Bitcoin X

snatoshi@yahoo.com

July 2018

Abstract

A purely peer-to-peer version of electronic cash scalable and friendly to use would allow online payments to be sent directly from one party to another without going through a financial institution. We propose a solution to the scaling problem using the Stellar Consensus Protocol (SCP). The network itself requires too minimal structure and everyone without the needing of mining infrastructure can participate and contribute to the network.

1 Introduction

Scalability issues has been around since the launch of Bitcoin in 2009. It exists because of the limits of the maximum amount of transactions the bitcoin network can process.

It is a consequence of the fact that blocks in the blockchain are limited to one megabyte in size. So, the current blockchain size is 1 MB, the blockchain scalability problem takes place to be. Bitcoin blocks carry the transactions on the bitcoin network since the last block has been created. In contrast to Visa's peak of 47,000 transactions per second, the bitcoin network's theoretical maximum capacity sits at under 7 transactions per second.

We want to empower the Satoshi's vision with *Bitcoin X* and rather than forking and harming bitcoin infrastructure, we will provide a purely peer-to-peer version of electronic cash were scalability issues are matter of the past. we choose Stellar for launching *Bitcoin X* since ethereum has also lot of troubles regarding scalability.

1.2 Ethereum Issues

Ethereum and bitcoin use a combination of technical tricks and incentives to ensure that they accurately record who owns what without a central authority.

The problem is, it's tricky to preserve this balance while also growing the number of users (especially to the point where average people can use the system to purchase coffee or run applications).

That's because ethereum depends on a network of 'nodes', each of which stores the entire ethereum transaction history and the current 'state' of account balances, contracts and

storage. This is obviously a cumbersome task, especially since the total number of transactions is increasing approximately every 10–12 seconds with each new block.

The worry is that, if developers raise the size of each block to fit more transactions, the data that a node will need to store will grow larger – effectively kicking people off the network. If each node grows large enough, only a few large companies will have the resources to run them.

Despite the inconvenience, running a full node is the best way for users to take advantage of privacy and security. Making full nodes more difficult to run would further limit the number of people that can verify transactions themselves.

In other words, decentralization and scalability are currently at odds, but developers are looking for ways around this.

1.2.1 Understanding Ethereum Issues

To understand the slow transaction speed of Ethereum blockchain it is important to understand the concepts of Blockchain, mining and smart contract.

Blockchain is a decentralized ledger which records all transactions and stores it in blocks. Once a block is full, it creates a new block. Any user can get this ledger, verify, and read it. Any computer or computing device with this ledger is referred to as the node.

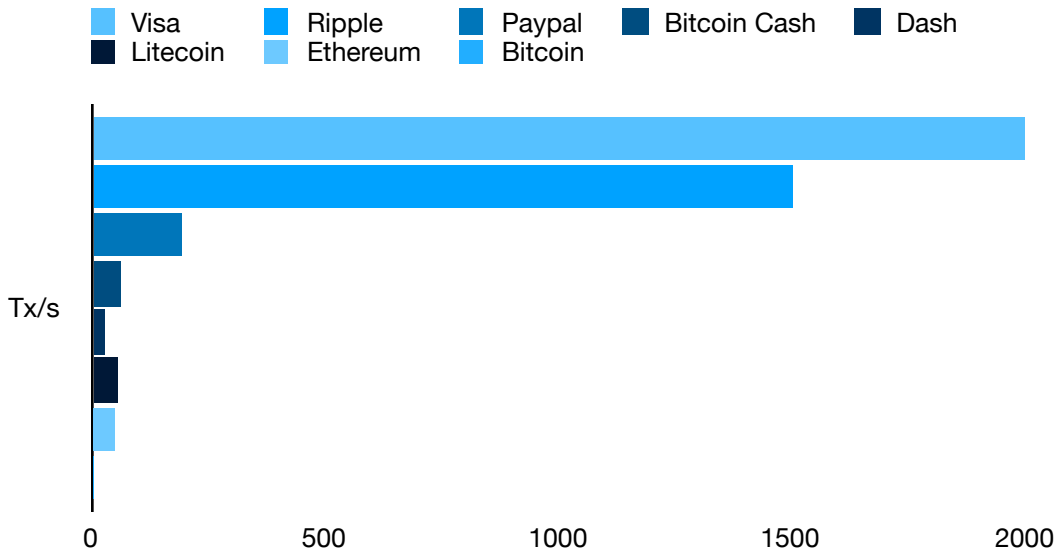
Whenever a new transaction occurs in the blockchain of any node it sends updated blockchain to other nodes for verification according to the rules defined in smart contract. This process of cross-checking blockchains, verifying the transaction and finding a new block for the blockchain is referred as mining and machines that do this work are called miners. It is not possible to transfer any coin safely, efficiently, and cheaply without having large number of miners dedicated for that coin. It is important to incentivize mining of cryptocurrencies to ensure large number of people mine otherwise any corporation with large number of mining machines can corrupt the blockchain.

To achieve this goal miners are provided with a small fraction of coin for every transaction verifications done by them and for playing their rule to solve mathematical equation to find a new block of the blockchain. The value of incentive received by miners depends on several factors including value of the coin, number of unlock coins, total number of miners, total number of transactions per second and nature of smart contract.

1.2.2 Transaction Processing speed comparison

Aided by the blockchain technology a number of cryptocurrencies are exchanging ownership in the market. Estimates say that there are over 1400 cryptocurrencies which are exchanging ownership on popular crypto exchanges and more are in use for a range of purposes.

Given the nature of cryptocurrencies and the fact that anonymity is the key attribute it is not possible to have an exact figure. Apart from making a decentralized currency and ensuring secure transactions one of the most important feature which is often talked about in relation to cryptocurrencies is fast transactions. However, the fact is that in general if we compare the transaction speeds that is offered by existing transaction mechanisms (visa, PayPal) that facilitate transactions for fiat currencies we see that in practicality none of the cryptocurrencies are even close to their transaction processing speeds.



While Visa can process 24000 transactions per second and PayPal can process about 200 transactions per second, the most popular cryptocurrency Bitcoin processes only 7 transactions per second on an average.

Though bitcoin cash has shown to process up to 60 transactions per second it is still very slow when compared to Visa or PayPal. To address the issue of slow transaction speeds and make crypto transactions quicker Ripple is the only blockchain based currency with a decent transaction speed which they claim to be up to 1500 transactions per second. “This makes ripple second only to VISA (popular peer to peer transfer) in terms of transaction speed as Ripple proves to be faster than PayPal by over 300%. PayPal with 218 million active users is still the most popular peer to peer fund transfer service provider.” But then amidst all the cryptocurrencies Ethereum is relatively very slow with a transaction speed of only up to 20 transactions per second.

Though Ethereum outperforms bitcoin in transaction speeds and was developed with a claim to offer better transaction speeds than that of Bitcoins, with growing congestion on the Ethereum’s blockchain it has failed to keep up to the higher transaction speeds. Often, the transactions are not processed and takes hours to get verified.

1.2.3 Conclusion

Blockchain technology can play a significant role in disrupting the fin-tech industry, the way we make transactions and Ethereum in particular provides a host of opportunities with its applications. However, the slow transaction speed which is largely due to the processes involved in functioning of Ethereum's blockchain while ensuring the decentralized nature of the platform is a major issue that has to be identified to the core.

With cryptocurrencies gaining popularity amongst individual and group investors the traffic and congestion on Ethereum's blockchain will further increase. Also, with smart contracts startups and businesses are creating their own tokens to raise funds through their ICOs.

This calls for faster transaction verification and processing to make the blockchain and businesses relying on the technology scalable and sustainable. While some research and innovative solution to this crisis is convincing it is yet to be thoroughly tested. Further research is required to explore the possibilities and performance of the proposed solutions.

2 Stellar's proposal

While Bitcoin and Ethereum can not handle considerably number of transactions per second and therefore being a sustainable and futuristic monetary option, Stellar came across with an intelligent concept where scalability issues can be taken to the next level.

Handling over 2000 transactions per second we believe Stellar offer us the chance of implement the vision of Satoshi's under Stellar Blockchain.

2.1 Stellar Lumens Blockchain

The Stellar Consensus Protocol (SCP), a construction for FBA. Like all Byzantine agreement protocols, SCP makes no assumptions about the rational behavior of attackers. Unlike prior Byzantine agreement models, which presuppose a unanimously accepted membership list, SCP enjoys open membership that promotes organic network growth. Compared to decentralized proof of-work and proof-of-stake schemes, SCP has modest computing and financial requirements, lowering the barrier to entry and potentially opening up financial systems to new participants.

2.2 Stellar Consensus Protocol

This section presents the Stellar Consensus Protocol, SCP. At a high level, SCP consists of two sub-protocols: a nomination protocol and a ballot protocol. The nomination protocol produces candidate values for a slot. If run long enough, it eventually produces the same set of candidate values at every intact node, which means nodes can combine the candidate values in a deterministic way to produce a single composite value for the slot. There are two huge caveats, however. First, nodes have no way of knowing when the nomination protocol has reached the point of convergence. Second, even after convergence, ill-behaved nodes may be able to reset the nomination process

a finite number of times.
When nodes guess that the nomination protocol has converged, they execute the ballot protocol, which employs federated voting to commit and abort ballots associated with composite values. When intact nodes agree to commit a ballot, the value associated with the ballot will be externalized for the slot in question. When they agree to abort a ballot, the ballot's value becomes irrelevant. If a ballot gets stuck in a state where one or more intact nodes cannot commit or abort it, then nodes try again with a higher ballot; they associate the new ballot with the same value as the stuck one in case any node believes the stuck ballot was committed. Intuitively, safety results from ensuring that all stuck and committed ballots are associated with the same value. Liveness follows from the fact that a stuck ballot can be neutralized by moving to a higher ballot.
The remainder of this section presents the nomination and ballot protocols. Each is described first in terms of conceptual statements, then as a concrete protocol with messages representing sets of conceptual statements. Finally, Section 6.3 shows the correctness of the protocol. SCP treats each slot completely independently and can be viewed as many separate instances of a single-slot consensus protocol (akin to the "single-decree synod" in Paxos [Lamport 1998]). Concepts such as candidate values and ballots must always be interpreted in the context of a particular slot even if much of the discussion leaves the slot implicit.

3 The ***Bitcoin X*** solution

Implementing Stellar Lumens technology we make it easy to move digital assets around the world, quickly, reliably and also empowering the true vision of Satoshi's.
We propose a peer-to-peer network using SCP to record a public history of transactions with a limited supply of 21 million coins in existence ever.
Our aim is to provide a global solution of the Bitcoin scalability issues. As eBTC was trying before but launching their token over Ethereum they will find also several scalability troubles. We offer the community who once believes the Satoshi's vision the following advantages:

3.1 Fast Transactions

Over the Stellar Network happens the fastest transactions ever build on the Blockchain. 2 ~ 5 seconds and your payment will be on your wallet. A transaction on the network consists of one or more *operations*. Payments, offers, and fees are all examples of operations that could make up a single transaction.

3.2 Low Fees

If too many transactions are submitted, nodes propose the transactions with the highest fees for the ledger's transaction set. The consequence is just 0.00001 xlm fee on the overall network. Less than both Ethereum and Bitcoin and with a much better transaction speed. Transactions that aren't included are held for a future ledger, when fewer transactions are waiting. No one profits from the base fee. The ledger collects the fees and redistributes them in the process of inflation.

3.3 Security

Stellar uses industry-standard public-key cryptography tools and techniques, which means the code is well tested and well understood. All transactions on the network are public, which means the movement of funds can always be audited. Each transaction is signed by whomever sent it using the Ed25519 algorithm, which cryptographically proves that the sender was authorized to make the transaction.

While all transactions are public, banks using Stellar to exchange funds on behalf of individual account holders can keep information about the individuals sending and receiving it private by storing encrypted or unique identifiers in the transaction's memo field. This allows banks to meet regulatory compliance requirements and keep transaction history verifiable while still keeping privileged information secure.

3.4 Scalability

Last but not least, depending on hardware and network configurations, a conservative estimate of Bitcoin X processing rate is 1000 operations per second. The distributed Stellar network is made up of servers running the Stellar Core software. These servers are maintained by different individuals and entities. Stellar Core maintains a local copy of the network ledger, communicating and staying in sync with other instances of Stellar Core on the network.

6 Stellar Implementations

6.1 Federation Server

The Stellar federation protocol allows you to convert a human-readable address like amy*your_org.com to an account ID. It also includes information about what should be in a transaction's memo. When sending a payment, you contact a federation server first to determine what Stellar account ID to pay. Luckily, the bridge server does this for you.

6.1.1 Federation

The Stellar federation protocol maps Stellar addresses to more information about a given user. It's a way for Stellar client software to resolve email-like addresses such as name*yourdomain.com into account IDs like: GCCVPYFOHY7ZB7557JKENAX62LUAPLMGIWNZJAFV2MITK6T32V37KEJU. Stellar addresses provide an easy way for users to share payment details by using a syntax that interoperates across different domains and providers.

6.1.2 Stellar Addresses

Stellar addresses are divided into two parts separated by *, the username and the domain.

For example: jed*stellar.org:

- jed is the username,
- stellar.org is the domain.

The domain can be any valid RFC 1035 domain name. The username is limited to printable UTF-8 with whitespace and the following characters excluded: <*,> Although of course the domain administrator can place additional restrictions on usernames of its domain.

Note that the @ symbol is allowed in the username. This allows for using email addresses in the username of an address. For example: maria@gmail.com*stellar.org.

6.2 Distributed Exchange

In addition to supporting the issuing and movement of assets, the Stellar network also acts as a decentralized distributed exchange of any type of asset that people have added to the network. Its ledger stores both balances held by user accounts and offers that user accounts make to buy or sell assets.

6.2.1 Offers

An account can make offers to buy or sell assets using the Manage Offer operation. In order to make an offer, the account must hold the asset it wants to sell. Similarly, the account must trust the issuer of the asset it's trying to buy.

When an account makes an offer, the offer is checked against the existing orderbook for that asset pair. If the offer crosses an existing offer, it is filled at the price of the existing offer. Let's say that you make an offer to buy 10 XLM for 2 BTC. If an offer already exists to sell 10 XLM for 2 BTC, your offer will take that offer–you'll be 2 BTC poorer but 10 XLM richer.

If the offer doesn't cross an existing offer, the offer is saved in the orderbook until it is either taken by another offer, taken by a payment, canceled by the account that created the offer, or invalidated because the account making the offer no longer has the asset for sale.

Starting in protocol version 10, it is no longer possible for an offer to be invalidated because the account owning the offer no longer has the asset for sale. Each offer contributes selling liabilities for the selling asset and buying liabilities for the buying asset, which are aggregated in the account (for lumens) or trustline (for other assets) owned by the account creating the offer. Any operation that would cause an account to be unable to satisfy its liabilities, such as sending away too much balance, will fail. This guarantees that any offer in the orderbook can be executed entirely.

Offers in Stellar behave like limit orders in traditional markets.

For offers placed at the same price, the older offer is filled before the newer one.

6.2.3 Cross-asset payments

Suppose you are holding sheep and want to buy something from a store that only accepts wheat. You can create a payment in Stellar that will automatically convert your sheep into wheat. It goes through the sheep/wheat orderbook and converts your sheep at the best available rate.

You can also make more complicated paths of asset conversion. Imagine that the sheep/wheat orderbook has a very large spread or is nonexistent. In this case, you might get a better rate if you first trade your sheep for brick and then sell that brick for wheat. So a potential path would be 2 hops: sheep->brick->wheat. This path would take you through the sheep/brick orderbook and then the brick/wheat orderbook.

These paths of asset conversion can contain up to 6 hops, but the whole payment is atomic–it will either succeed or fail. The payment sender will never be left holding an unwanted asset.

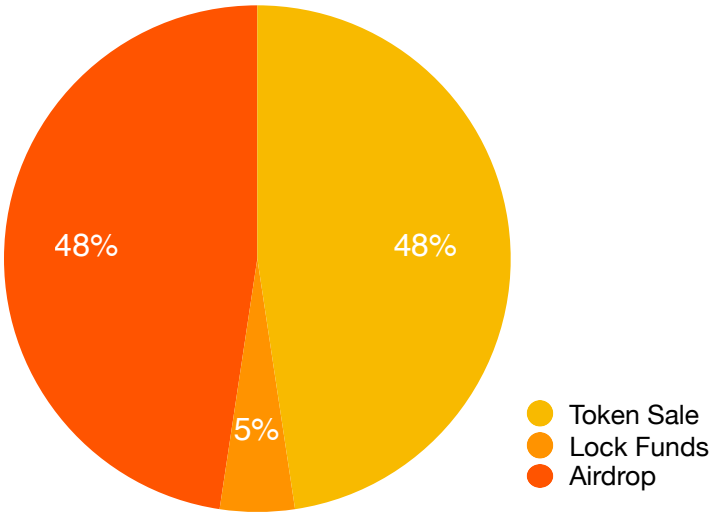
This process of finding the best path of a payment is called pathfinding. Pathfinding involves looking at the current orderbooks and finding which series of conversions gives you the best rate. It is handled outside of Stellar Core by something like Horizon.

5 Coin distribution

In total there will be 21, 000, 000 coins created. 10,000,000 coins for community token sale and 1,000,000 coins will be locked for development purposes. Also 10,000,000 coins will be distributed as an airdrop. After this no airdrop will be released. The token sale price will be 1BTX : 1XLM.

4.1Public wallets

We believe in the need of transparency and trust on the global network so we provide the wallets. The one with twenty million eight hundred thousand coins for the community token



sale, the one with the one hundred thousand coins for the airdrop and the final wallet with the one hundred thousand coins for the development purposes are displayed here:

Community token sale:
GCCU3GWEP7Q463T64VYTF274MNVQZCUWHRWJVITOIRHOWUUNZIEEFWWO

Airdrop campaigns:
GDRHNILGYHZXB3IKKITSHV2I46EJRRLEVJSCUZ4UUDYRZCPVOOXTSZ6H

Dev funds:
GDRQWPLGUPRNPJAHVVQBNJQEQYJ7KLF4JBFT2HUBCM4DCGQFEIKJASYE

4.2 Token Sale

Token sale will be available through StellarPort.io a Stellar Decentralized Exchange.