electric cash

Whitepaper v2.0.2

electriccash.global

2021

Tabela de conteúdos

Aviso legal

Este documento não é uma especificação técnica final.

O projeto aqui apresentado encontra-se na sua fase inicial e conceptual e pode ser modificado, alterado ou mesmo abandonado (por exemplo, por razões económicas, tecnológicas ou regulamentares) e nada neste documento será considerado como uma descrição ou visão final e vinculativa do projeto, oferta de serviços, ou qualquer das suas partes ou componentes, ou no que respeita à sua implementação.

Este documento não constitui um conselho financeiro.

A informação contida neste documento (Whitepaper) não deve ser considerada como conselho de investimento. O mercado de criptomoedas é altamente volátil. Deve considerar cuidadosamente se as criptomoedas são adequadas para si, tendo em conta as suas circunstâncias e recursos financeiros. Ao seguir o resto do documento (Whitepaper), reconhece que não procurou aconselhamento de investimento junto do autor, ou de quaisquer partes formalmente ligadas ao autor, uma vez que o referido autor e as partes não podem fornecer tal aconselhamento. Não se espera, nem é oferecido, que invista, compre ou execute quaisquer atividades financeiras relacionadas, sob qualquer forma ou formato, com base em qualquer informação contida neste “Whitepaper” e reconhece que tais ações são da sua exclusiva responsabilidade.

Electric Cash Whitepaper

Eyal Avramovich
Whitepaper v2.0.2

Resumo. Em 2009, foi lançada a primeira criptomoeda, Bitcoin (1). Hoje, 11 anos depois, apesar de ter batido recordes de preços, nem a Bitcoin nem qualquer outra criptomoeda foram ainda adotadas em massa. A maioria das criptomoedas, embora seguras, não são concebidas para funcionar como dinheiro. As transações não são eficientes, tendem a ser dispendiosas, e a experiência do utilizador continua a ser uma questão secundária para muitos projetos. No entanto, novas soluções tecnológicas permitem-nos conceber uma criptomoeda melhor, tão segura como a maioria dos blockchains, mas também rápida e de livre utilização. Neste documento, introduzimos um novo protocolo de pagamento rápido descentralizado – ELCASH – uma moeda baseada em SHA-256, concebida para ser semelhante ao dinheiro comum, para uso diário. As suas transações rápidas e gratuitas para os stakers (utilizadores que fazem staking), fazem dela o método perfeito de câmbio e uma excelente ferramenta para pagamentos diários. Além disso, o mecanismo de gestão do protocolo da Electric Cash dá aos seus detentores o poder de decidir sobre o futuro do desenvolvimento do ecossistema. Acreditamos que esta abordagem preenche uma lacuna existente no mercado e pode satisfazer as expetativas de um vasto número de utilizadores.

1. Introdução

1.1. Declaração do problema e abordagem à solução

Taxas blockchain

A primeira criptomoeda, Bitcoin, implementou um mecanismo simples, mas bastante fiável de taxas de transação concebido para proteger a rede contra o spam. As taxas de transação podem variar e depender de vários fatores, incluindo congestionamento da rede, tempos de confirmação da transação e tamanho da transação. Quando o congestionamento da rede é baixo, todas as transações são processadas rapidamente por taxas mínimas. As taxas são suficientemente baixas para que os custos sejam reduzidos ou nulos para que um indivíduo possa solicitar uma transação. Conforme aumenta o congestionamento e se aproxima dos limites pré-definidos, a procura para a confirmação das transações vai aumentando ao ponto de o minerador poder aumentar as taxas cobradas (2). Muitos projetos recentes copiaram este conceito sem resolver o problema do aumento das taxas juntamente com o crescimento da rede.

Hoje em dia, como muitos deles ganharam popularidade, estão sobrecarregados com elevadas taxas de transação. Em alguns casos, podem custar até dezenas de dólares por transação. Tal custo torna-os pouco rentáveis para uso quotidiano, desencorajando tanto os novos participantes da rede como os já existentes de os utilizar.

No caso das criptomoedas com o consenso "Proof-of-Work", as taxas são utilizadas para proteger as redes contra sobrecargas maliciosas e para dar prioridade às transações acrescentadas ao blockchain. O mesmo se aplica ao protocolo ELCASH. No entanto, a solução ELCASH recompensa os utilizadores que participam ativamente na rede permitindo transações gratuitas para os stakers. Os utilizadores que efetuam um stake (valor colocado em staking) de ELCASH são elegíveis para algumas transações gratuitas todos os dias, dependendo dos seus parâmetros de staking.

Desempenho do blockchain

Embora o blockchain tenha ganho popularidade no mundo financeiro, a sua utilidade real como tecnologia distribuída de confiança é dificultada pela sua falta de escalabilidade (3). A maioria dos blockchains de "Proof-of-Work" têm uma capacidade limitada de processamento de transações. Com o aumento da popularidade e utilização da rede (mais transações estão a ser colocadas no blockchain), a capacidade da rede para processar essas transações de forma atempada diminui. A maioria das criptomoedas do consenso PoW consideradas como as mais seguras são, portanto, raramente utilizadas numa base diária, mas antes como um substituto do ouro. Outras criptomoedas, tais como a Ethereum (4), aperceberam-se deste problema e estão a passar do consenso de "Proof-of-Work" para "Proof-of-Stake".

Muitas soluções têm sido propostas até à data. Neste projeto, implementámos a mais promissora: o chamado sistema de "camada rápida" para melhorar o rendimento do blockchain. Conjugámos o melhor de dois mundos, ou seja, os blocos são minerados em "Proof-of-Work", o que torna o blockchain seguro, mas as transações podem ser processadas numa segunda camada (C2) do blockchain, o que os torna quase instantâneos (5).

Influência da comunidade i

Os projetos no ambiente das cripto são geralmente governados pela equipa de blockchain ou pelo núcleo de criadores, pelo que são governados de forma centralizada. As decisões relativas a qualquer desenvolvimento futuro e mudanças na rede são controladas e tomadas por um número relativamente pequeno de indivíduos. Muitos dos principais utilizadores ou não têm uma palavra a dizer ou influência suficiente na tomada de decisões devido à falta de conhecimentos técnicos ou de capacidade financeira.

A Electric Cash mudou isso ao estabelecer um Fundo de Tesouraria para o Desenvolvimento. É criado a partir de uma fração das recompensas de mineração de "Proof-of-Work" e armazenado nessa "Tesouraria". Além disso, os membros da comunidade Electric Cash recebem Poder de Governação. Isto permite que a rede seja descentralizada onde as decisões sobre futuros desenvolvimentos de um projeto e a utilização de fundos do Fundo de Tesouraria para o Desenvolvimento são conduzidas pela comunidade do projeto. Esta democracia da rede é alcançada graças ao mecanismo de votação integrado no blockchain (6).

2. Ecossistema Electric Cash

A Electric Cash é uma moeda baseada em SHA-256 concebida para ser semelhante ao dinheiro comum para uso diário com uma função de staking adicional. O protocolo da Electric Cash é governado pelos detentores da moeda, que são elegíveis para gerir o desenvolvimento futuro do ecossistema. Todos estes aspetos estão integrados sob um único ecossistema, permitindo que a Electric Cash abranja uma grande variedade de necessidades do mercado e dos utilizadores.

STAKING

GOVERNAÇÃO

SEGUNDA CAMADA

Para incorporar incentivos dedicados não só aos mineradores, mas também a outros utilizadores da rede, as recompensas por bloco Electric Cash são divididas em três partes. A primeira e a maior recompensa vai para os mineradores de "Proof-of-Work". Os mineradores são cruciais para assegurar que a rede funciona corretamente e que é segura. Mas os mineradores não são os únicos interessados. As pessoas que utilizam a rede diariamente e expandem o ecossistema ELCASH são essenciais para o crescimento do projeto.

A moeda ELCASH como parte integrante do ecossistema

O aspeto chave da moeda ELCASH é a sua oferta a longo prazo a todos os utilizadores ativos. Foi assim concebido um ecossistema abrangente onde fazer staking de moedas desbloqueia recompensas e possibilidades adicionais. Graças ao sistema de governação, os recursos internos podem ser gastos em melhorias da rede.

Para alcançar tal sistema, foi implementado no protocolo um modelo único de distribuição (Figura 1), permitindo que todos os utilizadores da rede fossem recompensados pela sua contribuição, ou seja:

- Após a pré-mineração inicial (acumulação de moedas distribuídas de acordo com o plano de distribuição de moedas) ter terminado, a maior parte, 80%, do fornecimento total (stock) de moedas é distribuída aos mineradores.
- 10% do fornecimento total é utilizado para recompensas de staking.
- 10% do fornecimento total é atribuído ao Fundo de Tesouraria para o Desenvolvimento. Isto destina-se a ser utilizado para desenvolvimentos futuros (melhorias do protocolo). Os membros da comunidade da rede (utilizadores que fazem staking e ganham o PG) são as únicas pessoas com direito a geri-lo (ou seja, através de votação).

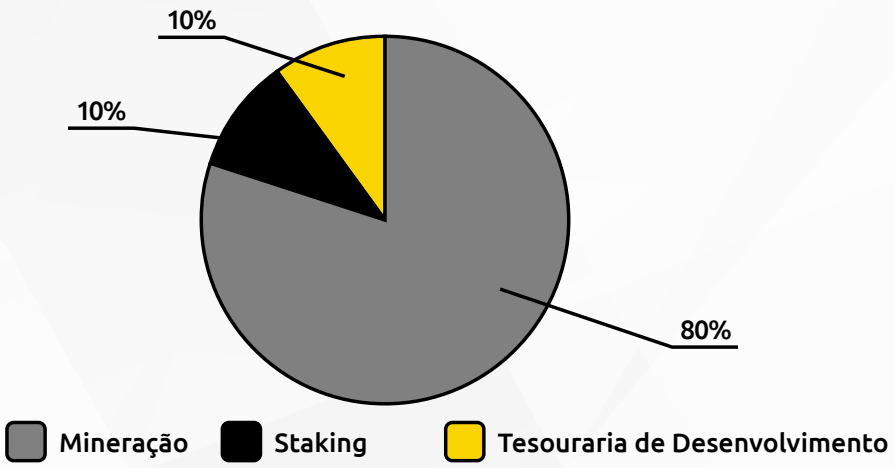

Figure 1. Block rewards distribution

Acreditamos que esta abordagem irá atrair mineradores na altura do lançamento. Como resultado, no final da fase de “bootstrap”, deverá haver moedas suficientes em circulação e uma quantidade significativa de potência de hash a proteger a rede para que outras funcionalidades da rede possam ser utilizadas e facilitar a adoção em massa no uso quotidiano.

2.1. Staking

Uma das principais funcionalidades da Electric Cash é o staking. Permite a criação de um bom sistema de gestão para os nossos utilizadores e incentiva um comportamento positivo por parte dos participantes da rede. Staking é uma forma de armazenamento de activos cripto. Ao fazer staking, cada utilizador pode contribuir ativamente para o crescimento da rede a longo prazo e ajudar a prevenir o problema do excesso de oferta da moeda que poderia afetar a questão global da inflação nos próximos anos. Isto, por sua vez, aumenta a estabilidade da rede.

2.1.1. Processo de staking

Os participantes da rede Electric Cash podem fazer staking de ELCASH para governar a rede e ganhar recompensas com o montante investido. O staking de ELCASH também recompensa os utilizadores com benefícios adicionais (Figura 2) tais como transações gratuitas e Poder de Governação (PG).

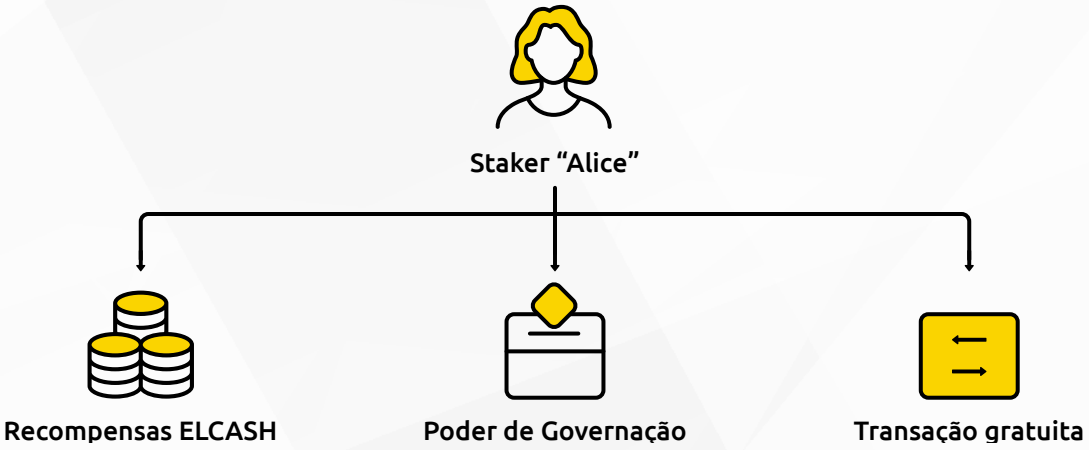

Figure 2. Electric Cash Staking benefits

Todos os utilizadores que possuem ELCASH podem gerir todo o processo de staking a partir da sua (carteira) Electric Cash Wallet. O utilizador tem o controlo total sobre os activos cripto e faz o contrato de staking diretamente com o protocolo.

2.1.2. Parâmetros de staking

As regras do processo de staking são as mesmas para cada participante e para cada montante colocado em staking. Cada utilizador pode escolher um contrato de staking fixo, que corresponde a taxas de juro específicas, e a sua duração.

Tabela 1. Juros de staking ELCASH (por ano) de acordo com os períodos contratuais.

Dias	Blocos	Recompensas [% por ano][1]
30	4 320	5
90	12 960	6
180	25 920	7,25
360	51 840	10

Uma vez que o blockchain funciona com base no número de blocos, a duração de staking é calculada em blocos e não como uma unidade de tempo. O número de dias indicado na tabela acima é estimado com base no tempo médio do novo bloco, que é de cerca de 10 minutos para o blockchain da Electric Cash.

1 Nota. Os valores são apenas números estimados e podem diferir ligeiramente ao longo da duração do contrato devido às variáveis da rede.

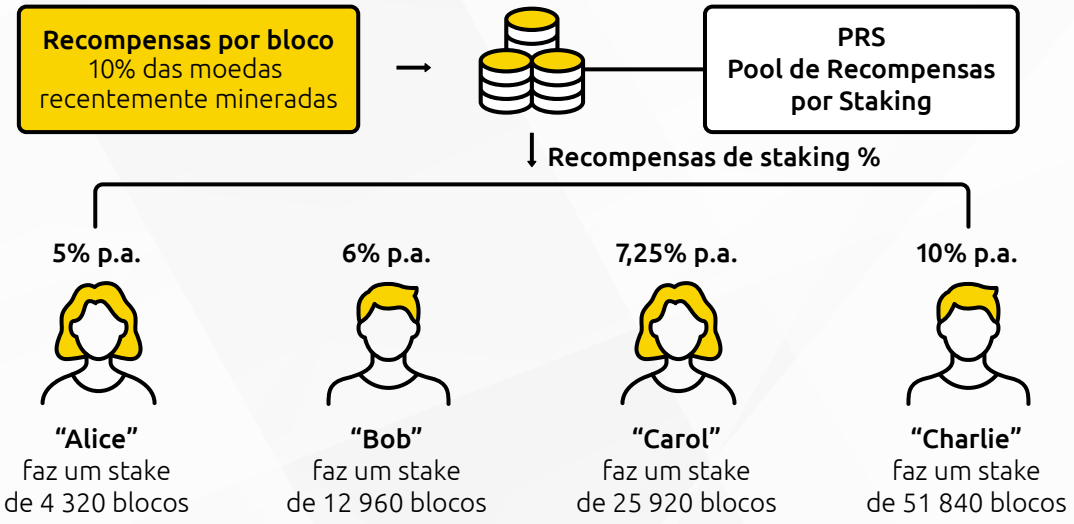

Figura 3. Percentagens da recompensa de acordo com a duração de staking

The As recompensas de staking diferem em função da duração do contrato – quanto maior for o período de staking, maior serão as recompensas de staking. As recompensas são calculadas por bloco e o valor atribuído ao utilizador é indicado na sua carteira. As recompensas de staking são um valor aproximado por ano; as recompensas finais podem diferir ligeiramente.

Para evitar um erro de arredondamento grave, o valor mínimo que pode ser colocado em staking é 5 ELCASH. Não há um valor máximo fixo.

2.1.3. Pool de Recompensas por Staking (PRS)

No protocolo Electric Cash, as recompensas de staking provêm diretamente das recompensas de mineração de “Proof-of-Work”. 10% da recompensa de cada novo bloco minerado é retirada e vai para a Pool de Recompensas por Staking.

As recompensas só podem ser transferidas para os stakers após o fim do período staking. A rescisão antecipada do contrato resulta na perda dos prémios ganhos até à data e numa multa. As recompensas que não são acumuladas permanecem na pool e são subsequentemente distribuídas entre todos os stakers ativos e a penalidade é transferida do utilizador para a PRS.

Detalhes da Pool de Recompensas por Staking:
Na variável que contém o valor da Pool de Recompensas por Staking (PRS) após cada bloco, realizam-se as seguintes ações:

- O valor da PRS é aumentado em 10% das recompensas do bloco.
- O valor da PRS é aumentado pelas penalidades de levantamento antecipado e os activos cripto que foram bloqueados e atribuídos ao staker que terminou o stake.
- O valor da PRS é diminuído através das recompensas de staking que são atribuídas a todos os stakers que têm contratos de staking ativos.

Todos os dados sobre o valor dos stakes são mantidos na base de dados de staking (BDS), que é uma representação do blockchain da Electric Cash e é automáticamente atualizada, pelo que todos os dados estão seguros. Após cada bloco, a base de dados é atualizada através das seguintes ações:

- Se for encontrada uma transação para um novo stake, esta é adicionada à base de dados.
- Se o período de staking para uma determinada entrada tiver terminado, ou se for encontrado um pagamento antecipado ("unstake"), ele é removido da base de dados.
- Todas as recompensas de staking (percentagens) são calculadas e adicionadas a cada entrada (cada stake ativo), de acordo com o montante desse stake.

Nota. A base de dados funciona apenas como uma representação mais conveniente do blockchain, mas é possível restaurar todos os dados da base de dados utilizando o blockchain.

2.1.4. Carteira de Staking

O elemento central do ecossistema da Electric Cash é uma carteira amiga do utilizador e intuitiva (Figura 4). A aplicação da carteira inclui uma Carteira de Gastos e uma Carteira de Staking. A Carteira de Staking permite aos utilizadores fazer stake facilmente das suas moedas para receber Poder de Governação, transações gratuitas e recompensas de staking.

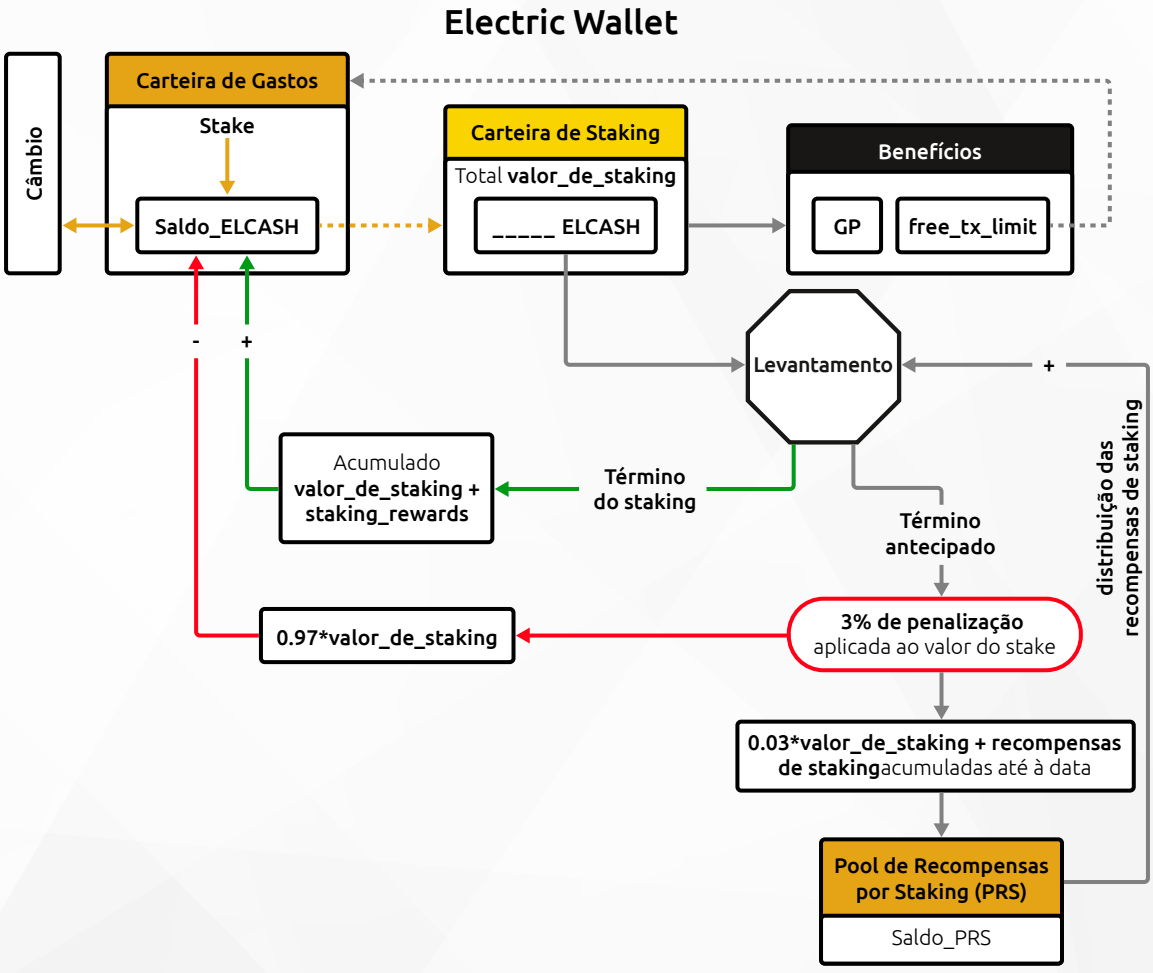

Figura 4. Processo de Staking de Electric Cash

A Carteira de Staking não tem um endereço separado da Carteira de Gastos. Uma semente protege e recupera ambas. A Carteira de Staking é uma instância UTXO no endereço da Carteira de Gastos. Atua como um valor reconhecido pelo blockchain em separado, mas armazenado no mesmo endereço.

Ao criar um novo stake (Figura 5), o início de uma transação retira as entradas da Carteira de Gastos do utilizador e cria saídas com todos os parâmetros de staking, e depois é criada um nova UTXO (saída de transação não gasta) de staking com os activos cripto colocados em staking. Se os activos da Carteira de Gastos forem superiores ao montante colocado em staking, a alteração é também colocada na nova UTXO de gastos.

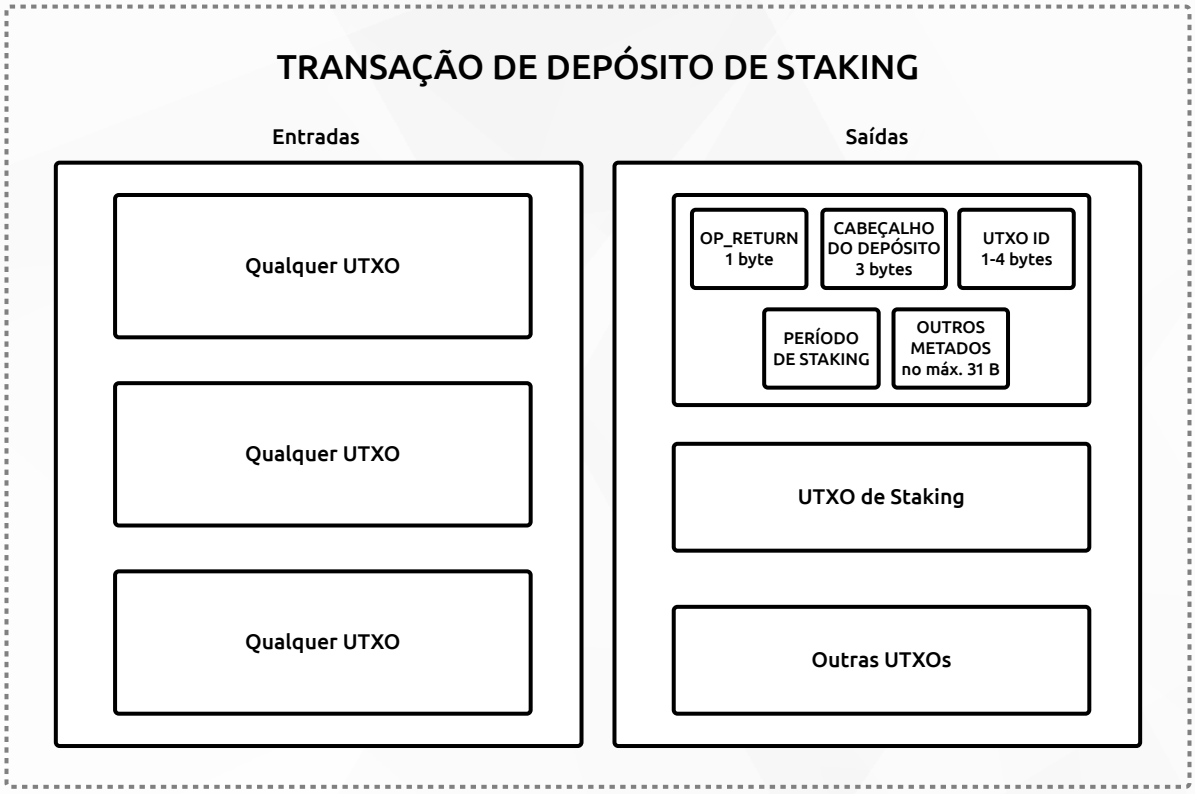

Figura 5. Transação inicial de staking

Regras de validação:

1. OP_RETURN + cabeçalho de staking é a primeira saída da transação (tx)
2. UTXO ID > 0
3. Período de Staking ≤ 4 (índice de uma tabela de pesquisa).
4. A UTXO de staking ter de ser ≥5e8 sat
5. Todas as regras normais de transação

Quando o staking termina, o protocolo verifica se o stake atingiu o seu vencimento ou foi terminado pelo utilizador. Se foi terminado prematuramente, a penalidade é imposta, e as recompensas da staking não são transferidas para o utilizador. Se o stake tiver atingido o seu vencimento, os activos cripto da UTXO de staking e a UTXO das recompensas são transferidos para a UTXO de gastos, conforme ilustrado no diagrama abaixo (Figura 6).

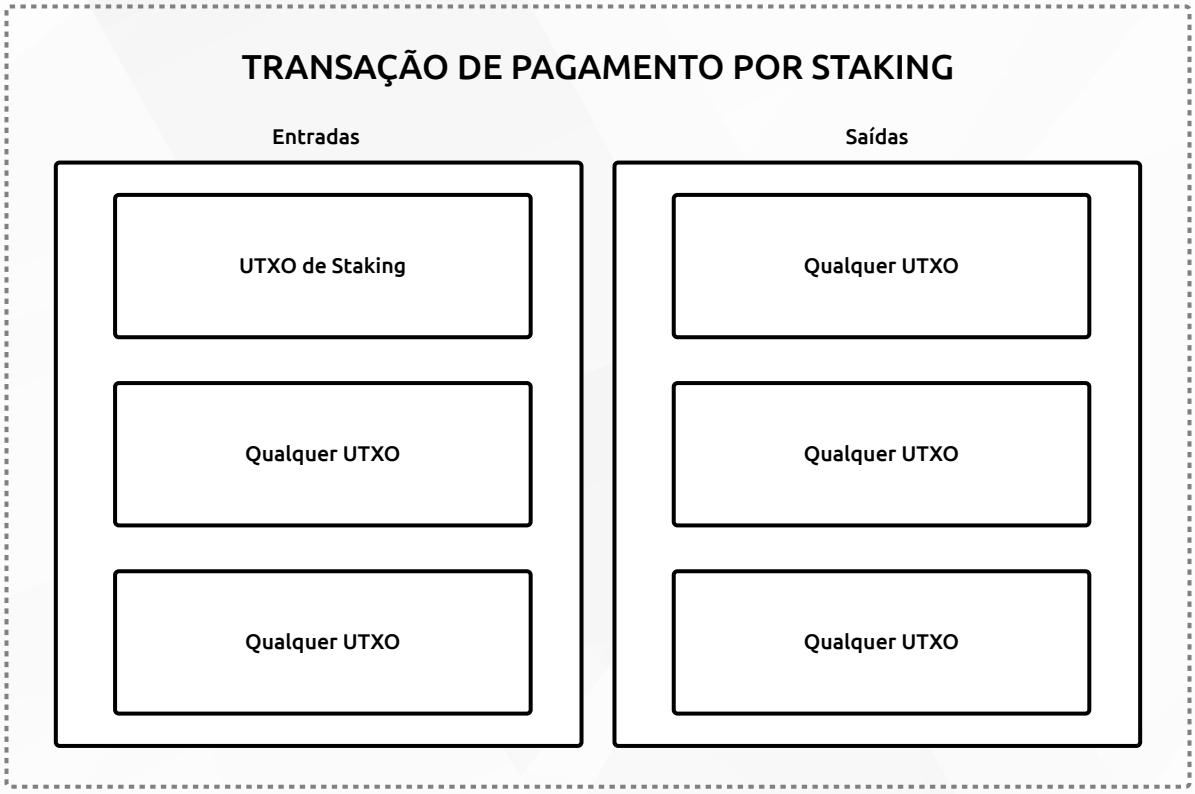

Figura 6 Transação de pagamento por staking

Regras de validação:

1. Verificar se algumas UTXOs de staking: verificar se a TX de entrada é a TX de depósito de staking (verificar primeira saída)
2. Verificar se o período de staking foi cumprido (altura atual do bloco ≥ {altura do bloco de entrada UTXO + período de staking})
   a. Se **sim**: verificar se o valor de saída é inferior a {entradas + recompensas de staking}. (calcular a recompensa por staking)
   b. Se **não**: verificar se o valor de saída é inferior a {entradas – penalização de staking} (calcular penalização de staking)
3. Todas as outras regras normais para a transação

Uma transação de queima de staking é utilizada para transferir activos de UTXOs normais para a Pool de Recompensas por Staking. A principal razão para a sua introdução é fornecer uma forma de encher a Pool de Recompensas por Staking após o "hard fork" de staking, com a devida percentagem de recompensas de mineração do período anterior ao mesmo.

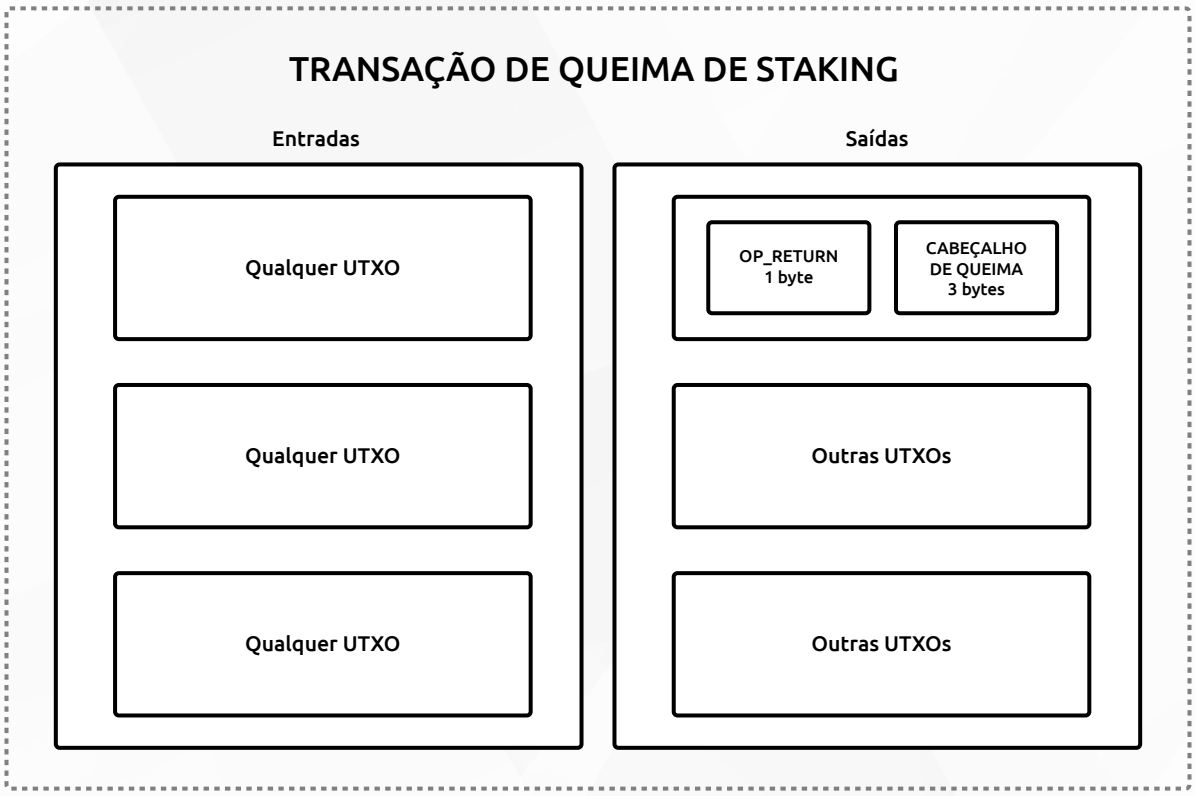

Figura 7 Transação de queima de staking

Regras de validação:

1. OP_RETURN + cabeçalho de queima é a primeira saída da transação (tx)
2. SUM(entradas) ≥ SUM(saídas) + montante_queimado:
   Período de staking ou como um número de blocos ou um índice de uma tabela pré-definida contendo o número de blocos

Nota: Os utilizadores estão em constante controlo dos activos e da chave privada relacionada tanto com a Carteira de Staking como com a Carteira de Gastos, assim sendo, a segurança é tão forte quanto os padrões pessoais do utilizador.

2.1.5. Levantamento

Uma vez concluído o staking, um staker poderá reclamar a recompensa utilizando a transação de pagamento de staking. Todos os participantes são obrigados a esperar até que o período de staking termine para levantar os seus activos [montante colocado em staking + recompensas de staking], caso contrário, será imposta **uma penalização fixa de 3%. O objetivo das penalidades é proteger as transações gratuitas na rede contra abusos, impedir as pessoas de votar fora da rede e evitar que a economia da ELCASH seja prejudicada.**

O levantamento antecipado dos activos resulta em penalizações e na perda das recompensas obtidas até à data. Nenhuma recompensa é acumulada antes da conclusão de um período de staking pré-definido. As recompensas que não forem acumuladas e as penalidades aplicadas ao utilizador serão devolvidas à **Pool de Recompensas por Staking (PRS)** e subsequentemente distribuídas entre os outros stakers que mantenham a sua posição.

2.1.6. Cálculo de recompensas e penalizações

A Pool de Recompensas por Staking e as recompensas individuais são atualizadas para cada novo bloco. O protocolo calcula todas as recompensas que os utilizadores devem receber e com base nisto verifica o estado da PRS. Simultaneamente, o protocolo verifica se o stake atingiu o seu prazo de vencimento e em caso afirmativo, as recompensas são enviadas ao utilizador. Se o stake ainda estiver em curso, o protocolo envia a informação para a base de dados de staking e as recompensas coletadas pelo utilizador são atualizadas (Figura 8).

Tabela 2. Atualização do protocolo – parâmetros de entrada

CONSTANS	ENTRADA NA BASE DE DADOS DE STAKING
MINING BLOCKS PER DAY= 144	STAKE {
MINING BLOCKS PER YEAR= 365*MINING BLOCKS PER DAY= 144*365	STAKED,
STAKING_PERCENTAGES = [0.05, 0.06, 0.0725, 0.1]	PERIOD,
STAKING_PERCENTAGE_VS_PERIOD: {	COMPLETE_BLOCK,
“lmo”: 0.05,	COMPLETE,
“3mo”: 0.06.	REWARD,
“6mo”: 0.0725,	SCRIPT,
“12mo”: 0.1}	TXID,
STAKING POOL EXPIRY BLOCKS = 180	NUM OUTPUT
STAKING MAX-YEARLY PROFIT PERCENTAGE = 0.1	}
PENALTY RATE = 0.03	
GLOBAIS	
STAKING POOL	
TOTAL_STAKED = { “lmo”: XXX ELCASH, “3mo”: XXX ELCASH, “6mo”: XXX ELCASH, “ly”: XXX ELCASH}	

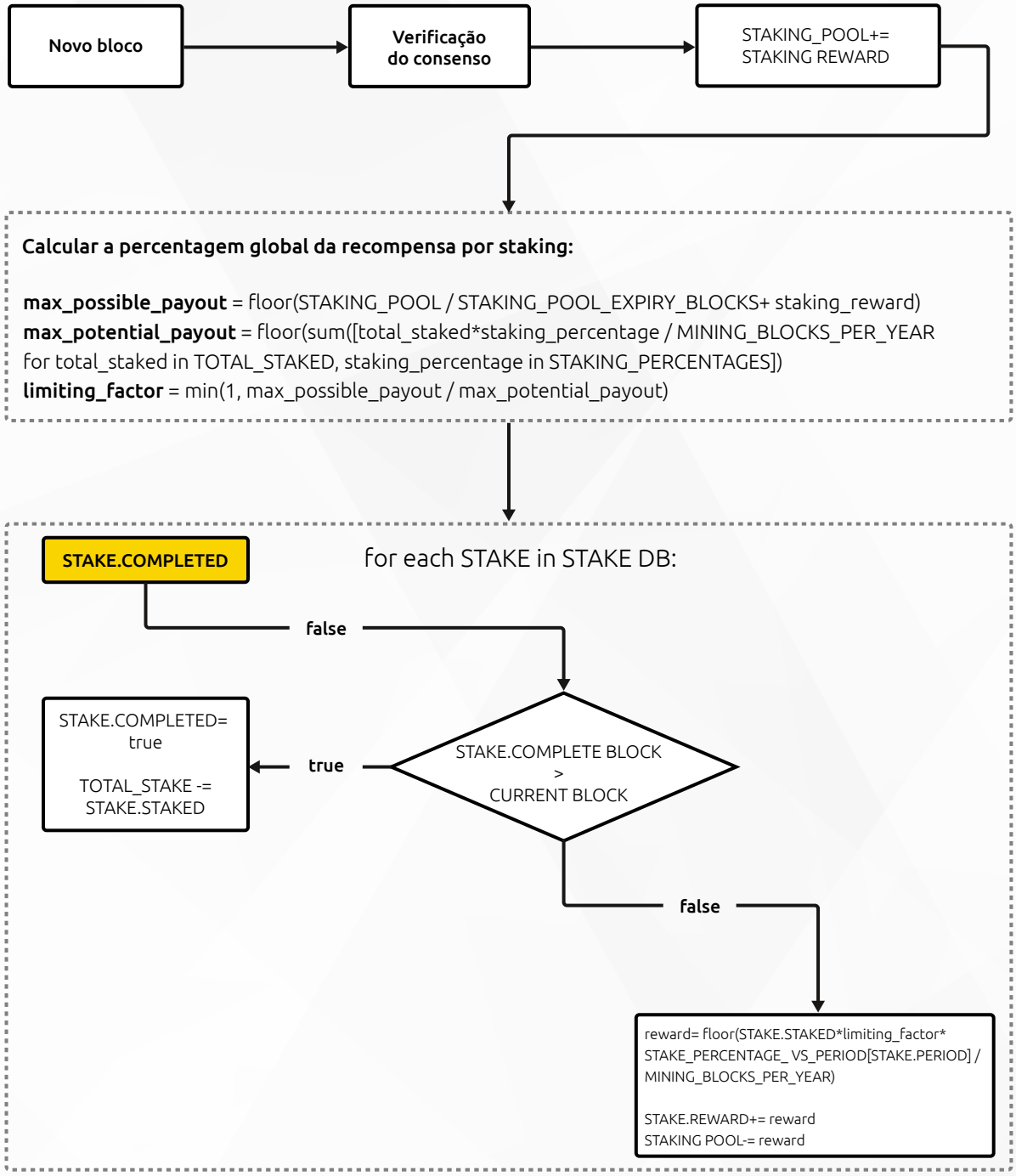

Figura 8. Algoritmo para os cálculos de staking

O protocolo está constantemente à procura de transações que ponham fim ao stake do utilizador. Se tal transação for encontrada, o protocolo verifica se o stake foi terminado prematuramente, ou se o contrato de staking atingiu o seu prazo de vencimento. Se o stake for cancelado antes do vencimento, a penalidade é imposta e o utilizador não poderá receber mais do que a percentagem calculada das moedas depositadas. Se o stake tiver atingido o prazo de vencimento, tanto os activos colocados em staking, como as recompensas acumuladas podem ser transferidos. Os stakes concluídos são removidos da base de dados.

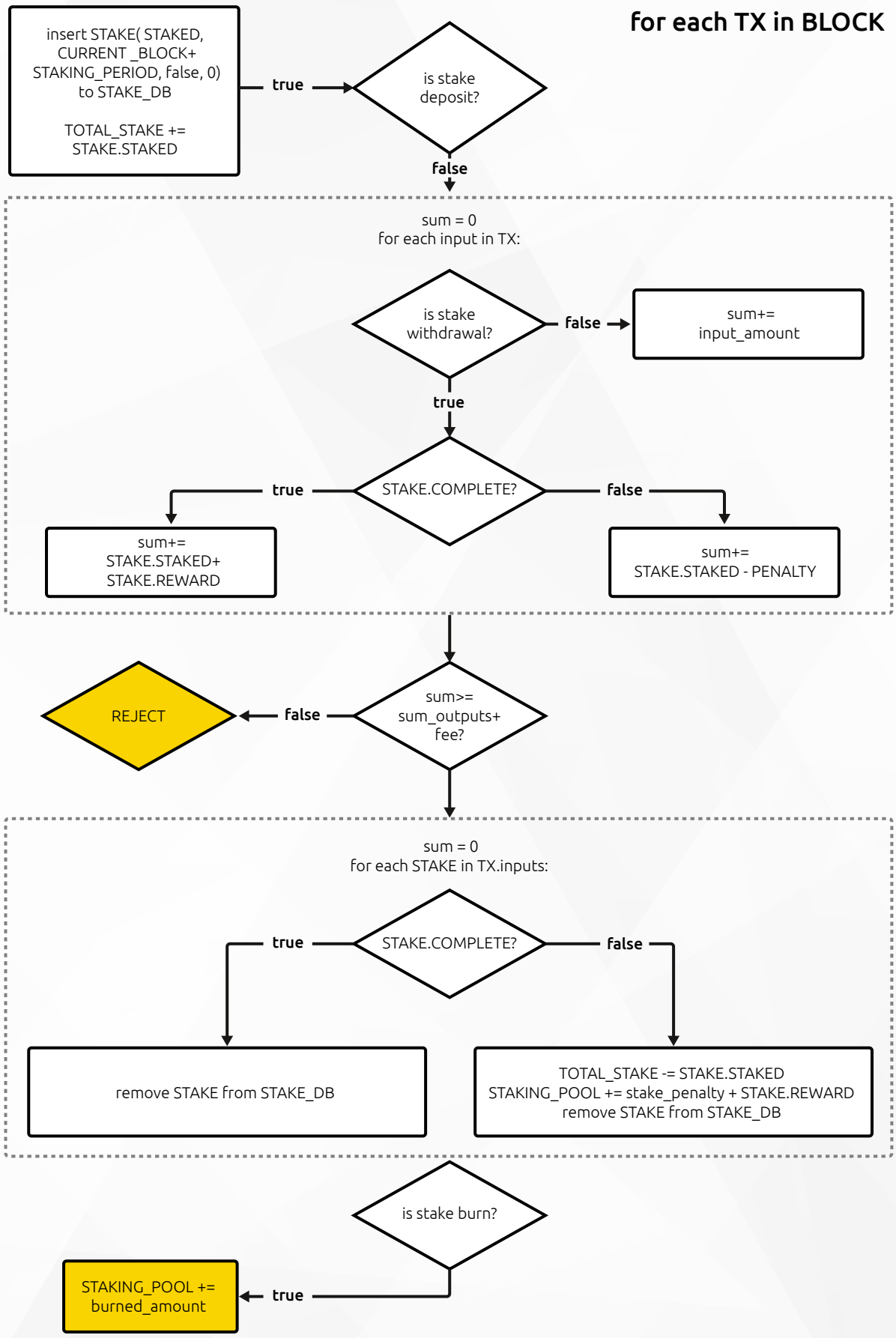

Figura 9. Pool de Recompensas por Staking e a lógica da atualização das recompensas dos utilizadores

Recompensa de staking (RS) – levantamento antecipado

Um utilizador que efetue o levantamento de ELCASH colocada em staking antes do prazo de vencimento do stake terá de pagar uma penalidade de levantamento antecipado "EWP" (abrevição em Inglês), que é de 3% do valor do stake.

Recompensa de Staking – levantamento bem sucedido após o prazo de vencimento

Para cada bloco, o protocolo calcula as potenciais recompensas de staking (PRS) e as recompensas máximas possíveis de staking (RMPS).

As RMPS são iguais à fração da "staking pool" que pode ser utilizada na data atual (Ex: 1/180 da reserva total da staking pool). Dividindo as RMPS por 180, as Recompensas de Staking serão garantidas aos utilizadores durante mais tempo (180 é o número de dias arbitrariamente escolhido, cujo objetivo é assegurar a menor variação possível nas recompensas de staking). As PRS são a soma das recompensas que o sistema deve pagar de acordo com todos os contratos de staking ativos.

O montante da reserva da "staking pool" usado, é deduzido dessa mesma reserva. Se as potenciais recompensas de staking (PRS) forem < às recompensas máximas possíveis de staking (RMPS), cada utilizador receberá um montante de recompensa contratado (ou seja, 5/6/7,25/10% por ano). Se as potenciais recompensas de staking (PRS) forem > às recompensas máximas possíveis de staking (RMPS), o fator limitativo (FL) deve ser calculado. O FL determina o pagamento máximo diário que pode ser fornecido no dia em questão. Este processo afeta todos os utilizadores proporcionalmente ao montante do seu stake e pode resultar numa recompensa ligeiramente diferente. Assegura que há sempre activos suficientes na Pool de Recompensas por Staking para recompensar todos os stakers.

2.1.7. Poder de Governação e transações gratuitas

A participação em staking de ELCASH concede aos utilizadores benefícios adicionais tais como Poder de Governação e transações gratuitas. O Poder de Governação (PG) é um valor intransmissível gerado com base no valor do stake e na duração do staking do utilizador. Permite que o utilizador participe nas votações de governação da ELCASH e crie novas propostas de governação. **O número de transações gratuitas é também condicionado pelo valor colocado em staking e pela duração do mesmo.** O limite é calculado diariamente, e as transações gratuitas não realizadas não são acumuladas. O principal objetivo é recompensar um stake mínimo (5 ELCASH para 4 320 blocos) com uma transação gratuita por dia.

Todos os detalhes específicos do Poder de Governação e os cálculos das transações gratuitas são discutidos em pormenor nos seus respetivos capítulos.

2.1.8. Staking Explorer

Os dados de Staking e o desempenho da rede podem ser monitorizados pelo Staking Explorer (Explorador de Staking) juntamente com o Painel de Governação. Os dados das transações e de staking são atualizados em tempo real. Os utilizadores podem facilmente

obter conhecimentos estatísticos gerais, tais como o Stake Total da Rede, o estado da SPR em tempo real e uma verificação analítica geral da rede.

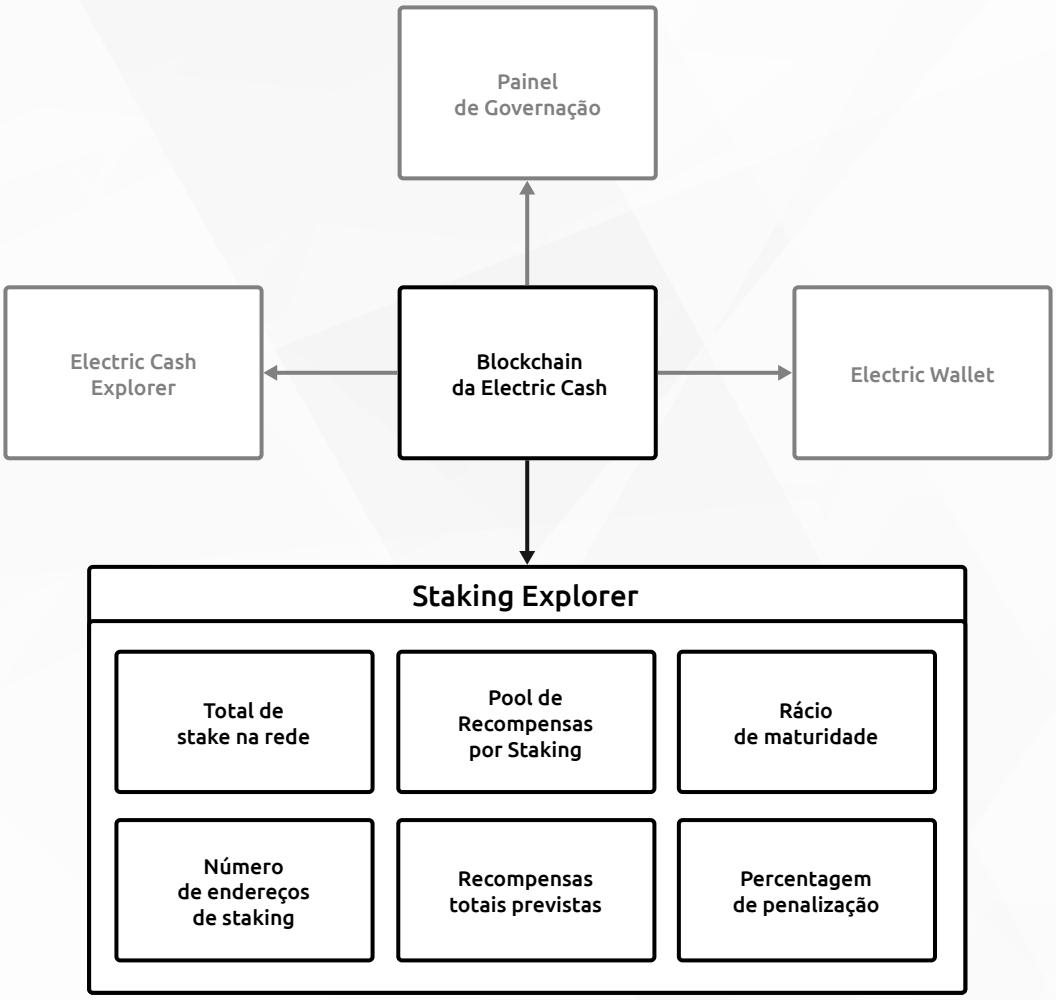

Figure 10. Staking Explorer overview

2.1.9. Segurança

O staking de Electric Cash é um processo seguro, uma vez que todos os parâmetros de staking estão incorporados no protocolo do blockchain e todo o processo de staking é automático – os criadores da Electric Cash não têm a posse dos activos em nenhuma altura. Não é possível que os criadores interfiram com os activos nas carteiras (nem na Carteira de Gastos, nem na Carteira de Staking) e a equipa não utiliza os activos para lucrar com eles de forma alguma.

O utilizador é a única pessoa com acesso aos activos tanto na Carteira de Staking, como na Carteira de Gastos.

Os criadores não têm acesso à Pool de Recompensas por Staking. A PRS é um valor que é automaticamente atualizado pelo protocolo e apresentado no Staking Explorer.

2.2. Sistema de Governação

A fim de alcançar a democracia direta, a Electric Cash implementa um sistema de governação. No processo de governação, as novas alterações podem ser propostas, elaboradas, acordadas e implementadas. As alterações não se limitam aos detalhes técnicos do código fonte do blockchain, mas podem também abranger outras questões importantes da rede e da comunidade. Utilizando o mecanismo de votação integrado no blockchain, os utilizadores podem votar nas propostas feitas tanto pelos membros da comunidade e/ou pelo núcleo da equipa de gestão da Electric Cash.

A importância da governação

A governação do blockchain não é apenas um gesto simbólico em relação à comunidade. É também um elemento importante do ecossistema blockchain. Torna os projetos mais transparentes e mais fáceis de gerir. A introdução do sistema de governação na Electric Cash torna o projeto mais competitivo, uma vez que as decisões podem ser tomadas mais rapidamente e responder melhor às necessidades do mercado e dos utilizadores.

O sucesso no mercado das cripto não pode acontecer sem o envolvimento dos intervenientes. As criptomoedas são frequentemente criadas sobre um código de fonte aberto, que é fácil de copiar, e só podem diferir umas das outras através das pessoas que apoiam o projeto. As comunidades devem ser consideradas como a parte mais importante e única de cada ecossistema blockchain.

2.2.1. Poder de Governação (PG)

Durante o processo de staking no protocolo da Electric Cash, os participantes da rede (stakers) obtêm Poder de Governação (PG). O Poder de Governação é diretamente condicionado pelos parâmetros de staking:

Quanto maior for o valor do stake e maior for o período de staking, mais direitos de voto (governação) os stakers têm sobre o ecossistema.

O Poder de Governação é intransmissível, criando um ecossistema de utilizadores credíveis que fazem mais stakes e por muito mais tempo. O sistema foi concebido para assegurar que um maior PG só esteja disponível para os membros mais ativos e dedicados da comunidade ELCASH. O Poder de Governação ganho pelos utilizadores mudará com o tempo se estes deixarem de estar ativos na rede.

O objetivo do sistema de governação da Electric Cash é criar um projeto que seja:

- **descentralizado:** todos os utilizadores da rede podem participar na governação. Todos os stakers podem fazer uma proposta e votar;
- **transparente:** todos os resultados da votação, juntamente com a sua fase de implementação, são visíveis no site do Explorador de Governação (Governance Explorer);
- **seguro e privado:** todos os utilizadores podem votar de forma anónima. A rede blockchain mostra apenas o endereço da carteira do utilizador que participa no processo de governação.

2.2.2. Cálculo do Poder de Governação (PG)

O Poder de Governação é calculado para recompensar os participantes mais importantes e mais ativos da rede. Cada utilizador que faça staking de Electric Cash ganhará Poder de Governação (PG). O fator Poder de Governação depende dos seguintes parâmetros:

1. **Montante em staking** – quanto mais ELCASH colocar em staking, mais Poder de Governação um utilizador obtém durante o período de staking.
2. **Tempo de staking** – como o staking a longo prazo é mais benéfico para a rede, os utilizadores que fazem stake por mais tempo obtêm mais benefícios, ou seja, os utilizadores que fazem staking uma única vez por um período de tempo mais longo e ininterrupto obtêm mais PG do que aqueles que voltam a fazer staking dos seus activos repetidamente, mesmo que o período de staking acumulado seja o mesmo.
3. **O requisito mínimo do protocolo para gerar PG**: 5 ELCASH colocados em staking durante 1 mês para obter 1 PG.

O PG não é uma moeda. É um direito não monetário ligado ao endereço ELCASH do utilizador e é intransmissível (de carteira para carteira).

2.2.3. GP Burning e Minting methods

A fim de manter uma rede saudável, cada voto e proposta exige que o utilizador utilize o seu PG como um método de "pagamento", que protege o blockchain da Electric Cash de ficar congestionado. No processo de votação (Figura 11) e criação de propostas (Figura 12), cada utilizador necessita de utilizar a quantidade escolhida de PG (cumprindo os requisitos mínimos indicados). O PG utilizado neste processo será queimado e não transferido. Queimar no blockchain significa remover um determinado valor de um activo da rede. Neste caso, o PG usado para "pagar" a proposta não é transferido para outro endereço, mas sim "destruído" pelo protocolo, de modo que ninguém mais pode aceder ao mesmo.

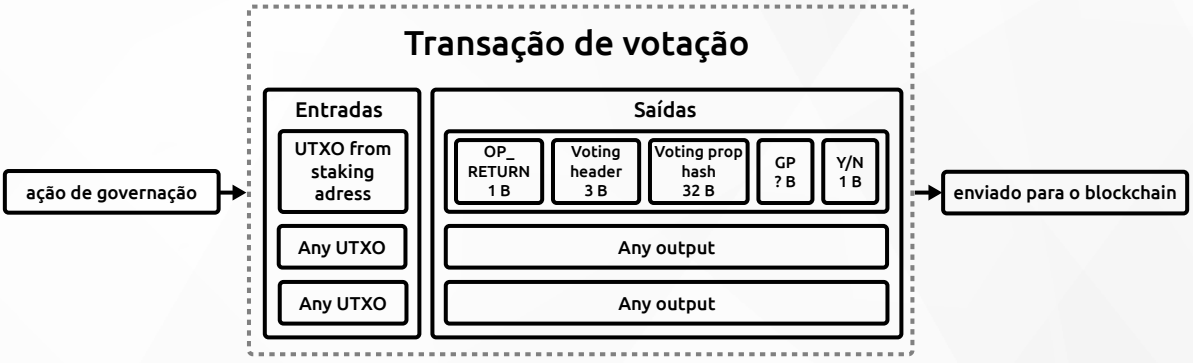

Figura 11. Processo de votação

Quando um utilizador vota, é criada uma transação de votação. O Blockchain guarda o endereço do utilizador, o montante de PG gasto, e a opção escolhida. Os resultados da votação são calculados com base em todas as transações de votação efetuadas pelos utilizadores.

O método de GP MINT (cunhagem do PG) permite que os utilizadores sejam recompensados com PG adicional. Minting (a cunhagem) cria uma certa quantidade de PG adicional, pelo que o PG não é enviado de qualquer endereço, mas sim criado pelo protocolo.

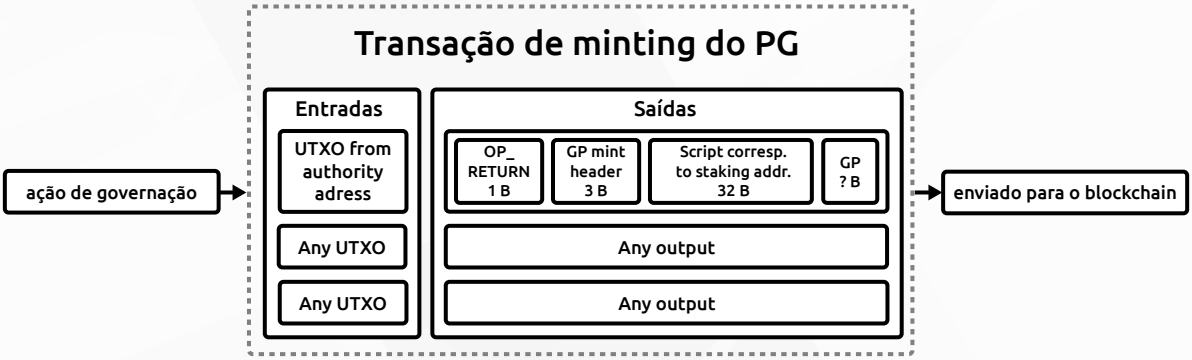

Figura 12. Processo de minting (cunhagem) do Poder de Governação

Quando um utilizador executa uma ação que é elegível para devolução do PG (votação ou criação de uma proposta bem sucedida), o blockchain realiza uma transação de GP minting (cunhagem do PG). A entrada vem de um endereço de autoridade, o qual é um endereço especial codificado, que informa o protocolo de que é necessária a cunhagem (minting) de uma determinada quantidade de PG.

2.2.4. Criação de propostas

A comunidade Electric Cash decide sobre a economia e o ecossistema da moeda. Cada utilizador pode criar uma nova proposta para que a rede vote. Os membros podem não só votar sobre funcionalidades adicionais, mas também sobre os parâmetros de mineração da Electric Cash, como a fornecimento total da moeda, o que ajudará a ELCASH a ser competitiva e um projeto atualizado para o futuro.

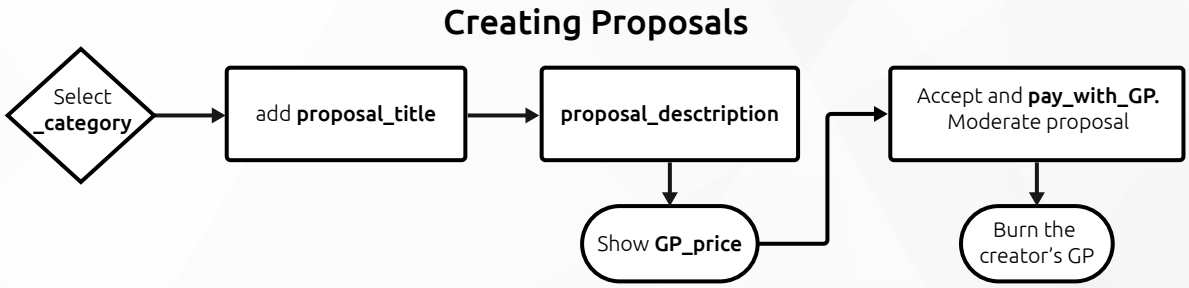

Figura 13. Mecanismo para a criação de propostas de governação da Electric Cash.

A proposta pode ser criada utilizando a Electric Wallet. No entanto, para evitar a sobrecarga da rede e impor as alterações propostas, a criação de uma nova proposta exige que o utilizador gaste o seu Poder de Governação. O custo inicial de para efetuar uma proposta é de 304 PG. Este valor pode ser alterado no futuro, dependendo das necessidades da rede.

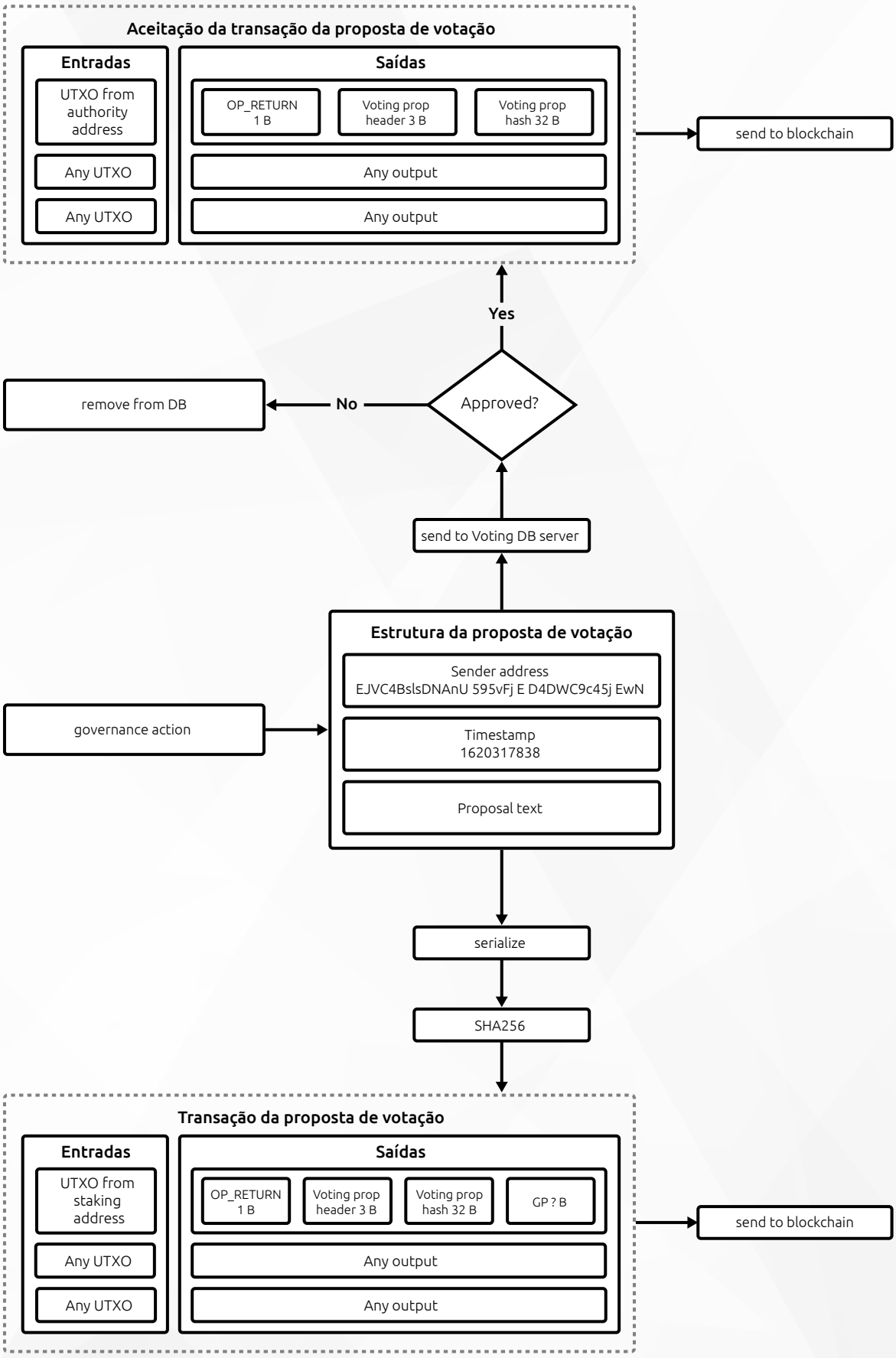

Figura 14. Processo de criação de propostas para votação

Quando um utilizador cria uma proposta, todos os dados (endereço do remetente, registo da hora e texto da proposta) são enviados rapidamente e enviados para o blockchain através de uma transação especial com a proposta para votação. Ao mesmo tempo, os dados da proposta são também enviados para uma base de dados de votação externa. O processo é transparente e seguro, pois cada utilizador pode comparar o hash da proposta da base de dados com o hash enviado para o blockchain, para garantir que ninguém fez alterações aos dados da proposta. Se a proposta for aceite pelos moderadores, a votação é iniciada.

2.2.5. Ciclo de vida das propostas

As propostas podem ser apresentadas tanto pela comunidade como pelos criadores da ELCASH. Novas propostas só podem ser acrescentadas no período de votação aberto, para tornar todo o processo de votação mais fácil de gerir e seguir. Após a submissão, as propostas da comunidade são moderadas pela equipa da ELCASH para eliminar quaisquer propostas maliciosas ou ilegais. As propostas aprovadas são adicionadas à "active_proposals_list" (lista de propostas ativas) e podem ser votadas. Se os votantes votarem a favor da proposta, esta passa, e depois a equipa da ELCASH decide se ela é adicionada à lista de propostas pendentes da equipa.

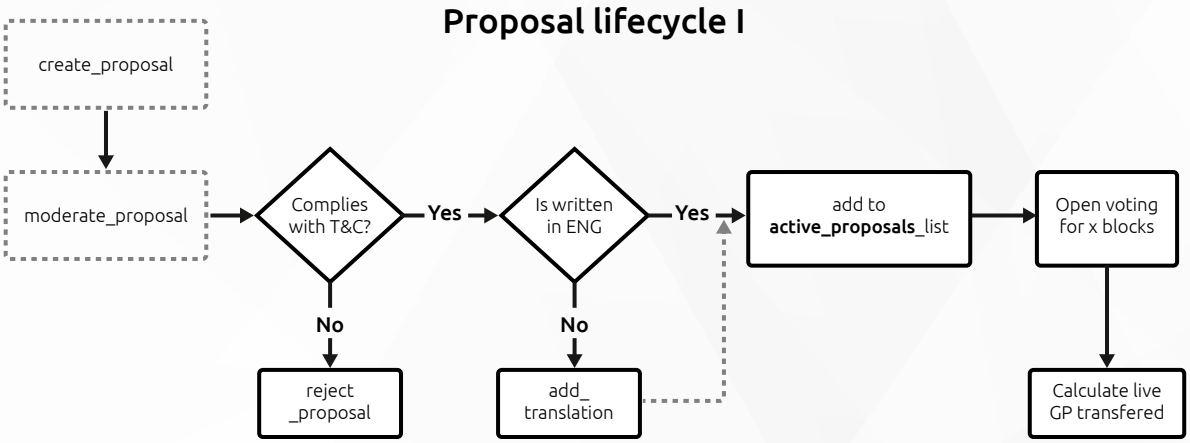

Figura 15. Ciclo de vida das propostas de governação da Electric Cash 1/2

Uma vez que a criação e a moderação favorável são submetidas, cada proposta é imediatamente visível no Painel de Governação no ambiente de trabalho (PG) e pode ser votada na Electric Wallet. Todas as propostas têm a mesma oportunidade de votação e todo o Poder de Governação transferido é calculado em direto nesse momento.

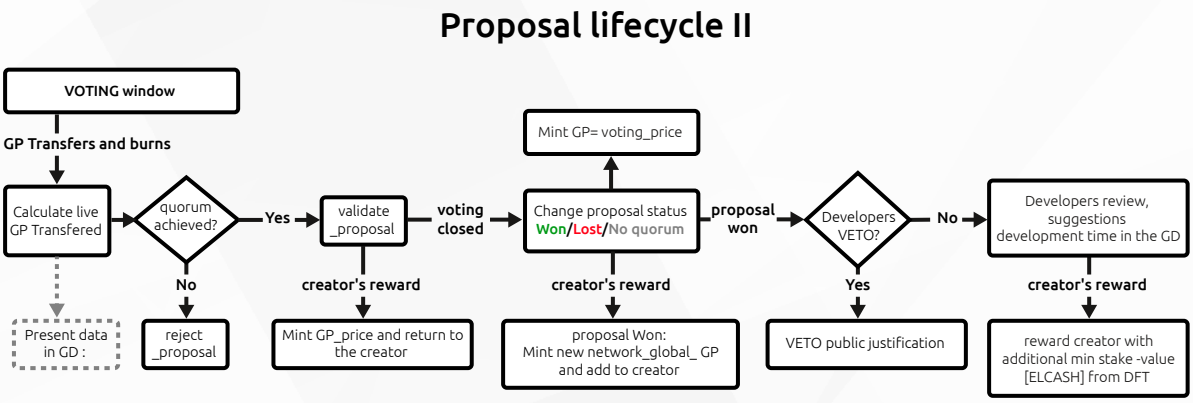

Figura 16. Ciclo de vida das propostas de governação da Electric Cash 2/2

Durante o período de votação, cada proposta tem o mesmo ciclo de vida. Após ser moderada, o primeiro grande passo para uma proposta é alcançar o quorum de rede. Se 15% de todo o PG global da rede foi transferido para uma proposta (ambos os votos sim e não), o quorum é alcançado. O quórum alcançado significa que há muito interesse na rede pelo que o criador recebe 80% (0,8*preço do PG da proposta) do PG gasto para apresentar a proposta. Esta "devolução" é feita através do método MINT (cunhagem). Se uma proposta não tiver alcançado quórum durante todo o período de votação, é rejeitada, e o utilizador perde o seu PG que foi queimado no processo de apresentação da proposta. Esta abordagem motiva os utilizadores a submeter apenas as propostas mais relevantes e a consultar a ideia da proposta com outros participantes da rede em canais de comunicação dedicados.

Durante o período de votação, a rede apresenta os dados da proposta on-chain (na corrente) no Painel de Governação e na Electric Wallet, com detalhes como:

Após o período de votação:

- Cada proposta muda o seu estado para um dos seguintes:
  - **WON** (ganhou e o PG foi transferido pelo voto maioritário – sim)
  - **LOST** (perdeu e o PG foi transferido pelo voto maioritário – não)
  - **NO_QUORUM** (sem quorum e o PG transferido pelo voto - sim e voto - não foi < a 15% do PG global da rede)
- Se o estado da proposta for = WON, o criador da proposta recebe adicionalmente o PG Minted (cunhado) com um valor de 0,01* PG da rede global. Esta regra mostra claramente que o valor global de PG dentro da rede pode aumentar não só por causa de novas moedas colocadas em staking.
- Os criadores podem utilizar o método VETO. Em situações necessárias devido à tokenomics (economia de tokens) da moeda e ao seu desenvolvimento, os criadores podem utilizar o VETO e não aceitar a proposta escolhida pela comunidade. O motivo da utilização do veto deve ser sempre devidamente analisado e justificado pela equipa de criadores, utilizando um painel dedicado no Painel de Governação. No entanto, se a proposta alcançar o estatuto "WON", o utilizador é recompensado mesmo que a proposta tivesse sido vetada.

2.2.6. Moderação da governação

Todas as novas propostas são moderadas pela equipa da Electric Cash para assegurar que todas as propostas são criadas para o bem da rede e não com intenções maliciosas ou mesmo ilegais. Se uma proposta for considerada maliciosa, é retirada e a votação não é conduzida.

Se a equipa da Electric Cash aprovar uma proposta, esta fica disponível para votação e é visível no Painel de Governação.

A moderação também tem lugar quando as propostas são apresentadas noutras línguas para além do inglês e traduzidas pela equipa da Electric Cash. Isto significa que tais propostas podem estar disponíveis para votação com um ligeiro atraso. Graças a isso, toda a comunidade verá sempre a versão original da descrição da proposta e também o seu equivalente ENG (inglês) no Painel de Governação e no painel simplificado dentro da Electric Wallet.

2.2.7. Votação

Todos os utilizadores que reuniram o Poder de Governação no processo de staking podem votar sobre as propostas apresentadas no Painel de Governação. A votação está aberta durante um período de bloco correspondente a aproximadamente 4 semanas a partir do dia em que a proposta é publicada. Após o fim da votação, todos os utilizadores podem verificar os resultados no Painel de Governação.

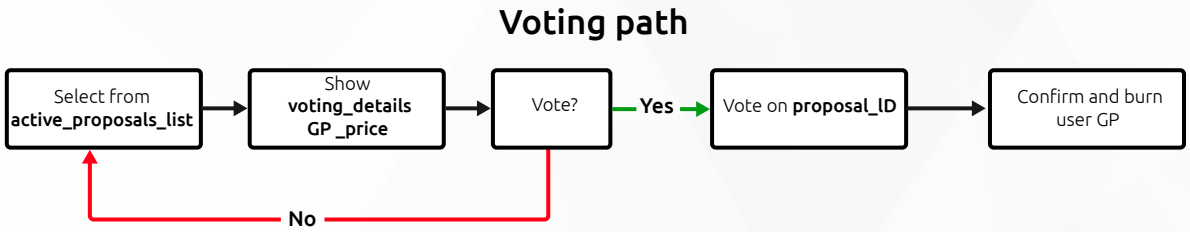

Figura 17. Mecanismo de votação dentro da governação da Electric Cash

A votação também tem um custo em PG. O preço, contudo, muda com cada voto adicional. O primeiro voto de um determinado utilizador é definido como o custo de 1 PG.

Qualquer outro voto custa um valor quadrático:
PG_preço = x^2,
onde x – número de votos
(ou seja: 2ª votação – 4 GP, 3ª votação – 9 GP, e assim por diante).

Tal solução assegura que os maiores stakers não assumam o controlo sobre a rede, pelo que cada utilizador tem a mesma importância para a comunidade, tornando a ELCASH verdadeiramente democrática.

2.2.8. Painel de Governação

Para aumentar a transparência do projeto da Electric Cash, permitindo a todos acompanhar o processo de governação mesmo sem uma carteira dedicada, foi criado o Painel de Governação. É um site dedicado que apresenta as informações mais importantes sobre governação, incluindo todas as propostas do passado e em curso, resultados das votações, a atividade dos eleitores, Poder de Governação na rede e outros parâmetros.

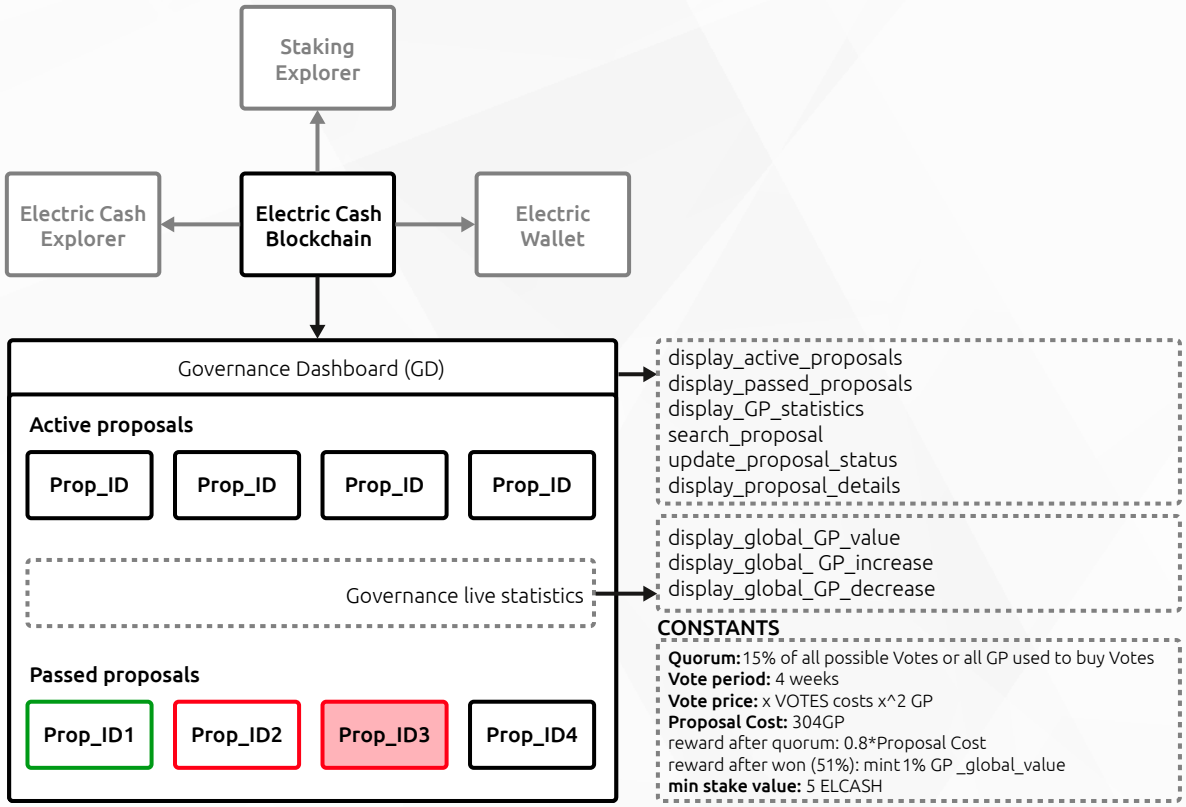

Figura 18. Vista geral do Painel de Governação da Electric Cash

Cada proposta aprovada (após o período de votação) pode ter um dos quatro estatutos:

Tabela 3. Possíveis estados das propostas

Prop_ID1	Prop_ID2	Prop_ID3	Prop_ID4
WON	LOST	VETO	NO QUORUM

O Painel de Governação é também um óptimo meio para trocar ideias e contactar os criadores que dão a sua opinião sobre cada proposta “WON” ou justificam a sua decisão/ou não.

2.2.9. Execução da proposta

Para garantir a segurança da rede, especialmente nos seus primeiros anos, as propostas de governação não são executadas automaticamente. A equipa da ELCASH verifica todas as propostas e seleciona as que terão maior impacto na rede.

2.3. Mineração combinada

Durante as primeiras fases de desenvolvimento, a ELCASH funcionará utilizando um processo de mineração combinada. Permitirá à ELCASH potenciar a poder de hash de correntes maiores baseadas em SHA-256 (tipo Bitcoin), garantindo a segurança global da nova rede.

A mineração combinada é implementada com a Bitcoin, uma vez que ambas as criptomoedas utilizam a mesma função de hash SHA-256. Neste caso, a BTC é a corrente principal e a ELCASH é a corrente auxiliar. Como resultado, as soluções de "Proof-of-Work" da Bitcoin (corrente principal) podem ser utilizadas para validar a ELCASH (corrente auxiliar) como mecanismo auxiliar de consenso "Proof-of-Work" (AuxPoW) (7).

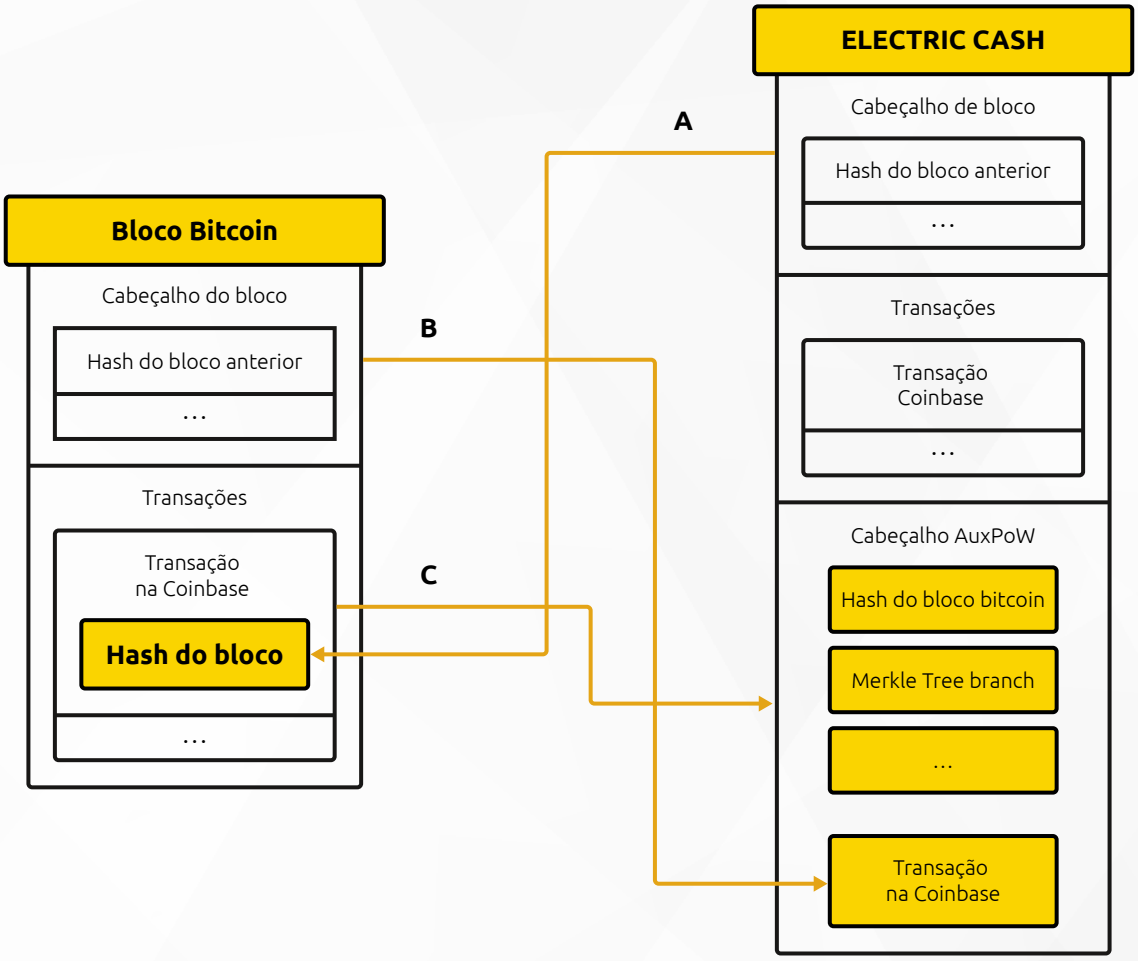

Figura 19. Estrutura dos blocos minerados combinados na Electric Cash.

A mineração combinada é um bom método para novos blockchains, como o da ELCASH, para aumentar a segurança e reduzir a vulnerabilidade a ataques de 51%. A implementação dessa arquitetura de mineração integrada no ecossistema dá-nos confiança de que a ELCASH cumpre as atuais normas de segurança da indústria.

3. Infraestrutura da Electric Cash

A Eletric Cash é um protocolo de pagamento concebido para ser acessível e simplificado, com foco na redução das taxas de transação e na utilização quotidiana e sem sobressaltos. Transações rápidas e gratuitas para os stakers numa rede segura e descentralizada tornam a ELCASH ideal para pagamentos do dia a dia.

3.1. Camada de transações rápidas

A fim de implementar transações rápidas, o blockchain requer capacidade de bloco suficiente para incluir todas as transações que estão à espera de confirmação, e para informar a rede sobre as transações o mais rapidamente possível. As transações rápidas são a chave para a adoção global, mas nos blockchains tradicionais de “Proof-of-Work”, as transações instantâneas são difíceis de conseguir devido a razões de segurança. Os destinatários das transações precisam de esperar pelo protocolo adicionar a transação nos blocos seguintes, o que é limitado pela dificuldade de mineração. Em média, demora cerca de 10 minutos para um novo bloco de ELCASH ser minerado. Isto poderia ser considerado suficientemente rápido para uma simples transferência para um amigo seu, mas seria inconveniente para pagamentos no comércio retalhista. É por isso que a ELCASH implementa uma camada de transação rápida, cortando o tempo necessário para uma transferência para tão pouco quanto 10 segundos, colocando a ELCASH entre os líderes na indústria blockchain. Este tempo pode variar em função do congestionamento da rede.

No topo da rede é criada uma camada de transação rápida (Camada 2) de masternodes (nós mestres) para melhorar a velocidade de transação. Os masternodes verificam se uma transação recentemente criada é válida e asseguram que a transação é irreversível, mesmo antes de ser adicionada a um novo bloco, bloqueando as entradas e partilhando a informação sobre a mesma com todos os nodes (nós). Graças a isto, é prometido à rede que a transação será incluída nos próximos blocos minerados.

A Camada 2
Permite transações rápidas.

Camada 1
Camada de consenso (PoW) assegura a integridade do blockchain executando o algoritmo de consenso entre os participantes.

Camada 0
Camada de blockchain é da maior importância para a escabilidade, segurança e privacidade da rede.

Camada de Hardware
permite protocolos eficientes e outras camadas.

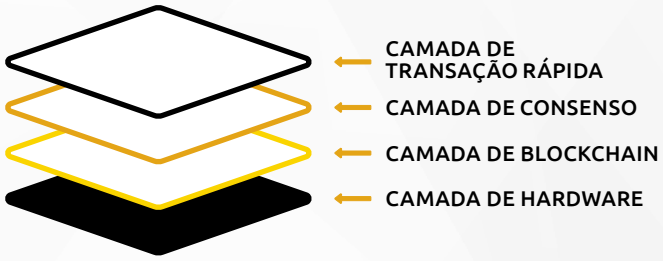

Figura 20. Arquitetura do ecossistema blockchain da Electric Cash (8).

Esta solução de camada rápida permite transações rápidas e garante um elevado nível de segurança da rede. As transações são transmitidas para o blockchain principal utilizando a camada 2, onde as transações são confirmadas antes de serem aprovadas pelos mineiros de "PoW". Todas as transações na rede Electric Cash são processadas pela camada de transação rápida, o que significa que todas as transações ELCASH são rápidas, sem taxas adicionais e sem necessidade de qualquer intervenção especial por parte de um utilizador.

O processo pelo qual cada transação passa é semelhante a uma validação de transação padrão, mas contém algumas etapas adicionais, onde os masternodes bloqueiam a transação (Figura 21).

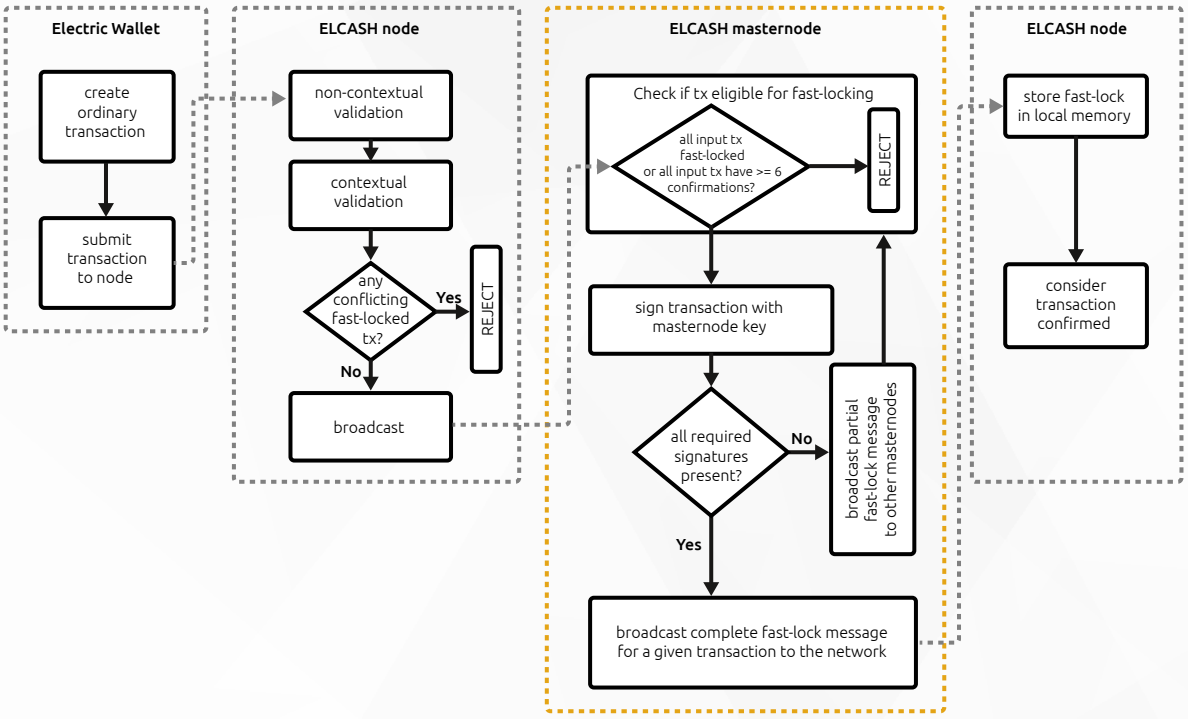

Figura 21. Processo de confirmação da transação rápida

Depois de um utilizador criar uma nova transação na carteira, a transação é submetida a um node (nó) ELCASH. A transação é validada e se não existirem transações em conflito, a transação é enviada pelo node ELCASH para o masternode ELCASH, caso contrário o node rejeita-a. O masternode verifica a elegibilidade da transação para um bloqueio rápido. Se a transação for aprovada, é assinada com a chave do masternode pelos masternodes. Esta parte do processo evita o gasto duplo dos activos cripto. As entradas da transação são bloqueadas de modo a só poderem ser gastas numa transação específica e uma vez bloqueada a transação, não é possível enviar os mesmos activos duas vezes ou alterar a transação de maneira alguma. Todos os nodes são informados de que a transação está bloqueada e será acrescentada ao blockchain com os blocos seguintes.

Se for alcançado o consenso sobre um bloqueio pela camada do masternode, todas as transações ou blocos em conflito serão rejeitados, a menos que correspondam à identificação exata da transação de bloqueio em questão.

Graças a tal solução, seria muito mais conveniente utilizar ELCASH na vida quotidiana, quer seja a pagar as compras numa loja ou apenas a enviar ELCASH a amigos. Além disso, o blockchain da Electric Cash ainda opera no consenso seguro de “Proof-of-Work”.

3.2. Transações gratuitas

As criptomoedas, por mais seguras que sejam, são frequentemente dispendiosas de utilizar, especialmente quando o projeto ganha popularidade e a utilização da rede aumenta. Isto causa uma situação em que quanto mais popular o projeto, mais dispendioso se torna o seu uso. Menos novos utilizadores estão dispostos a participar, impedindo assim o crescimento do projeto. Para conseguir a adoção global, os projetos precisam de atingir uma massa crítica, ou seja, um certo número de utilizadores que façam a rede apelativa para a adesão. Projetos como criptomoedas ou plataformas de redes sociais tornam-se mais úteis com cada novo utilizador, porque é possível ligar-se a mais pessoas. Na realidade, se o projeto se limita com o aumento das taxas de transação enquanto mais utilizadores estão na rede, torna a adoção global difícil ou mesmo impossível de alcançar (9).

A este respeito, as funcionalidades de transação da Electric Cash são um fator crucial para a adoção em massa de criptomoedas. Uma solução rápida e gratuita implementada compete não só com outros projetos blockchain, mas também com as instituições financeiras tradicionais.

3.2.1. Mecanismo de validação das transações

As transações gratuitas são realizadas graças à arquitetura do blockchain: durante o processo de staking, os stakers geram o “limite de transação livre” para gastar. A taxa é aplicada às transações e isto tornará os ataques maliciosos à rede mais difíceis de aplicar. No entanto, os utilizadores de staking serão elegíveis para algumas transações gratuitas, dependendo dos seus activos cripto colocados em staking e da duração de staking.

As transações gratuitas são ligeiramente diferentes das transações normais. Contêm informação adicional sobre o a UTXO de staking do remetente, para confirmar que o utilizador é elegível para uma transação gratuita (Figura 22).

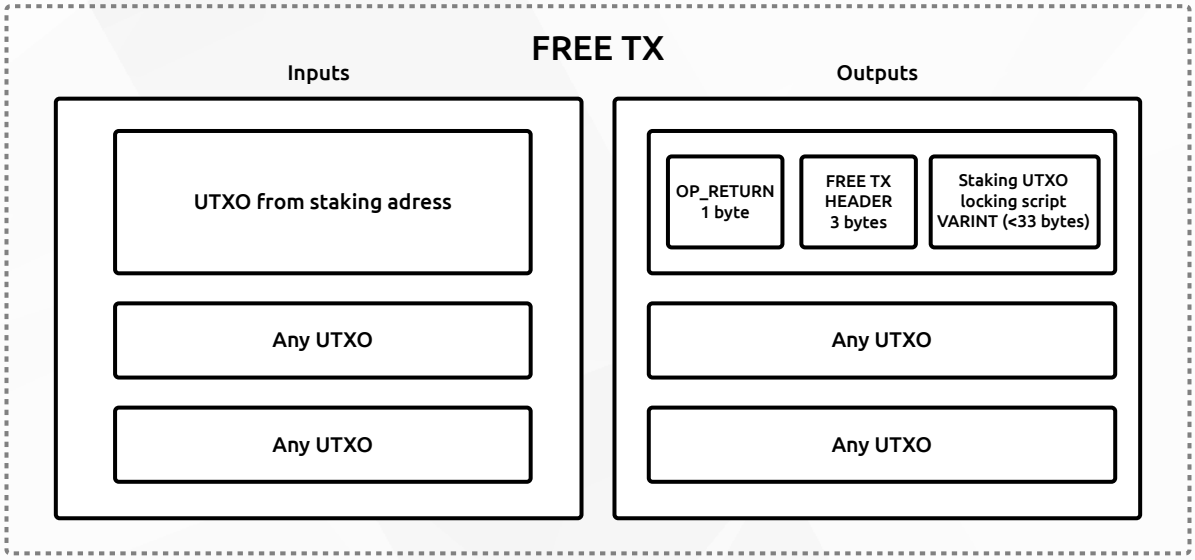

Figura 22. Estrutura da transação gratuita

Regras de validação não-contextuais:

1. OP_RETURN + O cabeçalho de transação gratuita é a primeira saída da transação (tx)
2. Todas as regras normais para a transação

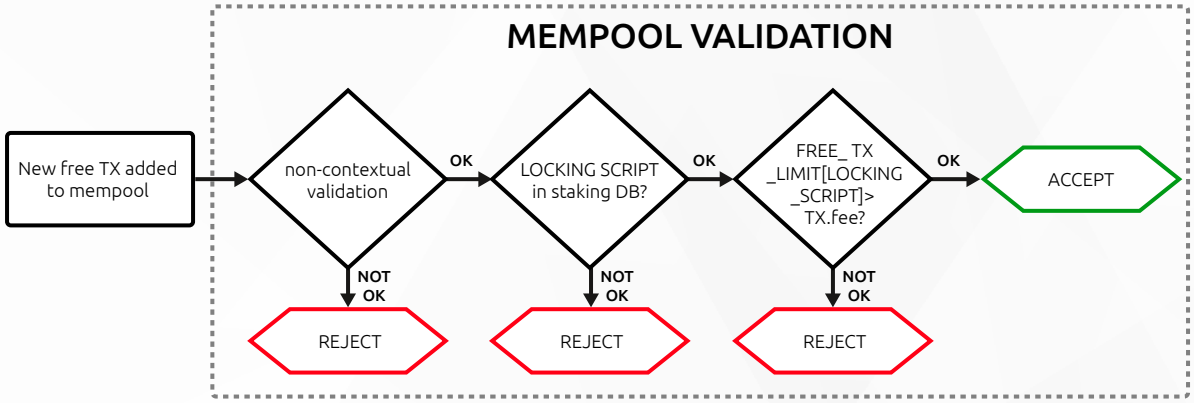

Figura 23. Validação de transações gratuitas na mempool

Como em todas as outras transações, as transações gratuitas aguardam na mempool para serem adicionadas a um novo bloco. No entanto, para além da validação padrão, a elegibilidade do remetente para efetuar transações gratuitas é também verificada. Se a transação estiver correta e o remetente for um staker com um limite suficiente de transações gratuitas, a transação é aceite e adicionada a um novo bloco.

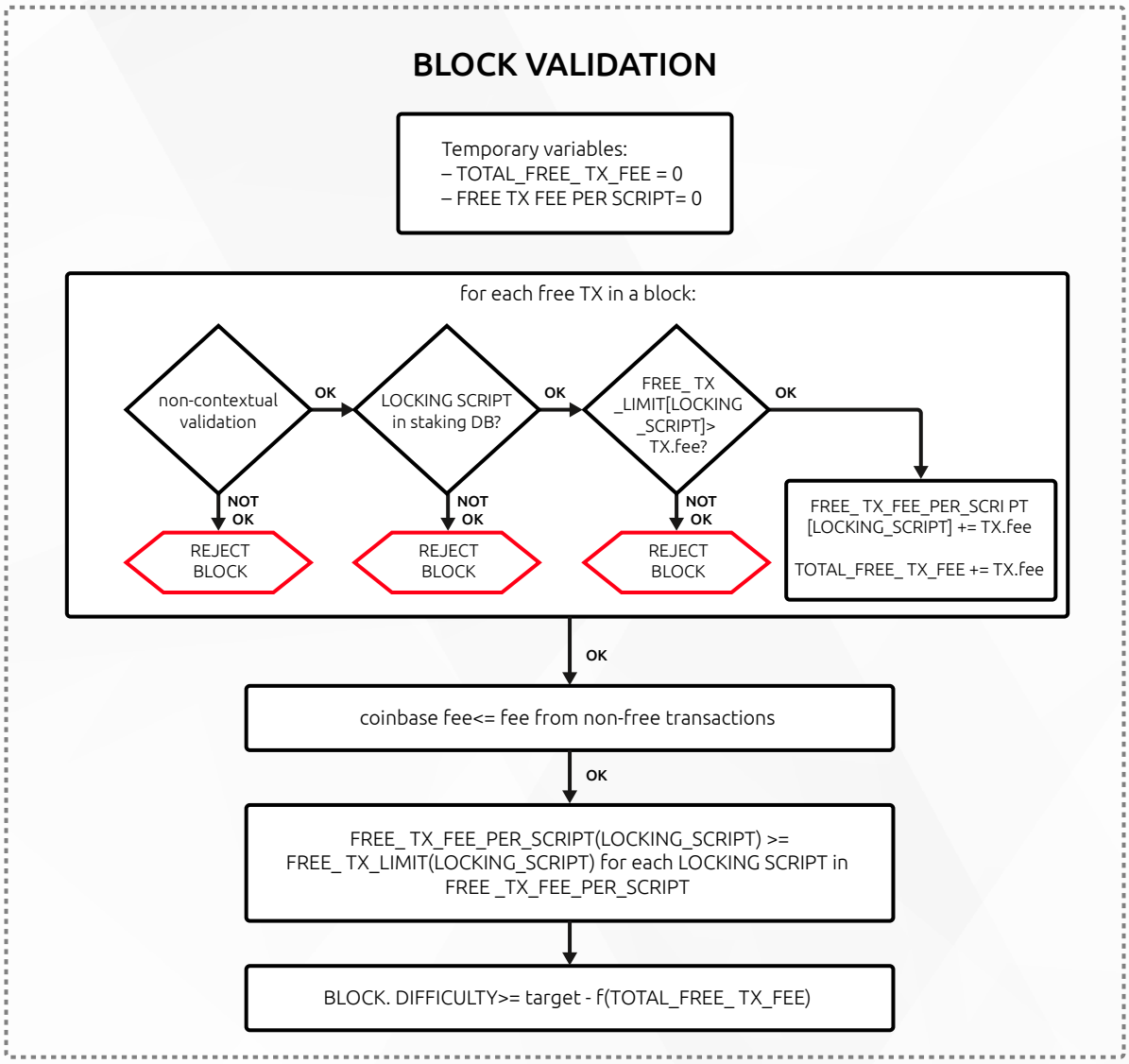

Figura 24. Cálculo da dificuldade do bloco

Para cada transação gratuita num novo bloco, o protocolo calcula que taxa seria cobrada se a transação não fosse gratuita e acrescenta todas as taxas estimadas (Figura 24). Para compensar os mineradores por aceitarem uma transação gratuita num bloco, a dificuldade do bloco é reduzida com base na soma das taxas estimadas das transações gratuitas.

Limite de transações ELCASH gratuitas

O blockchain ELCASH cobra taxas de transação, mas todos os utilizadores que fazem staking de ELCASH são elegíveis para algumas transações gratuitas por dia. O limite de transações gratuitas depende dos parâmetros de staking do utilizador.

Isto ajuda a manter a rede segura contra sobrecargas maliciosas, tornando os ataques dispendiosos, enquanto os utilizadores genuínos são capazes de fazer transações gratuitas.

Os mineradores não são sobrecarregados com trabalho adicional sem recebrem uma recompensa. Se for feita uma transação gratuita, a dificuldade de mineração é automaticamente reduzida proporcionalmente ao valor da transação gratuita incluída no bloco. Como resultado, as recompensas totais e finais dos mineradores não serão afetadas em nenhum sentido pelas transações gratuitas e o trabalho adicional dos mineradores será recompensado em conformidade.

Cálculo do limite

Cada stake tem um limite diário de tamanho de transações gratuitas. Este limite depende do valor e do prazo do stake. [tx_limit] ∈ N → STAKE_WEIGHT≥1.

Os pressupostos do protocolo devem ser: STAKE WEIGHT = 1 (o stake mínimo recebe um limite para efetuar 1 transação (tx) grátis / dia), e 5 ELCASH para um stake de um mês, é também o stake mínimo exigido para receber um limite;

stake_weight = (stake_period[blocks])/4320×(stake_value[ELCASH])/(5 ELCASH)

Por exemplo:

5 ELCASH para um stake de 12 meses:

stake_weight=510840/4320×5/5 ≅ 12 transações (tx)/dia

O limite de transações (tx) gratuitas não se acumula. O limite não utilizado para um determinado dia não pode ser utilizado após o fim desse dia. As transações (tx) gratuitas estão disponíveis para o utilizador 20 blocos após o início do staking.
No momento em que o staking termina ou é terminado pelo utilizador, o acesso às transações (tx) gratuitas é perdido.

3.2.2. Detalhes técnicos das transações gratuitas

Sintaxe das transações gratuitas

1. Uma das saídas são os metadados que apontam para o endereço de staking
2. Uma das entradas provém do endereço apontado no ponto 1
3. As transações não contêm fisicamente uma taxa. Não são necessárias devoluções.

Execução das transações gratuitas

1. É necessária uma configuração de carteira única (uma transação interna que pode ser executada no momento em que um depósito é colocado em staking) a fim de se poder executar transações gratuitas
2. O utilizador deve especificar um endereço de staking do qual será retirado o limite (isto pode ser feito automaticamente através de uma carteira)
3. O utilizador deve ter pelo menos uma stake ativo

Compensação do minerador

1. O minerador não receberá taxas de e para transações gratuitas
2. Os blocos contendo transações gratuitas terão as suas necessidades de dificuldade reduzidas. A dificuldade de mineração modificada para um determinado bloco é expressa como:

MODIFIED_DIFFICULTY= (1-FTX×TXS_total)×PoW

FTX – coeficiente da transação gratuita
TXS_total – tamanho total do bloco da transação gratuita
PoW – consenso de "Proof-of-Work"

3.3. Estratégia da redução de blocos e recompensas

A mineração de Electric Cash é lançada a partir de um novo bloco génesis. A estratégia apresentada na Tabela 1 visa satisfazer a procura esperada do mercado para a moeda, ao mesmo tempo que evita o excesso de oferta (durante os primeiros anos.

Prevê-se que a pré-mineração continue até que 10% da fornecimento total seja minerado e distribuído por atividades incluindo, mas não se limitando a, desenvolvimento de projetos, marketing, esforços promocionais e outros.

Esforçamo-nos por prevenir quaisquer atividades indesejáveis que possam surgir logo no início da existência da moeda, quando a moeda e o seu ecossistema ainda não estiverem consolidados. O plano para proteger os já mencionados 10% do fornecimento total da ELCASH também inclui o benefício adicional de desencorajar a manipulação do mercado por potenciais detentores de volumes substanciais de ELCASH.

Table 4. Block reduction and rewards strategy.

Período	Data	Blocos	Recompensa por bloco	Moedas
1	December 2020	4 200	500	2 100 000
2	January 2021	52 500	75	3 937 500
3	January 2022	52 500	70	3 675 000
4	January 2023	52 500	65	3 412 500
5	January 2024	52 500	55	2 887 500
6	January 2025	52 500	40	2 100 000
7	January 2026	52 500	25	1 312 500
8	January 2027	52 500	15	787 500
9	January 2028	52 500	7.5	393 750
10	January 2029	52 500	3.75	196 875
…	…	…	…	…

As moedas pré-mineradas serão utilizadas em várias atividades que têm um objetivo principal: atrair atenção e utilizadores para o ecossistema ELCASH. É uma solução comum e amplamente aceite para projetos de distribuição de um número designado de moedas para atividades de comercialização e desenvolvimento. Acreditamos que esta solução

proporcionará uma forma saudável de financiar o desenvolvimento do projeto e criará um futuro mais brilhante para o ecossistema blockchain.

Exemplos de alguns casos de utilização real – para os 10% pré-minerados do fornecimento total da Electric Cash:

- Airdrops promocionais
- Desenvolvimento do negócio
- Recompensas adicionais para os stakers
- Esforços de marketing
- Anúncios nas redes sociais
- Orçamento de software

Durante o primeiro ano, a recompensa por bloco ascenderá a 75 moedas. Cada período subsequente irá diminuir gradualmente. Após sete anos, a rede passará para uma estratégia de recompensas denominada "halving" (redução para metade), em que a recompensa do bloco será reduzida em 50% todos os anos a partir dessa altura.

O fornecimento total da Electric Cash está atualmente limitado a 21 000 000 moedas, idêntico ao fornecimento total da Bitcoin. Um fornecimento fixo ajuda a minimizar a potencial inflação e diluição. No entanto, se o projeto ganhar popularidade no futuro e a procura da moeda crescer, os utilizadores mais ativos da rede poderão aumentar a oferta através do voto democrático graças às ferramentas do sistema de governação, tendo em conta que isto pode resultar numa pequena inflação.

3.4. Fundo de Tesouraria para Desenvolvimento

O projeto ELCASH implementa um Fundo de Tesouraria para Desenvolvimento dedicado que constitui 10% das recompensas de mineração recolhidas numa carteira especial gerida pelo sistema de governação da Electric Cash. Os activos são mantidos em segurança até que a comunidade vote para os gastar. Pode cobrir os custos das melhorias e mudanças do protocolo, tais como o desenvolvimento de novas funcionalidades no ecossistema da Electric Cash. Para manter todo o processo transparente, o saldo dos activos recolhidos é apresentado no "Governance Explorer" (Explorador de Governação).

Electric Cash roadmap

Sumário

Neste documento, introduzimos a Electric Cash (ELCASH). O objetivo do projeto é fornecer um ecossistema abrangente e resolver vários problemas importantes na indústria das criptomoedas. A ELCASH facilita os pagamentos diários. Ao implementar a Camada 2 adicional ao blockchain, pode realizar transações rápidas, garantindo ao mesmo tempo a segurança da rede. Graças a esta solução, uma transação ELCASH pode ser processada em cerca de 10 segundos (dependendo do congestionamento da rede), o que torna a rede Electric Cash uma das líderes na indústria de blockchain. Os utilizadores não precisam de tomar quaisquer ações adicionais para enviar uma transação rápida, todas as transações são rápidas por predefinição.

O protocolo ELCASH, concebido para ser acessível e simplificado, também se foca na redução das taxas de transação. Todos os participantes da staking são recompensados com transações gratuitas, que são concedidas com base na dimensão e longevidade de stake total. Transações rápidas e gratuitas tornam a ELCASH perfeita para pequenos pagamentos diários, o que abre muitas oportunidades para a adoção global de criptomoedas.

O ecossistema não só introduz pagamentos rápidos e gratuitos, mas também benefícios adicionais como o Poder de Governação. Ao participar ativamente na rede, cada detentor de moedas ganha Poder de Governação (PG) e pode ter um impacto direto nas mudanças de protocolo. O PG é distribuído em função dos parâmetros de stake do utilizador e da atividade da rede. Dá o direito de participar no processo de governação e de votar

nas propostas disponíveis. Graças à governação comunitária, o projeto pode reagir rapidamente às necessidades do mercado e introduzir mudanças mais rapidamente. Acreditamos que este ecossistema descentralizado e centrado na comunidade irá garantir um crescimento saudável e uma perspetiva global de um projeto a longo prazo.

Fontes

Para saber mais sobre o projeto, visite:

Site: electriccash.global
Twitter: twitter.com/elcash_official
Telegram: t.me/elcash_official
Facebook: facebook.com/electriccash.official
GitHub: github.com/electric-cash
YouTube: youtube.com/c/ElectricCash

Referências

1. Nakamoto, S. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf: s.n., Oct 2008.
2. N. Papadis, S. Borst, A. Walid, M. Grissa, and L. Tassiulas. Stochastic models and wide-area network measurements for blockchain design andanalysis. IEEE Conference on Computer Communications: IEEE INFOCOM, 2018.
3. A Next-Generation Smart Contract and Decentralized Application Platform. [Online] December 2020. https://ethereum.org/en/whitepaper/.
4. N Papadis, L Tassiulas. Blockchain-based Payment Channel Networks: Challenges and Recent Advances. New Haven, CT 06511 USA: Department of Electrical Engineering, and Yale Institute for Network Science, Yale University, 2020.
5. N Kshetri, J Voas. Blockchain-Enabled E-Voting. University of North Carolina at Greensbor: IEEE SOFTWARE, 2018.
6. L Gudgeon, P Moreno-Sanchez, S Roos, P McCorry. SoK: Layer-Two Blockchain Protocols. London: Imperial College London, 2019.
7. Zamyatin, A. Merged Mining: Analysis of Effects and Implications – DIPLOMA THESIS. s.l.: TU Wien, 2017.
8. Shapiro, C. Information rules: a strategic guide to the network economy, 1999.
9. Shapiro, C. Information rules: a strategic guide to the network economy, 1999.