz com que suas comunidades se tornem diluídas e o objetivo se perca.

Espers é uma blockchain híbrida (Prova de Trabalho/Prova de Participação - PoW/PoS) que foi criada para ser a solução à divisão e ao subaproveitamento atualmente atribuído à tecnologia de blockchain, tanto unificando quanto expandindo possibilidades. As características implementadas, tais como mensagens seguras, interface de cadeia cruzada, cadeias laterais modulares, websites, armazenamento de documento, para nomear algumas, estão unidas a partir de uma interface universal que permite que qualquer projeto de criptomoeda possa participar, usando moedas ESP (Espers) como um “combustível” ou catalisador que proporciona os serviços que a cadeia opera, além de estimular o interesse em contribuir para o processamento/formação de blocos para a rede, resultando em uma geração de blocos consistente e garantindo, de forma geral, uma rede ultra rápida.

Mineradores/Apostadores são incentivados a cooperar, o que resulta em uma consistente geração de blocos e assegura uma rede leve globalmente rápida. Este documento pretende descrever em detalhes os diferentes sistemas que o projeto Espers utiliza e como eles operam em uníssono para prover ao usuário final de qualquer comunidade uma experiência intuitiva e sem descontinuidade.

ESPERS

AS BLOCKCHAINS (CADEIA DE BLOCOS)

- **Falhas atuais**

  A blockchain é associada atualmente à um sistema de função única com o propósito muito específico de gerar receita. O criador do Bitcoin esperava oferecer uma tecnologia verdadeiramente única, sem foco nas receitas, mas esta visão se tornou comprometida à medida que centenas de blockchains surgiram pelo mundo. Apesar do que as notícias e a mídia gostariam que você acreditasse, as blockchains não precisam ter apenas uma funcionalidade. Lamentavelmente, a mídia foca apenas em perdas e ganhos, desta forma pessoas com pouco conhecimento são constantemente direcionadas para blockchains que apenas fornecem tokens ou "moedas" sem qualquer fundamento. Contudo, individualmente, os feitos tecnológicos não foram capazes de unir as blockchains baseadas em Bitcoin, mesmo alternativas como a Ethereum não proporcionam esse tipo de solução.

- **Implementação Atual e Benefícios**

  As blockchains podem ser descritas como “Livros fiscais digitais nos quais transações em Bitcoin ou outra criptomoeda são registradas cronologicamente e publicamente” (–Google). Embora isto seja mais ou menos verdade, a afirmação de que a blockchain é usada para o registro de transações, leva as pessoas a restringirem o que elas acreditam que seja possível fazer com ela. Essencialmente, as blockchains são de fato utilizadas para distribuir amplamente para todo um sistema, um livro fiscal digital descentralizado que guarda dados de transações, permitindo que qualquer pessoa seja capaz de acessar contas e informações de maneira segura. Sem ponto central de falha por ser descentralizado, blockchains como as do Bitcoin são extremamente resistentes a qualquer tipo de tentativa de desmonte ou ataque contra o sistema. Livros fiscais descentralizados também provêem transparência ao permitir a visualização de informações gerais por qualquer pessoa, entretanto mantém informações mais específicas e particulares sob o sigilo de uma chave privada individual, exclusiva, que cada usuário possui. Informações de transações são guardadas em blocos de informações convenientemente conhecidos “blocos”, os quais são gerados por mineradores/apostadores, que por sua vez, contribuem com recursos para criptografar um bloco de informações e passá-lo à rede. Como uma blockchain gera blocos, também é possível manipular seu tamanho, facilitando a capacidade de armazenar uma grande quantidade e variedade de dados que posteriormente serão fornecidas aos usuários finais. Isso anula a necessidade de aumentar a blockchain, a não ser que seja exigido pelos parâmetros da cadeia. De uma maneira geral, uma blockchain é um sistema muito capaz em termos de moedas, mas sua versatilidade não pára por aí.

- **Possibilidades futuras**

  Uma blockchain pode ser utilizada por uma infinidade de softwares, no que diz respeito à segurança adicional e confiabilidade oferecida através de um consenso distribuído. A limitação é a própria imaginação e criatividade de cada um. Cada vez mais as comunidades falam sobre sistemas operacionais, sistemas de mensagens e sistemas de armazenamento, todos funcionando na blockchain, melhorariam significativamente nossos protocolos atuais. Uma vez que comunidades e projetos começam a se afastar do foco monetário e inclinam-se mais em direção ao desenvolvimento de possibilidades tecnológicas em si, será criada uma simplificação real, tanto em segurança quanto confiabilidade de nossas tarefas diárias.

ESPERS

MÉTODOS CONSESUAIS E MECANISMOS DE RECOMPENSA

Espers usa uma blockchain híbrida Prova-de-Trabalho/Prova-de-Participação (PoW/PoS) que afeta diretamente como o sistema lida com produção de blocos e estimula o interesse em fazê-lo.

Prova de Trabalho (Proof-Of-Work) ou PoW como frequentemente é chamado, é o mais notório método consensual, já que é um dos mais comuns entre os projetos de blockchains devido ao seu uso no Bitcoin. O Mecanismo PoW funciona com a participação de pessoas que contribuem com poder de computação através de uma forma conhecida como “Hash” ou “hashing”, em referência aos blocos de indexação das Blockchains.

Os participantes, também conhecidos como mineradores, são recompensados por submeterem corretamente blocos que são aceitos pela blockchain/rede e então confirmados à medida que o bloco evolui, assegurando subsequente geração (mineração) de futuros blocos pela manutenção do interesse dos participantes. Além disso, muitos participantes normalmente reúnem seus recursos utilizando um “pool de mineração”, ao contrário do que acontece normalmente de competir um contra o outro, o que permite que mesmo aqueles com com pouco poder computacional sejam capazes de receber recompensas pelo que eles fornecem, ao invés de tentar bater uma entidade com maior poder de hash. Este método de distribuição falha em alcançar a perfeição, entretanto, já que é possível atacar a blockchain controlando quais informações estão sendo garimpadas e submetidas. Estes blocos, conhecidos como "blocos ruins", são blocos com informações inválidas que normalmente não seriam aceitas e possivelmente dividiriam a Blockchain em duas versões de si mesma (bifurcação) para, em seguida tentarem ser validados e aceitos na rede por alguém se utilizando de um enorme poder de computação, que a maioria não tem acesso.

Prova de Participação (Proof-Of-Stake) ou PoS de maneira resumida, é o método mais recente de geração de blocos, entretanto, é indiscutivelmente um dos mais seguros métodos de distribuição, ainda que não imediatamente disponível para novatos que estão subindo à bordo de uma comunidade/projeto. Isso ocorre porque o PoS usa as moedas que um usuário possui para gerar um bloco. Possuindo assim, mais moedas e apostando-as, se oferece ao participante maior possibilidade de criar o próximo bloco. Apostar é o ato de permitir que a carteira de um cliente permaneça online, com objetivo de dar apoio à rede ao ter moedas selecionadas aleatoriamente, que se tornam temporariamente indisponíveis, enquanto a carteira/ cliente forma um bloco e assim compensa o participante com juros sobre as moedas utilizadas. Quanto mais tempo se possuir as moedas, maior é o peso que eles acumulam e maiores são as chances de se formar o próximo bloco. Uma vez que o bloco é formado, o peso das moedas é desfeito para permitir aos outros participantes/apostadores a chance de gerar um bloco. Este método é considerado o mais seguro, já que se for apropriadamente distribuído, os participantes irão invalidar a maioria dos ataques que tiram proveito do poder de hash para obter o controle de uma blockchain, entretanto, deve-se obter moedas para apostar, o que dependendo do seu valor, pode ser caro e em geral, um impedimento para o projeto se este for o único método disponível.

Híbrido (PoW/PoS), conhecido normalmente apenas como método de distribuição “híbrido”, mistura tanto PoW e PoS em uma blockchain única. Sistemas híbridos são relativamente novos, já que poucas blockchains utilizam uma dificuldade algorítmica suficientemente robusta que ajuste o tempo entre os blocos criados tanto por PoW ou PoS e, neste caso, ambos em harmonia. Uma dificuldade personalizada de algorítmico reorientado conhecido como “VRX”, foi criado pela Espers com o objetivo de permitir um rearranjo apropriado dos tipos de blocos criados dentro de uma blockchain híbrida completa. Fazendo isto, a segurança da Espers aumenta substancialmente, já que PoW e PoS complementam entre si as suas falhas, permitindo à blockchain, uma vantagem significativa sobre a operação singular em um método em particular.

A estrutura de consenso e recompensa, a partir da redação deste documento para o projeto Espers, é definida abaixo:

- **Tempo de Bloco (Pós implementação VRX)**
  Espaçamento mínimo imposto: 3,5 minutos por bloco
  Espaçamento ideal: 5 minutos por bloco
  Máximo (soft limit): 7 minutos por bloco

- **Proof-of-Work / PoW**

Bloco 0-10:	0 ESP por bloco	(*Blocos de início**)
Bloco 11-365:	50.000.000 ESP por bloco	(*Blocos reservados**)
Bloco 366+:	5.000 ESP por bloco + taxa de rede	(*Blocos padrões*)

- **Proof-of-Stake / PoS**

Bloco 2125-20,000:	250% juros anual	(*Erro de cálculo 2 d**)
Bloco 20.001-2.000.800:	25% juros anual	(*Fase padrão*)
Bloco 2.000.801-3.000.300:	5% juros anual	(*Redução de escala-1**)
Bloco 3.000.300+:	1% juros anual	(*Redução de escala-2**)

- **Suprimento Máximo de moedas Espers**
  Total de: 50.000.000.000 ESP (*50-Bilhões ESP**)

Blocos de início *: Refere-se a definir uma recompensa de bloco de "0" para que os primeiros blocos da cadeia possam ser analisados enquanto são extraídos sem gerar recompensa para o minerador.

Blocos reservados *: Inicialmente o projeto Espers doou 20% do blockchain total no que é conhecido como “Air-Drop” para qualquer um que quisesse participar de forma gratuita, reservando 5% que foi dividido igualmente entre os seis membros da equipe para financiar o desenvolvimento contínuo. Isso foi feito em abril de 2016, após o lançamento e transitado na troca de blockchain que foi realizada logo depois.

Erro de cálculo de 2 dias *: após a implementação do sistema PoS na Espers, houve inicialmente uma entrada de valor equivocada para a equação percentual anual que calcula as recompensas de participação de um usuário. Isso resultou em um período de 2 dias (48 horas) sobre a compensação das recompensas de participação geradas pelo PoS, mas não teve nenhum impacto importante na oferta / função geral e foi prontamente resolvido. Vinte mil blocos foram processados antes da implementação do VRX e a cadeia estava acelerando a geração de blocos durante esse período.

Fase de redução de escala-1 *: A fase padrão de recompensa PoS termina após aproximadamente 48 bilhões de ESP terem sido gerados.

Fase de redução de escala-2 *: Mais tarde, uma escala de redução final até 1% é conduzida bem próximo de atingir o suprimento máximo de moedas.

50 bilhões de ESP *: Estima-se que o suprimento máximo de moedas seja atingido em aproximadamente 30 anos após o lançamento (2016-2046 A.D.)

TAXA DE VELOCIDADE TERMINAL X (VRX)

VRX ou Taxa de Velocidade Terminal X é um sistema de blockchains de dificuldade redirecionada, que utilizando uma varredura em profundidade de vários blocos, rapidamente adapta os níveis de dificuldade de mineração ou de aposta na blockchain/altcoin para garantir uma alta proximidade em torno do tempo de geração de bloco desejado. Permitindo obviamente algumas inconsistências no espaçamento de blocos devido a aumentos ou diminuições significativas na taxa de hash/aposta. Independentemente se a blockchain é baseada em Prova de Trabalho (Proof-of-Work), Prova de Participação (Proof-of-Stake) ou Híbrida, o sistema VRX garante que os blocos sejam gerados em um ritmo consistentemente uniforme. Além disso, nas blockchains híbridas, que é o nosso caso, os blocos são divididos adequadamente em uma proporção de 50/50, permitindo que ambos os tipos de protocolos consensuais tenham chances iguais na geração de bloco.

De maneira simples, o VRX registra uma quantidade prévia estabelecida de blocos (a implementação típica se estabelece a partir dos últimos seis blocos) e então compara cada um deles entre os demais em relação aos seus tempos de mineração, determinando assim, o espaçamento entre estes blocos. O sistema então seleciona os espaçamentos de blocos determinados e os compara com os espaçamentos de blocos desejados, no que se chama “Rodada de Verificação”. Esta rodada de verificação é similar a outros sistemas de redirecionamento disponíveis, mas se ajusta a uma curva diferente que se adapta rapidamente às grandes mudanças na taxa de hash da blockchain, também assegurando de não se ajustar em excesso para não "confinar" a blockchain. Há uma rodada de verificação por pares de blocos registrados, assim, portanto, um VRX com seis contagens de blocos irá gerar cinco rodadas de verificação. Depois que o VRX executa suas verificações, ele determina se deve alterar a dificuldade para mais ou para menos, observando-se o tempo de mineração, se foi realizado em um período de tempo menor ou maior, em relação ao tempo de mineração desejado. O grau desta ação limita-se à um máximo de duas vezes a dificuldade do bloco anterior ou à sua redução pela metade. Finalmente, uma média é calculada entre as diferentes mudanças de dificuldade de modo que a mudança mais lógica na dificuldade seja aquela que melhor se adapte à blockchain e seja então, registrada pelo sistema Espers. Por favor, consulte o diagrama de funções na próxima página que descreve a função atual.

As versões mais recentes dos sistemas VRX (como a usada) apresentam um balanço de dificuldade de PoW/PoS único, no qual os sistemas híbridos distorcem a dificuldade em uma curva a favor do tipo de bloco menos frequentemente encontrado. Isso garante que nem um tipo de bloco possa vencer o outro, e que tanto mineradores quanto apostadores possam beneficiar igualmente a blockchain. O VRX foi projetado para interagir diretamente com o Sistema de Controle de Velocidade que a Espers possui, o qual é discutido com mais detalhes na próxima seção. Isso porque nenhum outro método de dificuldade redirecionada era compatível com ele, já que a dificuldade do bloco desempenha um papel importante dentro do próprio sistema de Controle de Velocidade.

(Exemplo de esquema de função)

[Buscar Bloco anterior-1**]** → **[**Tempo: e.x. 07:00**]**

- 7 – minutos espaçamento (mbs1)

[Buscar Bloco anterior-2**]** → **[**Tempo: e.x. 07:07**]**

- 9 – minutos espaçamento (mbs2)

[Buscar Bloco anterior-3**]** → **[**Tempo: e.x. 07:16**]**

- 8 – minutos espaçamento (mbs3)

[Buscar Bloco anterior-4**]** → **[**Tempo: e.x. 07:24**]**

- 5 – minutos espaçamento (mbs4)

[Buscar Bloco anterior-5**]** → **[**Tempo: e.x. 07:29**]**

- 5 – minutos espaçamento (mbs5)

[Buscar Bloco anterior-6**]** → **[**Tempo: e.x. 07:34**]**

Espaçamento = 5 minutos espaçamento (mbsT)

[Rodada-1**]**→**[**mbs1>mbsT**]**→**[**Ajuste para baixo**]**

[Rodada-2**]**→**[**mbs2>mbsT**]**→**[**Ajuste para baixo**]**

[Rodada-3**]**→**[**mbs3>mbsT**]**→**[**Ajuste para baixo**]**

[Rodada-4**]**→**[**mbs4=mbsT**]** →**[**Sem ajuste**]**

[Rodada-5**]**→**[**mbs5=mbsT**]**→**[**Sem ajuste**]**

Compare ações e selecione a mais escolhida

Ajuste para baixo =3
Sem ajuste = 2
Ajuste para baixo > Sem ajuste

O VRX ajusta a dificuldade de geração/mineração da blockchain para baixo para atender o espaçamento desejado.

ESPERS

SISTEMA DE CONTROLE DA VELOCIDADE DA BLOCKCHAIN

- **Característica gerais de funcionalidade**

O Sistema de Controle da Velocidade da Blockchain, aqui chamada de “Velocity”, é uma funcionalidade reprogramada, originalmente encontrada na Frycoin (uma antiga altcoin baseada em Bitcoin). Ao deparar-se com esse recurso, percebe-se que, embora seções significativas de código precisassem ser refeitas, o recurso em si tinha um bom princípio geral nos aspectos de segurança e estabilidade da cadeia, tornando-o muito desejável. O recurso foi reprogramado com sucesso, apesar de alguns pequenos contratempos e erros em versões anteriores, que na verdade, não afetam a estabilidade da cadeia ou a operação da moeda de qualquer outra forma que não a pretendida. Mais tarde, no desenvolvimento, foram criados sistemas adicionais que nunca fizeram parte da função original do recurso para a operação geral adequada da blockchain.

Um papel fundamental da funcionalidade “Velocity” é controlar a blockchain com os parâmetros já definidos dentro do código, ao invés de ter espaçamento entre blocos e outras propriedades de funcionamento como uma reação às operações na blockchain. Outras implementações da tecnologia blockchain, um aumento repentino na taxa de hash, o que pode indicar que um possível ataque, são ainda vulnerabilidades, mesmo que o melhor sistema de dificuldade direcionada disponível por aí a fora esteja implementado para controlar o espaçamento dos blocos.Taxas de rede, possíveis questões de balanços inválidos durante o envio de transações e outras partes da blockchain são executadas utilizando verificação dupla, mas são ainda suscetíveis a um ataque, seja ele temporário ou de gasto duplo, que quando confirmado, causa aflição e perdas para os usuários, o que é inaceitável.

Essa possibilidade, de um ataque utilizando esses parâmetros, é solucionada pelo sistema “Velocity” ao utilizar uma "verificação tripla". Mesmo depois de um bloco ter aparentemente atendido a todos os requisitos e ser gerado, ele não é mais aceito de maneira tão simples. Em vez disso, ele é verificado mais uma vez quanto à inconsistências e outros possíveis exploits. De forma notória, os usuários verão os blocos sendo rejeitados durante a fase de mineração ou aposta (ou ambos dependendo das propriedades da moeda). Apesar disso parecer que há de errado, já que blocos estão sendo rejeitados, isto é, na verdade, uma operação completamente normal e bem-vinda.

O raciocínio é que tempos de mineração mais rápidos, taxas incorretas, saldo insuficiente e outros problemas podem ser manipulados por um programador talentoso com intenção maliciosa. Para evitar esses tipos de situações, a Velocity verifica o bloco gerado em relação aos parâmetros da cadeia. Primeiro ele verifica o espaçamento dos blocos, se o bloco foi gerado muito rapidamente, então não atendeu à um dos principais parâmetros da cadeia, e é prontamente rejeitado, evitando possíveis ataques e qualquer tipo de aumento repentino na taxa de hash.

A próxima etapa verifica se o cliente que enviou previamente uma transação (se este tiver enviado no bloco anterior) enviou uma transação válida, comparando balanços prévios versus balanço atual, juntamente com taxas pagas versus taxa mínima requerida para pagar o bloco que está esperando para ser aceito. Se algum desses parâmetros não for atendido (lembre-se que esses são parâmetros padrões, não sendo nada estranhos), o bloco será rejeitado, apesar de gerado com êxito. Assim, esse sistema protege a blockchain, tornando-a mais estável, previsível e confiável de uma maneira geral, passando a

certeza de que os blocos aceitos são de fato blocos apropriados.

Estes atributos estão em desenvolvimento constante. Sua implementação na Blockchain da Espers (que é híbrida, usa PoW e PoS simultaneamente) causou pequenas falhas com o sistema de redirecionamento original que foram resolvidas movendo para o sistema VRX mencionado anteriormente. Essas falhas consistiram em fazer com que a dificuldade atingisse seu nível mais baixo até que um sistema adequado de redirecionamento pudesse ser usado. Dito isto, agora os blocos aceitos são espaçados de forma consistente a um mínimo de 3,5 minutos, permitindo que a blockchain funcione sem problema algum. Em seguida, as verificações de transação e as verificações de saldo anteriores são desativadas até que seus tempos de checagem se sejam impecáveis. A implementação dessas verificações específicas continua em desenvolvimento para que os parâmetros da cadeia sejam adequadamente certificados.

- **Análise de segurança**

Os mineradores também podem criar interrupções automáticas para o sistema, de modo a não desperdiçar energia, enquanto os blocos simplesmente não são aceitos pela cadeia, criando duas possíveis ações. Primeiro, os usuários com sistemas de mineração avançados podem ser capazes de pré-minerar efetivamente um bloco durante o tempo em que a cadeia não está aceitando os blocos, retardando a sua submissão até que o tempo mínimo tenha decorrido. Se o sistema empregasse uma verificação de segurança que analisasse a data/hora de geração do bloco para ver se um minerador retardou a submissão de um bloco, outra possibilidade seria definir uma data/hora válida para um bloco previamente retido, bastando que o minerador conhecesse cada janela de tempo válida. Estas duas ações são resolvidas, primeiramente, pela certificação conferida pelo método do sistema previamente definido, que a data/hora do bloco não venha de fora do bloco permitido. Isso desestimula ataques, criando mais etapas que o atacante deve passar antes de ter uma chance de sucesso. Em seguida, a implementação do VRX penaliza o tempo de mineração mínimo, fazendo com que a energia necessária para manter um possível ataque (mesmo com inserção de uma data/hora válido no bloco) aumente exponencialmente até que, após alguns blocos gerados, a dificuldade seja tão grande que o tempo mínimo não possa mais ser alcançado e outro minerador/apostador possa simplesmente encontrar o próximo bloco. Isso rapidamente impede qualquer possível progresso no ataque. É claro que o sistema Velocity requer que todos os parâmetros sejam atendidos, e não somente o tempo de mineração para aceitar o que parece ser um bloco gerado de forma válida.

O sistema pode ser expandido para incluir mais verificações e uma implementação ainda mais rigorosa que pode se adaptar a qualquer tipo de recurso adicionado ou removido. Isso torna o sistema Espers muito maleável e menos trabalhoso, pois ele pode crescer com a moeda, à medida que se torna mais refinado e maduro. Esse novo recurso de segurança é chamado de “Velocity”.

ESPERS

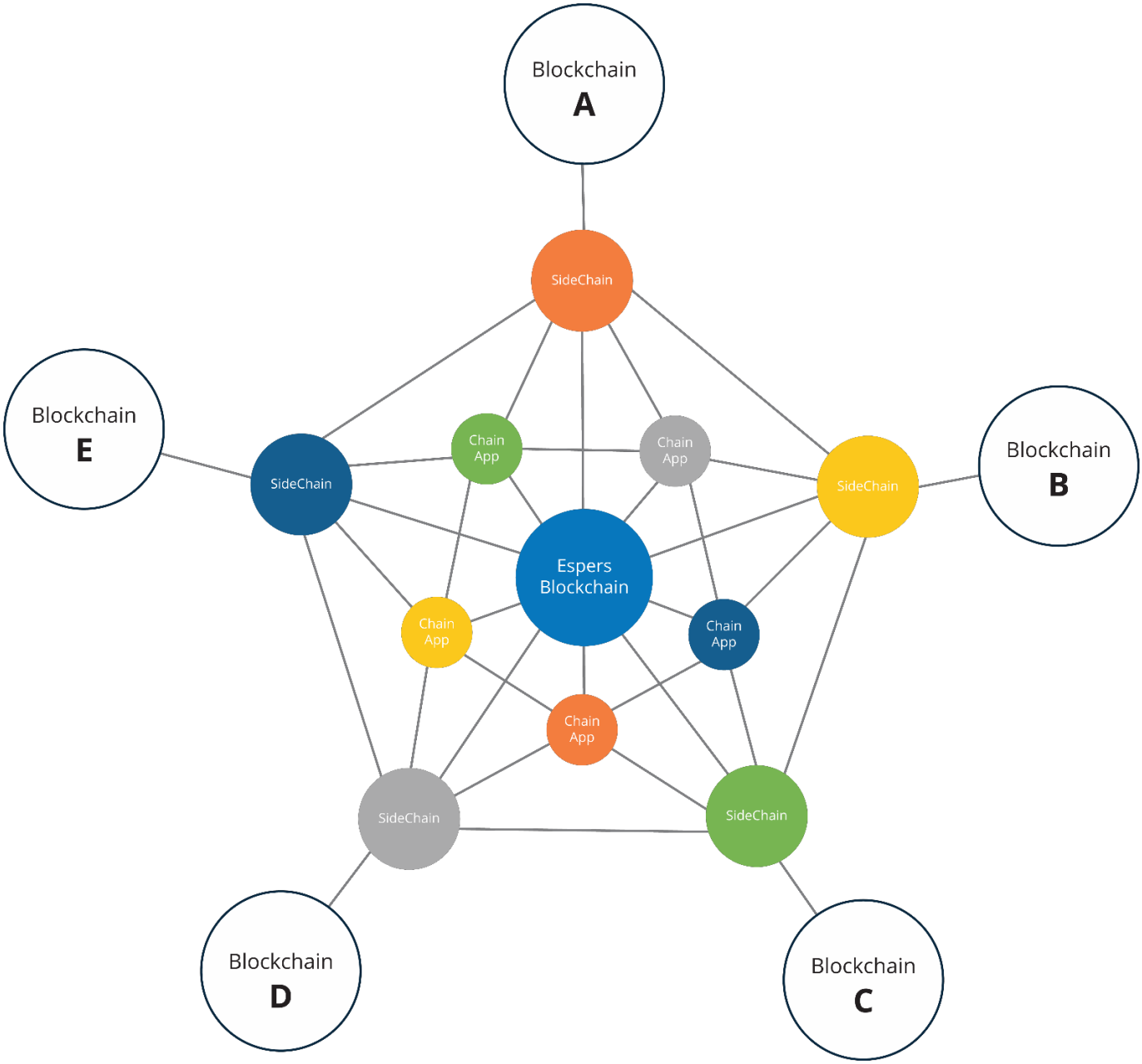
CADEIAS LATERAIS (SIDECHAIN) E

INTERFACE DE CADEIAS CRUZADAS (CROSS-CHAIN)

Ao passo que uma única blockchain é perfeitamente capaz de processar grandes quantidades de informações, surgiram novos métodos em que uma blockchain principal usará blockchains secundárias menores, que por sua vez, dependerão da blockchain-mãe que as criou (cadeias paralelas) para processar, simultaneamente, mais dados enquanto alivia a carga da rede de qualquer blockchain em particular. Algumas abordagens exigem que a blockchain principal interaja diretamente com as cadeias laterais, sendo estas totalmente dependentes da cadeia principal. Por outro lado, na Espers essa abordagem é de que as blockchains laterais sejam e permaneçam capazes de funcionar de forma completamente independente. Essas cadeias laterais, uma vez criadas, permanecem funcionando, até mesmo, sem a necessidade da existência da blockchain da Espers, pois são independentes. O uso de uma interface de cadeia cruzada para transmitir dados de uma cadeia lateral para outra permitirá que cada cadeia possa compartilhar cargas de trabalho enquanto permanece completamente independente. Essa independência significa que, independentemente de qualquer falha ou problema com uma determinada blockchain, o restante da rede permanecerá intacto e operacional, ao invés de sofrer um colapso completo. A utilização deste sistema permite até mesmo a interação com outros projetos e comunidades, permitindo que vários projetos se unam e beneficiem um ao outro se as comunidades optarem por fazê-lo.

Por exemplo, se um projeto que é capaz de enviar mensagens criptografadas e distribuir moedas, processa apenas dados de transações para uma moeda da blockchain “A”, enquanto processa apenas dados de texto de mensagem para a blockchain “B”, cada blockchain precisa processar apenas seus respectivos serviços. Assim, usando a interface de cadeia cruzada, as blockchains podem compartilhar dados entre si, fornecendo aos usuários finais um sistema fluido e intuitivo que é rápido, seguro e confiável. Para complementar o entendimento, se a blockchain "A" for hipoteticamente comprometida, a blockchain "B" permanece totalmente funcional assim como seus respectivos serviços também continuarão a operar. Permitindo que os usuários continuem usando os serviços que necessitam, mesmo que um ou mais elementos não estejam mais acessíveis. Este tipo de sistema também torna mais fácil para um projeto de blockchains se libertar de apenas oferecer um único tipo de serviço.

Consulte a figura A para uma ilustração visual do sistema proposto.


Blockchain
A
SideChain
Blockchain
E
SideChain
Chain
App
Chain
App
SideChain
Blockchain
B
Espers
Blockchain
Chain
App
Chain
App
Chain
App
SideChain
SideChain
Blockchain
D
Blockchain
C

(Figura A)

ESPERS

ENVIO SEGURO DE MENSAGENS

Na verdade, houve várias tentativas diferentes de implementar –Envio Seguro de Mensagem– em projetos de blockchains. Lamentavelmente, poucos deles realmente usam o algorítmo da blockchain para criptografar as mensagens. Para garantir uma entrega rápida, a mensagem não se fixa à blockchain, mas sim a uma chave privada para onde o conteúdo da mensagem é enviado e a partir do qual pode ser lido. Permitir transmissão de mensagens muito rápidas sem a necessidade de adicionar carga à rede de blockchains é uma solução inteligente. No entanto, uma implementação adequada no envio seguro de mensagens precisaria transmitir as mensagens entre os nós através da própria blockchain, assim como um bloco minerado normalmente faria.

Ao armazenar texto bruto em um bloco, semelhante à forma como o bloco de gênese do Bitcoin que contém o texto do título de um artigo de notícias, as mensagens podem, então, ser mais seguras do que somente serem criptografadas e enviadas à um destinatário. Isto se deve, não somente a criptografia de uma mensagem por meio de um algoritmo criptográfico, mas também à capacidade de confirmar que a mensagem enviada/recebida é de fato válida. Permitindo que a mensagem confirme sua validade da mesma maneira que a transação confirma sua validade dentro de uma blockchain, há a segurança de que as mensagens recebidas e enviadas contêm somente conteúdos intencionalmente desejados. Mensagens falsificadas ou mesmo spam são significativamente reduzidas ou até mesmo anuladas inteiramente em alguns casos.

Embora o conteúdo das mensagens permaneça privado, por motivos de transparência, a blockchain ainda informa quando uma mensagem é enviada e para qual chave pública. No entanto, o destinatário e o remetente são os únicos a par do conteúdo, já que publicamente há apenas uma anotação feita na blockchain da que foi enviada a mensagem, juntamente com as chaves públicas que já estão normalmente disponíveis. A transparência é necessária para qualquer tipo de transferência de dados, independentemente de ser para moedas ou para outro tipo de serviço. Isso ocorre porque, sem transparência, torna-se muito confuso verificar se o destinatário realmente recebeu o serviço pretendido, uma vez que as blockchains não registram adequadamente as ações executadas.

Indo muito além de simplesmente incluir texto como conteúdo de uma mensagem, o sistema de mensagens da Espers também foi projetado para processar e distribuir tudo, desde imagens básicas até arquivos e documentos compactados, permitindo que os usuários ultrapassem as limitações de texto padrão. Para alcançar este objetivo, utiliza-se o sistema de cadeia lateral e a interface de cadeia cruzada mencionados anteriormente. Com a Espers sendo a catalisadora para o processamento de dados de texto, suas outras cadeias laterais interagem diretamente com a blockchain da Espers, bem como com as outras cadeias laterais individuais, para também poder processar outros dados simultaneamente, mantendo a carga de rede leve. Isso é feito para remover um ponto central de falha do sistema, permitindo maior flexibilidade dos serviços. Por exemplo, se o usuário “A” envia uma mensagem para o usuário “B” da blockchain de Espers que contém dados de texto estilizados, bem como algumas imagens, a mensagem será realmente dividida e processada simultaneamente em seções.

Primeiro, a própria cadeia de Espers processaria e retransmitiria os dados da mensagem de texto, incluindo o código de estilo, que então será entregue no browser do usuário, mantendo o processamento de dados mais baixo. Em segundo lugar, as imagens enviadas pelo usuário “A” são processadas em uma cadeia lateral que notifica a blockchain Espers a respeito do anexo de imagem da mensagem enviada. Uma vez que a mensagem for confirmada, o usuário “B” poderá visualizar o conteúdo da mensagem, as imagens são enviadas pela cadeia lateral e o texto da mensagem é enviado inalterado, a partir da cadeia local, garantindo mais uma vez que, se algum aspecto falhar, como a imagem, a mensagem ainda seria entregue,

independentemente do estado do resto da rede. O oposto também é verdade. Se a cadeia de processamento de texto tiver um problema, a cadeia de processamento de imagens ainda transmitiria e entregaria o anexo ao usuário “B”, ainda que o texto não esteja visível. Isso cria um sistema muito mais robusto e balanceado do que ter um único ponto de processamento em tais cargas de dados.

Indo além, a Espers, usando a interface de cadeia cruzada (cross-chain) e as cadeias laterais (sidechains), também é capaz de interagir diretamente com outros projetos e suas comunidades, unindo-os ao permitir que usuários de uma comunidade interajam diretamente com usuários de uma outra. Sendo possível que dois usuários, de blockchains participantes, possam enviar uma mensagem de sua carteira local para uma outra carteira de usuário, independentemente de ser da mesma blockchain, comunidade ou projeto. Isso elimina o abismo que há entre as comunidades e permite uma maior possibilidade de uso real a partir dos sistemas atualmente existentes ou que ainda estejam em desenvolvimento. Cada Blockchain processa dados com uma taxa paga às suas respectivas redes, mantendo suas comunidades interessadas na mineração/processamento dos blocos.

Outro ponto chave que beneficia diretamente os objetivos da Espers: As entidades individuais, como as empresas, são capazes de operar de forma conveniente e efetiva cadeias autônomas para suas próprias necessidades internas, tais como mensagens e ou outros tipos de dados digitais que a entidade precisa manter seguro/criptografado. Esta comunicação de cadeia cruzada permite a interação com outro departamento ou uma entidade completamente diferente, mantendo a privacidade e a segurança individualizadas.

WEBSITES NA BLOCKCHAIN (SITE-ON-CHAIN)

Os protocolos atuais da Internet, incluindo SSL e TLS, ainda nos deixam desejando mais. Sites, servidores e até mesmo computadores pessoais são, diariamente, danificados incontáveis vezes ao dia, mesmo com as melhores práticas implementadas e seguindo os melhores protocolos de segurança. Isso ocorre porque grande parte do tráfego que se movimenta pela Internet não estão criptografados ou, de nenhuma maneira, protegidos. Sites e empresas mais respeitáveis garantem o uso de algum tipo de criptografia para o tráfego em seus sites, mas mesmo assim, um servidor ou rede danificados podem causar a queda de todo o sistema, prejudicando as informações do cliente, informações comerciais e outros dados confidenciais.

Em resposta a esse dilema, o projeto Espers propõe que os sites e outros serviços relacionados à Internet sejam operados/armazenados/hospedados através da blockchain, evitando quaisquer possíveis ataques aos sites e outros serviços relacionados, sem afetar a usabilidade. Ao usar a blockchain como um protocolo de internet, você efetivamente adiciona uma camada quase impenetrável de proteção a qualquer tipo de serviço operado, especialmente sites. Indo além de simplesmente adicionar uma camada de segurança, um site operado por uma blockchain não tem possibilidade de sofrer um ataque DDOS, pois não há servidores ou centros de informações para comprometer, nenhum arquivo para “hackear”, sem se preocupar com hospedagem, nenhuma dor de cabeça com domínio, sem preocupações de armazenamento, sem dados para interceptar, e assim por diante. A fim de atingir esse objetivo grandioso, os recursos discutidos anteriormente são todos usados em uníssono para criar um website devidamente renderizado e apresentável para qualquer usuário em qualquer blockchain/projeto.

Primeiramente, os serviços de hospedagem enviam seus sites através da carteira da Espers, a qual rapidamente converte os arquivos em código bruto e o armazena em blocos indexados na blockchain. As cadeias laterais individuais são usadas para armazenar cada tipo de informação assim como cada tipo de código, imagens, vídeos e outros dados, dessa forma, não saturando quaisquer das blockchains envolvidas no processo. Quando os provedores de hospedagem enviam seus sites para a Blockchain Espers, eles também pagam uma pequena taxa de rede para processar os dados com a blockchain, assim como se paga a taxa de transação pelo envio de uma transação. Esta taxa é de um valor nominal, e existe simplesmente, a fim de manter uma compensação razoável para qualquer minerador ou apostador que possa ter processado o bloco. Uma vez que os dados são processados em um bloco e o bloco foi confirmado, ele fica disponível para toda a comunidade usando o sistema Espers e quaisquer outras partes participantes. Ao navegar por sites, o cliente Espers consulta cada cadeia por seu tipo de dados predeterminado e o sistema a processa ao vivo, para que o usuário possa interagir. Isso significa que qualquer tipo de navegação na Web é sempre baseado em sessões, não sendo visíveis por outra entidade ou por terceiros. Qualquer informação processada entre o site e o usuário é, então, protegida, assim como todas as informações visualizadas pelo usuário, inclusive o acesso ao relatório da cadeia e outras variáveis de uso a serem armazenadas para fins analíticos. Ao fazer isso, um serviço de navegação na Web, como o Google, poderia enviar seu próprio navegador que rastrearia a cadeia de sites hospedados nele, sem oferecer diferença de transição entre o sistema atual da Internet e o que efetivamente pode ser chamado de “internet 3.0”, mantendo uma experiência segura, intuitiva e fluida.

Usando o sistema de interface de cadeia cruzada, Espers pode ser conectado a futuros projetos com idéias afins para que, ao invés de criar divisões, um usuário possa navegar em sites armazenados em outros projetos a partir do sistema Espers de blockchains, permanecendo completamente independentes para não haver risco de que haja uma falha que afete sua utilização pelo usuário. Isso incentiva a união, permitindo uma padronização, dispensando a necessidade de um sistema proprietário.

BLOCKCHAIN LEVE/MÓVEL

À medida que uma blockchain cresce, ele se torna “mais pesada”, no sentido de que ela armazena informações continuamente, sem levar em consideração possíveis limitações de hardware ou serviço para o usuário final. Para contornar essa preocupação por possíveis usuários móveis ou usuários que simplesmente não podem armazenar toda a blockchain naquele momento ou indefinidamente, é importante oferecer uma alternativa ao que é conhecido como carteira "completa". Carteira padrão ou “completa”, em geral, armazenam e verificam toda a blockchain, o que permite uma redundância e suporte significativos à medida que membros/usuários da comunidade usam o sistema, enquanto uma carteira “Leve” ou “Blockchain móvel” atua como um portal de acesso, consultando a blockchain e obtendo dados da mesma como um navegador de blocos, em vez de armazená-lo localmente.

Ao não armazenar a maioria dos arquivos localmente, o sistema Espers pode ser mais facilmente usado em grande escala em um dispositivo móvel ou por um usuário com capacidade limitada de rede / armazenamento. Embora grande parte do que torna este sistema “leve” seja simplesmente o rastreamento da blockchain, logicamente, ele também tem a capacidade de enviar dados para a blockchain para serem processados no próximo bloco, com ou sem sincronização da blockchain. Cada sistema deve permitir a personalização pelo usuário que o está utilizando e, como tal, a blockchain Leve / Móvel também é capaz de

sincronizar parcialmente ou totalmente. Se a opção for selecionada, o sistema irá sincronizar a partir do último ponto de verificação e "assumir" que as transações anteriores relatadas pelas cadeias hospedadas pelos nós são válidas. Outra opção é ter uma sincronização completa “silenciosa” para rodar depois da semi-sincronização ser concluída no último ponto de verificação, onde então, o cliente começa a sincronizar o restante da blockchain silenciosamente em segundo plano, permitindo que o usuário continue dando suporte completo à rede, de acordo com seu desejo.

APLICATIVOS DE CADEIA

Como o sistema de cadeias da Espers é projetado para usar cadeias laterais e recursos modulares, os Aplicativos de Cadeia (Chain Apps) se referem à capacidade do projeto de conectar qualquer tipo de aplicativo operado por uma blockchain e aumentar suas capacidades. Alguns desses aplicativos de cadeia vêm de recursos dos X-Nodes (discutidos logo abaixo), enquanto outros são de terceiros, verificados antes da implementação no sistema. Os aplicativos em cadeia criados pelo usuário podem ser enviados a qualquer momento por meio do sistema do cliente e, em seguida, são prontamente processados para receberem uma cadeia lateral exclusiva para o seu uso.

NÓS-X (X-NODES)

Os Nós-X (X-Nodes) não devem ser confundidos com os Masternodes, que é um sistema centralizado onde os usuários bloqueiam um saldo específico para participar de outros recursos adicionais de rede e apoiá-los, recompensando mais tarde o participante com algumas das moedas geradas no bloco seguinte, se estiverem aptos. Em vez disso, os X-Nodes são completamente abertos, inclusivos e opcionais, o que significa que qualquer membro da comunidade pode participar do sistema, independentemente do seu saldo atual ou experiência anterior. Isso garante que o aspecto de descentralização do projeto Espers e da blockchain em geral não seja perdida, mais uma vez fortalecendo a rede no geral.

A maneira como um Nó-X funciona é fazendo com que um participante se registre na rede como um processador de dados adicional, permitindo que eles armazenem cadeias laterais adicionais que são usadas para fornecer recursos de cadeia adicionais. Da mesma forma que um Masternode, um Nó-X (X-Node) requer uma conexão contínua com a Internet e penaliza qualquer participante que de desconecte para evitar conexões inconsistentes ou quaisquer possíveis falhas no serviço prestado aos usuários finais. Quanto mais tempo um usuário participa no sistema, maior a chance de fazer parte dos Nós-X compensados, que são automaticamente votados pela rede, dependendo da confiabilidade e dos dados processados. Um usuário participante pode então bloquear qualquer quantia desejada de seu saldo, que efetivamente ficará congelada, pois o participante não poderá mais apostar até que seja desbloqueado

pelo Nó-X e, ao fazê-lo, o saldo atuará como um multiplicador para a taxa de compensação fornecida. É claro que o multiplicador está em uma curva e implementa vários sistemas antiabuso, como a exigência de um período de resfriamento para as moedas recentemente trancadas. Até que o resfriamento seja concluído, um participante não verá um efeito multiplicador. Quanto menor a quantidade bloqueada, mais tempo o usuário deve esperar até que o bloqueio esfrie à uma taxa exponencial. Saldos maiores exigem que os usuários esperem menos tempo, enquanto possuem o multiplicador em uma curva exponencial. Isso nega a utilidade de balanços significativamente maiores, garantindo que os usuários sejam encorajados a bloquear quantias maiores para serem recompensados mais cedo, ao mesmo tempo em que penalizam a possível “poeira”, bloqueando-a a um grau que a torna impraticável.

Um saldo bloqueado ainda será capaz de encontrar o próximo bloco na cadeia, no entanto, todas as moedas criadas serão redirecionadas (após o resfriamento do bloqueio) para a votação do recurso selecionado de um participante. Votar na rede dessa maneira é crucial para estabelecer o rápido desenvolvimento de recursos pela equipe do projeto e aumentar o apoio à comunidade. Os participantes também podem escolher simplesmente não votar, no entanto, o aspecto do multiplicador é novamente penalizado, pois isso cria diminui o suporte para novos recursos de rede. Qualquer participante pode enviar um recurso solicitando voto pela rede para desenvolvimento futuro, no entanto, quando a rodada de votação termina, qualquer votação de recurso que não foi selecionada é agrupada e dividida em duas seções que são usadas independentemente. A primeira metade é dividida em seções que são transferidas de volta para a rede como taxas pagas, permitindo que mineradores e apostadores recebam um leve “bônus” até que o saldo se esgote, enquanto a segunda metade é voltada para as funcionalidades vencedoras na votação. Os usuários podem desbloquear seu saldo a qualquer momento enquanto participam do sistema Nó-X, mesmo que o saldo não tenha completado o período de resfriamento, dando aos usuários controle total sobre sua experiência. Da mesma forma, se um participante opta por sair em um determinado momento, assim como quando optou por participar, o participante incorrerá em outro resfriamento agora entre a desativação e o tempo de reativação permitido. Além disso, o sistema Nó-X é intuitivo e com um único clique, pode remover possíveis erros do usuário que geralmente ocorrem com recursos semelhantes, como os Masternodes, substituindo-os pelo interesse/imersão do usuário. Isso também tira uma carga considerável das necessidades de suporte, das inconsistências de rede e do incômodo geral de operar ou participar do sistema.

ESPERS

ROTEIRO

Q4 2017

- Atualização do website
- Revisão PoS & PoW
- Atualização da Carteira
- Campanha de Marketing (ativo)

Q1 2018

- Whitepaper
- Carteira Móvel
- Carteira Leve (Carteira Web)

Q2 2018

- Nós-X (X-nodes) – Em desenvolvimento
- Cadeias Laterais (Sidechains)
- Sistema de Mensagem

Q3 2018

- Nós-X (X-nodes)
- Cadeias Laterais (Sidechains)
- Sistema de Mensagem

ESPERS

CONHEÇA NOSSO TIME

UMA MISTURA PERFEITA DE CRIATIVIDADE E A MAGIA DO DESENVOLVIMENTO

CRYPTOCODERZ
Jonathan Zaretsky
Líder de Gestão de Projeto
Desenvolvedor Chefe

ARSONIC
Guillaume Huot
Líder de Desenvolvimento Web
Designer Gráfico

MONOXIDE
Assistente de Gestão de Projeto
Relações Públicas

CAFECONTIKI
Chefe de Marketing
Líder de Conteúdo

IPANDAMONIUM
Relações Públicas
Gestor de Comunidade

KEVINBOERLAND
Kevin Boerland
Desenvolvedor Assistente
Desenvolvedor Web

CTGIANT
Desenvolvedor MAC

BATYSTA
Antonio Batista
Logística de Projeto
Web Designer

BBOBB
Logística de Projeto

CORYVMCS1
Logística de Projeto
Desenvolvedor Assistente

ESPERS

DIVULGAÇÃO

Este guia (documento) é apenas para fins informativos e não um compromisso vinculativo. Não confie cegamente na linha cronológica de implementações ao interagir com a Espers, pois, em última análise, o desenvolvimento e o tempo permanecem a critério exclusivo da equipe Espers/CryptoCoderz.

Nós, a equipe Espers/CryptoCoderz, não temos a intenção de prejudicar ninguém, de forma alguma. Nunca houve um financiamento coletivo de moedas, pré-venda ou qualquer outro método de financiamento público usado para o projeto Espers/CryptoCoderz ou seus desenvolvedores. Por favor, entenda os riscos envolvidos com a tecnologia criptográfica das blockchains e suas respectivas moedas. A equipe Espers/CryptoCoderz não pode ser responsabilizada por quaisquer fundos perdidos, roubados, ou de qualquer maneira ausentes, pois somente você é o responsável pelos seus ativos. Se você não tiver certeza ou tiver duvida do sucesso deste projeto, pedimos que NÃO invista ou se envolva, já que este é um sistema tecnológico protótipo, conforme declarado em várias áreas e, portanto, para ser usado por sua conta e risco.

Nós não temos nenhuma afiliação com o produto da Yobit chamado "Espers". Pois o mesmo se trata de um produto separado, operado exclusivamente pela Yobit.

CRÉDITOS

Muito obrigado a todos que ajudaram a tornar este projeto uma realidade, agradecimentos especiais aos seguintes membros da comunidade (nomes de usuário) que contribuíram para a criação e revisão deste documento:

- ✓ Bit010
- ✓ CafeConTiki
- ✓ CryptoCarrot
- ✓ cXplexus
- ✓ Eugen
- ✓ Gandalf86
- ✓ IK
- ✓ Tekna
- ✓ Vin
- ✓ Wolf