Project X Open Source_Decentralized Multi Blockchain & Smart Contract Protocol*

L Ven
LV@project-x-opensource.com

Feb 9th, 2016

Abstract

Blockchain are trying to change the way the world does business. But until blockchain evolves further, and everyday services can trust this new technology and successfully function in a decentralized network, changes are not going to be significant enough. The first and best known blockchain network, Bitcoin has almost double in price in the last year alone with a price today of almost $400 a token, smart contracts at Bitcoin have become too expensive to run and is almost exclusively used as currency which represents a lost opportunity. Project X Open Source, a fully decentralized governance, third generation blockchain network with a smart contract platform focused on innovation, and sustainability. With our Proof of Stake Algorithm, XC, designed to scale as needed with multiple blockchains, private and public consensus allowing smart contracts to migrate across chains, in multiple languages. Project X, is the first blockchain to announce it will charge storage fee for blocks, and provides four different storage times for smart contracts ranging from perpetual time, to 30 days in the blockchain before being purged. Another interesting innovation from Project X, is allowing smart contracts from other blockchains to work seamlessly inside our public network, and a wallet with a built-in free currency exchange which recognizes most tokens and allows users to store them safely.

Introduction

Project X Open Source, is a decentralized consensus jurisdiction, created by a peer review legislation. The legislature of this project is a digital deliberative assembly with the authority to make laws for the governance of Project X. Our focus is to build a transparent governance lead by its citizen's vote.

CITIZENS = TOKEN

Any citizen can propose a debate of existing bylaws, or to create new law in the digital deliberative assembly of project X, all it's needed 15% quorum in 24 hours. Once the quorum has been reached, the assembly will be open for discussion. All laws and changes will require 51% approval to pass.

TOKENS = VOTES

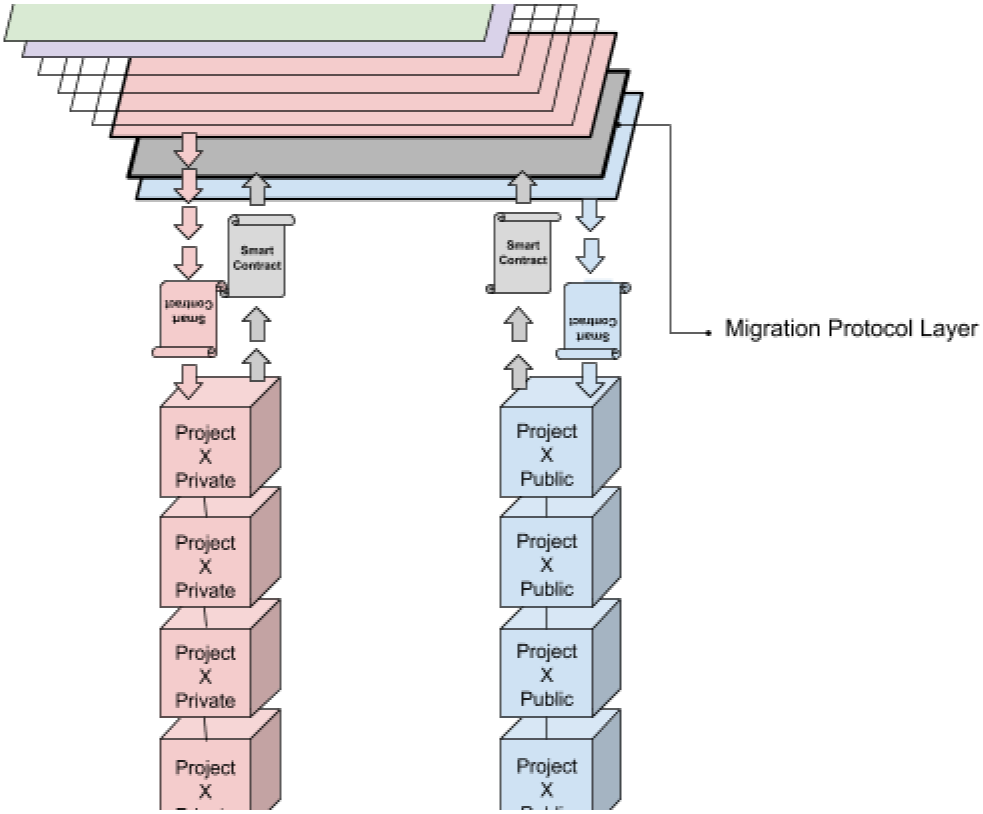
QUORUM & APPROVAL % = TOTAL CIRCULATING TOKENS AT THAT GIVEN TIME

Project X Open Source, is an ambitious project, and relies on the collaboration of many professionals around the world. Collaboration is a common factor in engineering, as a Civil & Mechanical Engineer, I have participated in various peer review engineering projects as invitee. The process to be successful needs to identify early roles and responsibilities; requirements; rigor; peer identification, independence, and external engagement; and follow-up actions. Peer review processes can yield consistent progress, Project X, is an invitation only collaboration between scientists, physicists, mathematicians, engineers, and computer programmers around the globe will work together to develop a system never seen before. Blockchain being a new technology has not much reference and we see this as an opportunity for more experimentation. Understanding the constraints and needs for a project of this magnitude represents a difficulty, by far the biggest challenge of Project X, is to build a fully Decentralized Governance which has checks and balances to **prevent any one person, a group or a corporation to acquire 51% of the total tokens = votes**

Project X Open Source, is a project that is trying to solve many challenges and break many thresholds, to predict a completion schedule will be to dilute the potential of the project. There are too many unknowns and very few references of blockchain development, and rush without experimenting will not only take away from the project's technology but will affect the progress of blockchain in general. Is my personal belief, most project failures are to be accredited to poor schedules, while completion is a necessity, one must always try to achieve an optimal result and not just a solution. Pushing the envelope as far as we can is what we are trying to do at Project X. Last year, in 2015 a trend of Initial Coin Offerings, leading the blockchain market, 1000's of blockchain developers got funding but I can only recall one name, Ethereum. Most projects today, in the same development phase Project X enjoys now, with a White-Paper, lock themselves in an Initial Coin Offering "ICO", which forces the founders to develop and agree to a public schedule with milestones. Many people are under the impression ICO's are funded by small investors, that is a miss conception, less than 6% of the funding comes from smaller investors the rest comes from institutional and venture capitals. "Successful ICOs" have Institutional or Venture Capitals backing, their views on success are based on time and not in technological advances. Schedules with progress updates take precedent, and not achieving optimal technology is almost irrelevant. Institutional and Venture Capital investors have financial backgrounds and only a few team members are engineers, but the great majority have almost null knowledge of engineering science and technology development, but their voices have a heavyweight in the project's development, as they have a financial responsibility to defend and protect. Only a few projects with *Initial Coin Offerings',* had successfully survived and lived up to its technology and development expectations, most projects got negative outcome. While an ICO will be of great financial help, it represents a greater risk to the engineering of Project X. For these reasons was early decided Project X, will not take part of an ICO funding, the project will be financed by the founders and collaborators in exchange for stakeholder equity from a pool of up to 7% of the total tokens to be shared. Stakeholders have strict vesting bylaws, including, only maximum of 20% of assigned tokens can be withdrawn annually, starting after the completion and final release of Project X to the public (early and test releases cannot be accounted)

Private and Public Blockchain

Project X Open Source, proposes a private & public consensus. Smart contracts will be able to migrate from private to public and vice versa without a specific order.

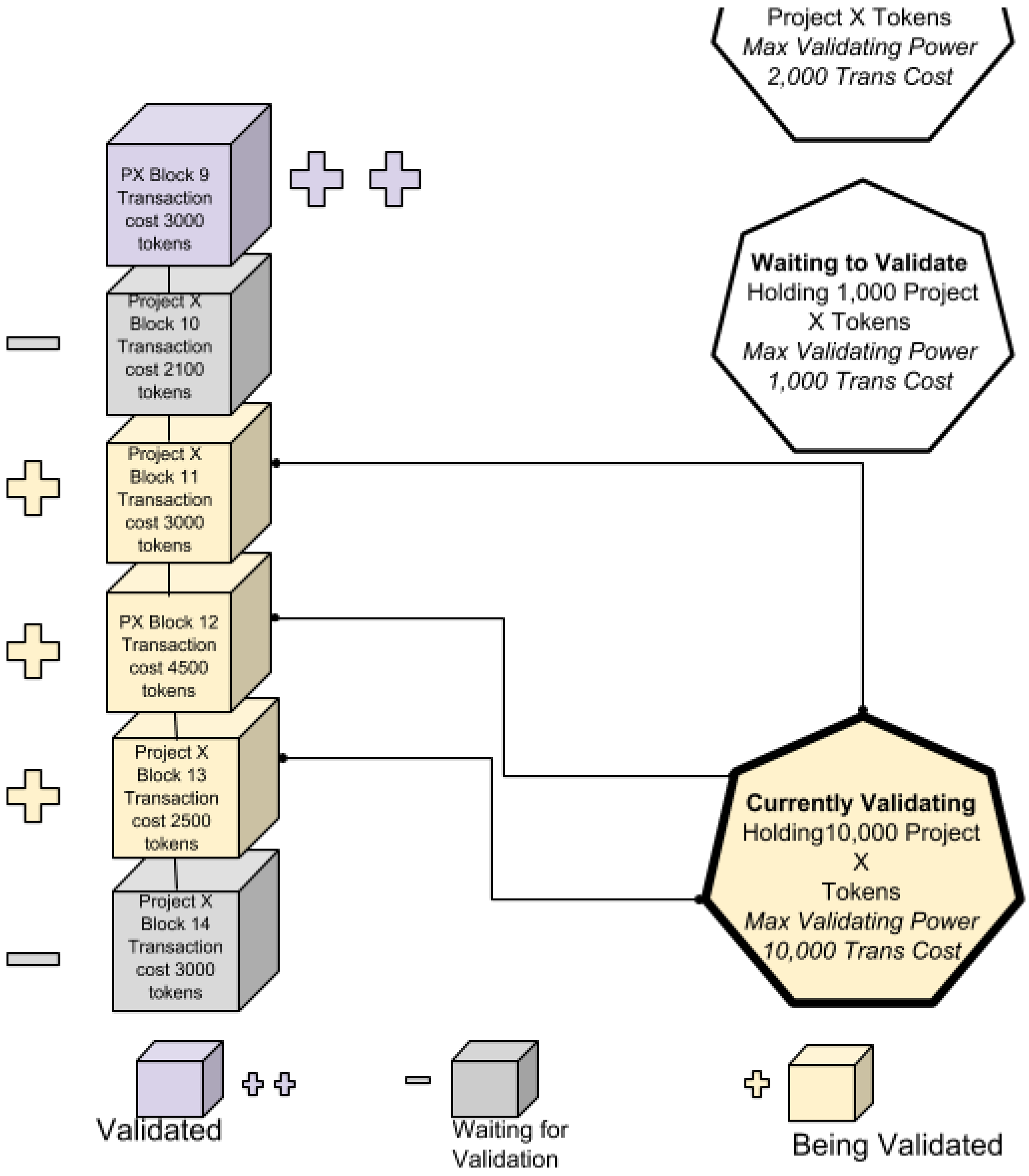


The contract administrator if using the Private Network will be able to select who reads the ledger, submit, and verify transactions. Project X, the private blockchain will be used with the standard private network setup which allocates nodes and "mining" triggered by deterministic concept. Or could also be customized with the selection of individual nodes to create a more selective network. The public network will remain decentralized, distributed consensus.

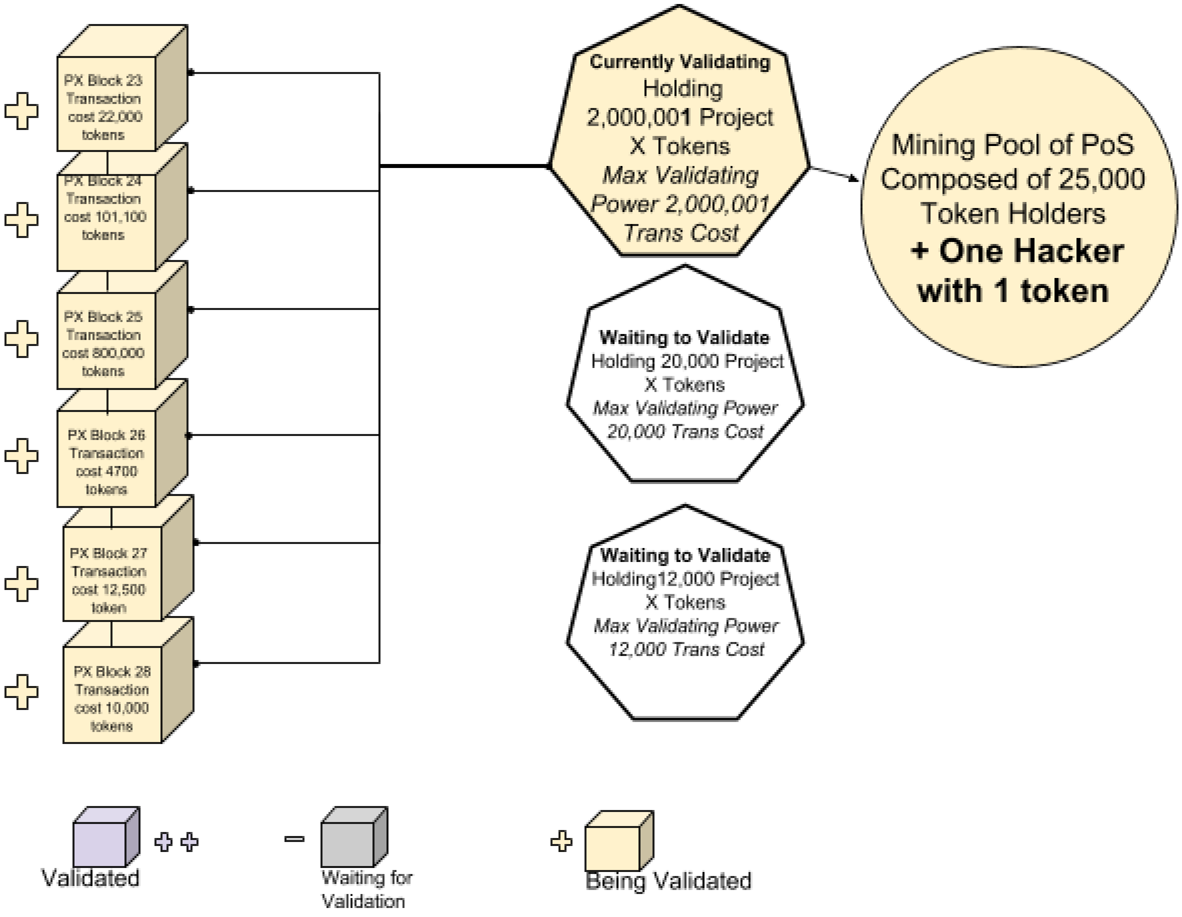
Project X, Proof of Stake “PoS” Protocol

The economics of cryptocurrency and its incentives are not problems everyone understands and so far the solutions provided are not optimal models. Proof of work (PoW)* was used by Satoshi Nakamoto in 2008. Bitcoin despite of being one of the greatest advances of the 21st century has several unexplained numbers assigned randomly, the amount paid per block, and deterioration over time by a factor of 2 every four years has never been explained, but so far has worked, and is a solution but there is no proof of being an optimal solution to the problem. Bitcoin price in the past months has fluctuated in a range of $350 and $450, and has almost double since last summer. The cost of the Bitcoin has made smart contracts too expensive to run, making the Bitcoin blockchain economically unsuccessful, too expensive to buy and equally expensive to mine, and environmentally counterproductive.

Proof of Stake idea was suggested on the bitcointalk forum back in 2011, and the first digital currency to use this method was Peercoin in 2012. The main idea behind Proof of Stake (PoS) is the validator needs to be equally financially vested in the transaction, miners or validators can create block transactions limited how many coins they own. The more cryptocurrency owned, the more mining-power he or she has.


Project X Tokens
Max Validating Power
2,000 Trans Cost
PX Block 9 Transaction cost 3000 tokens
Project X Block 10 Transaction cost 2100 tokens
Project X Block 11 Transaction cost 3000 tokens
PX Block 12 Transaction cost 4500 tokens
Project X Block 13 Transaction cost 2500 tokens
Project X Block 14 Transaction cost 3000 tokens
Waiting to Validate
Holding 1,000 Project X Tokens
Max Validating Power
1,000 Trans Cost
Currently Validating
Holding10,000 Project X Tokens
Max Validating Power
10,000 Trans Cost
Validated
Waiting for Validation
Being Validated

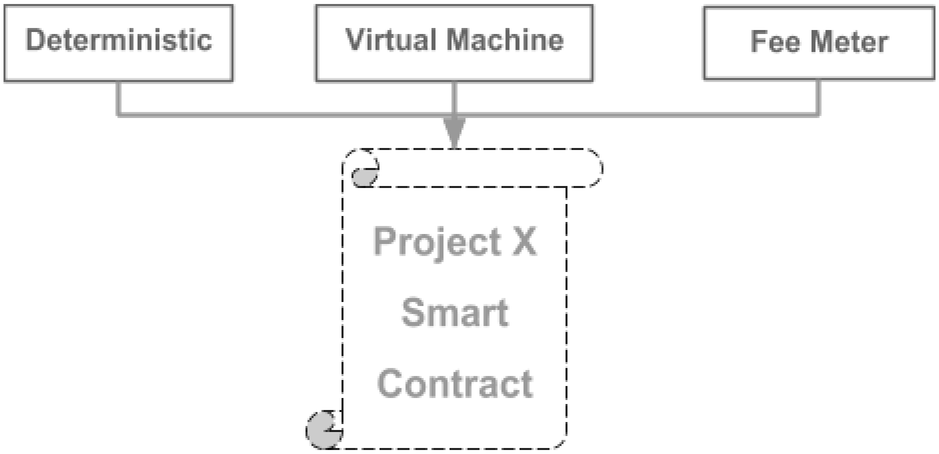
With Proof of Stake (PoS) networks has a different setup, and if design correctly, can promote good behavior among token holders. Price manipulation of the tokes is more difficult in PoS, price reacts faster when acquired in large quantities, and attacks to the network quickly reflects on the price of the token itself, although the attacks to PoS are cheaper than PoW but this could change soon. There are no block rewards on PoS, but rather transaction rewards, work out better for those performing the transactions.While Bitcoin miners spend an outrageous amount of electricity trying to solve the equations to be rewarded, PoS its environmentally safe and straightforward, miners get rewarded for executing each verification. Project X, will add checks and balances, with security mechanisms, and audits to minimize any possible attack. In Proof of Stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as **STAKE**, the validator has vested interests which forces a good behavior, for this reason mining pools in a Proof Of Stake can be very dangerous and should be conceptualized before allowing its participation.


PX Block 23 Transaction cost 22,000 tokens
PX Block 24 Transaction cost 101,100 tokens
PX Block 25 Transaction cost 800,000 tokens
PX Block 26 Transaction cost 4700 tokens
PX Block 27 Transaction cost 12,500 token
PX Block 28 Transaction cost 10,000 tokens
Currently Validating Holding 2,000,001 Project X Tokens Max Validating Power 2,000,001 Trans Cost
Mining Pool of PoS Composed of 25,000 Token Holders + One Hacker with 1 token
Waiting to Validate Holding 20,000 Project X Tokens Max Validating Power 20,000 Trans Cost
Waiting to Validate Holding12,000 Project X Tokens Max Validating Power 12,000 Trans Cost
Validated
Waiting for Validation
Being Validated

Mining Pools also defeats the concept of decentralization on both PoS and PoW. While mining pools continue to participate in blockchains, the individual miners without knowing are *relinquishing power to the Mining Pool Controller, which* may or may not have the best interest of the network, chain or investors at heart. Project X Open Source, will develop strict bylaws to prevent any centralization of power to be given to any individual, specific group, entity or government.

Smart Contract

Project X's Smart Contracts, need to be immutable and must have the ability not only to run through multiple nodes, but migrate between the private and public network without compromising the integrity of the contract. Our Smart Contracts have three basic elements among others, a) Deterministic, b) Terminable and c) Isolated. While the deterministic function will make sure the contract always provides the same output, and terminable will assure the contract is kill once performs a series of steps to complete the contract without looping. The isolated function will maintain the ecosystem safe from viruses



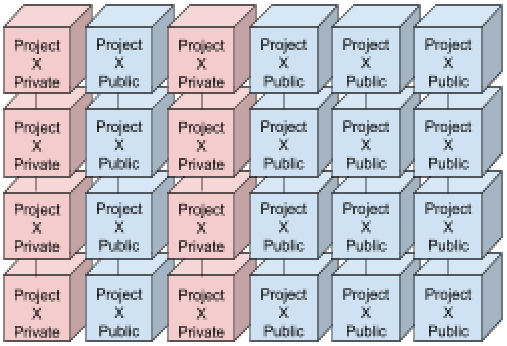
Scale

Project X's Smart Contracts, need to be immutable and must have the ability not only to run through multiple nodes, but migrate between the private and public network without compromising the integrity of the contract. Our Smart Contracts have three basic elements among others, a) Deterministic, b) Terminable and c) Isolated. While the deterministic function will make sure the contract always provides the same output, and terminable will assure the

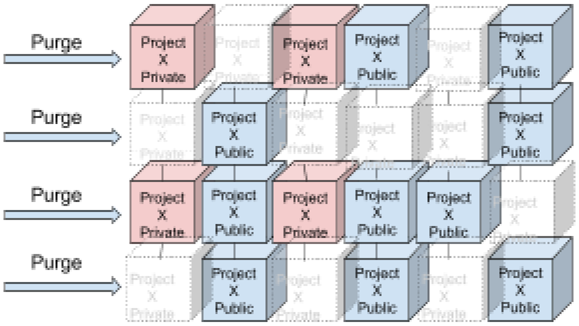
contract is kill once performs a series of steps to complete the contract without looping. The isolated function will maintain the ecosystem safe from viruses
BlockChain scale is affected by many elements, including number of transactions per second, “Bandwidth and Storage”**, ledger growth over time.
While Proof of Stake, being a virtual machine itself already reduces the data size and eases on the network scale other actions are required to improve the network's ability to scale in a future where everything will be stored in the network and nothing gets deleted, or does it?

*In the past many argued a block itself should be increased in size, but after arguments…. got discouraged. At Project X, we propose to create multiple chains instead of one, while our **X Consensus algorithm** “XC” will have a **data compression as a function of the blockchain which will be a map of the blockchain in a smaller footprint*** to save space, and making transactions faster, not all blocks should be stored perpetually. The idea that blocks cannot be deleted is a mistaken concept. XC, has a built in purge mechanism which reduces the size of the ledger once the required holding time has expired, this function can be altered for a gas price. Some people propose selective information, but that defeats the concept of a blockchain and also requires some type of centralization
A blockchain network has multiple functions, including making information almost impossible to get corrupted without notice, but perpetual storage is not one them. Like everything, storage has a cost, and if the user wants to keep block for a longer time than offered at Project X, it will have to pay a storage fee. While there are services that required all data long term storage in block like: DApp,Public Records, Books, Music, Videos, Papers, etc., some other services like credit card charges, bank statements, bills, and even some legal documents should be stored only for the legally required time.

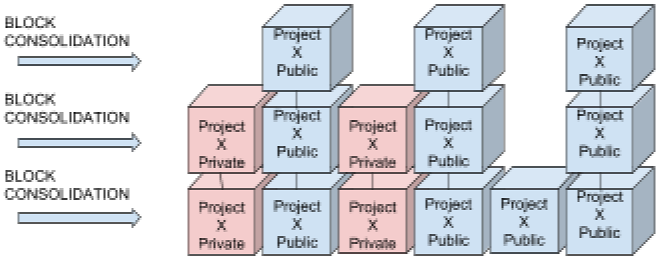
***How to Time-Stamp Digital Documents, Haber-Stornetta 1991*



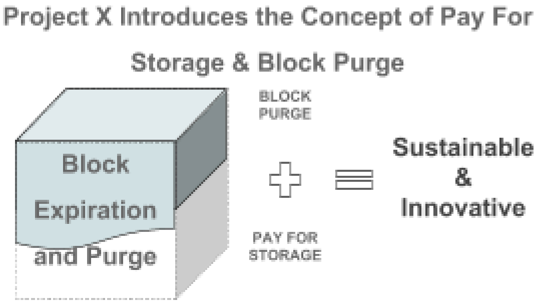
1. Multiple Blockchains

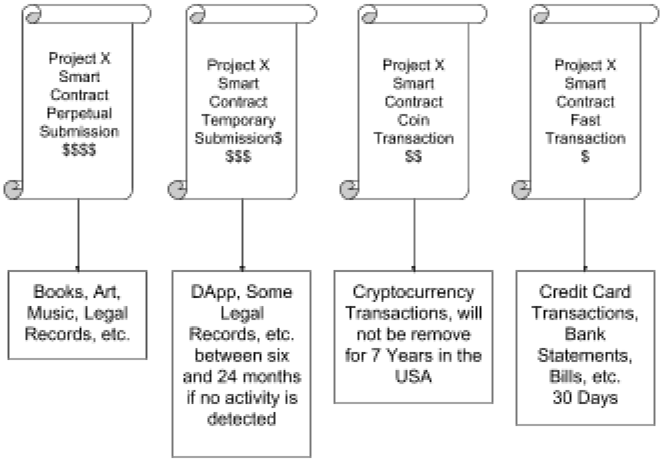


2. Purge Process



3. Block Consolidation After Purge


Project X Introduces the Concept of Pay For Storage & Block Purge
Block Expiration and Purge
BLOCK PURGE
PAY FOR STORAGE
Sustainable & Innovative


Project X Smart Contract Perpetual Submission $$$$
Project X Smart Contract Temporary Submission$ $$$
Project X Smart Contract Coin Transaction $$
Project X Smart Contract Fast Transaction $
Books, Art, Music, Legal Records, etc.
DApp, Some Legal Records, etc. between six and 24 months if no activity is detected
Cryptocurrency Transactions, will not be remove for 7 Years in the USA
Credit Card Transactions, Bank Statements, Bills, etc. 30 Days

User Friendly Interface

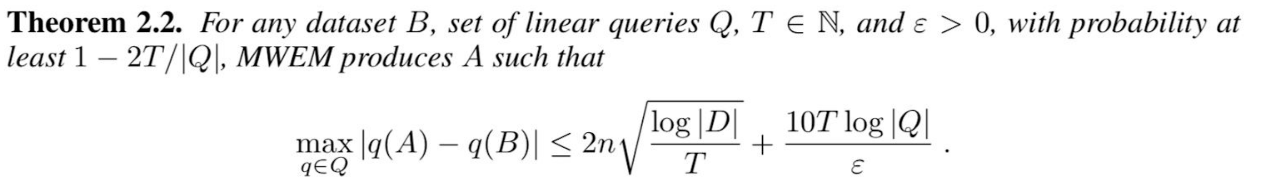
Blockchain, is not supposed to be exclusive, but rather an inclusive system, the peoples system. On Project X, we are working to develop a user friendly interface platform for the development and deployment of decentralized applications, this tool will be part of the main protocol in Project X. Once the project is release to main street we are planning to support those using our platform to create extraordinary DApps.

Exchange Wallet

Since the introduction of Bitcoin in 2008, cryptocurrency in general has maintained a distance from main street. The consequences of not adapting exchanges to be affordable and user friendly has affected the use and progress of Blockchain and Cryptocurrency. Project X, is planning to make a radical change by offering an easy to use, no fees Wallet & Exchange, being able to purchase tokens any time without charges will make the use of WPX attractive. The wallet itself will accept most valid currencies, and the user will be able to request new currency

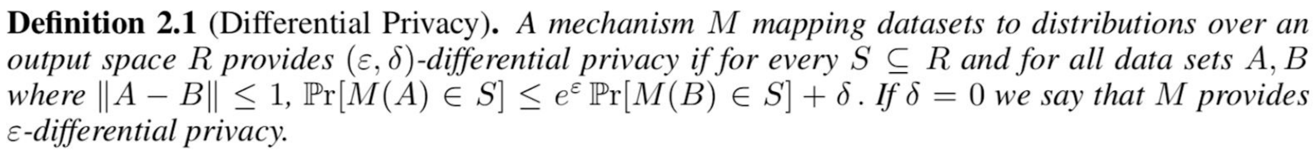
Network Security

Project X, is built in a nine-layer consensus protocol to enable a secure and faster more effective integration. We use a modified development of ***Differential privacy is a constraint on a randomized computation that the computation should not reveal specifics of individual records present in the input. It places this constraint by requiring the mechanism to behave almost identically on any two datasets that are sufficiently close.* ***



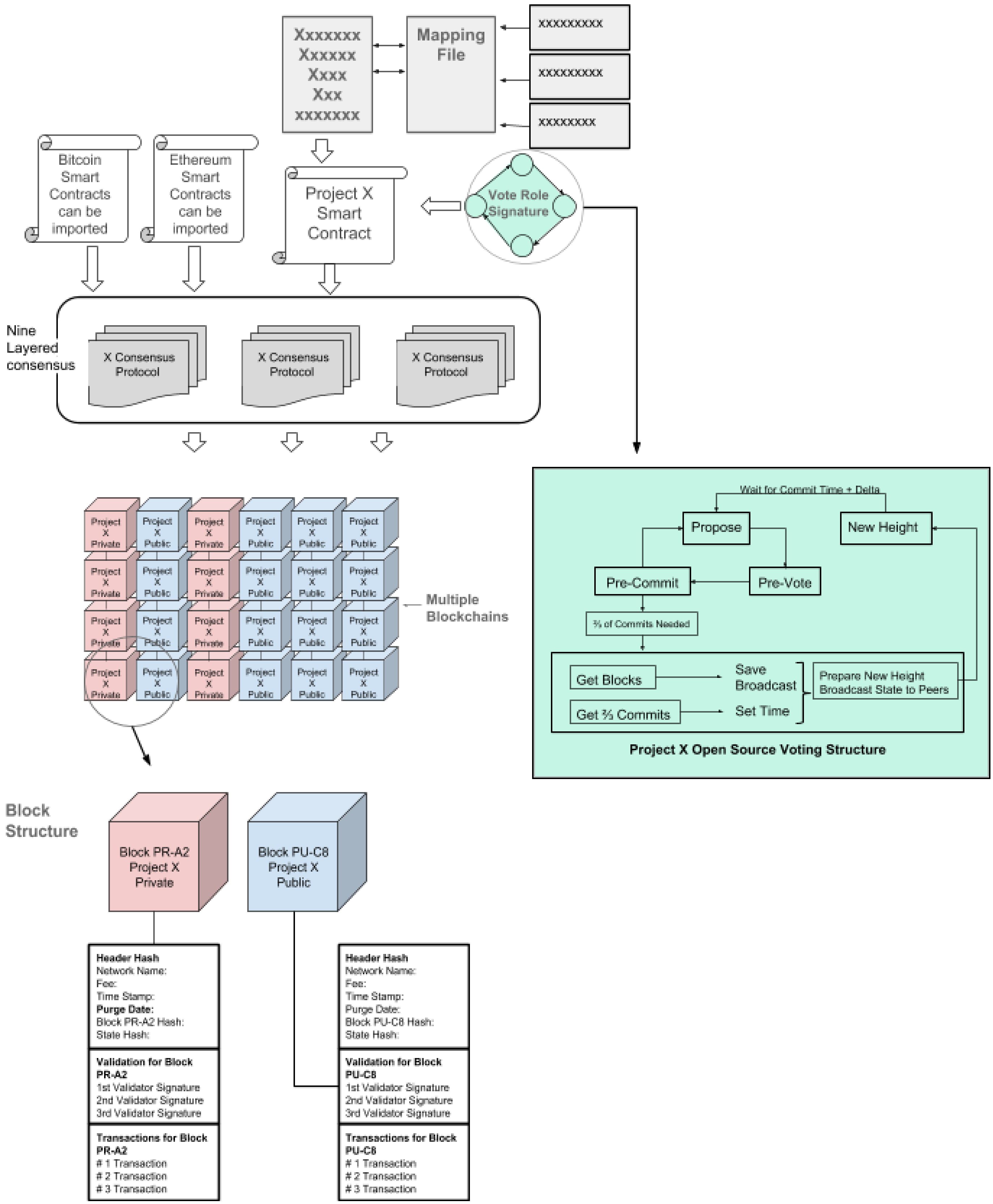
Theorem 2.2. *For any dataset B, set of linear queries Q, $T \in \mathbb{N}$, and $\varepsilon > 0$, with probability at least $1 - 2T/|Q|$, MWEM produces A such that*

$$\max_{q \in Q} |q(A) - q(B)| \leq 2n\sqrt{\frac{\log |D|}{T}} + \frac{10T \log |Q|}{\varepsilon} .$$



Definition 2.1 (Differential Privacy)**.** *A mechanism M mapping datasets to distributions over an output space R provides (ε, δ)-differential privacy if for every $S \subseteq R$ and for all data sets A, B where $\|A - B\| \leq 1$, $\Pr[M(A) \in S] \leq e^{\varepsilon} \Pr[M(B) \in S] + \delta$. If $\delta = 0$ we say that M provides ε-differential privacy.*

Project X Network Architecture



X Consensus algorithm **"XC"**

Distributed consensus is fundamental to building fault-tolerant systems. **X Consensus** algorithm allows a collection of nodes to work as a selected group that can survive the failures of some nodes or even choosing to turn off others. The basic idea behind the XC, is that node each vote on a proposed value, and at the end of voting, nodes must have a consensus about a suggested value. Let's say a Project X node wants to hold an election to decide if value proposed by other project x nodes wins the election. Nodes require a form of agreement upon a value suggested by one of the nodes in the group. Project X says, the suggested value is chosen if in a group of **n** nodes has at least 51% support.

$$\left\{\frac{n}{2}+1\right\} \text{nodes}$$

The majority in the bylaws is referred as a Quorum. A Group of nodes can make progress while reaching a quorum to agree upon a suggested value. Without a quorum distributed consensus system cannot make progress.

Validators: In the consensus process are in charge of signing votes for blocks. There are three types of votes: a pre-vote, a pre-commit and a commit. To receive more than $\frac{2}{3}$ of commits means to receive commits from a $\frac{2}{3}$ majority of validators. A block is said to be committed by the network when a $\frac{2}{3}$ majority of validators had signed and broadcast commits for that block.

Project X, is a true democracy, and the majority will judge and jurors. Validators fees are a reflection of what we are trying to do. Those signing an broadcasting their votes deserve to get paid. X Consensus Algorithm, is designed to expose the unfair player, the consequences will be up to the majority and what they choose to do.

Project X Protocol, so far in theory has been proven to be feasible, and we will continue to develop the theory during the construction part of the project, and even once is completed. Practical conditions are never perfect, but Project X Open Source team, has enough experience to understand conditions change and one need to adapt quickly and incorporate new developments. As previously explained blockchain is a new technology which is not fully understood yet, and the existing projects are very limited and basic, by the time Project X is completed, most likely this project will have new developments from its original design.

The White Paper of Project X Open Source will not be updated until the completion of the project. I am planning to compile and share the design process, including failures and mistakes of project X, one the project has been fully finalized, all documentation will be found at Project-X-Opensource.com.

References:

*S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no2, pages 99-111, 1991.

*PoW idea was originally published by Cynthia Dwork and Moni Naor back in 1993, but the term “proof of work” was coined by Markus Jakobsson and Ari Juels in a document published in 1999

*Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.
(http://www.bitcoin.org/bitcoin.pdf)

*The Byzantine Generals Problem
LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE SRI International
(http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9525&rep=rep1&type=pdf)

*A Simple and Practical Algorithm for Differentially Private Data Release

*American Society of Civil Engineering (ASCE.org) Peer Review