PIVX
ALLIANCE

Litepaper

Carl ‘Cryptosi’ Anthony
Strontium
Douglas ‘Brought’ Broughton

Abstract

Cryptocurrency projects are pushing towards decentralisation both in terms of development and usage, this decentralisation is often in direct conflict with legacy methods in terms of legal status and agreements. Because a blockchain does not have a legal status as an entity, organisation or person, we are developing a protocol which aims to standardise how legal entities can cooperate with masternode governed blockchains.

The goal is to produce a set of rules that satisfy the legacy legal system and the masternode governance system. This may take time as the legacy system takes a long time to acknowledge new paradigms.

Note: While this paper focuses on implementing Alliances for PIVX, it's important to encourage other decentralised projects to implement similar methods or clone the ones stated here, to create a recognised standard with the cryptocurrency industry

Table of Contents

1.0 Introduction

This Litepaper is being written to formalise the routines that decentralised projects go through when forming partnerships (known throughout this paper as Alliances) with companies or individuals. For all parties involved, it is important that they understands these nuances.

This introduction section should bring people up to speed with the basics of blockchain and the governance it may contain.

This is a living document therefore amendments with relevant state specific legal advice and audits will strengthen the legitimacy of this process.

1.1 What is a Blockchain

A **blockchain**, originally **block chain**, is a growing list of records, called *blocks*, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash).

By design, a blockchain is resistant to modification of the data: it is “an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way”. This distributed nature protects the ledger from alterations made at any point as many copies exist upon which the network agrees upon for consensus. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralised consensus has therefore been claimed with a blockchain. [1]

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency Bitcoin.[1] The invention of the blockchain for Bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The Bitcoin design has inspired other applications, and blockchains readable by the public are widely used by cryptocurrencies as a type of payment rail. Private blockchains have been proposed for business use. Sources such as the Computerworld called the marketing of such blockchains without a proper security model “snake oil”.

1.2 What is a PIVX

The **Private Instant Verified Transaction** (PIVX) cryptocurrency (formerly DNET), is a currency whose defining purpose is to provide users with a truly private means of expediently, securely, and stably transacting over the web. PIVX integrates features inspired by Bitcoin's pioneering distributed ledger consensus technology; speed and governance accessions from Dash, such as InstantSend and the Masternode network; and features the addition of the anonymity protocol Zerocoin on transactions and staking—all of these heavily customised. PIVX also incorporates its own features, such as a Proof of Stake consensus algorithm, the ability to stake both PIV and zPIV, and a dynamically calibrated coin-supply restrained by the burning of transaction fees.[2]

1.3 What is Masternode Governance

Masternode Governance is a decision making protocol for decentralised autonomous organisations in which "Masternodes" on a blockchain make decisions on behalf of all participants. Masternodes perform standard node functions like hosting a copy of the blockchain, relaying messages, and validating transactions on the network, and in addition act as shareholders, voting on proposals for improving their blockchain's ecosystem. Masternodes work alongside standard nodes; stakers/miners and are sometimes considered a second tier, though this is often debated.[3]

Running a masternode requires ownership of a certain amount of collateral. With PIVX it's 10,000 PIV. Besides collateral, further requirements include a static IP address, minimum requirements for CPU, RAM, disk space and network bandwidth. To incentivise their operation, masternodes receive a percentage of all newly created coins. In PIVX that percentage is 45% (with 45% going to stakers and 10% to the organisation's treasury).

A proof of service protocol ensures that masternodes have the most current blockchain protocol and are online.

Because of this two-tiered system in which only masternodes have a vote, it is uncertain if this protocol can be fully decentralised. Critics of masternode governance cite issues with early adopter influence over the system. When put to vote in 2017, the PIVX community voted in favour of further distributing power through the community. It is a high priority goal moving forward to settle on a form of Community Designed Governance—a governance designed by and for the community that all members of the community can agree is in everyone's best interest.[4]

Masternode governance is a simple process. Anyone can launch a proposal. Once the masternodes have voted that proposal is either passed or failed. The deadline for a decision being made is the next Superblock. This is a clear consensus mechanism and can be considered as the blockchain making a decision. This differs from conventional blockchain consensuswhich results in 'forks'. Masternode governance can only give a yes/no answer, though voters have the option to abstain. The governance model then disburses funds from newly minted coins. The yes/no/abstain could be an answer to the question, "Does PIVX want partnership under these certain parameters"

For more in-depth information on PIVX / Masternode governance model please see the PIVX whitepaper.

2.1 Legally Identifying Blockchains

The main issue that stops Blockchain from being a party to a legal contract or 'Partnership' is that, as laws currently written, do not recognize blockchains as legal entities. Common law will be an unpredictable route for the near term while cryptocurrency is still misunderstood. Statutes that identify blockchains as legal entities have not been established as the legal system works hard to catch up with the ever-evolving blockchain field. Bearing these things in mind we need to design methods that the current legal system can understand.

The current paradigm revolves around people's ownership of parts of blockchain, blockchains themselves are not seen as organisations yet, and that's because piercing that corporate veil is difficult and mechanisms to address the fluidity of balance ownership and privacy features are barriers to adoption.

The plan outlined in this paper is for privacy-centric crypto currencies, where the people who influence the decisions are pseudonymous and therefore not accountable for the outcomes of their choices. This level of privacy or pseudo-anonymity already exists within PIVX and other masternode based governance systems.

The lack of a legal status for blockchain is the reason for using the term 'Alliance' for this process.

This proposed system exists as a temporary stopgap until common law recognises Blockchain as a legal entity. It could be argued that anyone could initiate a class-action lawsuit against any company for not keeping to promises made within a legal contract, or the purposes of these contracts. A solicitor or custodian could take the place of the blockchain in instigating these proceedings, however this does not leave them liable to be instigated against. This enforcement is considered further in the legal enforcement section 3.2

2.2 Blockchain Partnerships

Blockchain partnerships are technically non-existent, however there are private companies that are foundations for, or associated with the development of, Blockchains that manage partnerships on behalf of these networks. This is a centralised way of forming partnerships but it is beneficial for several reasons.

1. NDA's can be signed with centralised entities much easier and enforced much easier.
2. Partnerships can be enforced much easier.
3. People respect and trust foundations and don't see the conflict with decentralisation as an issue.

3.0 Solutions

Mindful of the PIVX DAO's governance structure, legal ramifications, a blockchain project's legally defined status, and the nature of building partnerships, this document proposes the need for a partnership solution that encompasses these, but still affords room for negotiation and flexibility. The solution must include;

- Freedom to determine why and how the PIVX blockchain base will be utilized in the arrangement
- Conditions each party must abide by as set out within the agreed upon arrangement
- Commitments each party must fulfill as dictated by the arrangement
- Conformity with all legal determinations outlined by the governing bodies of which the members of the partnership fall under the jurisdiction
- The ability to outline and propose the association between PIVX and potential partner, satisfying the above, on which the PIVX governance can vote

It's important that the solution meets these items, yet maintain sufficient tolerance for contracts determined under this solution to satisfy all vested parties—those being PIVX, the potential partner/s, and governing bodies affected or to which it pertains.

3.1 The Alliance Protocol

The requisites above has produced the PIVX Alliance Protocol. The protocol will update via the PIVX governance system, ensuring it stays relevant, and able to accommodate all potential partnerships. This is the method that an organisation will use to use the term 'PIVX Alliance' and work together with PIVX towards specified projects and goals in an official capacity.

PIVX Alliance can ONLY be accepted as official IF a Specific Alliance proposal request passes via the Masternode Governance system.

All Alliance proposal requests must contain but are not limited to the following information:

1. Who is the person/organisation proposing the Alliance.
2. Reason for proposed Alliance.
3. Length of Time alliance will last recorded in months, from superblock date.
4. Alliance proposals are free to add plenty more information and variables.
5. An alliance proposal may be submitted in any language but an English translation must be available at the time of voting.

PROHIBITED ACTIONS

Alliances can not last longer than 12 months from acceptance date to completion. Where the alliance is for a project whose scope is longer than 12 months, the entity who submitted the original proposal must submit and gain passage of a 'continuation' proposal to continue the alliance activities.

Alliances proposals can NOT be passed, then started at a later date. An Alliance starts immediately when the relevant superblock is mined.

Alliances formed via this method cannot be nullified by any sort of "Alliance termination proposal".

3.2 Legal Enforcement

PIVX as a blockchain will have the ability to initiate court proceedings on any situation by issuing a class action lawsuit or its equivalent in a certain jurisdiction. While the exact details of this triggering procedure will not need to be stated before the Alliance is initiated, it would be advisable to disclose this process and potentiality thereof.

Class action lawsuits were born in the United States and they work by allowing a group of people (in this case PIVX holders), to be represented in legal matters by a 'representative plaintiff'. This in theory should work by a person being chosen through masternode vote to take on the role, leaving a clear signal to courts that this action is wanted. The representative plaintiff may have to disclose that they do not own PIVX so as not to be working within conflict, but this should be directed by the courts and another potential representative can be proposed to the PIVX masternodes easily enough. The class representative must be able to represent the interests of all the members of the class, by being typical of the class members and not having conflicts with them. He or she is responsible to hire the attorney, file the lawsuit, consult on the case, and agree to any settlement. In exchange, the class representative may be entitled to compensation (at the discretion of the court) out of the recovery amount.

Alliances will be formed with organisations based outside of the United States. It would be important to collect alternative enforcement methods, these methods should include similar legal statutes such as the Consumer Rights act 2015 in the UK. This is beyond the scope of this paper and should be addressed within a paper of its own.

Although PIVX has recourse against companies it allies with, companies or organisations allying with PIVX have no such recourse. Due to the nature of DAO consensus, No recourse mechanisms are needed because as a decentralised entity the ability and motivation to renege on any agreement are heavily mitigated.

3.3 Legal Audit

All views on the legality of this entire Alliance protocol are the expressed opinions of this paper's authors and should not be considered binding or legal advice. It would be prudent to have legal audits conducted in various jurisdictions to assess the feasibility, viability and legality of this protocol and also the practicality of the proposed enforcement methods.

4.0 Closing Word

This Litepaper defined the need for Alliances protocol, then defined the protocol itself and the methods for enforcing them should that become an issue. Authors wrote it with a technical background and not a legal background. This will be a living document so the second iteration should include more dependable legal theory.

The next steps for anyone wishing to start an alliance with PIVX is to join the community in Discord, Reddit or forums and put forward the basics of the proposal ideas in a pre-proposal. This should attract discussion, which should improve the dynamics and effectiveness of the proposed Alliance.

Please use the Git-process to add any audits conducted in your region of the world, we will have them verified by another legal professional in the same jurisdiction before being added. In the absence of Common law or referenceable case law, all views will be considered independent legal advice.

Thank you for reading this paper and we look forward to your action.

5.0 References

[1] Wikipedia, *https://en.wikipedia.org/wiki/Blockchain*

[2] PIVX whitepaper, *https://pivx.org/wp-content/uploads/2018/10/PIVX-White.pdf*

[3] Masternode Governance Dash Wikipedia, *httpws://en.wikipedia.org/wiki Dash_%28cryptocurrency%29#Governance*

[4] Article explaining the vote to pass CDG, *https://nulltx.com/pivx-to-redistribute-voting-power-to-the-community/*

PIVX
ALLIANCE

Litepaper

Carl ‘Cryptosi’ Anthony
Strontium
Douglas ‘Brought’ Broughton