CAUSEVEST

Causevest Coin White Paper

Version 1.0

Contents

Causevest Coin - A Peer to Peer Cryptocurrency with Proof Of Cause

White Paper Draft Version 0.9 - Working Paper is subject to change

Abstract

This paper covers the creation of Causevest Coins — the digital currency XCV that is linked to the Causevest Network. Causevest is the first standalone cryptocurrency that is designed to benefit both charitable and non-charitable causes around the globe.
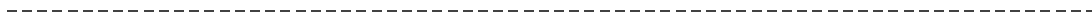
This document details how the Causevest Network incentivises activity that can benefit society as a whole. We combine Proof of Stake with Proof of Cause, rewarding users across the network for actively supporting, maintaining and policing good causes.

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 consensuses 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.

Our open source platform sits alongside the Causevest protocol, giving users utilising the coin's additional features the ability to make tailor-made smart donations and track the end use of their donations. This way, the need to trust a third-party with the power and control over a donation is minimised.

The Causevest Network allows causes to bypass the traditional financial services system. This disrupts and improves the global donation sector, which has become politically corrosive, inefficient and corrupt. We provide an auditable archive for charities, institutions and donation platforms, where they can record the end use of the donations they make and receive on our public blockchain.

Causevest Coin: A New Idea

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

Causevest builds on the idea of disrupting legacy banking systems and paves the way for a new wave of socially conscious cryptocurrency users around the world.

We want owning XCV to be easy and fun. Our platform creates some clear use cases and encourages light competition between users to define which causes should receive the most from our network. The mechanisms within the network enable capital to flow to good causes around the world. As soon as you buy or sell this coin, you have already helped a good cause — it is as simple as that.

There are more than 1000 cryptocurrencies, many of which solve a variety of problems, but the fact remains that much of the technology isn't focused on helping people beyond just making money and speculation. Most tokens are, in essence, socially useless.

The Causevest protocol produces a cryptocurrency you can be proud to own. With it, you can transact anonymously, securely and quickly while effortlessly helping people around the world at the same time.

It is easy to forget that many early adopters of Bitcoin were altruistic in nature. We believed in the idea of creating a new type of cryptocurrency that could scale globally for the common good. Causevest is a new idea and a new type of money that is in its very nature designed to do good, regardless of the desires of the individuals using the coin.

"A cryptocurrency is like a stock, not of a company, but of an idea."

Benjamin Mahala
Technical Architect

Causevest Coin: Now You Decide

Our financial system is designed to reallocate resources from areas of saturation to areas that benefit a few individuals at the top of society. We are then forced to rely on these individuals to reallocate capital from the top down across the economy. We have seen time and time again that this simply does not happen; instead, these people are incentivised to act in ways that have negative externalities and are socially useless.

Causevest was created to change this. By supporting our network, you can allocate resources more efficiently to causes from the bottom up. As a coin holder using the tools we provide, you can help define the causes that the network supports and help causes you believe in.

Causevest encourages altruistic activity in as many people as possible, incentivising positive externalities in a way currently not seen in the world. We foster a form of disruptive altruism, in that each interaction with the Causevest Network leads to a positive impact on a cause, regardless of the user's personal intention.

Every single user of the Causevest Network can generate wealth at the same time as helping good causes around the world: passively by using the coin or actively by directly supporting causes on the network.

> Causevest is broken up into three parts: the Causevest protocol, the Causevest platform and the Causevest foundation.

The Causevest protocol is a decentralized blockchain protocol distributed amongst users who download and run node software. It is independent of, but works in conjunction with, the Causevest platform and the Causevest foundation.

The Causevest platform lets you pick the things your fees are funding from an app on your screen, it sits on top of the protocol and operates as a social enterprise.

The Causevest foundation reinvests excess capital into good causes on the network, helping to create a sustainable cycle of giving.

----
https://www.oecd.org/eco/How-to-restore-a-healthy-financial-sector-that-supports-long-lasting-inclusive-growth.pdf
https://positivemoney.org/wp-content/uploads/2013/10/Banking-Finance-and-Income-Inequality.pdf
https://www.theguardian.com/business/2009/aug/27/fsa-bonus-city-banks-tax

Causevest Coin (XCV)

Technical USPs At A Glance

Use it as a cryptocurrency

You can use Causevest Coins to buy goods, make transfers between your personal wallets, transact anonymously and even hide your transactions. Transactions recorded on the P2P ledger are trustless, there is no double spending and there is a limited supply of 5 billion easily divisible coins. You can protect your wealth from the traditional financial sector by utilising Causevest Coins.

1) XCV utilises a powerful dual-node architecture that maximises decentralisation and is a much cheaper method of storing the world's audit data than other chains'.

2) Moving away from mining means no environmentally damaging electricity waste.

3) Inbuilt security features provided on the protocol layer greatly improve the security of the network and make it easier for the average person to secure their assets.

4) An independent chain means full control of where the transaction fees go, which allows us to have a bigger impact on causes our network users support.

5) We provide clear, easy-to-digest, low-cost public audit trails that charities and other donation platforms can connect to. Anyone can use the protocol as a base layer for this.

6) Like savings in a bank account, users can generate income in XCV by running nodes or by working to maintain the network in order to earn 'Proof of Cause' rewards.

7) The option of strict or relaxed pre-built smart contracts allows donors to have more control over their funds' end use without burdening their end beneficiaries.

XCV

Ownership Stages

There are three stages to your ownership of Causevest tokens.

1) First, when you have purchased our presale ICO tokens, you will be provided with a tokenized receipt of your transaction stored on-chain.

2) This will then be exchanged for XCV, including any bonuses when our ICO goes live. You can trade these coins on exchanges or with brokers.

3) After development is complete, these tokens (old XCV) will be linked to our network and swapped for Causevest Coin (new XCV) directly on our blockchain.

XCV

Use Cases — What Can You Actually Do With XCV?

Use it as a cryptocurrency

You can use Causevest Coins to buy goods, make transfers between your personal wallets, transact anonymously and even hide your transactions. Transactions recorded on the P2P ledger are trustless,there is no double spending and there is a limited supply of 5 billion easily divisible coins. You can protect your wealth from the traditional financial sector by utilising Causevest Coins

Vote with your coins

Causevest Coins have an inbuilt voting mechanism used to signal instructions to the network. Coins are powerful: users have a direct impact on decisions that affect people's lives.

Vote with your coins

Delegate your votes

Not everyone has the time to look for causes or support categories of causes. Special users, called operators, can bid for your voting power for a set period of time and you can earn a share of the rewards they generate by utilising your votes.

Cause One   Cause Two   Cause Three

Work as an operator

Operators can earn rewards for maintaining the network, but after they earn more than £250 worth of rewards, they must hold XCV as a deposit. This XCV is confiscated if they are proven to be a bad actor.

Network cause pool tilting

There is a fixed amount of capital that will automatically flow through the network. By default, it will flow equally across all categories; however, members with XCV can influence how much capital flows into each cause category by voting with their XCV. This adjustment happens quarterly and is somewhat similar to a friendly tug of war inside the network.

Run Nodes

If you have XCV you can make money by staking your coins and running a full node. If you hold a minimum of 10000 coins, your node becomes stacked and earns a higher rate of interest. Finally with100000 XCV, you can run archive nodes that generate the highest staking reward.

XCV: Value Case

Like with all coins, speculation will play a part in the value of our coin. However, XCV also incorporates direct forms of intrinsic value. The value of Causevest Coins will be impacted by three key factors in the early stages of its existence.

Network community growth

As more causes are added, more users are adopted and more operators join the network. Our community will grow. With this comes a fundamental value case for the coin. That is, as more users adopt the coin, its price will go up.

Network profit recycling

Profits generated from the Causevest network services are recycled into the network and distributed to good causes. We need XCV to help redistribute these profits. This creates a natural bid for the coin,boosting the price.

Liquidity growth

When causes receive network donations, these donations are denominated in XCV. To sell the coin,they need to exchange it into (fiat) cash. Doing this increases the amount of liquidity in the network.The market created between donors buying coins and causes trying to sell coins creates a natural non-speculative liquidity, which, in turn, will boost the price positively.

XCV

Coin Economics

To help pay for the development and maintenance of this new cryptocurrency, The first batch of 1.5 billion XCV can be purchased directly by stakeholders. The rest of the coins are created by users staking coins that have already been purchased and using Proof of Cause to generate new coins.

- Total coin supply: 5 billion XCV
- Max coin ICO distribution: 1.5 billion XCV
- Time for 99% of funds to be distributed, assuming no inflows: 70 years

XCV Coin Supply vs Time (Years)
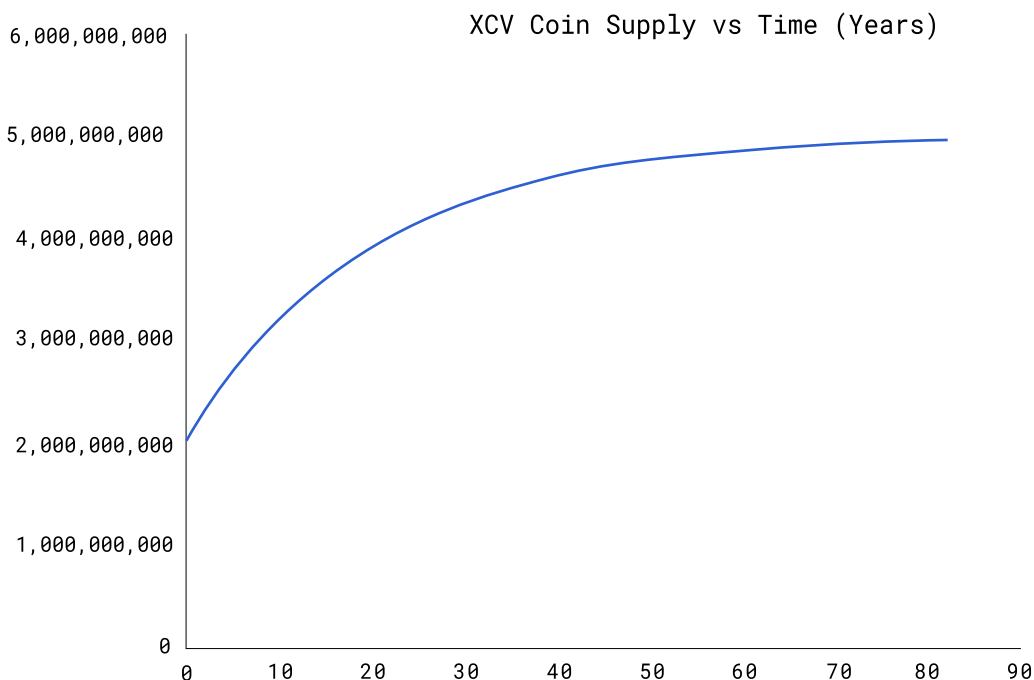
How will the system change after all coins are distributed?

By 2100, over 99% of coins in the Proof of Stake pot will be distributed. At this point, there will be two options available to users: either increase the max coin supply, or redirect a portion of the fees from good causes to staking rewards to support node upkeep. In the case of the coin supply increase, the supply can be increased sustainably by requiring the value of new coins generated to always be less than the amount of profit generated by the entire network. This prevents the creation of new coins from leading to price volatility.

Four Problems Donors Face

Problems the Causevest Network provides solutions to:

The intermediary problem

Almost all donation-based transactions are handled by intermediaries that push up costs and can block recipients from receiving payments. For example when WikiLeaks donations were blocked in 2011. Our blockchain works like bitcoin, in that it allows network users to transact without having to depend on a trusted third party.

A problem of trust post donation

How can you trust that the charity will act as promised once you make a donation? During the Syrian Refugee crisis, a minimum of $70 out of every $100 was wasted from a total package of more then $3 Billion. Our solution is to provide a blockchain-based audit trail and post-donation-based observation tools. Every donor and institution can track the end use of their donations on the public blockchain; if anything goes missing, everyone will see.

Countries with no domestic donation platforms

There are many countries where the level of corruption makes it almost impossible to trust someone to receive and distribute a donation safely. The existence of our network resolves this, as our protocol incentivises users to expand the network and enter multiple markets, seamlessly filling gaps left by the absence of any traditional donation platforms.

Good causes not being supported

There are many examples of good causes that get little support, yet, collectively, have a major positive impact. This problem is not limited to charities, as it includes a range of causes, such as free software, educational videos, volunteers and other quasi-public goods. How do we reach these smaller individuals that can slip through the cracks? Our solution is to reward Causevest users who identify, support and provide proof of a cause existing through our Proof of Cause mechanism.

----
https://wikileaks.org/Banking-Blockade.html
https://www.theguardian.com/world/2017/mar/09/how-greece-fumbled-refugee-crisis
To find out more about investing read our dedicated investors guide https://www.causevest.io/faq#
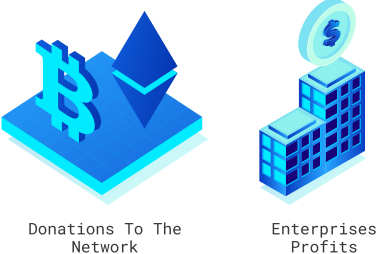
The Causevest Network
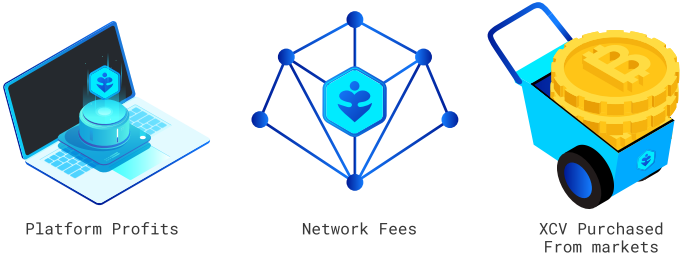
The Causevest Network

The Causevest Network is made up of many individual parties that interact with the Causevest protocol. These individuals may have a multitude of personal objectives, but the Causevest Network is designed to ensure that the end results of these interactions benefit good causes.

Our network involves both internal and external network operations. We define direct interaction with the Causevest protocol as internal network operations. These interactions will often result in a direct record being made on the Causevest blockchain. All other, indirect interactions we define as external network operations.

External Fund Flows

Donations To The
Network

Enterprises
Profits

Internal Fund Flows

Platform Profits

Network Fees

XCV Purchased
From markets

The Causevest protocol will be open source, allowing for anyone to utilise Causevest software to build, operate or connect platforms to our network. Institutions that want to track the downstream impact of their donations will be able to audit and compare their impact on one dedicated and specialised blockchain.

Providing Audit Data
Releases Funds From
Smart Contract

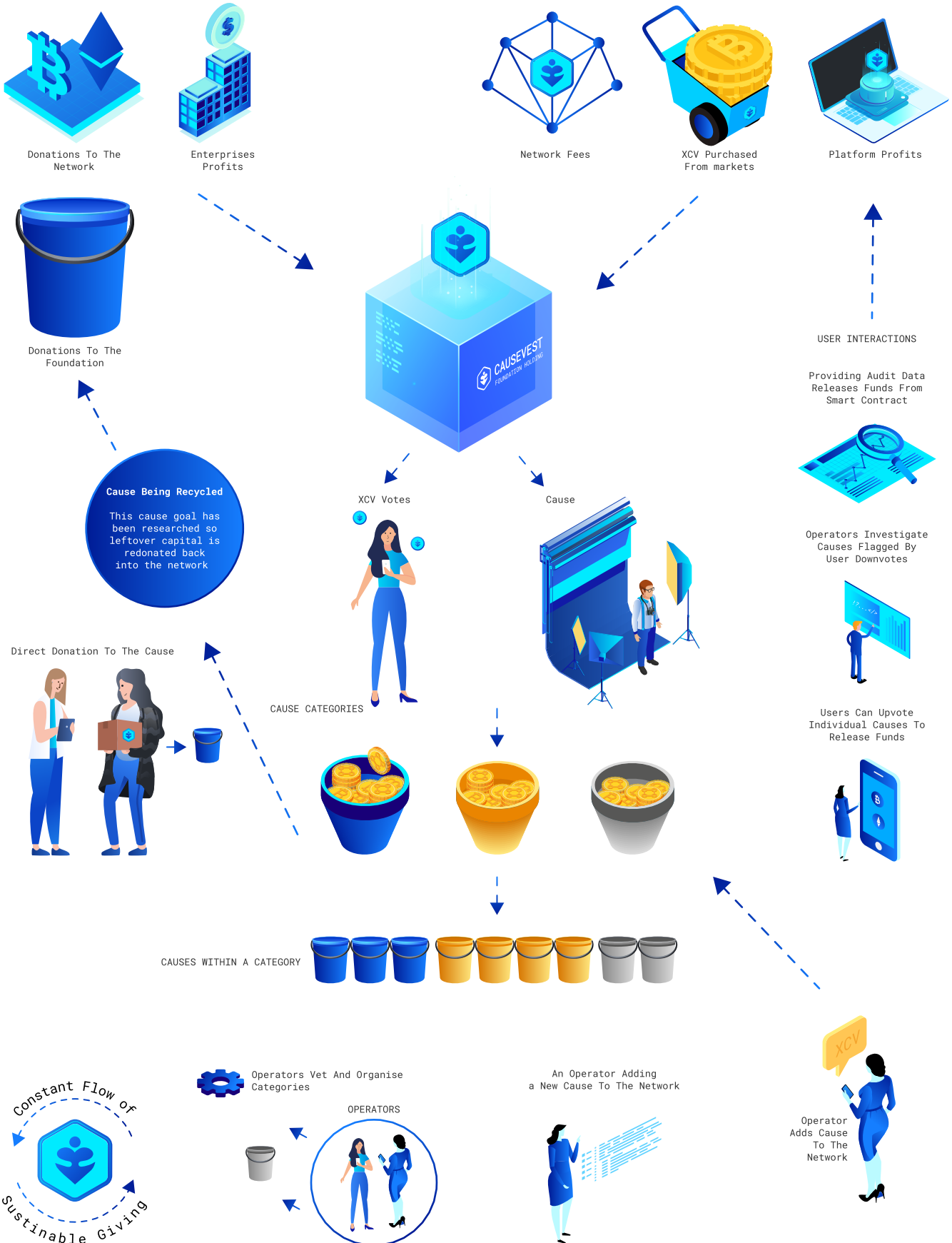Operators Investigate
Causes Flagged By
User Downvotes

One key feature of the Causevest Network is that anyone can set up a campaign and raise funds on behalf of a cause. This enables the network to expand organically, based on user desire and need.

Network Fund Flows

External Fund Flows

Internal Fund Flows

Donations To The
Network

Enterprises
Profits

Network Fees

XCV Purchased
From markets

Platform Profits

Donations To The
Foundation

USER INTERACTIONS

Providing Audit Data
Releases Funds From
Smart Contract

Cause Being Recycled

This cause goal has
been researched so
leftover capital is
redonated back
into the network

XCV Votes

Cause

Operators Investigate
Causes Flagged By
User Downvotes

Direct Donation To The Cause

Users Can Upvote
Individual Causes To
Release Funds

CAUSE CATEGORIES

CAUSES WITHIN A CATEGORY

Operators Vet And Organise
Categories

An Operator Adding
a New Cause To The Network

Constant Flow of
Sustinable Giving

OPERATORS

Operator
Adds Cause
To The
Network

Causevest Fund Pools

Capital donated into the foundation and stored on the network will be held in separate pools. Everything is audited and fully transparent on the blockchain. Donations can come from internal and external sources. We aggregate these pools together and refer to them as the Causevest Pot.

Within the pot are two pool categories: Spec Pools and Gen Pools. Spec Pools contain capital that is distributed only to specific causes, whereas Gen Pools spread capital generically across all network causes, with distribution being effected only by network protocol consensus interactions.

The primary Gen Pool would be the Sustainable Giving Pool (SGP) of £38,351,000 at hard cap.These funds are reinvested and used to distribute income sustainably across the network.

Causes receive network donations from the pot in the form of Causevest Coins purchased at market price. Our sustainable cash flow target of 15% per annum, would equate to £5,752,500 across 1000 causes. We could then provide £500 a month worth of Causevest Coins to each good cause in perpetuity.

+2000 VOTES

2300 CAUSES VOTES   1500 CAUSES VOTES   300 CAUSES VOTES

CAUSEVEST NETWORK CAPITAL
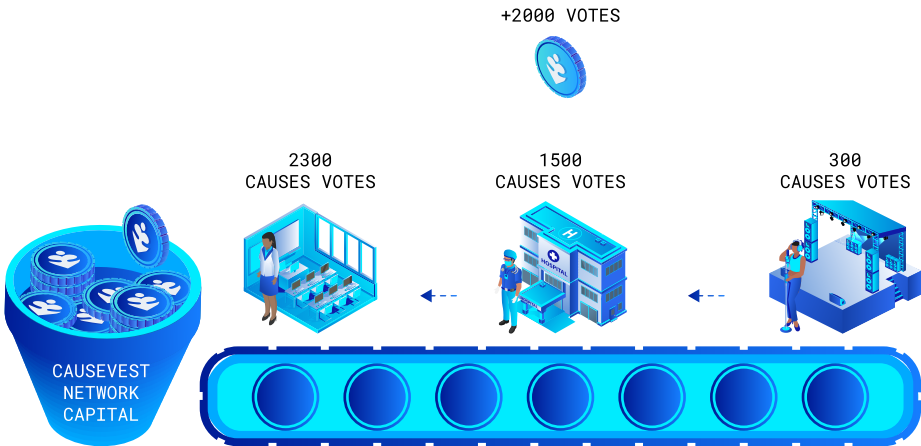
As the number of validated causes ultimately grows, reducing the amount of capital available to each cause, we will move to a conveyor belt system that gives funds to all causes, but prioritises campaigns that users believe will have the biggest impact.

The total Causevest Pot will increase due to donor inflow and user adoption increasing the network size. This increase in network size will be correlated positively with coin value and increase the value of the total Causevest Pot. The Causevest Pot creates a sustainable demand for Causevest Coin, with causes providing a constant supply of Causevest Coin. The end result is a natural and sustainable market for XCV liquidity

The Causevest Platform

The platform itself is revenue-generating, with all profits put back into the network pot. The platform sits on top of the blockchain protocol and the interface between the two allows users to seamlessly interact with the protocol without any coding experience.

The main user types that would have a reason to interact with our networkare token users, donors, operators and the beneficiaries (causes) receiving donations. Donors have more control of their donations, users can set up campaigns for causes and users can generate revenue.

The Causevest Platform: Users

All users can employ Causevest Coins to transfer, speculate or protect their wealth. Users can exchange different cryptocurrencies in the platform's multi-wallet system. An internal marketplace allows users to offer services to charities and causes directly for XCV. Owners of XCV can vote to affect the flow of foundation capital through the network and make use of social media integrations to raise awareness about specific causes.

Fund the causes you believe in

Causevest give users the opportunity to leverage on the power of community to acheive their dreams.

Get Started   Explore Campaigns

See how far a little can go by funding campaigns

Get Started

The Causevest Platform: Donors

Donors include any user that makes a donation to a cause listed on the Causevest blockchain. They can give directly to causes via the platform or donate to unverified causes via the protocol. Donors that utilise the Causevest Network are rewarded with the chance of generating XCV rewards when they make donations.
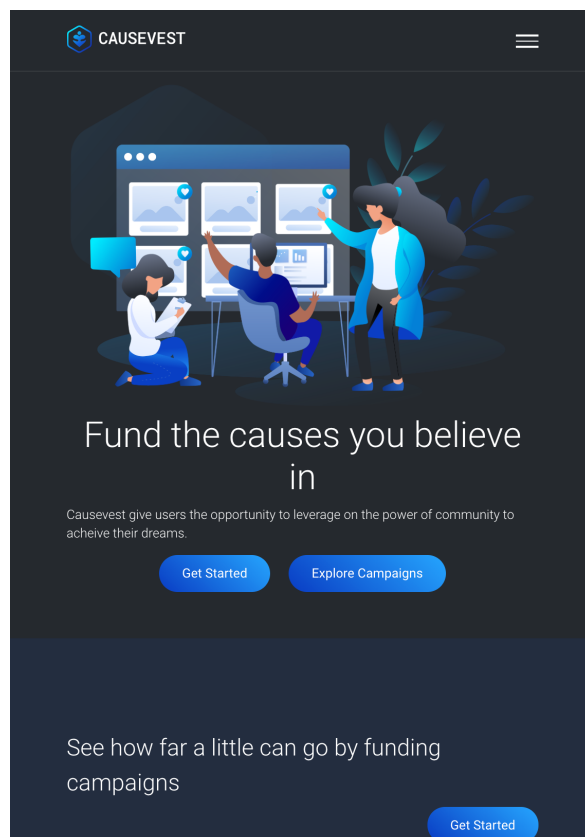
Donors have more control

Donors can utilise a variety of donation types, including direct, periodic and smart donations. Smart donations involve creating a smart contract that only releases funds to the cause if certain criteria are met, effectively removing the need for a trustee and encouraging better behaviour from causes that receive funding.

No fees will be added to transactions done via the platform to verified causes. Donors can track and audit the downstream impact of their donation on our blockchain, and they can make either traceable or anonymous donations utilising our protocol. We boost and reward those who donate to popular causes or have pledged their XCV to a particular cause.

The platform helps users visualise the audit process by taking multitudes of complex data and summarising it into easy-to-digest information and images. Donors that donate via our platform can also encourage others to support their causes. This counts as Proof of Cause (POC) and increases the probability of generating new coins for all donors.

Platform: Smart Donations

There are three types of smart donations that can be automatically generated on the platform: strict smart donations, flexible smart donations and Vested smart donations.

Strict smart donations have a list of criteria, created by the donor, to be met before the donation goes through. Flexible smart donations are an open donation type with softer guidelines.

Flexible donations are monitored by the community, with user collaboration ensuring that causes behave according to the donor's original intentions. The users that monitor these flexible donations are called operators and their work is rewarded via Proof of Cause (POC). These contracts would continue to be executed even in the event of the donor's death, allowing users to create smart donations that act as digital wills on the blockchain.

A Vested smart donation is a special donation that is designed to pay out in perpetuity or until a cause's objectives are completely satisfied. This is done by taking the initial donation from the donor and gifting it to the Causevest foundation. These funds are then invested by the foundation to generate a steady stream of cash flow, with the profits paid out to the donor's selected cause.

Example of fund release:

The Causevest platform will have a set of smart donation contracts we have vetted as safe, but you can create your own contracts if you desire. For example, the following pseudocode describes a contract that releases funds to a donation address when someone uploads data as proof to the chain.

```python
class SmartDonation:
    def __init__(self):
        # Initial Donation address
        self.donation_address = "d-BvBMSETstWetgTFn5Au4m4GFg7xJaNVN2"
        self.transfer = xcv_python.Transaction

    def release_funds(self, proof, address):
        # Set the address, if none is passed, use default in __init__ function
        self.donation_address = address
        try:
            # Check for proof of cause
            if proof:
                # Send funds via xcv_python library
                self.transfer.send_transaction(self.donation_address)
        except Exception as e:
            print(e)
```

Donors can change the end recipient at a later date. If a donor is unhappy with a cause or just wants to change who receives their gifts, they can notify the network and the flow of funds will be redistributed to a new cause. This is very different from how donations made to charities normally work. Currently, donors lose all control over the donation once it is made, even when much of their capital ends up being held in investment companies.

The Causevest Platform: Operators

We define users that actively work to maintain, support or expand the network as operators. Our platform acts as a focal point for operators, allowing them to generate additional coins by doing a multitude of deeds we define as providing Proof of Cause. Anyone can act as an operator. We split operators into two general types: Supporter Operators and Maintainer Operators.

Supporter Operator

A supporter will actively find a cause that they want to support, publish it on the blockchain via the platform and utilise platform tools to see if anyone else wants to support the same cause. If other users support the cause with donations, Causevest capital is added as well. Supporters get a sustainable share of the funds donated to the cause, which also increases their probability of generating new XCV via Proof of Cause (POC).

Maintainer Operator

A maintainer will uphold community guidelines and procedures for due diligence. When a cause is created, maintainer operators help to validate the identity of the end beneficiary, check audit data for mistakes, present due diligence on causes, organise categories, resolve any contract disputes and vote on the overall integrity of the cause. With user permission, operators can harness voting power from users' dormant coins and use that to assist with their role as a maintainer. These actions also increase the probability of generating new XCV via Proof of Cause.

A PERSON MAKING A DONATION

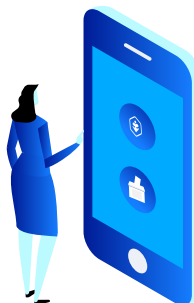

A PERSON HELPING TO RAISE MONEY

A PERSON VERIFYING A CAUSE

AN OPERATOR CREATING A NEW CATEGORY
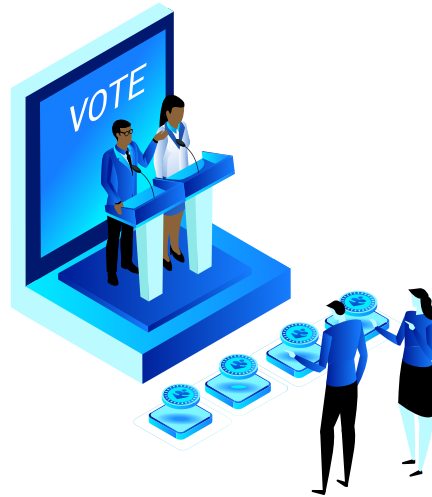

AN OPERATOR VOTING

AN OPERATOR AUDITING A CAUSE

There is no initial financial barrier to entry for an operator and operators have the freedom to decide how involved they want to be. There are many causes that currently accept online donations, these are easy targets for operators to receive rewards by registering them on our network.

Operator rank and reputation are effected by deeds on the network. Operators can choose to work at a geographical level and encourage collaboration in larger groups, they can focus on only working within a specific category of causes or they can opt to work alone on causes that are important to them. Whatever the chosen method, the Causevest Network provides a new way to incentivise
actions that have a positive downstream impact.

The Causevest Platform: Beneficiaries (Causes)

A beneficiary is any end recipient of a listed cause that has registered, or has been registered by an operator, on the blockchain with an activated donation wallet address. It is possible for beneficiaries to receive donation capital from users; however, to gain full access to the Causevest Pot, a cause's end beneficiary must be validated. Charities that register as causes can make use of any tax bonuses that they currently receive on the platform.

A beneficiary can receive donations directly in multiple cryptocurrencies, in fiat via the platform's internal exchange or in XCV donations using our software client. They can also create campaigns, request to be supported periodically, advertise themselves, upload audit data, set up automatic cashouts through our exchange, add our social media links to their websites and spend XCV directly on our internal market place.

The Causevest Platform: Beneficiary Audit Trails

Audit data can be uploaded to our blockchain and if linked to a smart donation contract, unlock additional capital from the Causevest Pot. The Causevest Network has storage space for charities, platforms and causes around the world to provide an audit of their downstream donation data. This includes receipts, images and small videos. The data is given a hash and recorded on our blockchain. This database of information aims to improve the standards of beneficiaries around the world that receive capital.
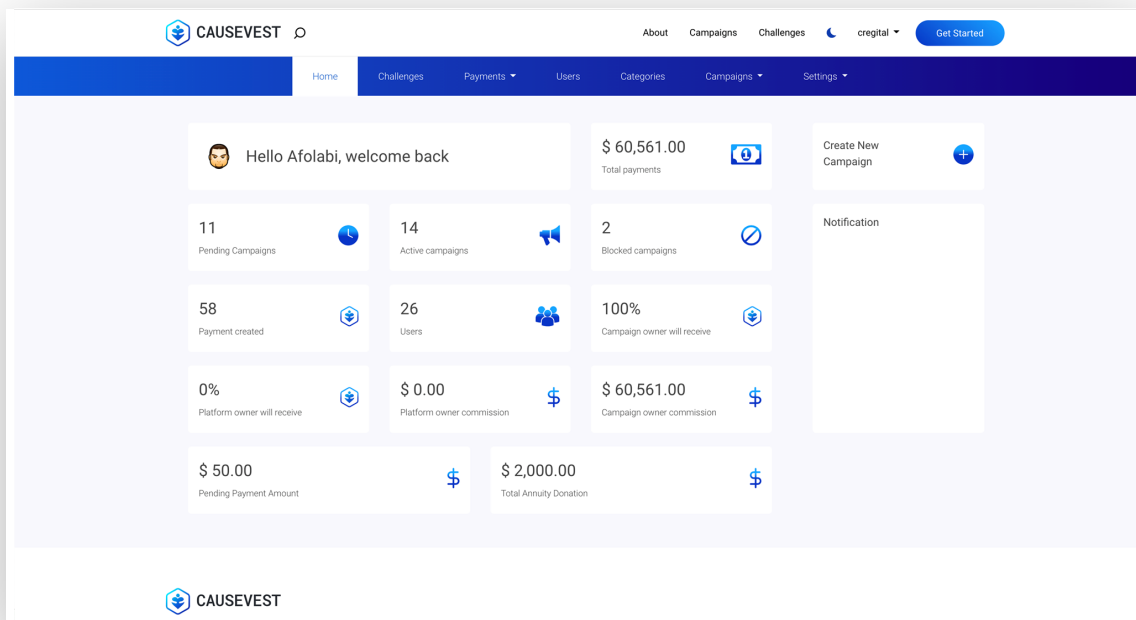
The end beneficiary can claim any causes linked to them, as well as set up their own campaigns on the platform's cause manager.

Beneficiaries can also tag causes to give themselves a unique cause wallet identifier. This allows donors to match causes they see offline to their Causevest wallet addresses easily

External Network Operations

Our external operations capture all activities that interact with the blockchain indirectly. They include activities that extend past development and protocol maintenance. The primary focus is always generating revenue back into the network to help good causes.

Offline Fundraising

We will actively fundraise for causes listed on our network offline. When we raise capital for causes, we forward it to them in a mixture of local fiat and XCV. The aim is to grow the network capital pot, create a natural demand for XCV and increase general cryptocurrency adoption.

Corporate Partnerships

We will work with different corporations to highlight good causes they are currently supporting, as a form of brand promotion. This is similar to how Fairtrade operates, but with a focus on providing proof that the end use of the donated funds is a good cause.

When someone sees the Causevest logo, they will know a portion of their money goes towards good causes in a way they can monitor, debate and influence. Operators can also work with partners to help manage their campaigns on the network.
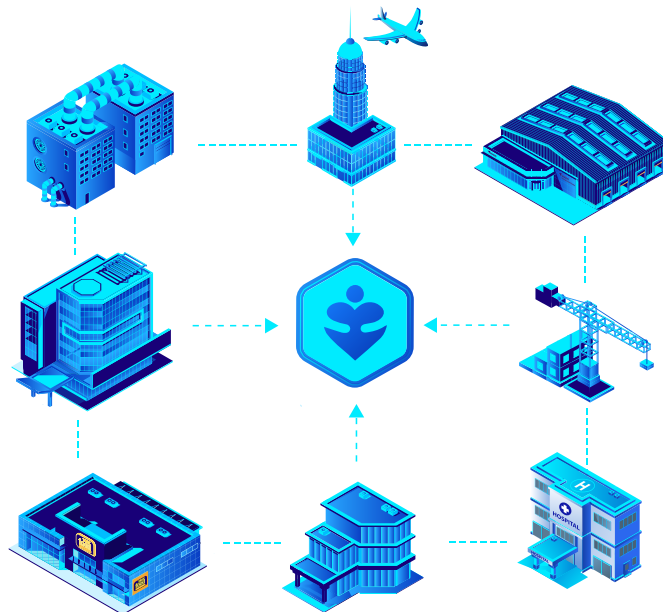
Investment Strategy

We have a proven track record of investment success within and outside of the cryptocurrency sector. Working with chosen partners, we will focus on strategies that generate sustainable sources of income back into the network.

Timeline

Stage 1
3 months after raise

Development and infrastructure setup work begins.

We will also establish any infrastructure and structural setups in jurisdictions.

- Creation of holding company, investment funds, fundraising arms, charity and social enterprises

- Enterprise hub setup

- Creation and localisation of foundation

- Providing cash flow to charities via our flagship fund, Cryptovest, begins

- Pre-registration of causes

- Development of MVP (minimum viable product) begins

Stage 2
9 months after soft cap

The goal of this stage is to release a MVP to showcase the core system architecture of the Causevest Network.

We begin work on a functional donation platform that users can donate to and raise on. Development of the platform's backend begins.

- Protocol test net released on GitHub

- Wallet building with backward compatibility

- MVP platform created

- Database setup

- Beta testing

- Testing of full net of protocol on GitHub begins

Stage 3
12 months after soft cap

At this stage, we will look at testing and functionality, primarily focusing on removing bugs in our system.

Our trade market, Causevest Pool and smart contracts will be tested with causes listed on our platform. We will also begin testing and finalising the POC code, integrating it into the protocol through nodes linked to the platform.

- Exchange and market place integrated into platform

- Full Operator functionality

- Functioning audit features linked to blockchain

- Testing of smart contract functionality begins

- Old XCV coins swapped for new XCV coins

Stage 4
24 months after soft cap

After 24 months, we expect to have full network functionality, primarily resulting in a fully functioning, standalone blockchain.

POC will be perfected and allowed to run, with tools to link institutions and charities onto our blockchain's auditable nodes.

- Finalised protocol created on GitHub

- Full client with wallet for user access

- Creation of test net

- Open source donation platform API link to our protocol developed

- Expansion of enterprise hub

- Work with corporate partners begins

The Causevest Protocol

- **Purpose build participatory budgeting blockchain -** Transaction fees get pooled on the Causevest Network and redistributed to good causes as voted by coin holders like you.

- **On Chain Vaults -** These special addresses allow you to store coins in a hot (online) wallet while maintaining the safety of a cold or hardware wallet.

- **Dual Node Architecture -** This allows us to drastically cut the cost of storing audit data alongside our nodes while preserving data integrity.

The Causevest Protocol

The Causevest protocol is the protocol for the decentralised Causevest Network. This protocol specifies the creation and maintenance of a Proof of Stake (PoS) and Proof of Cause (POC) blockchain.

This blockchain is specifically designed for optimised audit trails and reallocating transaction fees to causes that coin holders signal by voting. Initially, the protocol will be specified by the Causevest open source wallets; when the system has stabilized and needs no further improvements, a formal specification will be written and released.

The Causevest Protocol: A Focus on User Experience

The cryptocurrency space has a problem with hostile user experience that holds back adoption and has led to millions of pounds of losses.

There are a large number of actions users can inadvertently take that can lead to a compromise of their funds, such as the loss of keys due to hacking, forgetting passwords, drive failure, mistyping addresses, contract bugs and phishing sites.

The Causevest protocol minimises these issues and has fail-safes that can save funds. In particular:

1) The address formats are unique, containing a mandatory checksum.

2) The protocol incorporates multisignature wallets on the base layer, and the core wallet has a simple multisig GUI (General User Interface) that makes securing your coins with many keys easy without using the command line.

3) The protocol has Sirer vaults on the base layer and the core wallet has a simple GUI that lets you lock up your coins in a vault using two keys. In the worst case, criminals cannot steal your funds, only have them donated to the protocol.

4) To help protect users from the failure of counterparties, such as exchanges, funds caught in a wide-spread attack are donated to the network. If a user is found to have lost both keys of a vault to an attacker, they can petition the network for a forgiveness payment from the Proof of Cause funds. These funds come from the protocol and do not require reversing transactions or forking, preserving immutability

Protocol Block Structure

The protocol has two types of blocks: transaction blocks and data blocks. These blocks are intertwined to form one chain, even though they have different properties and are handled differently by two types of nodes. Transaction blocks are handled by transaction nodes, which are responsible for generating transaction blocks via the Proof of Stake mechanism, holding transfer transactions in their mempool and verifying the integrity of the chain. Data blocks contain audit data for the Causevest chain. This audit data is uploaded to the chain by causes, to verify that they are not fraudulent. Causes upload audit data as part of their operations, making it publicly available to all.

Data blocks are handled by archive nodes; however, the header of each data block contains a Merkle tree of all the data transactions in the block, and all the headers are distributed to the transaction nodes. This way, not every node needs to have a full copy of the data; the system allows the archive nodes to store the audit data, while also allowing any node to check that the data has not been tampered with by comparing the hash of the data with the hash in the block header.

The transaction chain has a shorter block time of around 1 minute. Transaction blocks only include transactions that move XCV into or out of addresses. The transaction chain includes the data block headers. Data blocks contain a header with the hashes of all the data stored and the data itself. Data blocks have a longer block time of around 10 minutes. Archive nodes generate data blocks using Proof of Stake. They then create finality by using a variation of the technique described in https://arxiv.org/pdf/1710.09437.pdf, called the Casper friendly finality gadget (Casper FFG). This allows archive nodes to generate finality for the entire system.
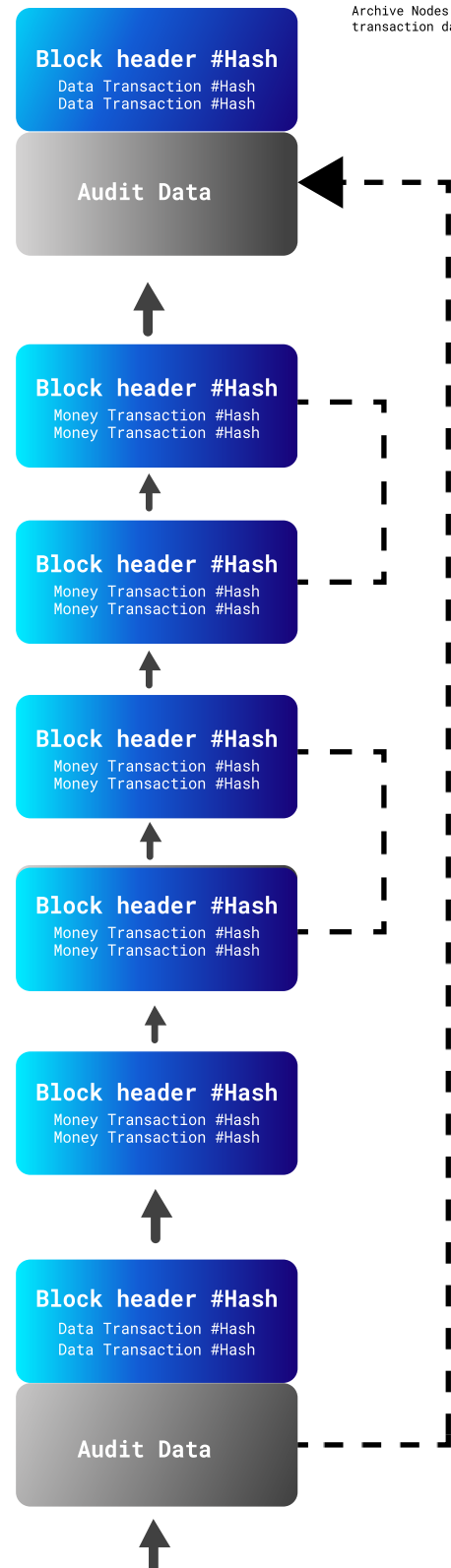
An Example of Network Protection

Finality refers to a state in which a checkpoint is created on a block that cannot be reverted without violating a slashing condition. If a slashing condition is violated, the validator loses part of their deposit. Finality is created by voting on blocks during a time period called an epoch. Once two thirds of the validators (weighted by their deposit amounts) have voted on a block, that block can be said to have achieved finality.

The slashing conditions are illegal votes. For instance, voting on different blocks in the same epoch is violating the no-double-vote slashing condition. If a block does not achieve finality in one epoch, validators get a chance to vote again on the next epoch. Due to the way blocks are linked in a blockchain, finalising one block means finalising all blocks before it, so even if finality is not achieved for a period of time, once a block is finalised, it is fully restored.

Validators get rewards when they vote on the block and lose money if no block gets two thirds (2/3) of the vote. This means that the best an attacker can do is revert finality, by losing one third (1/3) of all staked coins or by not voting with at least one third (1/3) of all staked coins, which will slowly drain their coins until the subset that does vote has two thirds (2/3) of the weight and finality can be reestablished.

Block Proposal Mechanism

Blocks are proposed by transaction and archive nodes using a NXT-style Proof of Stake mechanism (https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf). Archive nodes need to hold Causevest tokens in escrow, on chain, in case they violate a slashing condition. If they violate a condition, their escrow is donated to the network. Archive nodes have a minimum deposit size of 100,000 XCV at risk to insure good behaviour and a minimum withdrawal time of at least 3 months since the last stake.

to make sure the archive nodes actually keep a copy of the data and do not delete old blocks, the creation of a data block requires hashes of shards of data from random points in the data chain, along with Merkle proofs that this data is part of the main chain.

Other archive nodes do not accept blocks that have faulty or absent proofs. As an additional requirement, transaction nodes must download and check these proofs before they accept a data block header into the main chain.

Protocol Level Features

In addition to simple transfers, the Causevest protocol supports multisignature addresses and Sirer vaults. A multisignature transaction requires the signature of multiple parties to be valid, increasing security.

A Sirer vault is an address with two keys and has a time delay between when a withdrawal request is confirmed and when the funds move. A withdrawal can be created with the first key, but it can also be cancelled before the funds move, with a special cancel transaction signed by the second key. This second key can also be used to move the funds to a safe wallet that uses different keys. In case the second key is also compromised, the second key can irreversibly donate funds in the vault to the network before the transaction goes through.

Even if an attacker gets access to both your keys, they cannot make a profit from trying to steal from you. Having multisignature addresses, as well as vaults, on the protocol layer greatly improves the security of the network and makes it easier for the average person to use and to secure their assets. These features are also easily accessible in our main wallet, so people can access them without having to go to a third party or use the command line.

Simple Address: An address that has one key and one lock. The funds can be accessed instantly when the lock is opened.

Pros: Funds can be sent instantly by one person. Good for small payments.

Cons: Funds can be lost if the key is missing or stolen.
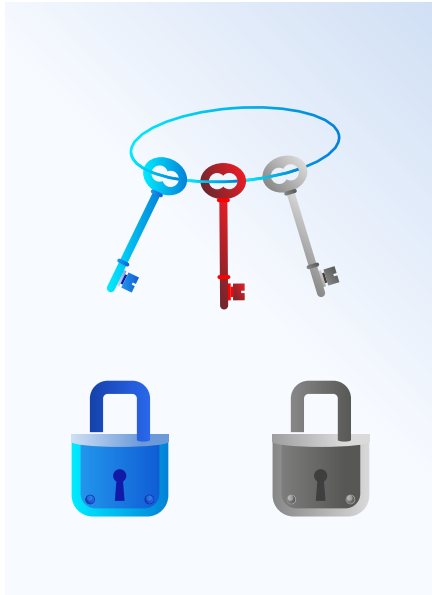
Multisignature Address:
This address has M keys and N locks, with the restriction that the number of keys be greater to or equal to the number of locks. Each key can only be used once, but it can open any of the locks.

Pros: Funds cannot be used without access to multiple keys. If the keys are distributed to multiple people, the system is more secure. Cons: All participants might sign off on every transaction. This can cause coordination problems. If all the keys are stored together, this is no more secure than a simple address.
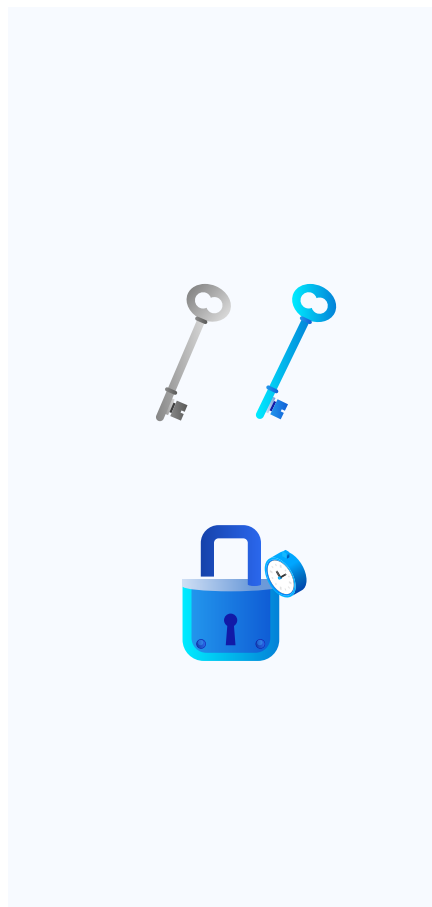
Vault Address:
A vault has a time lock and two keys. One of these keys is a send key, the other is the master key. To make a transfer from a vault, you must wait a predetermined amount of time before the transaction is finalized. Either key can initiate a transfer, but the master key can reverse transfers started by the send key before the time is up. The master key can also donate funds directly to the network, and this action is instant and irreversible.

Pros: The master key can be heavily secured, preferably offline, while the send key can be kept available for convenience. If the send key is lost or stolen, the master key can be used to reverse the transaction. In addition, if both keys are stolen, the funds can be irreversibly donated to the network to prevent the thief from profiting.

Cons: The time lock on the address cannot be bypassed, so instant transfers are not possible.

Proof of Cause

Proof of Cause (POC) is a mechanism for rewarding those who do work in the Causevest Network. We want to reduce the barrier to entry for new adopters and incentivise work that has a positive impact. The POC system rewards users outside of simply running nodes, so cryptocurrency adopters who are less technically proficient can still be involved actively in new coin generation.

The ultimate goal is a decentralised voting mechanism that rewards operators for their work
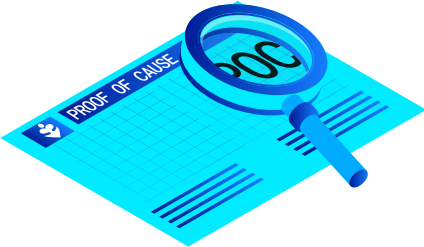
The Cause Worker Node

Proof of Cause rewards are allocated using a special Cause Worker Node. This 'Cause Worker Node' differs from wallet nodes and archive nodes. The node does not interfere with the decentralised network consensus, only with Proof of Cause reward distribution.

The 'Cause Worker Node' takes new coins out of the protocol pot to distribute as POC rewards. These rewards are based on preset criteria being fulfilled in the form of inputs and rules.

Generating Proof

Operators are rewarded in two ways, a fixed share of the profit generated in fees from any cause associated to them that receives donations and new coins for the work they do within the network.

POC is concerned with the distribution of new coins within the network. When a Supporter or Maintainer Operator completes a task that is recognised by the Cause Worker Node, they generate 'proofs' which increase the probability of generating a new XCV Coin. The more work you do in the network, the more proofs generated and the more coins you earn.

Proofs represent the artificial mining power generated by each user who does work in the Causevest Network or makes donations to causes. The more proofs a user generates, the more likely they are to receive new coins in the form of XCV.

Use Of The Platform In POC

The Causevest platform allows operators to interact with the protocol and rewards operators who create and police good causes on the Causevest Network directly. It is possible to interact with the protocol directly however the platform allows users to do this with ease. For example Maintainer Operators can help police the network by verifying popular causes and removing look-alikes who are stealing the brand of legitimate causes for their own gain. Operators who vote actively signal information to the network and again are rewarded with 'proofs'. The goal is to move to a community policing standard and reward hard-coded POC rewards on the protocol, so that we can provide decentralised rewards for work done on chain without the need for any platform.

The Causevest platform acts as a temporary authority that can verify good actors and expel bad actors, building governance in areas that do not affect the protocol's ability to create blocks or verify transactions.

As time goes on, we will move to a quasi-decentralised system and then a fully decentralised system where many different platforms live on the Causevest blockchain. This requires adopting decentralised cryptoeconomic methods to curb abuse and reward public goods in ways that cannot be exploited by bad actors. The type of jobs captured by POC will increase and Cause Worker Nodes will be operated by users outside of the foundation.

Coin Holders Can Use Their Votes In The Following Ways:

1) On causes, for visibility and for the distribution of network fees.
2) On categories of causes, for the distribution of network fees.
3) On evidence / audit data, for visibility and to reward people for uploading important evidence both for and against causes. Evidence of fraud is an important thing to upvote.
4) On dispute resolution using prediction market voting. This is for important decisions, such as deciding whether a cause is a scam or has committed fraud or some other crime.

Forgiveness payments

These are reimbursements for funds that have been donated to the network from a vault or from a node deposit, if the owner can prove they lost the funds due to hacking or error. These do not change the history of the network and are not given out easily. Evidence must be presented to the community and transactions cannot be reversed. We use this mechanism to help protect our users from failing exchanges.

Voting and Proof of Human Work

In general, humans vote to decide what counts as a good cause on the network. This is one of the easiest ways for users to generate new XCV. 1 XCV gives the user 1 vote on any area of the network.

We also provide tools to help analyse collected data and automate the voting process. This means that collective voting is the main way for the protocol to achieve distributed consensus on what is a good cause and what audit data is fraudulent. To prevent Sybil attacks, votes must be connected to something that is not easily reproducible — mostly likely XCV itself, although we are interested in alternative methods of using decentralised identity to prevent Sybil attacks.

We propose the following systems within the framework of a liquid democracy:

Direct voting with XCV
1 XCV = 1 upvote or downvote. This system is most useful for visibility and is not damaging to the network when people change their votes rapidly.

Locking XCV to vote.
For example, locking 1 XCV for 1 unit of time = 1 vote. This relationship need not be linear. This system is useful when it is important for voting to be costly, and it keeps a small oligarchy from controlling many votes at once. This system allows a smaller, dedicated entity to outvote a larger, richer, less dedicated entity.

Prediction market voting
In this system, people can vote by staking XCV with either an upvote or downvote on a question that is decidable (e.g. whether a cause is fraudulent). Then, a panel of operators decides if the question is true or false. If it is true, the upvoters get a portion of the money that the downvoters staked, and vice versa, if it is decided to be false. A panel need not decide on any particular question; the threat of a decision can keep people from trying to exploit the system for considerably less labor. This system is useful for questions of fact, such as 'Is this cause scamming?' It is not useful for questions that might cause contention, as any answer would be very controversial.

Vote delegation
In order to increase efficiency, people can delegate their votes to a third party to go through research causes and vote on their behalf. An operator that accepts vote delegation is eligible for Proof of Cause rewards, and the full history of voting is public and shown on the platform to provide accountability

During the development of the Causevest Network beta, we will run simulations of these voting algorithms, along with any other promising techniques we find for solving this voting problem. We will model various usage levels, XCV prices, voting patterns, payout rates and possible fraud rates to find an acceptable model for a Proof of Cause that rewards participants and is not gameable.

Stages of Decentralisation

Initially, knowledge of the protocol's and platform's construction will be centralised in the foundation.The wallet's code will, of course, be open source, but the institutional knowledge of how that code works and how to improve and maintain it will be centralised in the minds that created it.

Within 2 years, we plan to have moved the system to greater decentralisation by creating, testing and releasing a fully decentralised Proof of Cause system and removing the powers of our master node. We also want to encourage the development of full node and archive node wallet software controlled by teams independent of the Causevest foundation. We will also encourage other platforms to use our protocol and grow on top of it.

The purpose of encouraging decentralisation is to create antifragility in the Causevest system. If the development team is decentralised, not only can work on the protocol be continued if the Causevest foundation can no longer continue development, but diffusion of knowledge acts as a check on the Causevest foundation's power. If the foundation supports an unpopular hard fork, the remaining development teams can support the other side of the fork and continue work on the popular vision.
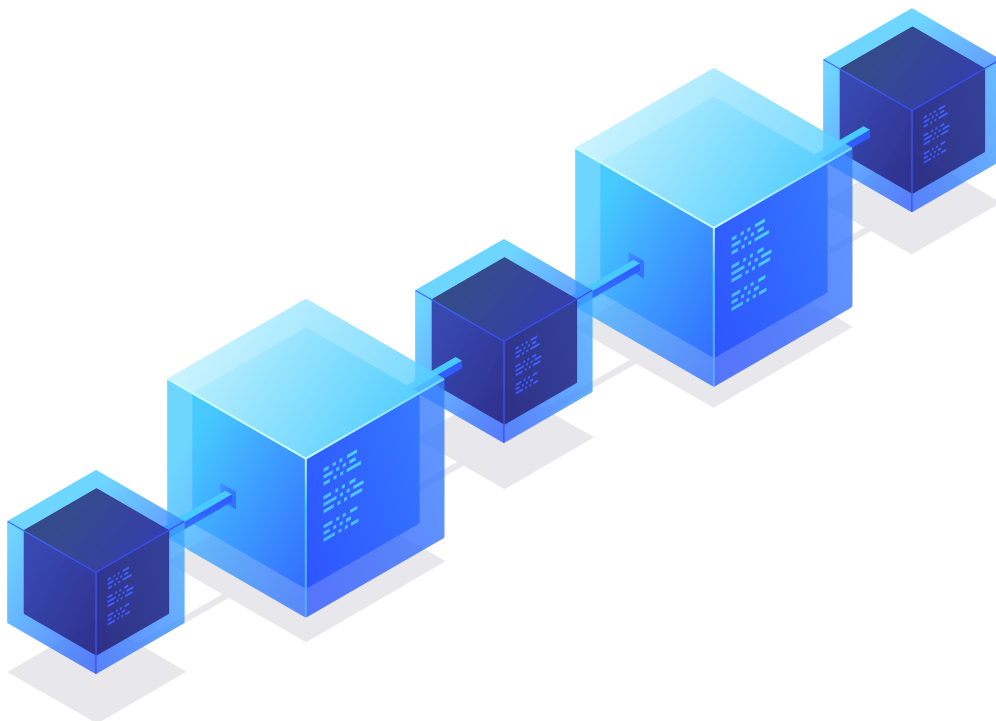
Coin Distribution

Equations

The equation for the total coin supply at a given time (t) is as follows:

$$C_s(t) = C_T + (C_I - C_T)F(t)$$

Where F(t) is the current supply CT is the total supply, which can be constant, and CI is the initial supply of 2 billion XCV. F(t) is a distribution function with the following properties:

1) $F(0) = 1$
2) $F(\infty) = 0$
3) F is monotonically decreasing.

Imagine a pot full of coins that has holes in it. At every moment, each coin has a chance to escape the pot. The number of coins left in the pot after some time depends on how many coins are in the pot, and how the probability of escaping the pot depends on the number of coins still in there. In the limit that each coin can escape independently of the others and is not impeded by them, the total amount of coins in the pot will decrease exponentially, and F(t) is an exponential decay function. However, if the presence of other coins increases or decreases the probability of a coin to escape, the amount of coins may decrease faster or slower than an exponential

The equation for the rate of change in the coin supply is given by:

$$\frac{dC_s(t)}{dt} = (C_I - C_T)\frac{dF(t)}{dt}$$

This is the derivative of the first equation. If you continue the analogy of having coins that can escape a pot, this defines the amount of coins that escape at any given time. If you think of the stakers as being in the business of catching coins as they escape the pot, this is the amount of coins they will be rewarded with. Since, in the proof of stake model, you must use coins to catch coins, this equation defines the effective minimum interest rate. Note that the real interest rate experienced by a staker is dependent on the percentage of coins being staked. If everyone shows up with all their coins, they get the minimum interest rate. If only a few people show up, they collect all the coins that escape, even if they only have a handful of coins themselves.

Nodes

Running and operating a node is a way to generate new XCV. The most basic node involves you holding at least 1 XCV and the full blockchain via a downloaded wallet. In this case the more XCV you own and stake in your wallet the more new XCV you can earn as interest.

There is a universal interest rate for stakers that run nodes, with higher rates going to loaded nodes that hold a minimum amount of 10,000 XCV and to archive nodes.

We want to encourage archive nodes, so incentivising people to pool their funds to run an archive node is good, so long as they are willing to pay for the extra costs of storage. In order to allow for stake pooling requiring minimal trust and protect individuals pooling, we will create a new kind of vault pooling address. It will have a minimum of 3 months' unvault time, allowing staking for the owner of the address, but can be withdrawn only into the address that sent the coins into it and only by the person who originally sent the coins, not the address owner. The interest is calculated at withdrawal time and added to the withdrawal amount.

Since there is a limited amount of coins, the interest rate must decrease with time so long as new coins are not added. To maintain network integrity, the interest rate should vary smoothly to prevent fast drop-offs in the interest rate, which could cause problems for stakers. Once a test net is running, we will run simulations to try to find the optimal decay rate depending on probable network conditions. In the meantime, it should be assumed that an exponential decay rate will be used, as it is the simplest function that meets our requirements.

Protocol Changes

The publicness of the blockchain's data and the necessity of open-sourcing the wallet software imply that anyone can make changes to the protocol and fork the coin. This is an acceptable check on the power of the official foundation protocol and encourages innovation by allowing new players to build off existing tech. To maximise this freedom, the Causevest foundation prefers to do major protocol updates with hard forks. This gives users the chance to fork off into another chain instead of implementing our changes, if they so desire. In the beginning, it is unlikely anyone will choose to support the fork chains, because the Causevest foundation holds most of the development experience and resources. However, as the system grows, this creates a check on the foundation's power and allows stakers or other platforms to opt-in to any controversial changes.

Privacy

The system uses pseudonymous addresses, similar to Bitcoin. We have a decentralised mixer in the wallet, and we will add additional privacy in the future, as new features are developed and tested in the cryptocurrency ecosystem. The current technology behind privacy protection, such as ring signatures, zero knowledge proofs and bullet proofs. is very new and undergoing rapid improvement. We do not want to compete directly in the privacy market, and the current tech is too new to incorporate directly without opening us up to risks that may not be fully understood. As the technology behind these privacy controls matures, we will add these features into the system.

Ring Sigs: https://cryptonote.org/whitepaper.pdf
ZK Proofs: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf
Bullet Proofs: https://web.stanford.edu/~buenz/pubs/bulletproofs.pdf

Transaction Fees and Block Throughput

In any blockchain system, a transaction fee is required to prevent spam attacks against the system that overwhelm the nodes and bloat the blockchain. However, if the number of transactions entering the system is greater than the capacity of the system, the fees must increase to decide which transactions are allowed. This can eventually lead to exploding fees that render the network unusable for many applications, as in the case of Bitcoin having fees so high that they prevent microdonations. In order to prevent this, we will try to have the system throughput be as large as possible without harming decentralisation.

Fees will be charged to block creators and passed on to the users. This means that block creators do not get to keep all the fees they include in their blocks and, as such, cannot collude with users to avoid the minimum fee. A portion of this fee goes to the network and will flow to good causes and operators. With this system, even moving funds around or making purchases using XCV helps good causes.

To accomplish this, we will create a standard computer made of consumer hardware to keep the costs reasonably low (<£1500). We set the system's effective block throughput to make sure that this computer is capable of syncing and maintaining connection to the chain, along with a 2-4x overhead factor. As we improve the efficiency of our software, and as technology improves, we will update the standard computer and increase the block throughput. This will allow the network to improve with time.

In addition, as the price of XCV changes, the minimum fee will increase or decrease. This can cause problems if the price changes much faster than we can increase or decrease the minimum fee. To accommodate this, part of the node software will allow quick changing of the minimum fee, based on using archive nodes as pricing oracles. Archive nodes will provide pricing info to other nodes to make sure that the minimum fee is a reasonable reflection of the cost of the transaction. Nodes will be able to opt-out of this feature if they so choose.

Conclusion

By supporting the Causevest Network, you support a community that believes in incentivising cryptocurrency use as a force for good. We believe that blockchain technology can be used to materialise the ideologies that developers and the community behind them are trying to support.

When someone invests in and holds a token in any cryptocurrency, they should first ask themselves: What is the ideology that this coin represents?

Causevest Coin is a scalable alternative cryptocurrency that takes small transaction fees from across the network and lets it's users redistribute them to incentivise activities that are socially useful. Causevest improves upon the base layer protocol of Bitcoin to increase security for users by reducing human error and by protecting against exchange-based counterparty risk.

We are building a network that allows capital to flow quickly, cheaply and directly to the places where it's needed the most. Now, individuals working together in new ways to help good causes will be empowered by the Causevest Network.

Ultimately, regardless of our users' intentions, whether they are trying to make a profit or help others, interaction with our network will always have a positive, auditable impact on good causes around the world. By introducing Proof of Cause as a new method of rewarding work in a sustainable way and lowering the barrier to entry for new cryptocurrency adopters, we can create a network that is truly unique.

Appendix

Technical Justification of using a blockchain instead of a database

It is true that the social enterprises that form the Causevest network could work with an entirely centralised database system on the backend. What do you gain from using a blockchain over a traditional database that is publicly accessible? After all, a blockchain is only data, and if that data is publicly accessible, there is no point in using a blockchain, right?

In the winter of 2016, there was a panic in a community that dealt with open, publicly accessible data. Over 40 terabytes of climate data stored on US government databases was hastily backed up by independent researchers over fears that the incoming, climate-hostile Trump administration would destroy the data when it came to power.

A kickstarter raised over £16,000 to preserve this data and make sure it remained publicly available to all(http://math.ucr.edu/home/baez/azimuth_backup_project/). The servers that the government used were well run, and the data was publically accessible to all; and yet, it came close to being lost forever. The open, public databases used by the government were not as safe as people were led to believe. Based purely on their technical merits, they had an unexpected and dangerous single point
of failure.

Data on a public blockchain is public in a way that even secure, open, publically accessible, backedup data run by the government cannot be. Because the data stored on a blockchain is held by an arbitrary number of independent entities in unknown jurisdictions, kept alive by automatic and internal rewards, it is free in a way that even open source software cannot match. GitHub could go down or be censored, private servers can be destroyed, but the data stored in the Bitcoin and Ethereum blockchains is the most secure data on the planet.

A point of centralisation is a point of leverage, a point of weakness. A chain is only as strong as its weakest link, be it a chain made of metal or of custody. No matter how many backups you have, how strong your encryption is or how convinced you are of the righteousness of your operators, if all knowledge of your data structure is held in a single mind, that mind is the weakest link. In a blockchain system, nobody — not even the people who developed the system — knows where all of the data is being stored, and so long as someone is willing to pay for the upkeep of the chain, the data is safe.

There is important enough data that makes paying the extra cost for a public blockchain worth it. Data whose history and content should not be changed by anyone and should be freely available to everyone for as long as humanly possible. Charity audit data is one such use case. Charity is one of the most vulnerable sectors for data loss and corruption, because fraud is endemic to the sector. In nearly all business transactions, customers get something for their money. If the item or service is faulty, they have personal knowledge about it and a direct incentive to punish the offending party. However, in the charity sector, people give away money and get nothing directly in return. This makes finding and punishing fraudsters difficult.

Why we created our own cryptocurrency instead of using a BTC sidechain / Ethereum plasma chain Token

The primary use of the Causevest protocol is immutable data storage, especially data of significant size (> 1 MB). Obviously, it is entirely uneconomical to store this data directly on an another chain. We could start a sidechain of a major cryptocurrency and use that to store data while being able to use that chain's cryptocurrency as a medium of exchange, but there are problems with this plan.

First and foremost, the code and tooling for sidechains are non-existent or still in their infancy. We know of no major projects that are currently running on sidechains or plasma chains. In order to make Causevest a sidechain, we would have to develop and test all of the sidechain technology in addition to all of the Causevest-specific technology, increasing our workload by an order of magnitude. Secondly, all current, major blockchains have issues with scaling, backlogs or large fees. These problems may eventually be fixed via second-layer solutions or sharding, but we consider it best to start development of the Causevest Network now instead of waiting and hoping for better solutions to become available.

Causevest, being a specialized chain, does not expect to run into scaling issues for some time; during that time, new solutions will be developed and implemented.

Once sidechain and scaling technology is better developed, Causevest is open to moving the system into a sidechain of a major blockchain in order to be able to use their medium of exchange in a decentralised fashion. In this case, donations could be made on-chain in the main chain cryptocurrency, but the use of XCV to power the stake network would still exist. Until then, XCV is to be used both for staking and as a medium of exchange for the Causevest Network.
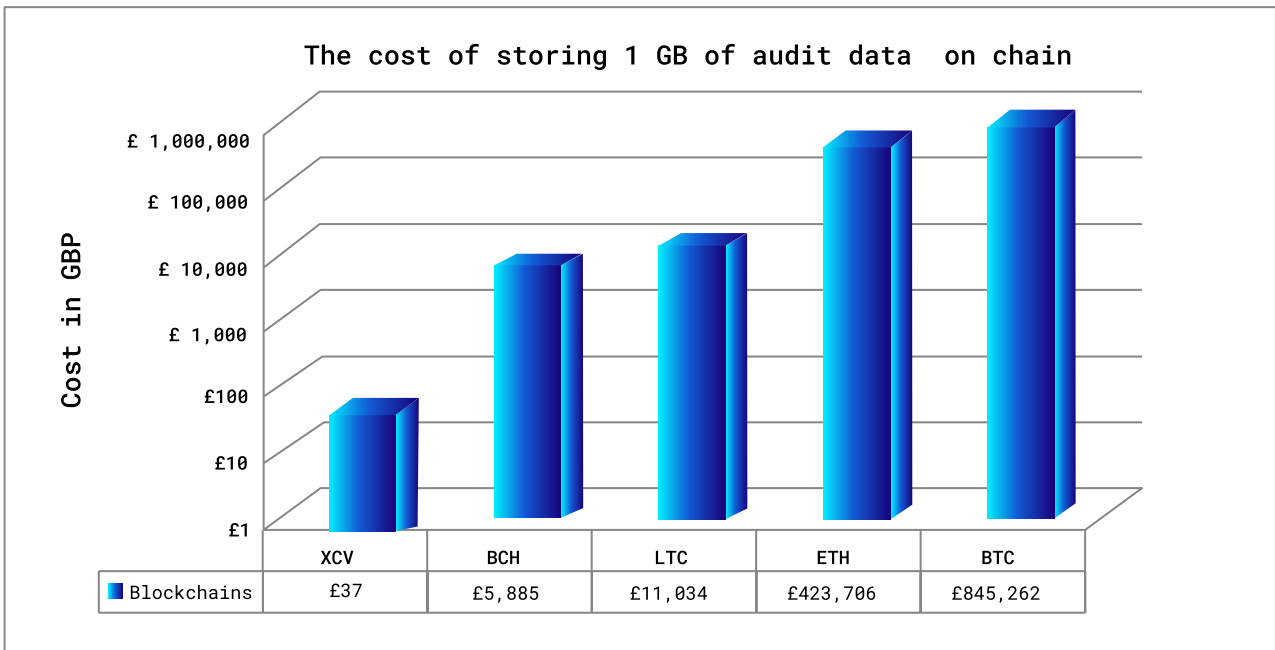
Competitors - Audit Data storage

Although our project is partially based around data storage, we are not competing with Storj, Filecoin, IPFS, Sia, Swarm, etc.

There are multiple competing projects dealing with decentralised data storage; however, they all are based around the premise of cheap, peer-to-peer, transient data storage. Such drive sharing would be a useful product, but Causevest is seeking a different set of storage parameters. We want the audit data stored in the Causevest blockchain to be as permanent and as immutable as possible.

The trade-off is a cost increase of data storage. To mitigate this, only a small number of nodes are directly responsible for data storage, with the rest of the nodes auditing the archive nodes by holding the hashes of the data. This allows us to secure data in a way that is somewhere between the transient, cheap drive sharing and the maximally redundant, expensive Bitcoin blockchain. As such, we are exploring a unique area of the trade-off matrix of decentralised data storage.

The cost of storing 1 GB of audit data on chain

	XCV	BCH	LTC	ETH	BTC
Blockchains	£37	£5,885	£11,034	£423,706	£845,262

There are many projects that want to increase transparency or make use of audit trails by utilising the technology of multiuse utility chains like Ethereum (ETH); as you can see, however, the cost of storing this data makes this unviable for most charitable organisations. Our solution is practicable and innovative; we believe that other projects will migrate to blockchain over time. So while we are more expensive then a dedicated storage blockchain, we are considerably cheaper then utility chains.

References

Section 1:
https://www.oecd.org/eco/How-to-restore-a-healthy-financial-sector-that-supports-lonlasting-inclusive-growth.pdf

Section 1:
https://positivemoney.org/wp-content/uploads/2013/10/Banking-Finance-and-IncomeInequality.pdf

Section 1:
https://www.theguardian.com/business/2009/aug/27/fsa-bonus-city-banks-tax

Section 1: https://wikileaks.org/Banking-Blockade.html

Section 1:
https://www.theguardian.com/world/2017/mar/09/how-greece-fumbled-refugee-crisis

Section 1: Read our dedicated investors guide at: https://www.causevest.io/faq#

Section 3: https://arxiv.org/pdf/1710.09437.pdf

Section 3: https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf

Section 3: http://math.ucr.edu/home/baez/azimuth_backup_project/

Section 3: Ring Sigs https://cryptonote.org/whitepaper.pdf

Section 3: ZK Proofs
http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

Section 3: Bullet Proofs https://web.stanford.edu/~buenz/pubs/bulletproofs.pdf