CAUSEVEST

2026
WHITE PAPER

WWW.XCVESTING.IO

ABSTRACT

This paper starts with an introduction to the new cryptocurrency Causevest Coin, then goes on to explain how the Causevest Network operates and finishes with the technical details behind our protocol.

We make use of collaborative consensus via our coin holders to provide a wide range of use cases, such as redistributing network profits to registered causes. Meanwhile Improved security features and incidents of collective forgiveness provide new methods of protecting coin users from bad actors.

The Causevest Network blockchain allows causes and their supporters to bypass the traditional financial services system and provide end use audits while still protecting their privacy.

EXECUTIVE SUMMARY

The Causevest Protocol is a new fully functional standalone Layer 1 blockchain, wallet and cryptocurrency with low node costs that uses votes via Causevest Coin to redirect protocol income.

The blockchain is secured by Proof of Stake (PoS) finality generation and has a unique reward mechanism called Proof of Cause (PoC). PoC distributes rewards among users who support Causes on the network. This gives users who earn smaller amounts a chance to receive significant amounts of XCV.

To power both PoC and PoS, the protocol relies on self-sustaining revenue flows. A core flow comes from Layer 1 transaction fees, which are sent to a Network Income Pool and redistributed in a way that ensures the protocol can never "go bankrupt." While higher income leads to higher rewards, the system remains stable even if income decreases.

The Causevest Protocol includes a range of enhanced security features, such as multisig wallets, an external threat forgiveness mechanism and time-reversible vaults, providing users with additional protection in case of accidental or unauthorized transactions.

The protocol will include a Layer 2 system. Each secondary connected sidechain, called a Neighborhood, can have its own ruleset including Turing Completeness or any particular smart contracts that a user could desire. All neighborhoods use the same XCV, share in finality generation and send a portion of their fees back to the L1. Users can flow XCV from neighborhood to neighborhood seamlessly, just like they were making L1 transactions by using pooled cross-chain liquidity.

CAUSEVEST COIN

A layer-1 blockchain built for disruptive altruism

Causevest Coin (XCV) is a standalone ("layer 1") peer to peer payment protocol that incentivises good. Causevest is not reliant on any individual business's success; it does not depend on any other coin's technology to function and has use cases based around the core ideology of disruptive altruism.

It is easy to forget that many early adopters of blockchain technology were altruistic in nature. Causevest is a new type of money that is built to facilitate a positive impact at scale, regardless of the desires of the individuals using the coin.

THE CAUSEVEST PROTOCOL - PROOF OF CAUSE

A proof of stake blockchain with the new reward mechanism proof of cause (PoC)

The Causevest Protocol is a P2P network protocol that uses economic finality to generate persistent global state. The reference client is written in Go and will be publicly available after mainnet launch*. Generating independent economic finality requires the introduction of a new base layer asset - Causevest Coin (XCV).

The initial mainnet release of the Causevest Protocol will have many fundamental features. The Vote, Cause, Nominee, RANDAO, Network Pools and Pots, Proof of Cause, and Finality systems are embedded into the chain. These features are the core of the Causevest Protocol, which is why we decided to release them as part of the main chain.

In particular, the Proof of Cause system allows ordinary users to get rewarded for actions on the Causevest Network in the form of proofs. Users can earn proofs by creating, donating or voting for Causes. They can also buy Proofs outright to support the network and for a chance of converting them to XCV rewards. These rewards come from the Proof of Cause pool and ultimately are funded by Network fees.

The Proofs system is a novel rewards distribution mechanism that lets a large number of people participate and earn meaningful rewards while being sustainable to the network. Actions can earn proofs, which are associated with addresses but are not tradable. Every time period, proofs go through a redemption process. Blocks of XCV are given out randomly to proof holders proportionally. This means that even having a small number of proofs has a chance of earning significant rewards. After redemption, all proofs are reset to zero and the cycle begins again.

THE CAUSEVEST PROTOCOL - SMART CONTRACT INFRASTRUCTURE

Scale to 8 Billion users with our L2 smart contract neighbourhood system

A Causevest Neighbourhood is economically tied to the main chain and shares in its economic finality. Causevest Neighbourhoods use XCV as their base currency, transmitting a portion of their transaction fees to the Causevest base layer and as such support good causes.

To not overcomplicate the base layer, Turing complete programmatic functions ("smart contracts") are designed to be captured by the Layer 2 neighbourhood sidechain system. Any sidechain can have inbuilt smart contracts or the ability for users to deploy their own as the case may be. Anchored in the stability and robustness of the L1, the Causevest Network Neighbourhood System is designed to scale the Causevest Protocol to the over 8 billion people around the world.

A Neighbourhood can have other rules that differ from the base layer, such as arbitrary smart contracting capacity, a larger block size for more transaction throughput, an instant finality mechanism for small transfers or links to external institutions, platforms or chains. Creating a new neighbourhood is fundamentally permissionless, but requires a significant XCV investment. That XCV is used to provide liquidity for users exiting the neighbourhood using instant swaps.

A Neighbourhood is linked to the base layer through a combination of economic incentives, cryptographic proofs and a fundamental time delay for independent withdrawals. Instant withdrawals can be done via a liquidity provider using the Neighbourhood liquidity provisioning network for a small fee.

The vision for Neighbourhoods is for them to be specialised "application" chains for specific use cases. A neighbourhood could be sponsored by a particular institution for their application, or could be a more general field for all applications of a particular class. For instance, there could be a neighbourhood focused on issuing tokens or DEX trading. Some applications might even get enough usage to require multiple neighbourhoods of a particular class to scale.

THE CAUSEVEST PROTOCOL - CAUSE CREATION

Create, receive and earn on chain

On the Causevest base layer anyone can create a Cause to receive funding. Causes have addresses, a category and a donation limit. To create a Cause, a user must pay the cause creation fee: a set fee plus an additional fee that increases depending on the donation limit. The cause can then receive donations and votes to one of their Cause addresses. This allows it to collect transaction fee income from the Causevest leaderboard pot, which allocates funds based on voting power.

THE CAUSEVEST PROTOCOL - VOTING

Vote with XCV to continuously power causes 1 XCV = 1 Vote per day

A user votes with their coins (XCV). Votes are set up once then power the Cause continuously. For example, if a user votes for a Cause with 100 XCV, every block will have (100/720 ~ 0.14) vote power added to the Cause. This is scaled so that 1 XCV voting for 1 day will generate 1 vote power.

A single coin can only vote for one Cause (vote target) at a time and the vote target will continuously collect vote power while it is eligible. Coins that do not have a vote target do not accumulate any extra vote power, so it is incentivised for users to keep their coins voting for maximum reward and impact. This both helps Causes and generates Income for the user.

THE CAUSEVEST PROTOCOL - CAUSE LEADERBOARD

The Cause leaderboard lets you earn from votes

The votes a Cause receives are tallied over the month. At the end of the month Causes can claim XCV for placing on the leaderboard. Higher voted Causes are able to claim more coins. The accumulated votes are then reset and the tally begins anew for the next month.

In addition to positive votes to support Causes, users can also make negative votes at a reduced vote power. If a Cause's vote balance becomes too negative, it is terminated as a Cause stopping it from receiving transaction fee income (although its addresses continue to function as regular addresses). This feature is designed such that only bad or abusive Causes will receive negative votes, if users prefer one cause over another positive voting is much more efficient at supporting Causes.

Once a Cause reaches its donation limit, it is successful and finishes. At this point, it has reached its goal so the network will not award it any leaderboard rewards. The Cause retains its hash and can be reactivated later and its donation limit updated if it is necessary and the appropriate fee is paid.

THE CAUSEVEST PROTOCOL - NOMINEE SYSTEM

The nominee system lets others vote for you

Because there are always new diverse Causes to support, users may want to outsource Cause discovery to a specialist in particular categories. To solve this problem, we introduced Nominees. A nominee is a vote redirector: users can delegate their votes to nominees and these votes empower the nominee in their own vote choices. For instance, if a Nominee votes with 10 XCV for Cause A and 20 XCV for Cause B, a user who delegated their votes to this nominee would get their vote power split 33% (10/30 or 1/3rd) for Cause A and 67% (20/30 or 2/3) for Cause B. A Nominee is like a prism, refracting its delegated votes to the Causes it has voted for.

Nominees can change their vote distribution at any time, but since Causes only accumulate voting power over time a Nominee that radically changes their votes to support different Causes gives delegators plenty of time to change their votes as well. Nominees can also add other Nominees to their vote distribution (but vote cycles are not allowed and Nominees cannot vote for themselves).

The main advantage of this system is that the Nominees are incentivised to find active and live causes that will maximise the users XCV reward generation as they get a small share of these rewards.

THE CAUSEVEST PROTOCOL - ON CHAIN LOTTERY

Proof Of Cause System (PoC) turns good deeds into sustainable lottery-style blockchain rewards

In the Causevest Network, we want good acts to be rewarded so we created the Proof of Cause mechanism, which rewards users that support causes on chain with proofs, allowing them to generate a blockchain income without needing to stake.

A large number of small balances burdens the node runners and users don't appreciate very small rewards. In order to solve these problems we invented the Proofs system (PoC).

Proofs are non-tradeable ticket balances that are associated with addresses on the Causevest blockchain. After a given time period, a random set of proofs are chosen and those addresses can claim XCV from the Proof of Cause pot. The proofs that do not become claims expire and are reset to zero. This system allows many small actions to earn proofs allowing some users to claim a significant amount of XCV.

Randomizing XCV rewards this way allows the creation of an on-chain lottery with the ability to issue a sustainable amount of XCV while also keeping users excited about earning meaningful rewards and reducing the on-chain impact of the rewards.

THE CAUSEVEST PROTOCOL - TRANSACTIONS

Economic system uses automated UTXO accounts to manage rewards

The Causevest Protocol uses a UTXO (Unspent Transaction Output) system for internal coin control. This has advantages with scalability and privacy vs. an accounts model. However, for handling internal network flows (for example, Proof of Cause rewards) there are a series of programmatically controlled Network accounts called pools.

The Causevest Pools direct coin flows in a sustainable manner by having transfers and payouts be a percentage of the pool. This means that the output from a particular pool decreases as the input decreases - making the system sustainable in the long term.

THE CAUSEVEST PROTOCOL - VAULTS

Vaults allow you to reverse transactions to prevent accidental losses

At Causevest, we believe users should have control over their coins. This means transactions can be irreversible if they choose. However, we believe there is often value in placing limiters on what your future self is able to do, to protect yourself. People make mistakes and there is a $3.3 billion dollar problem linked to the incorrect sending of funds. To this end, we introduce the Causevest Vaults system, a system where users can choose to have reversible transactions within well defined limits using vault addresses allowing users to stop losing funds accidentally.

A vault address is similar to a multisignature address in that it is created using multiple keys; however instead of being equal members such as in a multisig, these keys have a hierarchical relationship with each other. Making a transaction from a vault address ("vault withdrawals") requires a signature from one of the keys ("origin key"). There is a pre-set time period which users can pick("withdrawal time") where the outputs of the vault withdrawal cannot be spent and may be reverted using either the origin key or a key higher on the hierarchy.

For example, Alice has a two-key vault with a lower level key (called the "Spend Key") that she keeps on her phone and a higher level Key (called the "Revert Key") she keeps in cold storage. She can initiate a vault withdrawal with the spend key and revert a withdrawal within the vault time using either the spend or revert key. This way if her phone is stolen, the thief cannot take her coins as long as she can react within the vault time. Once a withdrawal transaction is reverted, the key that initiated the withdrawal is ineligible to make another for a limited time, giving Alice a chance to use her revert key to make another withdrawal from the vault to a new address. Since this withdrawal was initiated by the revert key, it cannot be reverted by the spend key, and she recovers her coins.

THE CAUSEVEST PROTOCOL - COUNTERPARTY RISK PROTECTION

Mitigate counterparty risk by tagging vaults and getting stolen coins returned

To enhance security further users can "tag" an empty vault address. A tag is an encrypted string that is linked to the address which cannot be changed while the vault is full. If you tag an address and then deposit coins into it, you can decrypt ("reveal") the tag even if an attacker has a full copy of all of the vault keys. Since the vault is full, the attacker cannot change the tag, even with all of the keys.

This sets the groundwork for the Proof of Forgiveness (PoF) system. There is an on-chain pot called the Proof of Forgiveness pot that can accept coins from any vault using the highest level vault key (the root key). Using the root key it is possible to send the full amount in a vault address directly and irreversibly to the Proof of Forgiveness pot. Once the coins are in the PoF pot, the user can reveal their tag and prove their original ownership of the coins. They can then make a new account and get their coins returned to them.

The PoF system provides a pathway for a diligent user to recover their coins even in the case of catastrophic loss of their keys while maintaining a fully decentralised protocol. This helps exchanges and other institutions who execute the (PoF) feature to protect against theft by allowing them to prove their ownership and have their coins returned in the case of a successful attack against them.

THE CAUSEVEST PROTOCOL - FEES

A dynamic base fee keeps network costs low and blocks stable

In order to keep the cost of operating a full node and permissionlessly verifying the state of the network reasonably low, the throughput of the network must be limited. This is done via a dynamic network base fee that all transactions must pay to be included in a block. This fee is redirected to the network income pool for powering the network's internal pool system. The block generator also gets a 'tip' to ensure they are incentivised to add transactions to blocks.

There are two fundamental limits that must be contented with: first the worst-case time to process a block cannot be larger than the block time, otherwise the system is unstable. Secondly, the computational work to reprocess the full blockchain history cannot be too large. The first limit requires the setting of a hard max block size to prevent the creation of a block too big for the network to process in time. The second limit is more flexible, it requires setting a target for the long run block size that is less than the max block size. This is done dynamically using the base fee. If the block size is above target, the base fee increases and vice versa for being below target. The base fee is designed to change relatively slowly over the day, so users have some idea on what the near term base fee is likely to be and fees do not dramatically increase in a short period of time.

DATASHARES - STORAGE

Update important information without bloating the chain

There is some information (metadata on specific causes and nominees) that is important, small, but needs to be easily updatable and does not need to be stored directly in the chain state. To handle this data we built the datashare system. A datashare is a small signed data packet that is broadcast across all nodes in a p2p manner. A datashare is similar to a transaction that never enters the chain but lives in the datashare mempool. It is not stored as part of the blockchain and nodes can safely discard it if they do not want it.

For example, a Cause address is stored on chain as it is critical consensus information, but the regular name of a Cause and a short description of what it is about is kept in a datashare signed by a key to the Cause address. Datashares are time stamped and can only be updated once per second (nodes will reject datashares that are time stamped in the future. Once the datashare has been updated, nodes will discard the datashare from that Cause with an out of date time stamp. This makes updating data shares free without causing an undue burden from spam.

THE CAUSEVEST ECOSYSTEM

A dynamic ecosystem of on-and off-chain partners

The Causevest base layer (L1) acts as the central building block in a network of interconnected chains and provides security, funding and governance to the whole network. The Causevest Ecosystem sits on top of this and is designed as a dynamic blend of on-chain infrastructure and off-chain enterprise partnerships, working together to create sustainable, transparent, and purpose-driven financial tools.

INTERNAL AND EXTERNAL ECOSYSTEM

INTERNAL ECOSYSTEM

Comprises all applications, protocols, and contracts built directly on the Causevest blockchain.

EXTERNAL ECOSYSTEM

Includes enterprises and service providers that interact with, but are not directly built on our blockchain. These may include NGOs, fintech platforms, oracles, and other integrators.

The full Causevest Layer 2 is built for scalability and flexibility, enabling developers to create specialised modules or subchains that serve distinct purposes, including: Token generation, Stable coins, lending, trading, on-chain oracles, provably fair gaming, incentivised data storage and testing zones for inventing and testing new on-chain programs.

CAUSEVEST SOFTWARE DEVELOPMENT TOOLS

Allowing you quickly build secure and reliable apps

To help facilitate this we will provide a Causevest Software Development Kit (SDK) – a suite of developer tools enhanced by AI-assisted contract creation and standardised libraries. The SDK is designed to reduce friction and accelerate the deployment of secure and reliable applications on the Causevest network.

THE CAUSEVEST FOUNDATION

Cause-focused" on and off chain operations

The Causevest Foundation has elements of both on and off chain operations. The Causevest Foundation acts as a buyer of last resort for all Causevest Coins. Its primary role is to assist with on-chain governance and the distribution of off-chain capital to causes selected by the causevest network.

CONCLUSION

The Causevest blockchain will integrate with the $550 billion digital giving industry. Built entirely from scratch, our blockchain empowers users to have a direct positive impact on the causes that matter to them.

Our custom-built CLI and user-friendly GUI deliver unparalleled on-chain security and privacy that goes beyond merely safeguarding private keys with a focus on ensuring ease of use.

Finally, we incentivise users to compete for their favourite causes, creating a self-sustaining loop of giving that will help with our aim of channelling the world's altruistic transactions through our decentralized network.


CAUSEVEST