

AUSTERE CAPITAL
WEEKLY RESEARCH REPORT
STELLAR (XLM)



Website: <https://www.stellar.org/>

Consensus Mechanism: *Stellar Consensus Protocol*

Function: *International Payments Platform*

Token Supply (Circulating, Total): *18.5 Billion XLM, 103 Billion XLM*

Market Capitalization, Rank: *\$4.4 Billion, 8th*

Founder: *Jed McCaleb (formerly of Ripple)*

Summary:

Stellar is a complete, decentralized, multi-faceted financial services platform that originally derived from the Ripple protocol.

What It Does

- Asset-Transfer Marketplace
- Decentralized Exchange/Cross-Asset Payments

Asset Transfer Marketplace

Stellar allows for near instantaneous (3–5 seconds settlement time) transactions of any asset, through asset-issuers or Anchors. **Anchors** are entities that issue assets on the Stellar Network. Holding an asset on the Stellar Network is akin to holding credit from an Anchor through **trustlines**. If you wish to exchange an asset via Stellar, you hold the credit from the Issuing/Anchoring entity — when you offer credit to the Anchor at some point in the future, you will then receive that asset (outside of the Stellar Network).

Thus, actual assets are not being exchanged via the Stellar Network, but rather credits for assets.

All trustlines within the network are consistently monitored via the Stellar Ledger — this includes the limit of the trust to a particular Anchor (i.e. the amount you're willing to extend them credit) as well as the amount they are currently credited to you.

Credited assets on the Stellar Network are all uniquely identified by an asset code and the specific issuer. In addition, Anchors can vet credit holders through permissioned only access, and can also freeze credit held by an account — effectively allowing a revocation of credit if it was issued mistakenly or obtained nefariously.

Decentralized Exchange/Cross-Asset Payments

Account holders on the Stellar Network can also exchange assets through a decentralized exchange— an orderbook is created between buyers and sellers (issuers) of assets. What’s interesting is that a user can convert between two thinly traded assets by **pathfinding**, in that the Stellar protocol can convert between several different pairs of assets before the ultimate conversion (called “hops”). The process is atomic — meaning all or nothing — so that the user is never left with an unwanted asset.

Essentially, Stellar allows users to store money in whatever asset they prefer, cashing out only at the point of sale. This means you can simply hold Google stock for example and cash out at any point when you need to make a purchase.

Additionally, if an account needs to submit a high-rate of transactions, it can do so through so-called channels which essentially use a base (source) account from which to send multiple transactions. Using channels allows transactions to be sent from multiple accounts within the base account, and the fact that this base/source account is not tied in to the operations behind each individual transaction induces a high processing rate.

Lastly Stellar can also function as an ICO platform, similar to Waves and Ethereum.

The Role of Anchors (Issuers)

Anchors play an important role as they are the “bridge/gateway” between existing assets and the Stellar Network — thus, *the more anchors involved in the network, the more diverse set of assets that can be provided within the Stellar protocol.*

For a list of current Anchors using the Stellar Network, see here — <https://www.stellar.org/about/directory>

Anchors interact with an individual Bridge Server, a Federated Server as well as a Compliance Server provided by the Stellar Network. An Anchor is expected to make payments, monitor accounts, respond to requests for federated addresses and comply with Anti-Money Laundering (AML) regulations.

Stellar’s *Federation Protocol* allows multiple account users to be under one main account. It also can provide more information on a certain user.

Stellar’s *Compliance Protocol* allows for AML regulation compliance. Public info required generally includes a full name, birth date, and address.

Operations

The operational protocol on the Stellar network runs on specific thresholds depending on the “level of privilege” the operation requires in order to be executed. The thresholds are based on varying levels of security — Low, Medium, and High. Additionally, there are two distinct validity checks on each operation.

Fees

Fees on the Stellar network are paid with the protocol’s native token — *Lumens* (XLM) — calculated through the base fee which is currently 100 “stroops” (0.00001 XLM). Fees for transactions equal *# of operations × base fee*, which are then deducted from the source account.

Fees collected in the Stellar Network are transferred to a fee pool, which are then redistributed in a weekly inflation voting process (see **Inflation** below). They are not retained by the Stellar network.

The base reserve for minimal account balances is 10 XLM. The minimal account balance is equal to $(2 + \# \text{ of entries}) \times \text{base reserve}$. Entries include trustlines, offers, signers, and data entries.

Inflation/Supply Schedule

Inflation on the Stellar Network is fixed at 1% annually and stems from the Lumen fee pool in addition to new Lumens added to the existing network token supply. Inflation is voted on and then distributed amongst network accounts. Inflation voting occurs weekly and is distributed on a prorated share of the inflation pool (i.e. An account with 2% of the total vote will receive 2% of the inflation pool). Accounts need a minimum of 0.5% of the total vote in order to receive their prorated share.

Consensus

Stellar utilizes the Stellar Consensus Protocol (SCP) which is a variation of the Federated Byzantine Agreement (FBA). Consensus is achieved through a voting process amongst nodes. All nodes on the Stellar Network utilize quorums and more importantly, quorum “slices” to achieve consensus.

What’s novel about the SCP is that network functionality does not depend on full agreement amongst nodes. Quorum slices allow for greater consensus flexibility — in a typical quorum, all nodes must be in agreement for consensus to occur. However the allowance of consensus amongst quorum slices represent various quorum subsets where consensus can occur at a minimal level, as to not impede the liveness of the network. Essentially this means that nodes can enter slices (i.e. quorum subsets) that are in general consensus, even if each individual node within their own quorum is not.

Byzantine failures (i.e. malicious/nefarious nodes impacting network functionality) can result from nodes that block consensus and disrupt network liveness (i.e. consistently countering other nodes) and those that challenge the safety of the network by sending conflicting messages or inconsistent statements to different nodes. The SCP accounts for these faulted nodes by assuming for “Dispensable Sets.” Dispensable sets consist of the total number of faulty nodes the network can tolerate to achieve consensus (and are hence “dispensable”). Based on mathematical proofs the Stellar Consensus Protocol is able to ensure consensus is achieved — every 3–5 seconds — whilst accounting for a wide variety of conditions these dispensable sets may assume.

History

The Stellar Consensus Protocol is a novel type of consensus — pioneered by Professor David Mazieres, Head of the Secure Computer Systems Group at Stanford University (see <http://www.scs.stanford.edu/>) — originally stemming from the Ripple consensus protocol. Back in December of 2014, the Stellar network ran into issues while using Ripple’s consensus, and thus began research in to their own proprietary version. Read more here — https://www.stellar.org/blog/safety_liveness_and_fault_tolerance_consensus_choice/

Network Activity

See here — <https://dashboard.stellar.org/>

In summary, transactions and operations on the Stellar network have soared in the past month with the addition of IBM as a major participant.

Competitors

Waves, Lightning Network, OmegaOne, OmiseGo, as well as 0x all boast decentralized exchange platforms, although arguably none are as flexible and robust as the Stellar network (in my opinion based on underlying consensus mechanisms, network activity, and fee structure).

Team

See here — <https://www.stellar.org/about/>

Risks

The Stellar Network provides an incredibly vast range of financial services for individuals as well as enterprises — *at the core of any decentralized network's robustness is its consensus protocol.*

So far, the Stellar Consensus Protocol has proved resilient enough with the on-board of additional Anchors and subsequent network activity. Only time will tell if the network is truly capable.

Additional Info

For a deep micro-dive into the Stellar Network's operations, see here — <https://www.stellar.org/developers/guides/>