electric cash

Whitepaper v2.0.2

electriccash.global

2021

Table of Contents

Legal disclaimer

This document is not a final technical specification.

The project presented herein is in its initial, conceptual phase and can be modified, changed, or even abandoned (e.g., for economic, technological or regulatory reasons) and nothing in this document shall be considered as a final and binding description or view of the project, offer of services, or any of its parts or components, or with regard to its execution.

This document does not constitute financial advice.

Information in this document (Whitepaper) is not to be considered as investment advice. The cryptocurrency market is highly volatile. You should carefully consider whether cryptocurrency is right for you considering your circumstances and financial resources. By following the rest of the document (Whitepaper), you acknowledge that you have not sought investment advice from the author, or any parties formally connected to the author, as said author and parties may not provide such advice. You are not expected, or offered, to invest, buy, or perform any related financial activities in any shape or form based on any information in this Whitepaper, and you acknowledge that any such actions are solely your responsibility.

Electric Cash Whitepaper

Eyal Avramovich
Whitepaper v2.0.2

Abstract. In 2009 the first cryptocurrency, Bitcoin (1) was released. Today, 11 years later, despite breaking price records, neither Bitcoin nor any other cryptocurrency has yet seen mass adoption. Most cryptocurrencies, although secure, are not designed to function like cash. Transactions are not efficient, tend to be expensive, and the user experience is still a secondary issue for many projects. However, new technological solutions allow us to design a better cryptocurrency that is as secure as most blockchains, but also fast and free to use. In this paper, we introduce a new decentralized fast payment protocol – Electric Cash (ELCASH) – a SHA-256 based coin, designed to be cash-like, for everyday use. Its fast and free transactions for stakers, make it the perfect means of exchange and a great tool for daily payments. In addition, the governance mechanism of the Electric Cash protocol gives its coin holders the power to decide on the future of the ecosystem development. We believe that this approach fills an existing gap in the market and can meet the expectations of a wide range of users.

1. Introduction

1.1. Problem statement and solution approach

Blockchain fees

The first cryptocurrency, Bitcoin, implemented a simple, yet quite reliable mechanism of transaction fees designed to protect the network from spam. Transaction fees can vary and depend on several factors, including network congestion, transaction confirmation times and transaction size. When the network load is low, all transactions are processed quickly for minimal fees. The fees are low enough for there to be little-to-no cost for an individual to request a transaction. As the load increases and approaches pre-defined limits, the demand for transaction confirmation increases to the point that the miner can increase the fees charged (2). Many recent projects copied this design without solving the problem of fees increasing along with the growth of the network.

Today, as many of them have gained in popularity, they are burdened with high transaction fees. In some cases, they can cost up to dozens of dollars per transaction. Such cost makes them unprofitable for everyday use, discouraging both new and existing network participants from using them.

In the case of Proof-of-Work cryptocurrencies, fees are used to protect networks from malicious overflooding and for prioritizing transactions added to the blockchain. The same applies to the ELCASH protocol. However, the ELCASH solution rewards users who actively participate in the network enabling free transactions for stakers. Users who stake ELCASH are eligible for some free transactions every day depending on their staking parameters.

Blockchain performance

Although blockchain has gained in popularity in the financial world, its actual usefulness as a distributed trusted technology is hindered by its lack of scalability (3). Most Proof-of-Work blockchains have a limited transaction processing capacity. With the increase in popularity and use of the network (more transactions are being placed on the blockchain), the network's ability to process those transactions in a timely manner diminishes. Most of the PoW consensus cryptocurrencies considered to be the most secure are therefore rarely used on a daily basis, but rather as a substitute for gold. Other cryptocurrencies, such as Ethereum (4), realized this problem and are shifting from Proof-of-Work to Proof-of-Stake consensus.

Many solutions have been proposed to date. In this project, we have implemented the most promising one: the so-called "fast layer" system to improve the blockchain throughput. We combine the best of two worlds, i.e., blocks are mined in Proof-of-Work, which makes the blockchain secure, but transactions can be processed on a second layer (L2) of blockchain, which makes them almost instant (5).

Community influence

Projects in the crypto environment are usually governed by the blockchain team or core developers, so they are centrally governed. Decisions regarding any further development and network changes are controlled and taken by a relatively small number of individuals. Many mainstream users either don't have a say or enough influence in decision making due to a lack of technical knowledge or financial leverage.

Electric Cash has changed that by establishing a Development Fund Treasury. It is created from a fraction of Proof-of-Work mining rewards and stored in such a "Treasury." Additionally, the Electric Cash community members receive Governance Power. This allows the network to be decentralized where decisions on future project developments and use of funds from the Development Fund Treasury are driven by the project's community. That network democracy is achieved thanks to the blockchain's built-in voting mechanism (6).

2. Electric Cash ecosystem

Electric Cash is a SHA-256 based coin designed to be a cash-like cryptocurrency for everyday use with an additional staking feature. The Electric Cash protocol is governed by its coin holders, who are eligible to manage the future development of the ecosystem. All these aspects are integrated under one ecosystem, allowing Electric Cash to cover a wide variety of market and user needs.

STAKING

GOVERNANCE

SECOND LAYER

To incorporate incentives dedicated not only to miners, but also to other network users, Electric Cash block rewards are divided into three parts. The first and the biggest reward goes to Proof-of-Work miners. Miners are crucial to ensuring that the network functions properly and that it is safe. But miners are not the only stakeholders. People who use the network on a daily basis and expand the ELCASH ecosystem are essential for the project growth.

ELCASH coin as an integral part of ecosystem

The key aspect of the ELCASH coin is its long-term offer to every active user.
A comprehensive ecosystem was therefore designed where staking coins unlock rewards and additional possibilities. Thanks to the governance system, internal resources can be spent on network improvements.

To achieve such a system, a unique distribution model (Figure 1) was implemented into the protocol, allowing all network users to be rewarded for their contribution, i.e.:

- After the initial pre-mining (accumulating allocated coins according to the coin distribution plan) is over, the largest part, 80% of the total coin supply is allocated to miners.
- 10% of the total supply is used for staking rewards.
- 10% of the total supply is allocated to the Development Treasury Fund. This is intended to be used for future developments (protocol improvements). The network community members (users who stake and gain GP) are the only people with the right to manage it (i.e., by voting).

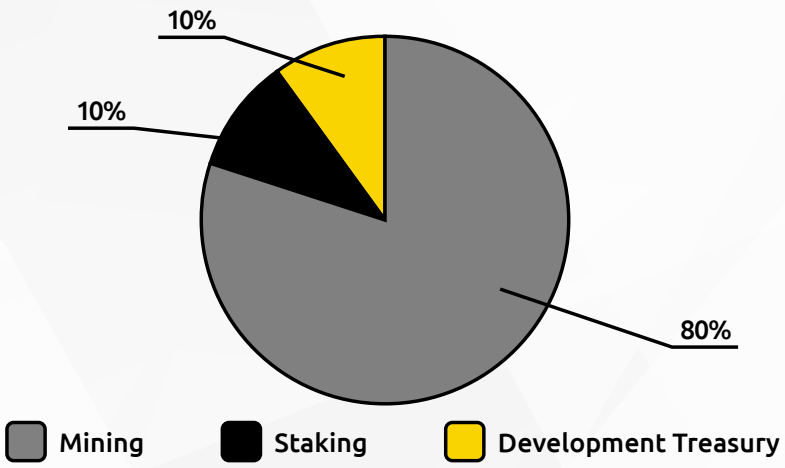


Figure 1. Block rewards distribution

We believe that this approach will attract miners at the launch. As a result, by the end of the bootstrap phase, there should be enough coins in circulation and a significant amount of hash power securing the network so that other network functionalities can be used and facilitate mass adoption in daily use.

2.1. Staking

One of the core features of Electric Cash is staking. It allows a sound governance system to be created for our users and incentivizes positive behavior from the network participants. Staking is a form of storing funds. By staking, every user can actively contribute to the network growth in the long run and help prevent the oversupply problem that could affect the overall inflation issue in the years ahead. This in turn increases the network stability.

2.1.1. Staking process

Electric Cash network participants can stake ELCASH to govern the network and earn rewards from the staked amount. ELCASH staking also rewards users with additional benefits (Figure 2) such as free transactions and Governance Power (GP).

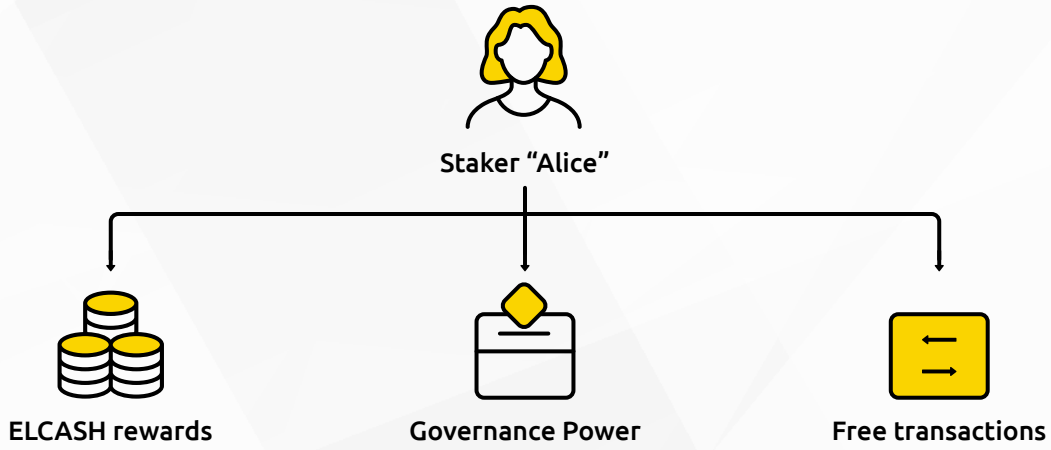


Figure 2. Electric Cash Staking benefits

Every user that owns ELCASH can manage the whole staking process from their Electric Cash Wallet. The user has full control over the funds and makes the staking agreement directly with the protocol.

2.1.2. Staking parameters

The rules of the staking process are the same for every participant and every stake value. Each user can choose a fixed staking contract, which corresponds to specific interest rates, and its duration.

Table 1. ELCASH staking interest (per annum) according to contract periods.

~Days	Blocks	~Reward [% p.a.][1]
30	4,320	5
90	12,960	6
180	25,920	7.25
360	51,840	10

Since blockchain operates on the number of blocks, the duration of the staking is calculated in blocks rather than as a unit of time. The number of days shown in the table above is estimated based on the average new block time, which is about 10 minutes for the Electric Cash blockchain.

1 Note. Given values are estimated numbers only and may slightly differ over the duration of the contract due to network variables.

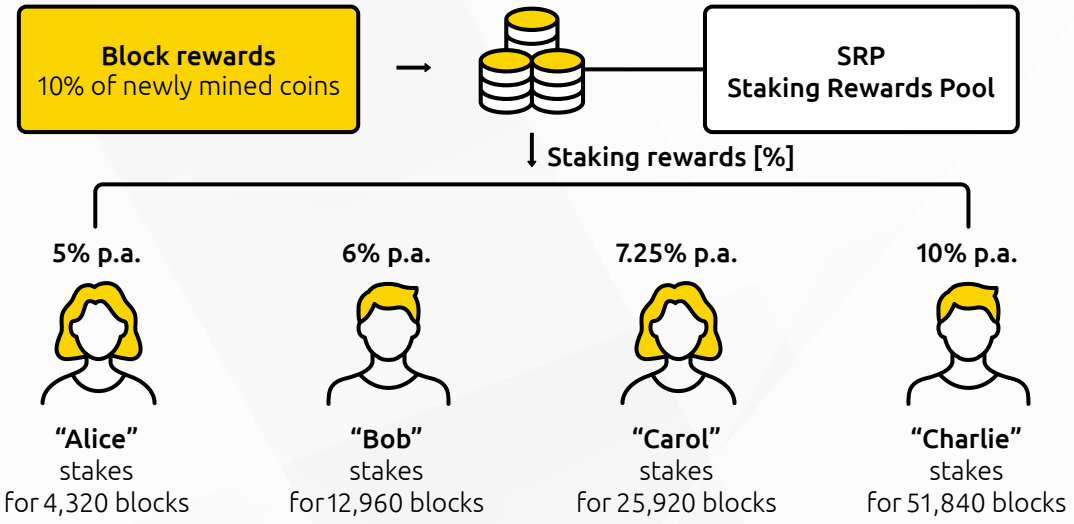


Figure 3. Rewards rates according to the stake duration

The staking rewards differ depending on the duration of the contract – the longer the period of staking, the higher the staking rewards. Rewards are calculated per block and the value allocated to the user is shown in their wallet. The staking rewards are an approximate value per annum; the final rewards might differ slightly.

To avoid a severe rounding error, the minimum value that can be staked is 5 ELCASH. There is no fixed maximum value.

2.1.3. Staking Rewards Pool (SRP)

In the Electric Cash protocol, staking rewards come directly from Proof-of-Work mining rewards. 10% of each new mined block reward is taken from and goes to the Staking Rewards Pool (SRP).

The rewards can only be transferred to the stakers after the locking (staking) period ends. Early contract termination results in the loss of the rewards earned to date and a penalty charge. Rewards that are not accrued stay in the pool and are subsequently distributed among all active stakers and the penalty is transferred from the user to the SRP.

Staking Rewards Pool details:
In the variable containing the value of the Staking Rewards Pool (SRP) after each block, the following actions take place:

- The value of the SRP is incremented by 10% of the block rewards.
- The value of the SRP is incremented by the early withdrawal penalties and funds that were locked and set aside for the staker that terminated the stake.
- The value of the SRP is decremented by staking rewards that are set aside for all the stakers who have active staking agreements.

All the data about the value of stakes is kept in the staking database (sDB), which is a representation of the Electric Cash blockchain and is automatically updated, so all the data is secured. After each block, the database is updated by the following actions:

- If a transaction for a new stake is found, it's added to the database.
- If the staking period for a given entry has ended, or an early payout (unstake) has been found, it is removed from the database.
- All staking rewards (percentage) are calculated and added to each entry (each active stake), according to the staked amount.

Note. The database acts merely as a more convenient representation of the blockchain, but it is possible to restore all the data from the database using the blockchain.

2.1.4. Staking Wallet

The core element of the Electric Cash ecosystem is a user-friendly and intuitive wallet (Figure 4). The wallet application includes a Spending and a Staking Wallet. The Staking Wallet allows users to easily stake their coins to receive Governance Power, free transactions and staking rewards.

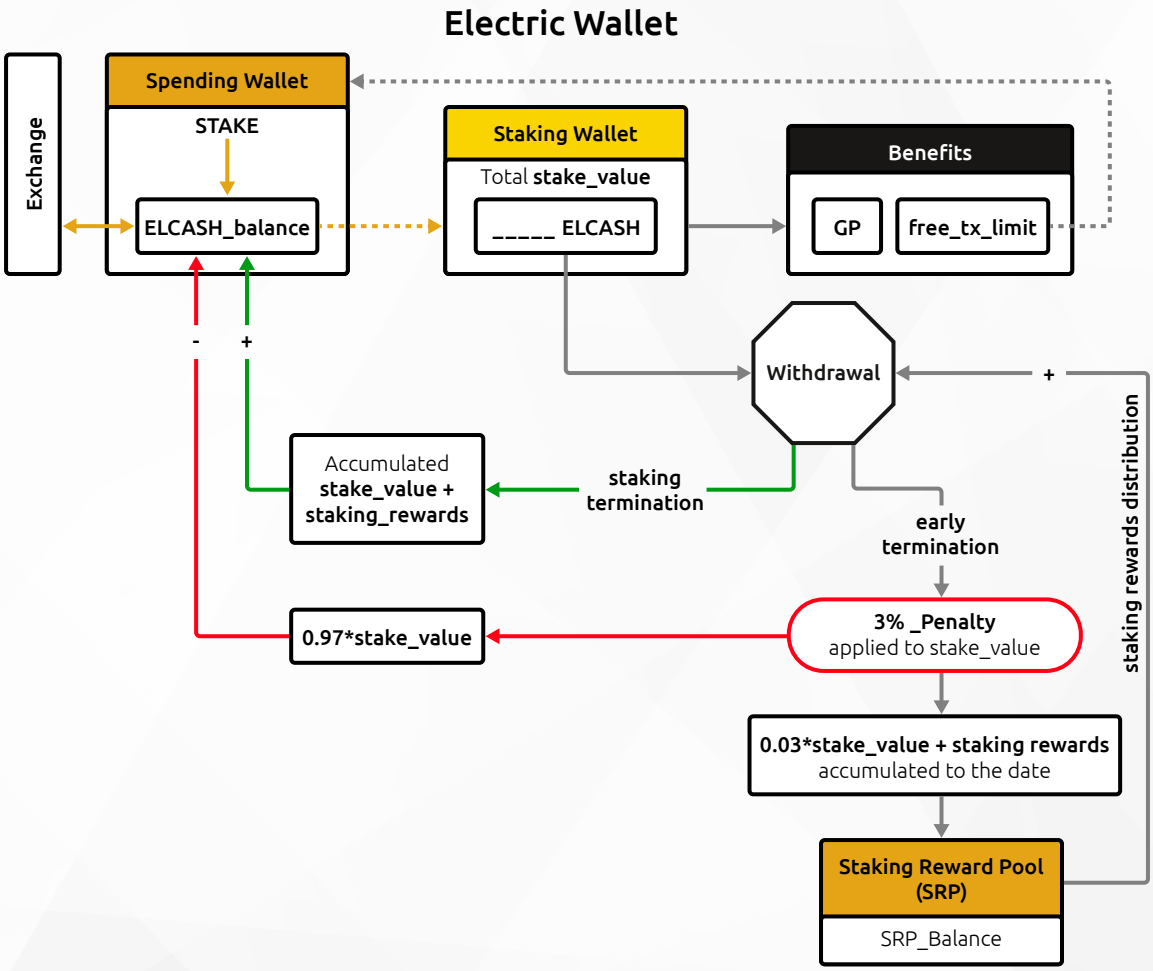


Figure 4. Electric Cash Staking process

Staking Wallet does not have a separate address from Spending Wallet. One seed secures and recovers both. Staking Wallet is a UTXO instance at the Spending Wallet address. It acts as a value recognized by the blockchain as separate but stored at the same address.

When creating a new stake (Figure 5), initiating a transaction takes inputs from the user's Spending Wallet and creates outputs with all staking parameters, and then a new staking UTXO with the staked funds is created. If the funds from the Spending Wallet were higher than the staked amount, the change is also put in the new spending UTXO.

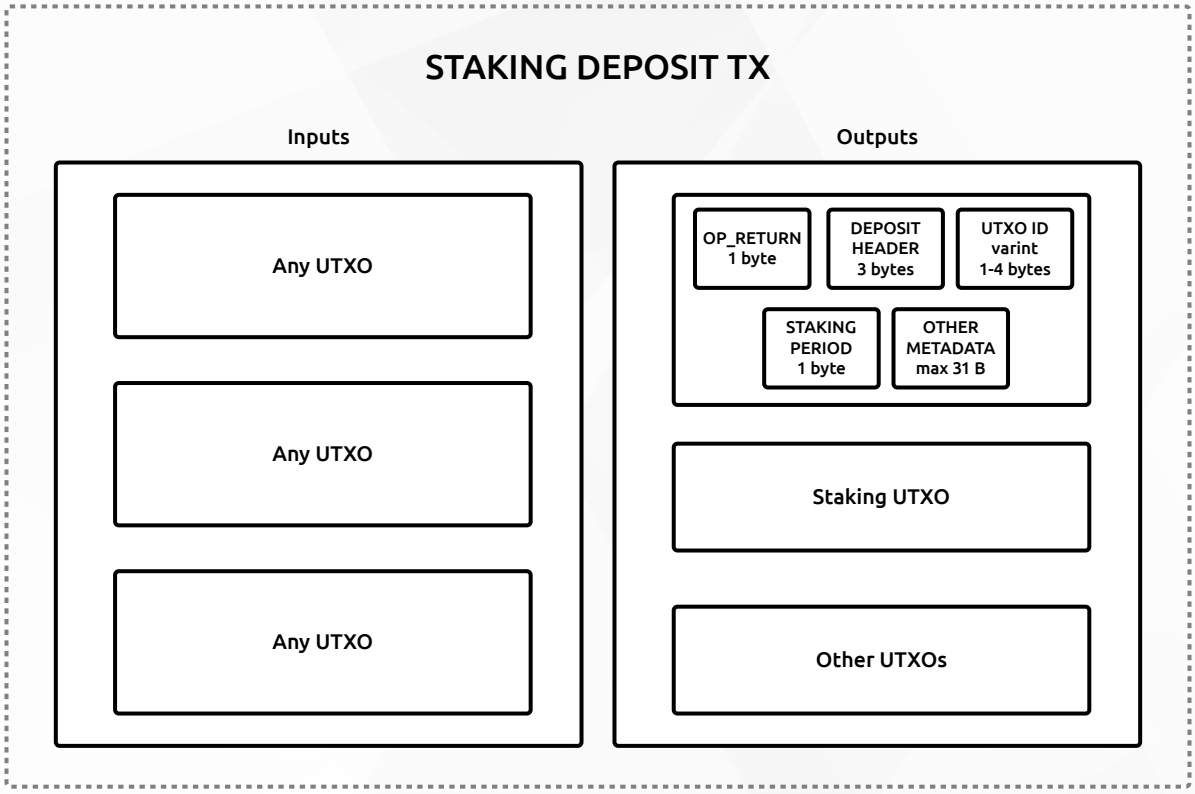


Figure 5. Transaction initiating staking

Validation rules:

1. OP_RETURN + staking header is the first output of the tx
2. UTXO ID > 0
3. Staking period ≤ 4 (index to a lookup table)
4. Staking UTXO amount must be ≥5e8 sat
5. All the normal rules for transaction

When the staking ends, the protocol checks whether the stake has matured or was terminated by the user. If it was terminated prematurely, the penalty is imposed, and the staking rewards are not transferred to the user. If the stake has matured, the funds from the staking UTXO and the rewards UTXO are transferred to the spending UTXO as shown on the diagram below (Figure 6).

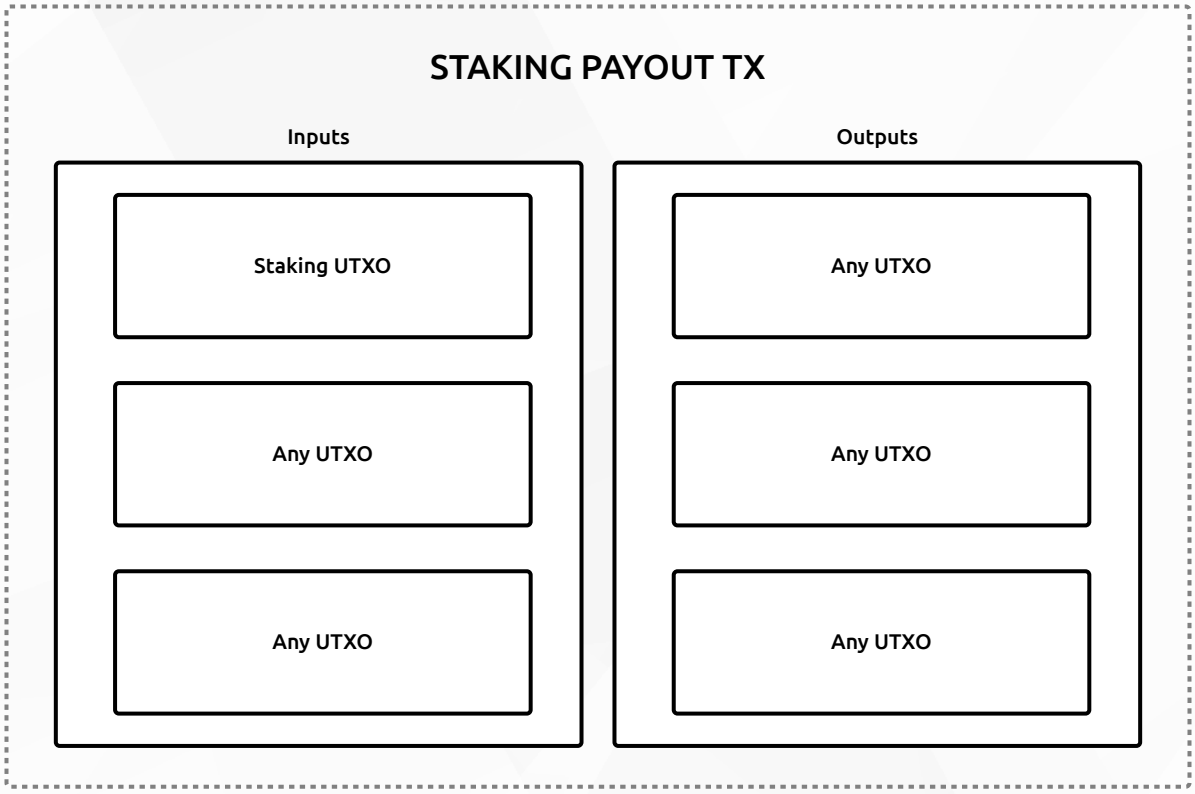


Figure 6. Transaction with staking payout

Validation rules:

1. Check if any staking UTXOs: check if input TX is staking deposit TX (check first output)
2. Check if staking period was fulfilled (current block height ≥ {block height of input UTXO + staking period})
   a. If **yes**: check if output value is less than {inputs + staking reward} (calculate staking reward)
   b. If **no**: check if output value is less than {inputs – staking penalty} (calculate staking penalty)
3. All the other normal rules for transaction

A staking burn transaction is utilized for transferring funds from ordinary UTXOs to the Staking Rewards Pool. The main reason for introducing it is to provide a way to fill up the Staking Rewards Pool after the staking hard fork, with the due mining reward percentage from the period before it.

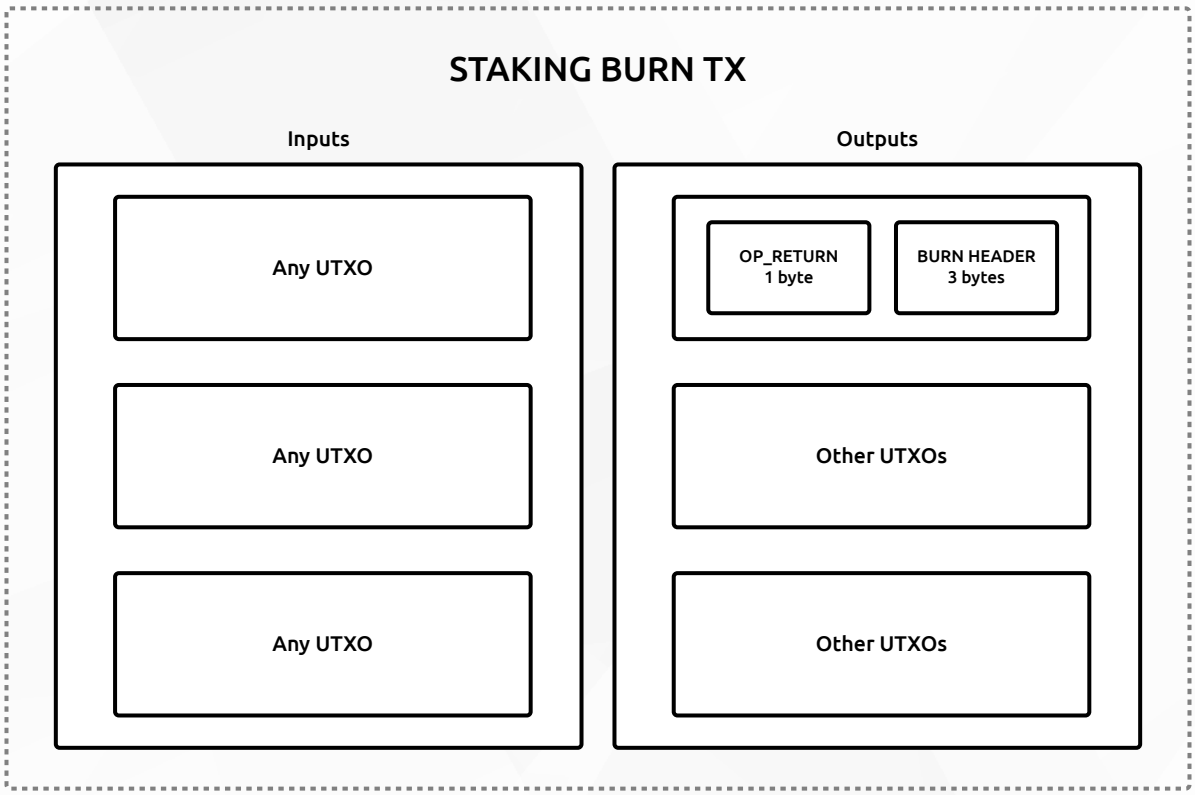


Figure 7. Staking burn transaction

Validation rules:

1. OP_RETURN + burn header is the first output of the tx
2. SUM(inputs)≥SUM(outputs) + burn_amount:
   Staking period as an index to a predefined table containing the number of blocks

Note: Users are in constant control of the funds and the private key related to both the Staking and Spending Wallet; therefore, the security is as strong as the user's personal standards.

2.1.5. Withdrawal

After the staking is completed, a staker will be able to claim the reward using the staking payout transaction. All participants are required to wait until the staking period ends to withdraw their funds [staked amount + staking rewards], otherwise, a fixed **3% penalty** will be imposed. **The aim of the penalties is to protect free transactions on the network from being abused, to stop people voting from outside the network, and to prevent the ELCASH economy being disrupted.**

Early withdrawal of funds results in penalties and the loss of the rewards earned to date. No reward is accrued before the completion of a predefined staking period. The rewards that are not accrued and penalties taken from the user will be sent back to the **Staking Rewards Pool (SRP)** and subsequently distributed among other stakers holding their position.

2.1.6. Rewards and penalties calculations

The Staking Rewards Pool and individual staking rewards are updated for each new block. The protocol calculates all rewards that users should be paid and, on this basis, checks the state of the SRP. Simultaneously, the protocol checks if the stake has matured and, if so, the rewards are sent to the user. If the stake is still ongoing, the protocol sends the information to the staking database and the rewards gathered by the user are updated (Figure 8).

Table 2. Protocol update – input parameters

CONSTANTS	STAKE DB ENTRY
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	
GLOBALS	
STAKING POOL	
TOTAL_STAKED = { “lmo”: XXX ELCASH, “3mo”: XXX ELCASH, “6mo”: XXX ELCASH, “ly”: XXX ELCASH}	

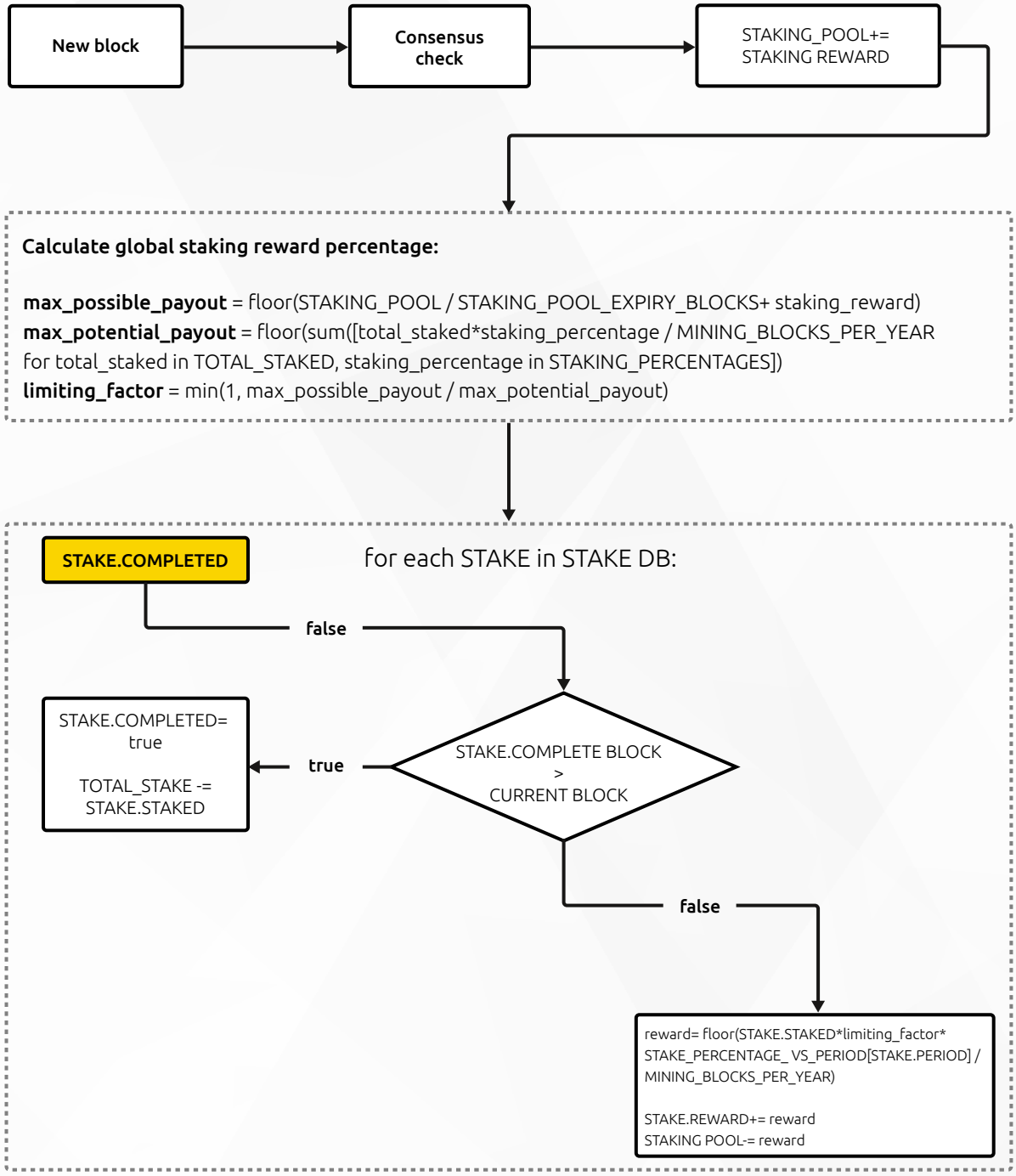


Figure 8. Staking calculations algorithm

The protocol is looking constantly for transactions which are ending the user's stake. If such a transaction is found, the protocol checks whether the stake was terminated prematurely, or whether the staking contract has matured. If the stake is terminated before the maturity, the penalty is imposed and the user is not able to pay out more than the calculated percentage of deposited coins. If the stake has matured, both staked funds and the accumulated rewards can be transferred. Completed stakes are removed from the database.

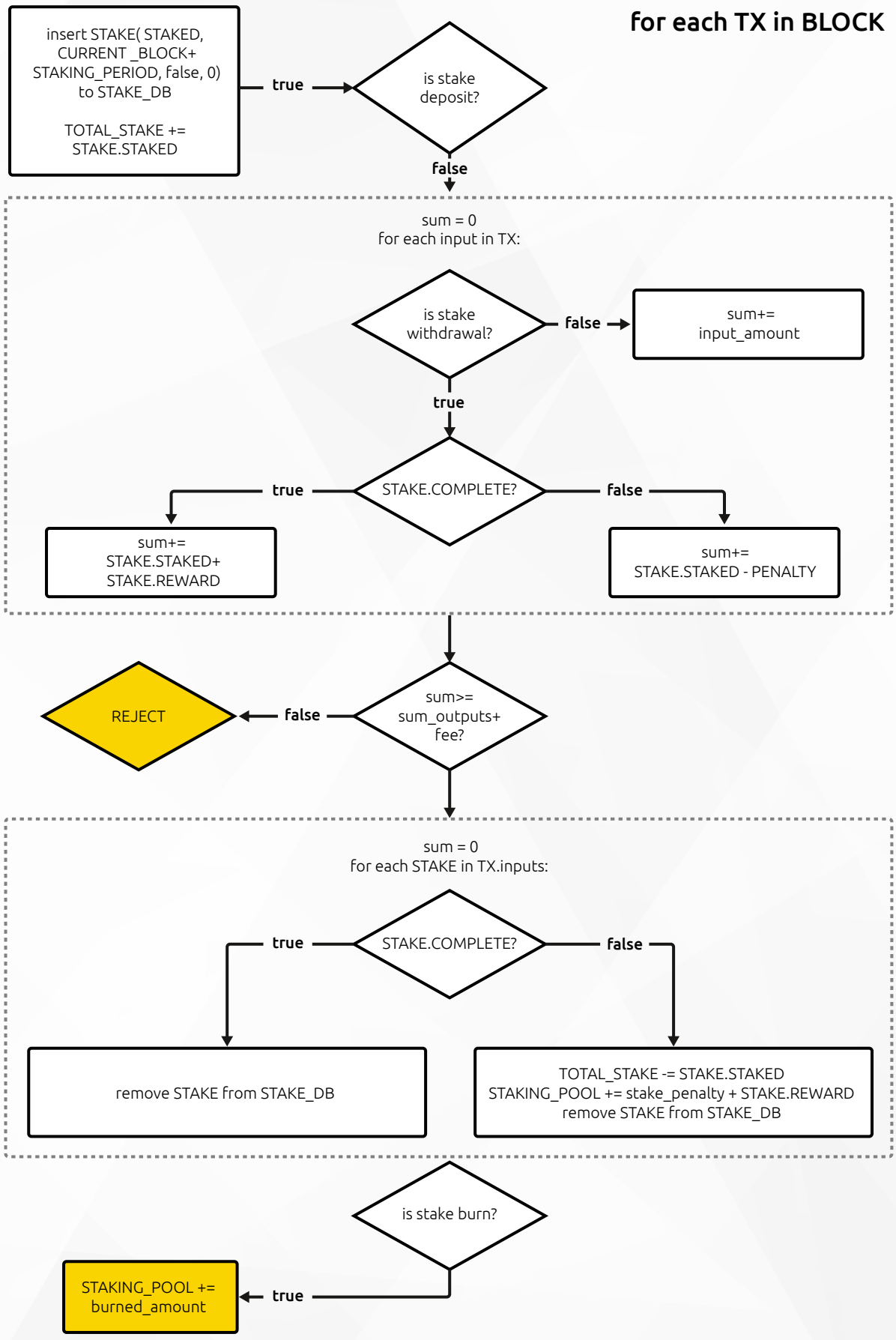


Figure 9. Staking Rewards Pool and users' rewards update logic

Staking reward (SR) – early withdrawal

A user who withdraws staked ELCASH before the maturity of the stake will have to pay an early withdrawal penalty (EWP), which is 3% of the stake's value.

Staking reward – successful maturity withdrawal

For each block, the protocol calculates the potential staking rewards (PSR) and maximum possible staking rewards (MPSR)

The MPSR are equal to the portion of the staking pool that can be used on the current date (e.g., 1/180 of the total staking pool reserve). By dividing the MPSR by 180, the Staking Rewards will be guaranteed for users for longer (180 is the arbitrarily chosen number of days, the purpose of which is to ensure as little variance in the staking rewards as possible). The PSR are the sum of rewards that the system should pay in accordance with all active staking agreements.

The amount of used staking pool reserve is deducted from the pool reserve. If the potential staking rewards (PSR) < max possible staking rewards (MPSR), each user will receive a contracted reward amount (i.e., 5/6/7.25/10% p.a.). If the potential staking rewards (PSR) > max possible staking rewards (MPSR), the limiting factor (LF) must be calculated. The LF determines the maximum daily payout that can be provided on the day in question. This process affects all users proportionally to their stake amount and might result in a slightly different reward. It ensures that there is always enough funds in the Staking Rewards Pool to reward all stakers.

2.1.7. Governance Power and free transactions

Participating in ELCASH staking grants users additional benefits such as Governance Power and free transactions. Governance Power (GP) is an untransferable value generated based on the user's staked value and staking duration. It allows the user to participate in ELCASH governance voting and to create new governance proposals. **The number of free transactions is also conditioned by the staked value and staking duration.** The limit is calculated daily, and the unspent free transactions are not accumulated. The main assumption is to reward a minimum stake (5 ELCASH for 4320 blocks) with one free transaction per day.

All specific details of Governance Power and free transaction calculations are discussed in detail in their respective chapters.

2.1.8. Staking Explorer

Staking data and network performance can be followed by Staking Explorer together with the Governance Dashboard. Transactional and staking data are updated in real time. Users can easily obtain general statistical insights such as Total Network Stake, SRP live status and a check on general network analytics.

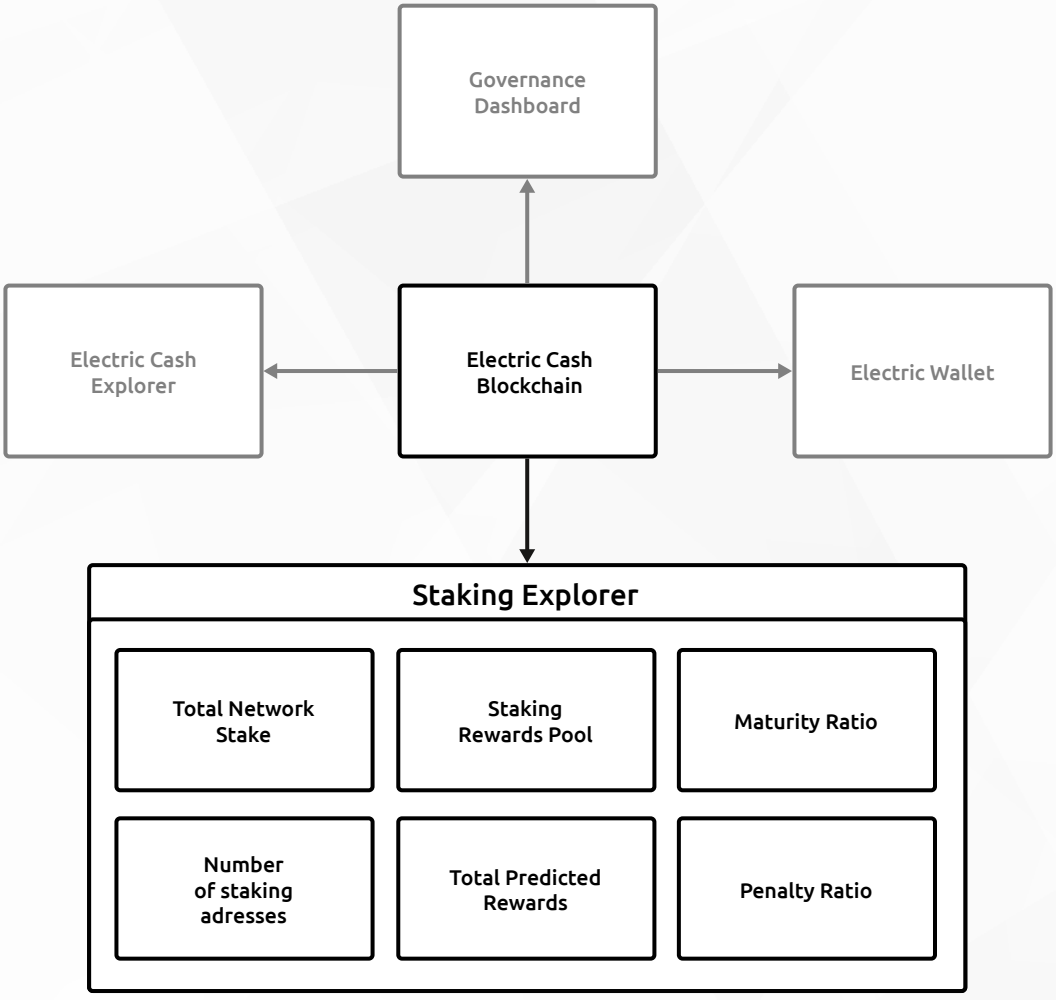


Figure 10. Staking Explorer overview

2.1.9. Security

Electric Cash Staking is a secure process as all staking parameters are embedded into the blockchain protocol and the whole staking process is automatic – Electric Cash developers do not have custody over the funds at any point. It is not possible for the developers to interfere with the funds in the wallets (neither Spending Wallet, nor Staking Wallet) and the team does not use the staked funds to profit from them in any way.

The user is the only person with the access to the funds in both Staking Wallet and Spending Wallet.

The developers do not have access to the Staking Rewards Pool. The SRP is a value that is automatically updated by the protocol and presented in Staking Explorer.

2.2. Governance system

In order to achieve direct democracy, Electric Cash implements a governance system. In the governance process, the latest changes can be proposed, designed, agreed upon and implemented. Changes are not limited to the blockchain source code technical details but can also cover other important network and community issues. Using the blockchain's built-in voting mechanism, users can vote on proposals made both by the community members and/or the core management team of Electric Cash.

Importance of governance

The blockchain governance is not just a symbolic gesture towards the community. It is also an important element of the blockchain ecosystem. It makes projects more transparent and easier to manage. Introducing the governance system in Electric Cash makes the project more competitive as decisions can be made faster and better address the market and user needs.

Success on the crypto market cannot happen without engaged stakeholders. Cryptocurrencies are often built on an open-source code, which is easy to copy, and they can only differ from each other through the people supporting the project. Communities must be considered as the most important and unique part of every blockchain ecosystem.

2.2.1. Governance Power (GP)

During the staking process in the Electric Cash protocol, the network participants (stakers) obtain Governance Power (GP). Governance Power is directly conditioned by the staking parameters:

The higher the value of the stake and the longer the staking period, the more voting (governance) rights stakers have over the ecosystem.

Governance Power is untradable and untransferable, creating an ecosystem of credible users with "skin in the game" who stake more and for a longer time. The system is designed to ensure that greater GP is only available to the most active and dedicated members of the ELCASH community. Governance Power gained by users will therefore change over time if they cease to be active in the network.

The goal of the Electric Cash governance system is to create a project that is:

- **decentralized:** every network user can participate in the governance. Every staker can make a proposal and vote;
- **transparent:** all vote results, together with their implementation stage, are visible on the Governance Explorer site;
- **secure and private:** all users can vote anonymously. The blockchain network shows only the wallet address of the user participating in the governance process.

2.2.2. Calculating Governance Power (GP)

Governance Power is calculated to reward the most valuable and the most active network participants. Every user staking Electric Cash will gain Governance Power (GP). The Governance Power factor depends on the following parameters:

1. **Staked amount** – the more ELCASH staked, the more Governance Power a user gets during the staking period.
2. **Staking time** – as long-term staking is more beneficial to the network, users who stake for longer get more benefits, i.e., users staking once for a longer unbroken period of time get more GP than those who re-stake their funds repeatedly, even if the cumulative staking period is the same.
3. **The protocol minimum requirement to generate GP**:
   5 ELCASH staked for 1 month to get 1 GP.

GP is not a separate coin. It is a non-monetary right connected to the user's ELCASH address and it is untradable and untransferable (from wallet to wallet).

2.2.3. GP Burning and Minting methods

In order to maintain a healthy network, each vote and proposal require the user to use his GP as a "payment" method, which protects the Electric Cash blockchain from getting clogged up. In the voting process (Figure 11) and proposal creation (Figure 12), each user need use the chosen amount of GP (fulfilling the given minimal requirements). GP used in this process will be burned and not transferred. Burning in blockchain means removing a given value of an asset from the network. In this case, the GP used to "pay" for the proposal is not transferred to another address but "destroyed" by the protocol, so no one can access it anymore.

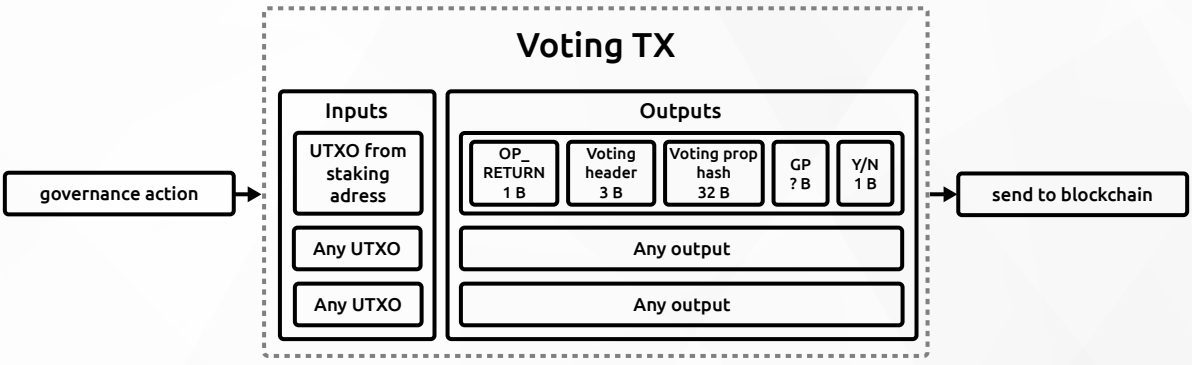


Figure 11. Voting process

When a user votes, a voting transaction is created. Blockchain saves the user's address, the amount of GP spent, and the chosen option. Voting results are calculated based on all voting transactions made by the users.

The MINT GP method allows users to be rewarded with additional GP. Minting creates a certain amount of additional GP, so GP is not sent from any address but created by the protocol.

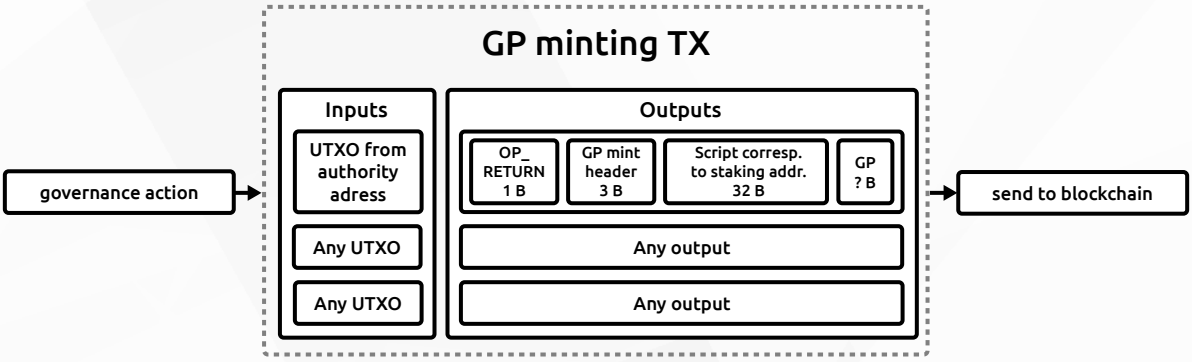


Figure 12. Governance Power minting process

When a user performs an action that is eligible for GP return (voting or creating a successful proposal), blockchain carries out a GP minting transaction. The input comes from an authority address, a special hard coded address, which informs the protocol that minting of a certain amount of GP is needed.

2.2.4. Creating proposals

The Electric Cash community decides on the economy and ecosystem of the coin. Every user can create a new proposal for the network to vote on. Members can not only vote on additional features, but also on the Electric Cash mining parameters, like the coin's maximum supply, which will help ELCASH to be competitive and an up-to-date project in the future.

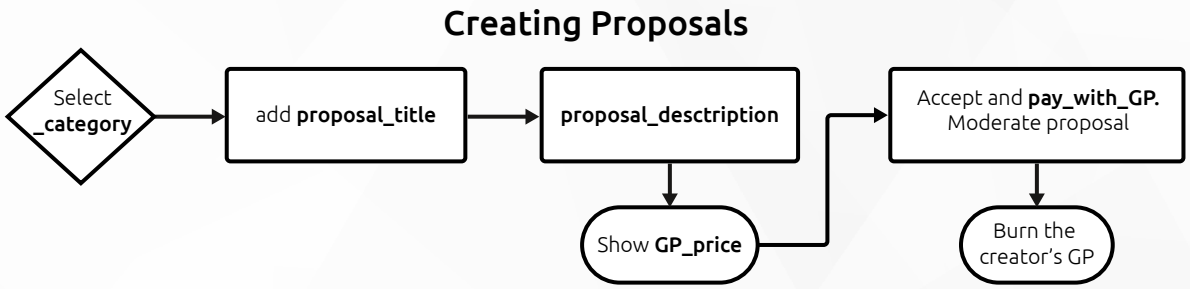


Figure 13. Electric Cash governance proposal creation mechanism.

The proposal can be created using Electric Wallet. However, to prevent the network being overloaded and enforce the proposed changes, creating a new proposal requires the user to spend their Governance Power. The initial price of proposals is 304 GP. This value can be changed in the future depending on the network's needs.

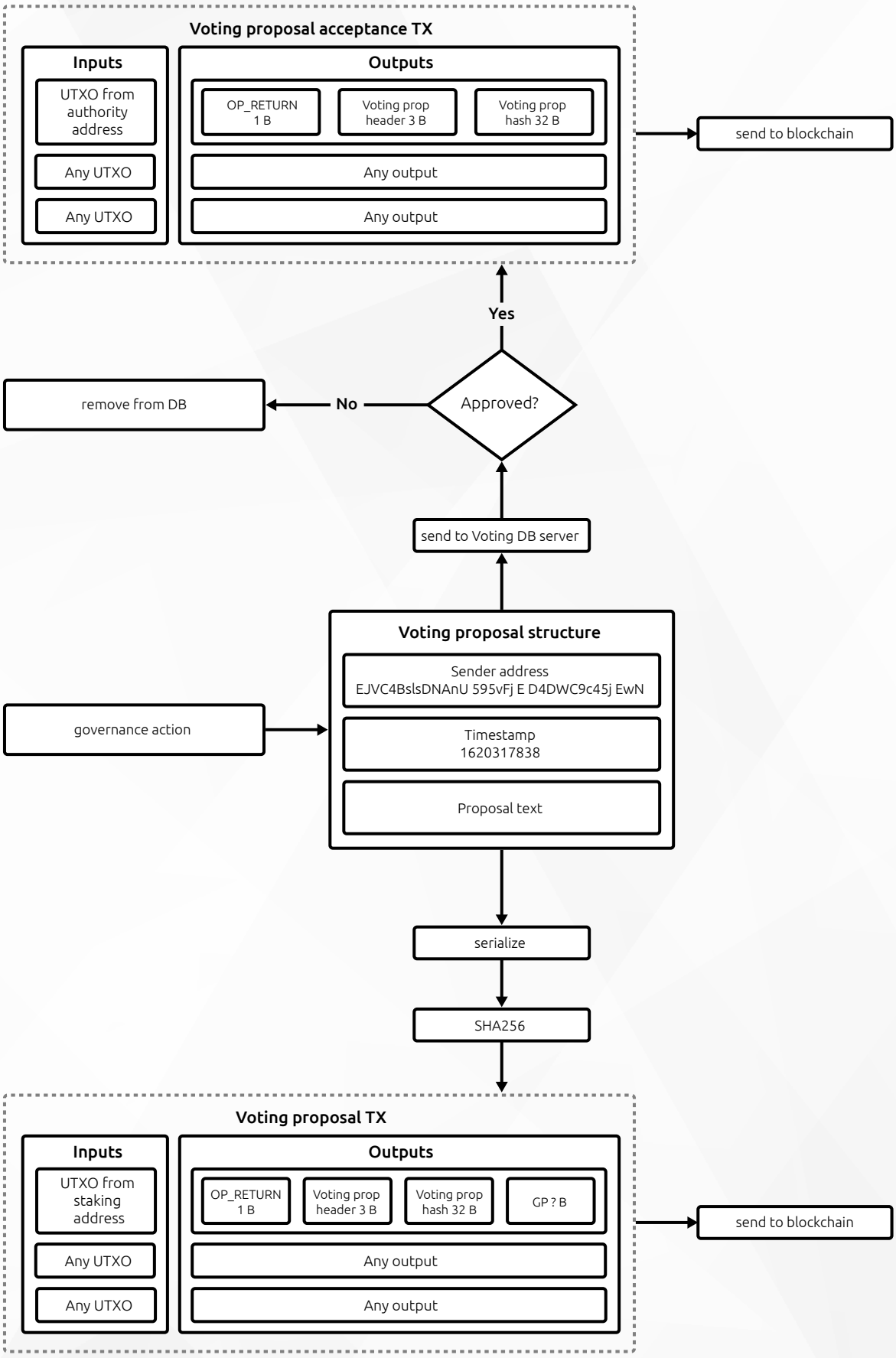


Figure 14. Voting proposal creation process

When a user creates a proposal, all the data (sender address, timestamp, and proposal text) is hashed and sent to the blockchain with a special voting proposal transaction. At the same time, the proposal data is also sent to an external voting database. The process is transparent and secure, as every user can compare the hash of the proposal from the database with the hash sent to the blockchain, to make sure no one made changes to the proposal data. If the proposal is accepted by the moderation, the voting is opened.

2.2.5. Proposal lifecycle

Proposals can be submitted both by the community and the ELCASH developers.
New proposals can only be added in the open voting window, to make the whole voting process easier to manage and follow. After submission, community proposals are moderated by the ELCASH team to eliminate any malicious or illegal proposals. Approved proposals are added to the active_proposals_list and can be voted on. If the voters vote in favor of the proposal, it passes, and afterwards, the ELCASH team decides if it is added to the team's backlog.

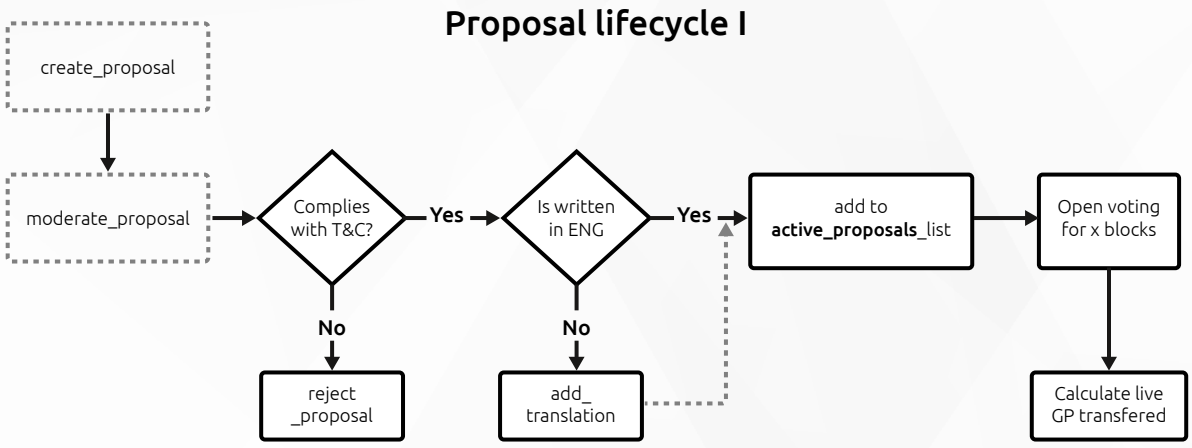


Figure 15. Electric Cash governance proposal lifecycle 1/2

Once creation and positive moderation are submitted, each proposal is immediately visible on the desktop Governance Dashboard (GD) and can be voted on in Electric Wallet. Each proposal has the same voting window, and all transferred Governance Power is calculated live at this time.

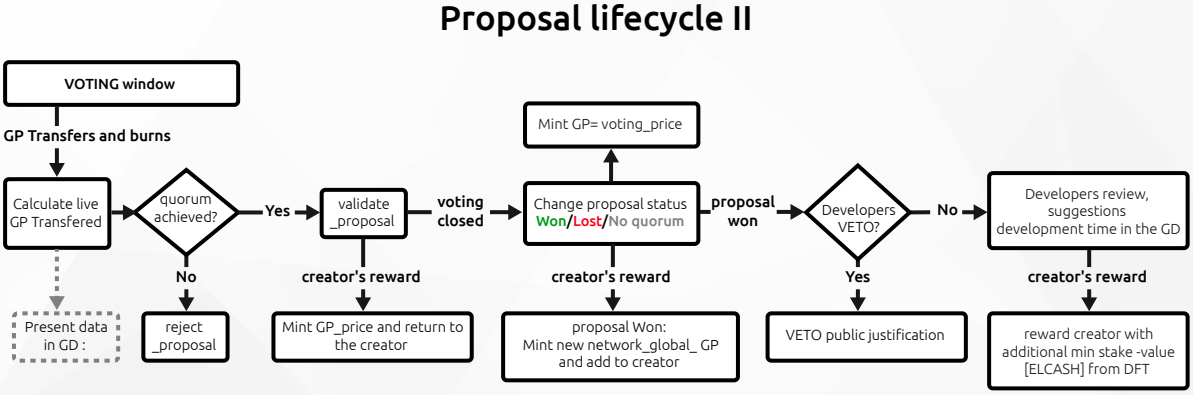


Figure 16. Electric Cash governance proposal lifecycle 2/2

During the voting_period, each proposal has the same lifecycle. After moderation, the first big step for a proposal is to achieve network quorum. If 15% of all network_global_GP was transferred to a proposal (both Yes and No votes), quorum is achieved. Achieved quorum means that there is a lot of interest on the network and, therefore, the creator gets 80% (0.8*proposal_GP_price) of the GP spent for submitting the proposal. This "return" is made using the MINT method. If a proposal has not achieved quorum for the entire voting period, it is rejected, and the user loses their GP that was burned in the process of submission of proposal. This approach motivates users to submit only the most relevant proposals and to consult the proposal idea with other network participants on dedicated communication channels.

During the voting period, the network presents on-chain proposal data on the Governance Dashboard and Electric Wallet, with details such as:

After the voting period:

- Each proposal changes its status to one of the following:
  - **WON** (GP transferred for majority vote – yes)
  - **LOST** (GP transferred for majority vote – no)
  - **NO_QUORUM** (GP_transferred for vote –_yes & vote -_no < 15% of network_global_GP)
- If the proposal status = WON, the proposal creator receives additionally Minted GP with a value of 0.01*network_global_GP. This rule clearly shows that the global value of GP within the network can increase not just because of new staked coins.
- Developers can use the VETO method. In necessary situations due to the tokenomics of the coin and its development, developers can use VETO and not accept the proposal chosen by the community. The reason for using the veto must always be properly analyzed and justified by The Developers Team using a dedicated panel on the Governance Dashboard. However, if the proposal achieved the status WON, the user is rewarded even if the proposal had been vetoed.

2.2.6. Governance moderation

All new proposals are moderated by the Electric Cash team to ensure that all proposals are created for the network's good and not with malicious or even illegal intent. If a proposal is considered to be malicious, it is removed, and the voting is not conducted.

If the Electric Cash team approves a proposal, it becomes available for voting and it is visible on the Governance Dashboard.

Moderation also takes place when the proposals are submitted in languages other than English and are translated by the Electric Cash team. This means that such proposals can be available for voting with a slight delay. Thanks to that, the whole community will always see the original version of the proposal description and also its ENG equivalent on the Governance Dashboard and simplified GD inside Electric Wallet.

2.2.7. Voting

Every user who gathered Governance Power in the staking process can vote on the proposals presented on the Governance Dashboard. Voting is open for a block period corresponding to approximately ~4 weeks from the day the proposal is published. After the voting ends, every user can check the results on the Governance Dashboard.

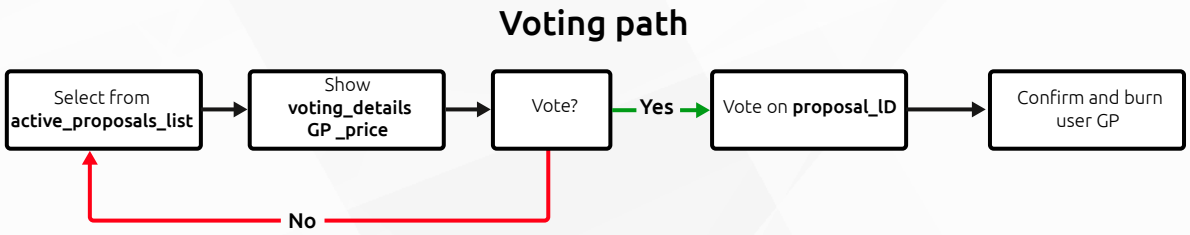


Figure 17. Electric Cash governance voting mechanism

Voting also has a cost in GP. The price, however, changes with each additional vote. The first vote of a given user is set as the cost of 1 GP.

Any further vote costs a quadratic value:
GP_price = x^2,
where x – number of votes
(i.e.: 2nd vote – 4 GP, 3rd vote – 9 GP, and so on).

Such a solution ensures that the biggest stakers don't take control over the network, so every user has the same importance for the community, making ELCASH truly democratic.

2.2.8. Governance dashboard

To increase the transparency of the Electric Cash project, allowing everyone to track the governance process even without a dedicated wallet, the Governance Dashboard has been created. It is a dedicated website presenting the most important information regarding governance, including all the active and past proposals, voting results, voters' activity, Governance Power on the network and other parameters.

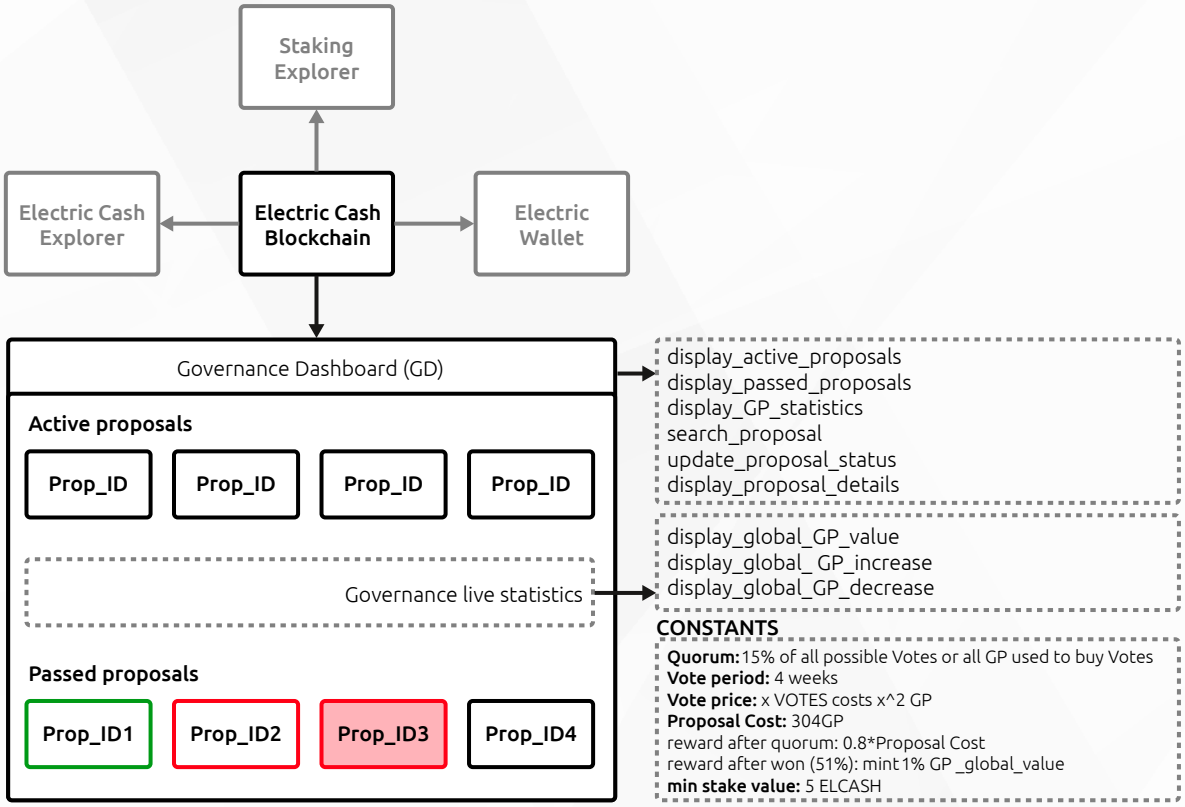


Figure 18. Electric Cash Governance Dashboard overview

Each passed proposal (after voting_period) can have one of four statuses:

Table 3. Possible proposal statuses

Prop_ID1	Prop_ID2	Prop_ID3	Prop_ID4
WON	LOST	VETO	NO QUORUM

The Governance Dashboard is also a great medium to exchange ideas and to contact developers who give their opinion on each WON proposal or justify their decision/or not.

2.2.9. Proposal execution

To ensure network safety, especially in its early years, the governance proposals are not executed automatically. The ELCASH team verifies all the proposals and selects the ones that will have the greatest impact on the network.

2.3. Merged mining

During the early stages of development, ELCASH will operate using a merged mining process. It will allow ELCASH to leverage the hashing power of larger SHA-256 (Bitcoin-like) based chains, ensuring the overall security of the new network.

Merged mining is implemented with Bitcoin, since both cryptocurrencies use the same SHA-256 hash function. In this case, BTC is the parent chain and ELCASH is the auxiliary chain. As a result, Bitcoin's (parent) Proof-of-Work solutions can be used to validate ELCASH (auxiliary chain) as an auxiliary Proof-of-Work (AuxPoW) consensus mechanism (7).

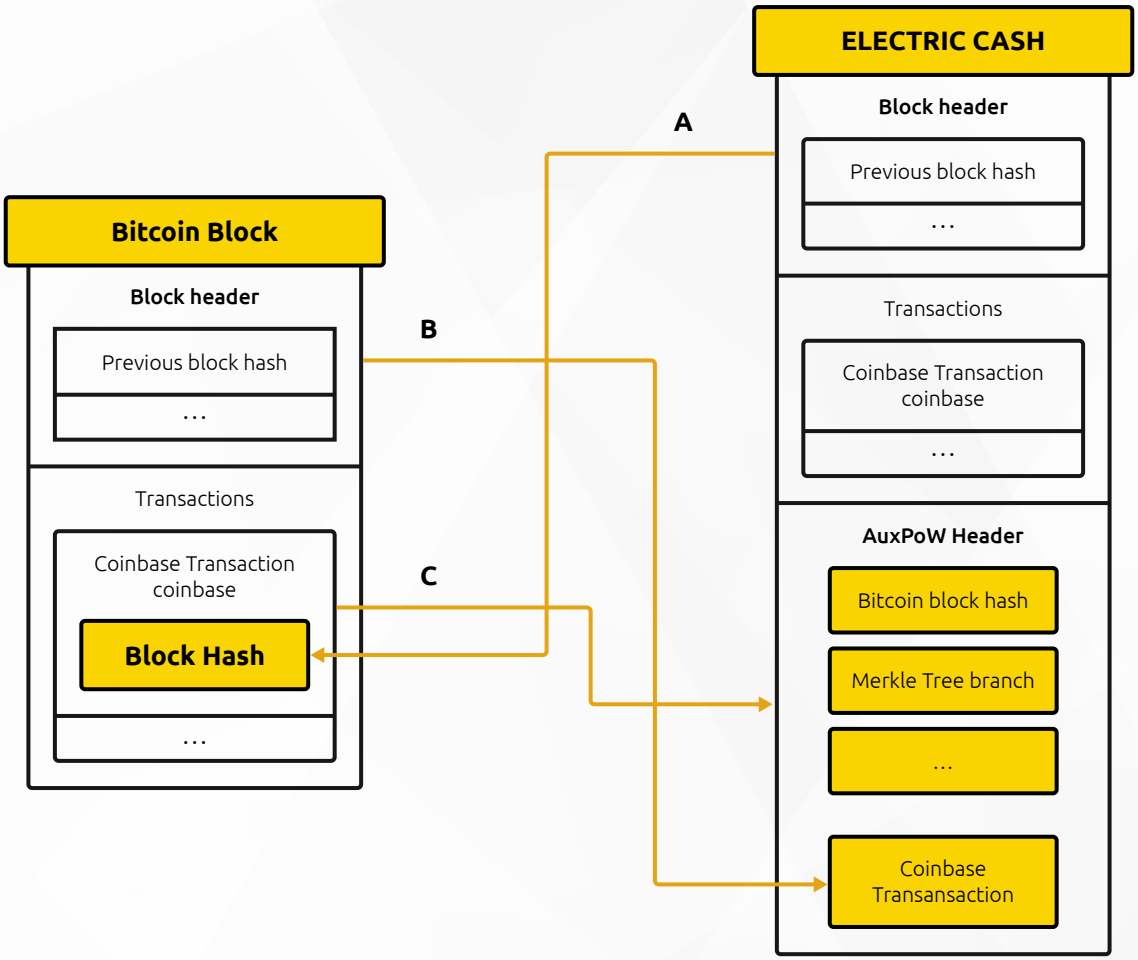


Figure 19. Structure of merged mined blocks in Electric Cash.

Merged mining is a good method for new blockchains, such as ELCASH, to increase security and reduce vulnerability to 51% attack. Implementing that integrated mining architecture into the ecosystem gives us confidence that ELCASH meets current industry safety standards.

3. Electric Cash infrastructure

Electric Cash is a payment protocol designed to be accessible and lightweight, with a focus on reducing transaction fees and making daily use almost seamless. Fast and free transactions for stakers on a secure and decentralized network make ELCASH ideal for everyday payments.

3.1. Fast transactions layer

In order to implement fast transactions, the blockchain requires enough block capacity to include all the transactions which are waiting for confirmation, and to inform the network about the transactions as quickly as possible. Fast transactions are the key to global adoption but in the traditional Proof-of-Work blockchains, instant transactions are hard to achieve due to security reasons. The receivers of transactions need to wait for the protocol to add the transaction in the next blocks, which is limited by the mining difficulty. On average, it takes about 10 minutes for a new ELCASH block to mine. This could be considered fast enough for a simple transfer to a friend, but it would be inconvenient for retail payments. This is why ELCASH implements a fast transaction layer, cutting the time needed for a transfer to even as little as ~10 seconds[2] putting ELCASH among the leaders in the blockchain industry. This time can differ depending on the network congestion.

A fast transaction layer (Layer 2) of masternodes is created on top of the network to improve the transaction speed. Masternodes check whether a newly created transaction is valid and ensure that the transaction is irreversible, even before being added to a new block by locking inputs and sharing the information about it with all the nodes. Thanks to this, the network is being promised that the transaction will be included in the next mined blocks.

Layer 2
Enables fast transactions.

Layer 1
Consensus Layer (PoW) ensures the integrity of the blockchain executing the consensus algorithm across participants.

Layer 0
Blockchain layer is of utmost importance to the scalability, security, and privacy of the network.

Hardware Layer
Enables efficient execution of protocol at other layers.

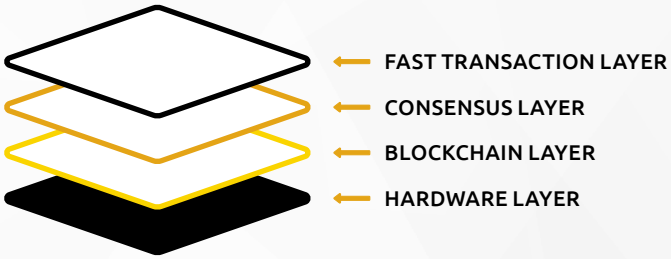


Figure 20. Architecture of the Electric Cash blockchain ecosystem (8).

2 Note. This is the value estimated for optimal network conditions. It may slightly differ depends on the network load.

This fast-layer solution enables fast transactions and ensures a high level of network security. The transactions are propagated to the main blockchain using Layer 2, where transactions are confirmed before being approved by the PoW miners. All transactions on the Electric Cash network are processed by the fast transaction layer, which means that all ELCASH transactions are fast with no additional fees and no special action required from a user.

The process which every transaction goes through is similar to a standard transaction validation, but it contains a few additional steps, where masternodes lock the transaction (Figure 21).

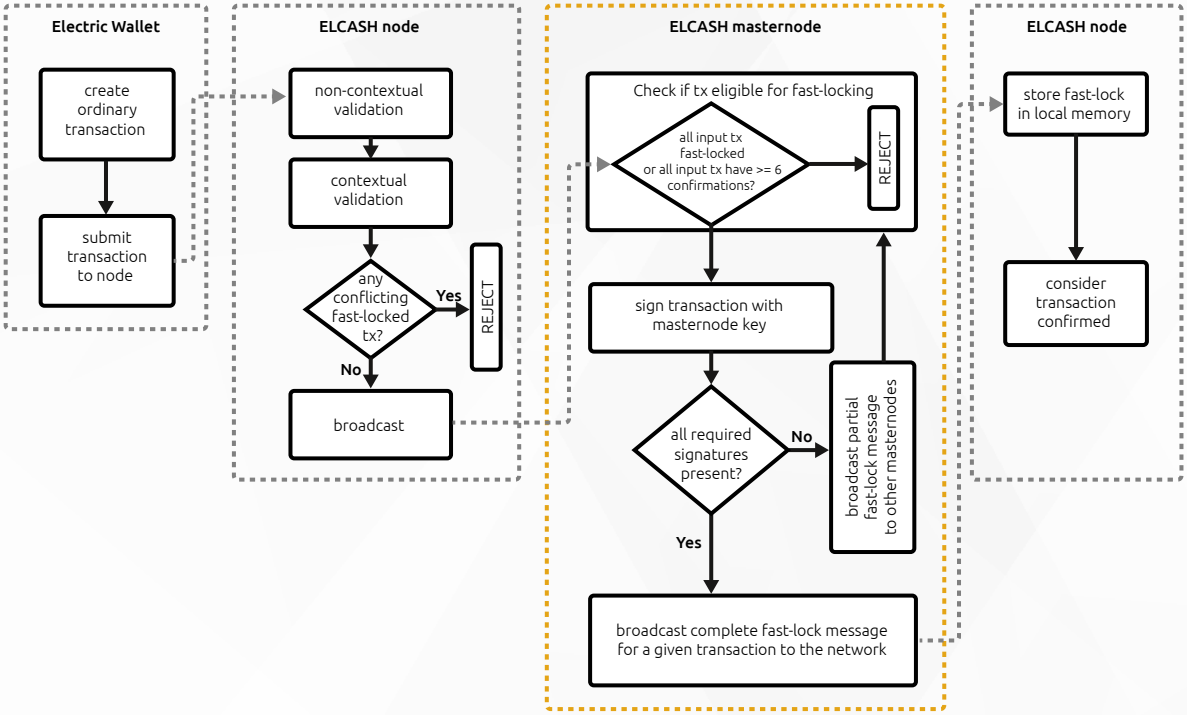


Figure 21. Fast transaction confirmation process

After a user creates a new transaction in the wallet, the transaction is submitted to a ELCASH node. The transaction is validated and if there are no conflicting transactions, the transaction is sent by the ELCASH node to the ELCASH masternode, otherwise the node rejects it. A masternode checks the eligibility of the transaction for fast locking. If the transaction is approved, it is signed with the masternode key by the masternodes. This part of the process prevents double-spending of the funds. The inputs of the transaction are locked so that they are only spendable in a specific transaction and once the transaction is locked, it is not possible to send the same funds twice or to change the transaction in any way. All nodes are informed that the transaction is locked and it will be added to the blockchain with the next blocks.

If consensus is reached on a lock by the masternode layer, all conflicting transactions or conflicting blocks would be rejected, unless they matched the exact transaction ID of the lock in place.

Thanks to such solution, it would be much more convenient to use ELCASH in everyday life, whether it is paying for groceries in a store or just sending ELCASH to friends. In addition, the Electric Cash blockchain still operates on a secure Proof-of-Work consensus.

3.2. Free transactions

Cryptocurrencies, however secure, are often expensive to use, especially when the project gains popularity and the network use increases. This causes a situation where the more popular the project, the more expensive its use becomes. Fewer new users are willing to participate, thus hindering the project's growth. To achieve global adoption, projects need to reach a critical mass, i.e., a certain number of users that make the network appealing to join. Projects like cryptocurrencies or social media platforms become more useful with every new user because it is possible to connect to more people. In effect, if the project limits itself with rising transaction fees while more users are in the network, it makes the global adoption hard – or even impossible – to achieve (9).

In this regard, Electric Cash transaction features are a crucial factor for mass adoption of cryptocurrencies. An implemented fast and free solution competes not only with other blockchain projects, but also with traditional financial institutions.

3.2.1. Free transaction validation mechanism

Free transactions are achieved thanks to the blockchain architecture: during the staking process, stakers generate the "free transaction limit" to spend. The fee is applied to the transactions and this will make malicious network attacks more difficult to enforce. However, staking users will be eligible for some free transactions depending on their staked funds and staking duration.

Free transactions are slightly different to normal ones. They contain additional information about the sender's staking UTXO, to confirm that the user is eligible for a free transaction (Figure 22).

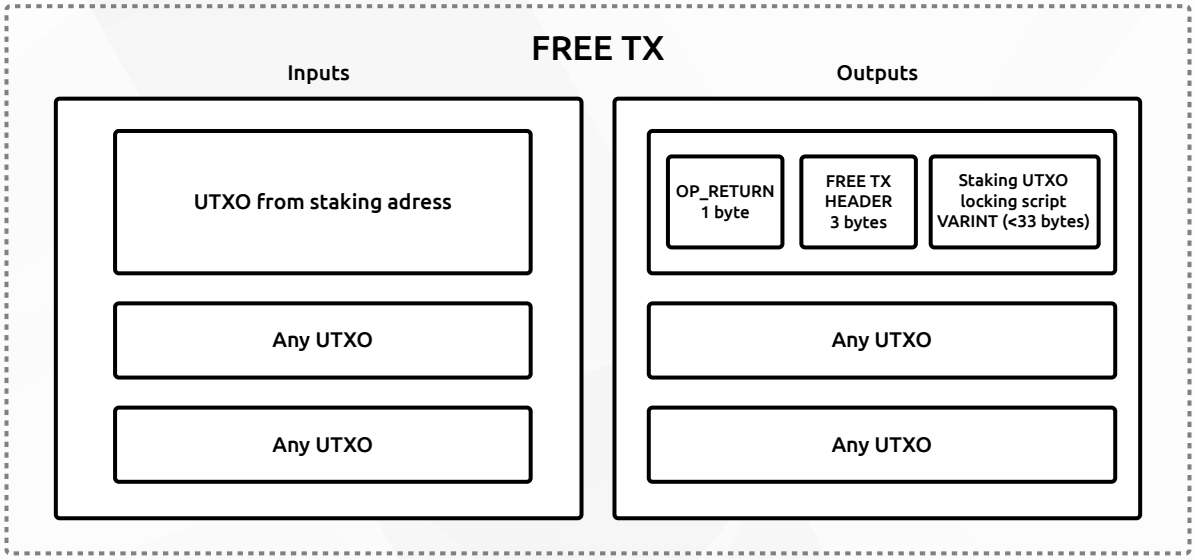


Figure 22. Free transaction structure

Non-contextual validation rules:

1. OP_RETURN + free TX header is the first output of the tx
2. All the normal rules for transaction

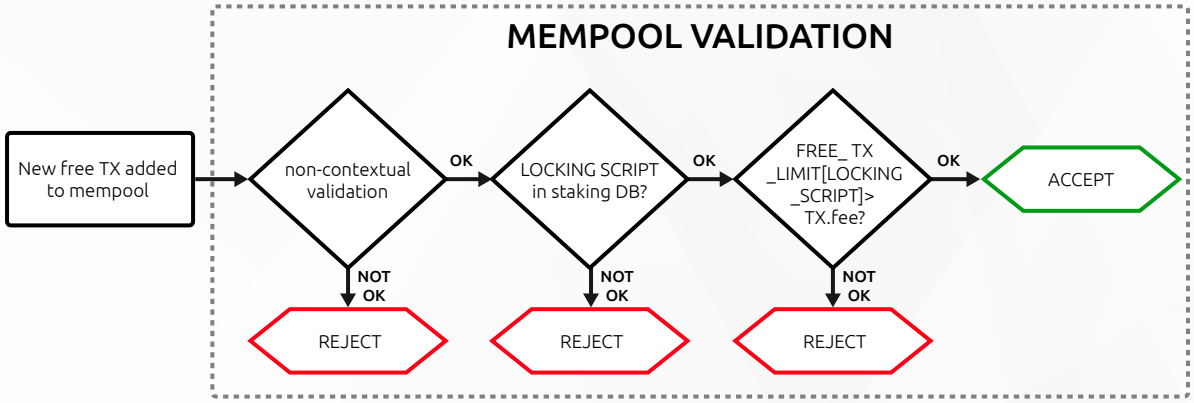


Figure 23. Free transaction mempool validation

As with all other transactions, free transactions wait in the mempool to be added to a new block. However, besides standard validation, the sender's eligibility for free transactions is also checked. If the transaction is correct and the sender is a staker with a sufficient free transaction limit, the transaction is accepted and added to a new block.

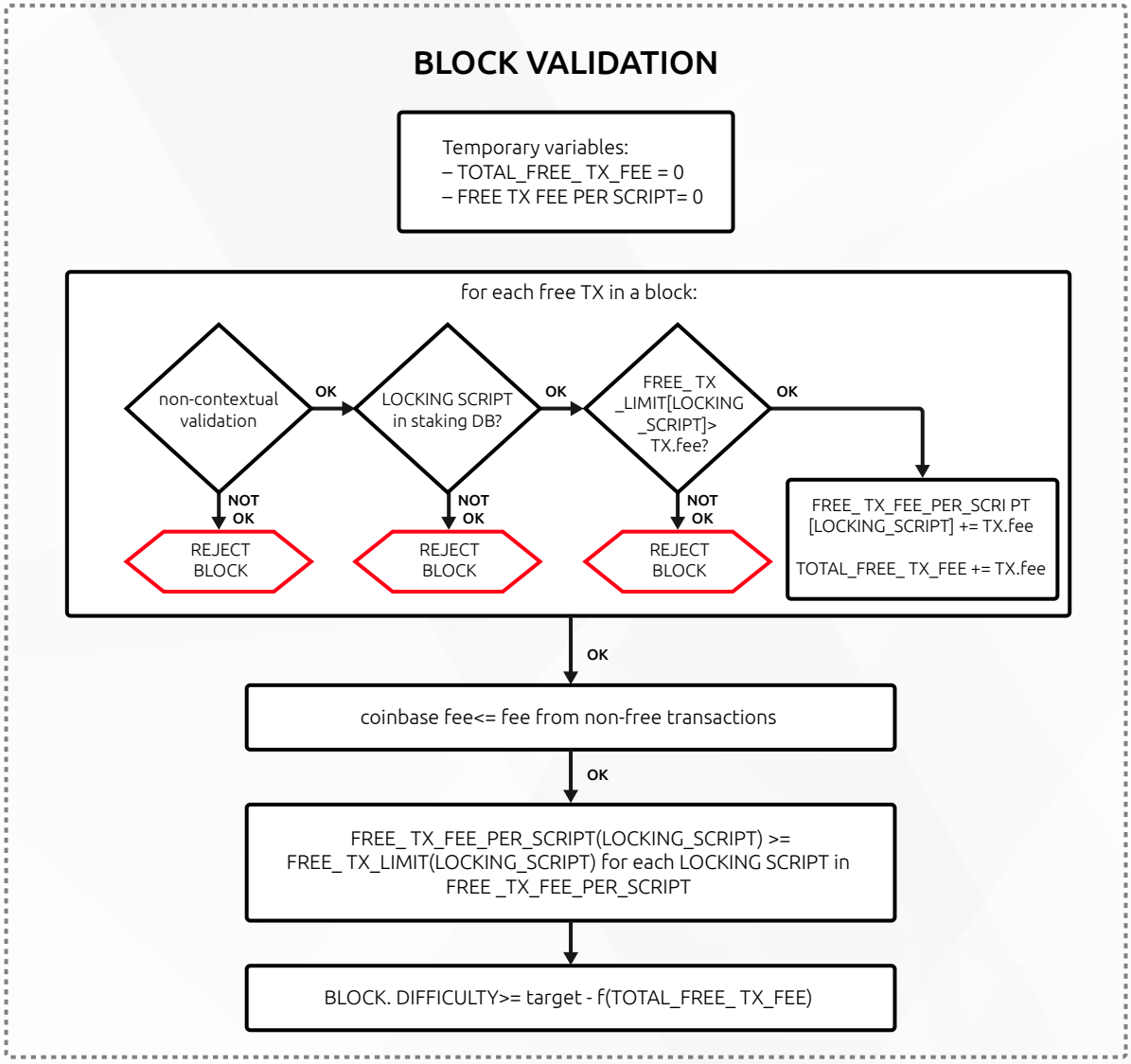


Figure 24. Block difficulty calculation

For each free transaction in a new block, the protocol calculates what fee would be charged if the transaction were not free and adds all estimated fees (Figure 24). To compensate miners for accepting a free transaction into a block, block difficulty is decreased based on the sum of the estimated fees from the free transactions.

Free ELCASH transaction limit

ELCASH blockchain charges transaction fees but every user who stakes ELCASH is eligible for some free transactions per day. The free transaction limit depends on the user's staking parameters.

This helps keep the network secure against malicious overflooding, making attacks expensive, while genuine users are able to make free transactions.

Miners are not burdened with additional work without a reward. If a free transaction is to be made, mining difficulty is automatically reduced proportionally to the free transactions value included in the block. **As a result, the miners' total and final block rewards will not be affected in any sense by the free transactions and the miners' additional work will be rewarded accordingly.**

Limit calculation

Every stake has a daily size limit of free transactions. This limit is dependent on the stake value and period. [tx_limit] ∈ N → STAKE_WEIGHT≥1.

Protocol assumptions must be: STAKE WEIGHT = 1 (minimal stake receives a limit to perform ~1 free tx / day), and 5 ELCASH for a one-month stake is also the minimum stake required to receive a limit;

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

For example:

5 ELCASH for a 12-month stake:

stake_weight=510840/4320×5/5 ≅ 12 free tx/day

Free tx limit doesn't stack. Unused limit for a given day can't be used after the day ends. Free tx are available for the user 20 blocks after staking starts.
The moment staking ends or is terminated by the user, the access to free tx is lost.

3.2.2. Free transactions, technical details

Free transaction syntax

1. One of the outputs is metadata pointing at the staking address
2. One of the inputs comes from the address pointed at in point 1
3. The transactions do not physically contain a fee. No returns are needed.

Free transaction execution

1. A one-time wallet setup (an internal transaction that can be performed at the moment a deposit is staked) is needed in order to be able to perform free transactions
2. The user must specify a staking address from which the limit will be taken (this can be done automatically by a wallet)
3. User must have at least one active stake

Miner compensation

1. The miner won't receive fees from and for free transactions
2. Blocks containing free transactions will have their difficulty requirements lowered Modified mining difficulty for particular blocks is expressed as:

MODIFIED_DIFFICULTY= (1-FTX×TXS_total)×PoW

FTX – free tx coeff.
TXS_total – total block free tx size
PoW – PoW difficulty

3.3. Block reduction and rewards strategy

In Table 1 aims to meet the expected market demand for the coin, while preventing oversupply during the early years.

Pre-mining is planned to continue until 10 percent of the supply is mined and allocated to activities including, but not limited to, project development, marketing, promotional efforts and more.

We strive to prevent any undesired activities that may arise at the very beginning of the coin's existence when the coin and its ecosystem are not yet mature. The plan to secure the previously mentioned 10 percent of the total supply of ELCASH also includes the added benefit of discouraging market manipulation by potential holders of substantial volumes of ELCASH.

Table 4. Block reduction and rewards strategy.

Period	Date	Blocks	Block Reward	Coins
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
…	…	…	…	…

The pre-mined coins will be used in various activities that have one main goal: attracting attention and users to the ELCASH ecosystem. It is a common and widely accepted solution for projects to allocate a designated number of coins to marketing and development activities. We believe this solution will provide a healthy way of funding the project's development and create a brighter future for the blockchain ecosystem.

Examples of use-cases for the pre-mined 10 percent of the total supply of Electric Cash:

- Promotional airdrops
- Business development
- Additional rewards for stakers
- Marketing efforts
- Social media advertisements
- Software budget

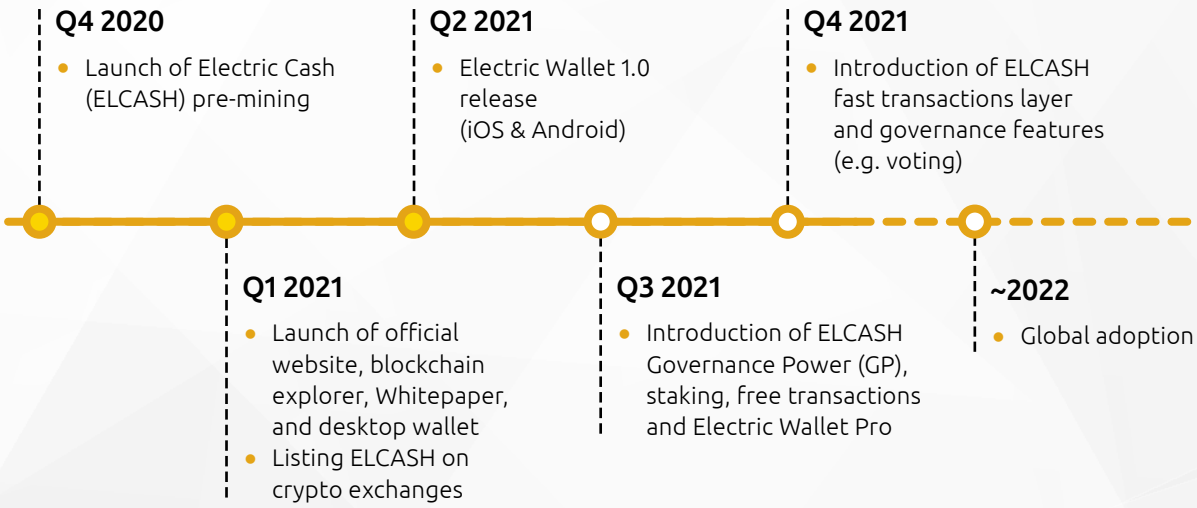
During the first year, the block reward will amount to 75 coins. Each subsequent period will gradually decrease it. After seven years, the network will switch to a rewards strategy called “halving” where the block reward is decreased by 50 percent each year from that time.

The total supply of Electric Cash is currently capped at 21,000,000 coins, identical to the total supply of Bitcoin. A fixed supply helps minimize potential inflation and dilution. However, if the project gains popularity in the future and the demand for the coin grows, the most active network users will be able to increase the supply through democratic voting thanks to the governance system tools, bearing in mind that this may result in small inflation.

3.4. Development Treasury

The ELCASH project implements a dedicated Development Treasury Fund that constitutes 10% of the mining rewards collected in a special wallet managed by the Electric Cash governance system. The funds are kept safely until the community votes to spend them. It can cover the costs of the protocol improvements and changes such as developing new features in the Electric Cash ecosystem. To keep the whole process transparent, the balance of the collected funds is presented on Governance Explorer.

Electric Cash roadmap



Summary

In this paper, we introduced Electric Cash (ELCASH). The project's goal is to provide a comprehensive ecosystem and solve several major problems in the cryptocurrency industry. ELCASH facilitates everyday payments. By implementing an additional Layer 2 to the blockchain, it can perform fast transactions while still ensuring network security. Thanks to this solution, an ELCASH transaction can be processed in about ~10 seconds (depending on the network congestion), which makes the Electric Cash network one of the leaders in the blockchain industry. Users don't need to take any additional actions to send a fast transaction, all transactions are fast by default .

The ELCASH protocol, designed to be accessible and lightweight, also focuses on reducing transaction fees. All staking participants are rewarded with free transactions, which are granted based on the size and longevity of the total stake. Fast and free transactions make ELCASH perfect for small, everyday payments, which opens up many opportunities for the global adoption of cryptocurrencies.

The ecosystem not only introduces fast and free payments, but also additional benefits like Governance Power. By actively participating in the network, each coin holder earns Governance Power (GP) and can have a direct impact on the protocol changes. GP is distributed depending on the user's stake parameters and network activity. It gives the right to participate in the governance process and to vote on available proposals. Thanks to the community governance, the project can quicky react to market needs and introduce changes faster. We believe that this decentralized and community-focused ecosystem will ensure healthy growth and a global long-term project perspective.

Sources

To find out more about the project, please visit:

Website: 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

References

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.