CrushCrypto

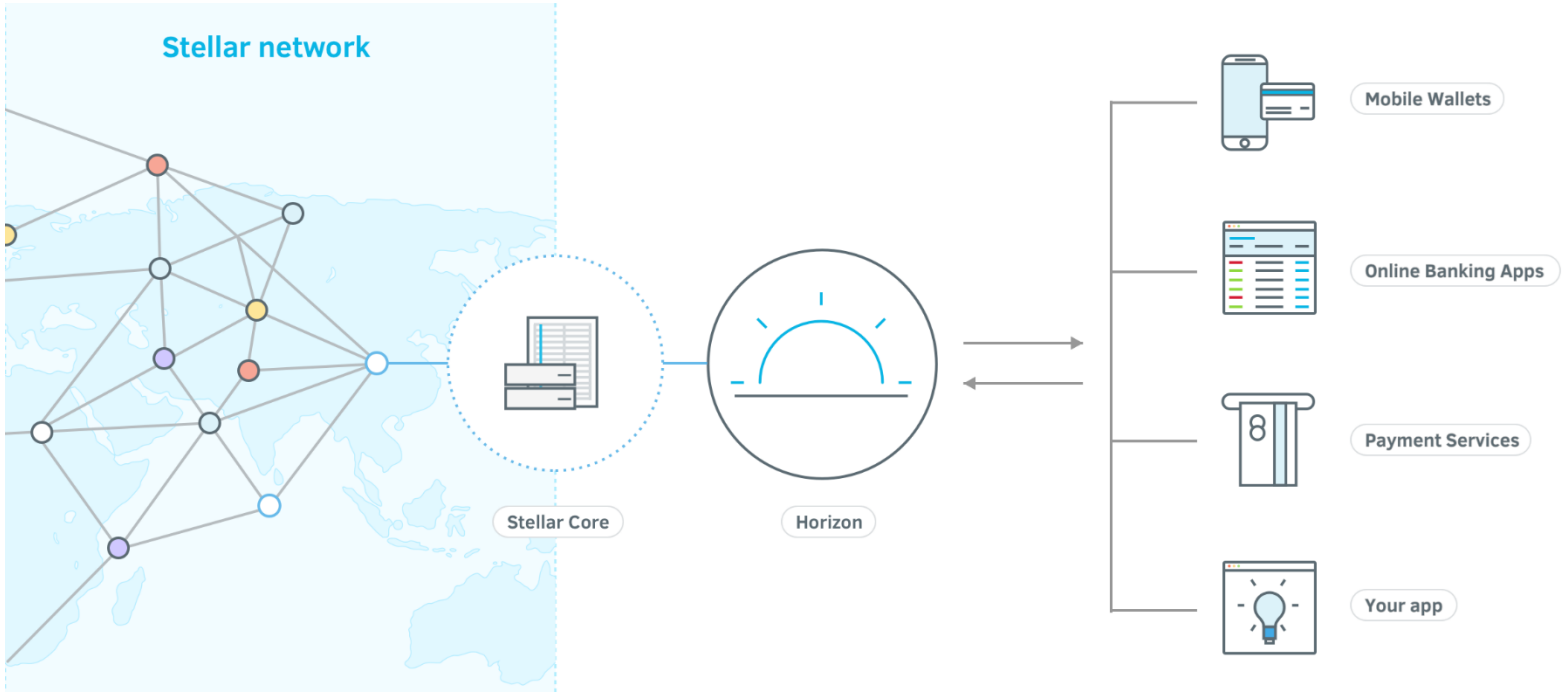
Deep Dive Into Stellar (XLM)

Facilitating global cross-asset transfers

August 22, 2018

What is Stellar?

- A blockchain-based platform that facilitates global cross-asset transfers, including payments. The goal of Stellar is to allow users to move money across borders in a quick, reliable, and cheap way.

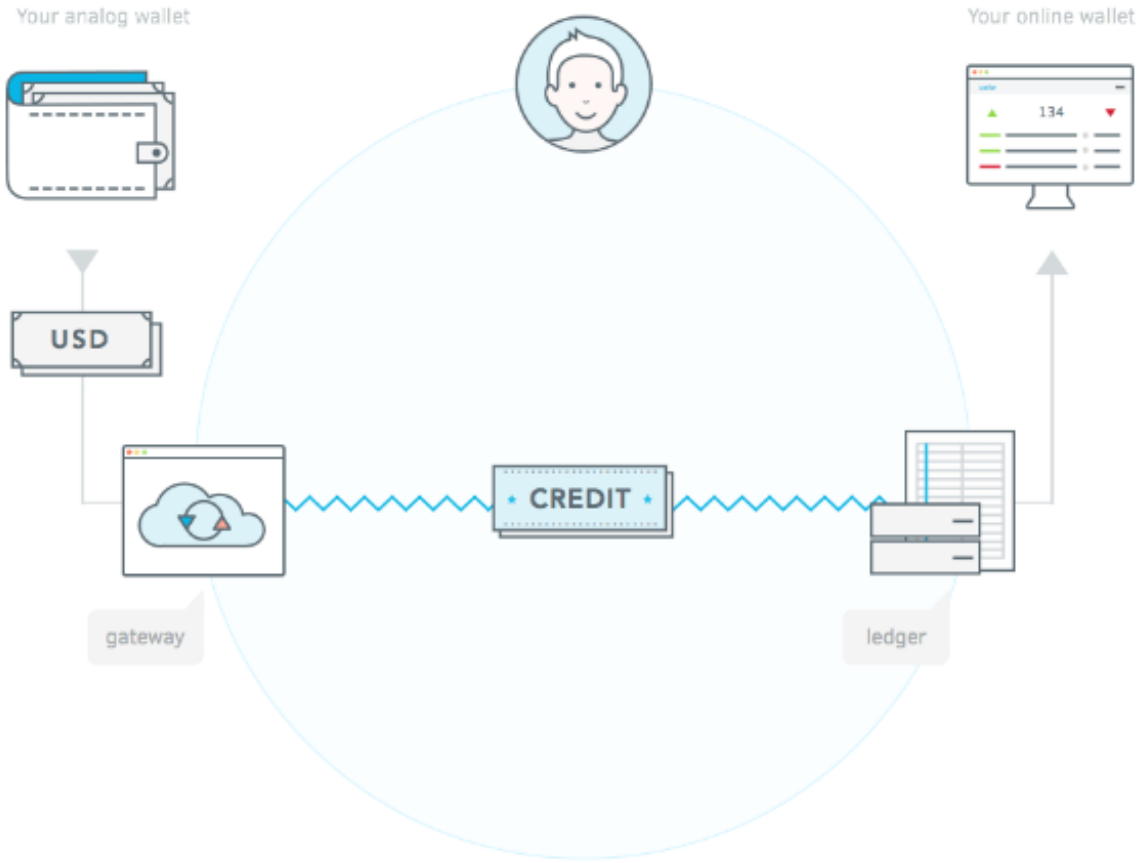


Lumens (XLM)

- Launched in mid-2014 with a native currency is called Lumens (XLM). Stellar received US$3M in seed funding from Stripe, and there was no ICO to launch the token.
- 100 billion Lumens were initially created (but only 5 billion were initially released), and the inflation rate is held constant at 1% per year, based on the total XLM supply.

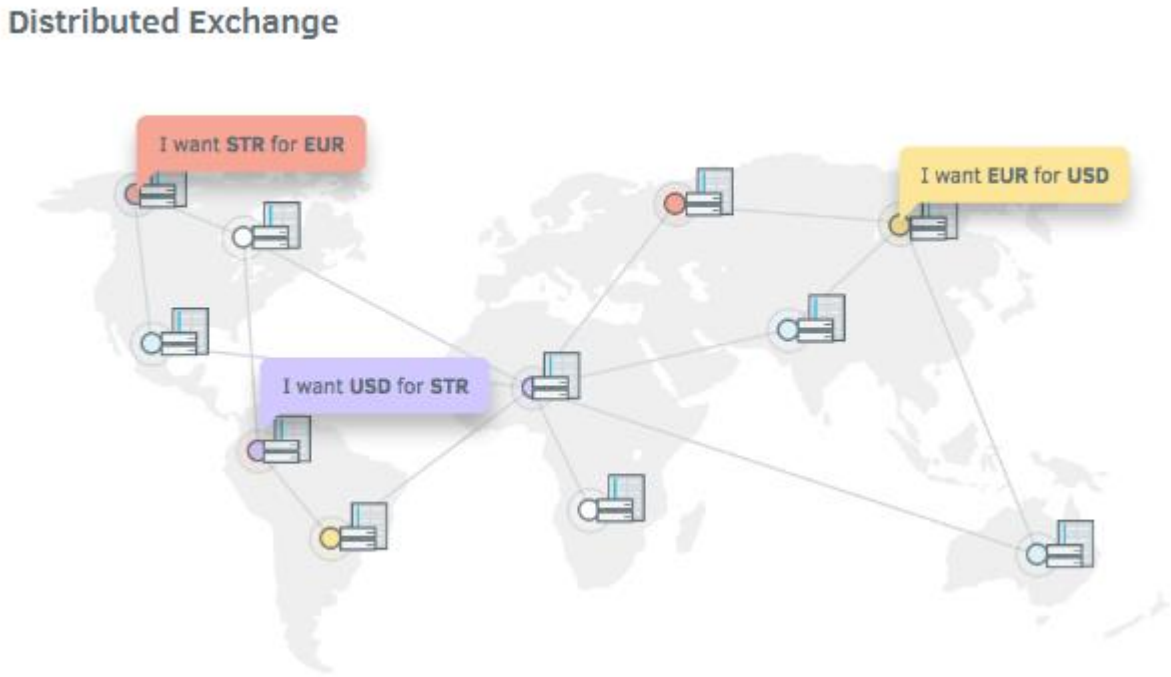
Distributed ledger

- The Stellar distributed ledger records money as credit, which is issued by anchors. An anchor on the network acts as a bridge between a given currency and the Stellar network.
- Credit is issued to a user's account that acts like a virtual wallet in exchange for a deposit. Anchors are then trusted to hold the money and honor withdrawals. Credit can be sent and received between network users across the globe.



Distributed exchange

- Stellar's distributed exchange, allows for automatic conversion of credits into other currencies.
- Example: a user can send EUR credits to a friend with their USD credit balance, where the distributed exchange automatically converts the currency at the lowest rate. The receiver can then withdraw using an anchor that supports EUR.



Smart contract platform

- In addition to operating as a payment network, Stellar functions as a smart contract platform. Smart contracts on Stellar utilize multi-signature verification for security and can be written for things such as crowdfunding. However, these smart contracts are not Turing complete and thus not as flexible as Ethereum.

Stellar Consensus Protocol

- Stellar was initially released as a fork of the Ripple protocol, which uses a consensus mechanism based off Practical Byzantine Fault Tolerance (PBFT).
- Within a year of Stellar's release, the Stellar Consensus Protocol (SCP) whitepaper was released, utilizing a concept called Federated Byzantine Agreement instead of PBFT.
- The implementation of SCP changed the network's entire code base, meaning there was no longer a significant association with the Ripple protocol.

mechanism	decentralized control	low latency	flexible trust	asymptotic security
proof of work	✓			
proof of stake	✓	maybe		maybe
Byzantine agreement		✓	✓	✓
Tendermint	✓	✓		✓
SCP (this work)	✓	✓	✓	✓

SCP vs. PBFT

- PBFT is a closed system of nodes, where network validators are pre-determined by a company or group (e.g. Ripple Labs).
- The Stellar team realized the shortcomings of operating a closed system and designed the SCP as an open network where anyone can operate a node and become a validator.
- Nodes in the SCP are free to choose which other nodes they trust, and a sub-group of nodes trusting each other is called a quorum slice. The quorum slices are then linked through mutual nodes and eventually form a quorum, or network consensus.

SCP vs. PBFT (continued)

- The SCP was designed to operate as a more decentralized alternative to PBFT, but in choosing decentralization some security risks are exposed. There are no block rewards, and thus very little incentivization for people to operate a node.
- Unlike PBFT, where validators are chosen by a central group and known to be trustworthy, anyone can spin up a node on the SCP. It is possible to create a group of malicious nodes that attack the network, and the fewer nodes there are, the more dangerous that group becomes.
- However, the SCP is designed such that in the event of partition or misbehaving nodes, network progress is halted until consensus is reached. This theoretically should be able to handle most attack vectors, but at the cost of freezing the entire network for an undetermined amount of time.

Key features

- **Stellar Consensus Protocol**
- **Assets and tokens**: Stellar's network allows for anyone to create assets/tokens and launch ICOs. Assets created on Stellar benefit from quick and cheap transactions, built in exchange with any other tokens/assets/ currencies in the network, voting/dividend functionality, and optionality to control who can hold the token.
- **Anchors and credit**: Stellar allows for near-instant, global asset transfers because users are trading credit. The system of anchors across the world act as a gateway from the fast, crypto-based credit transferring system to that of real world currencies.

Key features (continued)

- **Confirmation time and network fees**: The Stellar Consensus Protocol allows for 3-5 second transaction confirmations, and each transaction has a low fee of 0.00001 XLM. The fees are not taken by Stellar - they are collected in a pool that is distributed in the weekly process of inflation voting.
- **Distributed exchange**: On top of asset transfers, Stellar will act as a distributed exchange of any type of asset added to the network that can automatically exchanges any currency into another one at the lowest rate. This will reduce friction on the network and remove the need for people to swap currencies while traveling.

Historical milestones

2014-15

Jul 2014: Stellar Protocol established.

Sep/Oct 2014: Multi-currency support released. Currency trading enabled on the web client.

Nov 2014: Stellar wallet V2 released.

Feb 2015: Partnership with Praekelt.

Oct 2015: Stellar network upgraded.

2016

Feb: Software provider Oradian integrated Stellar to create a low-cost payment transfer network in Nigeria.

Jun: Partnership with Deloitte to build a cross-border payments application.

Dec: Coins.ph, Flitterwave, ICICI, and Tempo joined the Stellar ecosystem.

2017

Apr: Partnerships with bext360, MatchMove, Bahrain Finance Company, IZP Group.

Jun: Protocol for creating tokens on Stellar is released.

Sep: Stellar Partnership Grant Program announced.

Oct: IBM and KlickEx partner with Stellar to develop a blockchain-based cross-border payments solution.

2018

Mar: Partnership with Keybase announced, plans for integrating the lightning network into Stellar released.

Jul: Stellar obtained a Sharia compliance certification, allowing the ecosystem to grow in regions where financial services require compliance with Islamic financing principles.

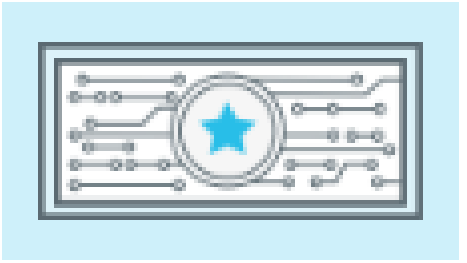
Future development

- Completing SDEX, or Stellar Decentralized Exchange. Key properties of the SDEX include: Day one trading for any ICO token launched on Stellar, atomic pathfinding to discover the cheapest rates between any two assets, low trading fees, and end-user control of private keys.
- Create better ecosystem support, which means: Better brand communication, more walk-throughs to help get people going, better technical documentation, and continued improvement to Horizon API and the surrounding SDKs.
- Implement the Lightning Network by the end of 2018 – an off-chain micropayment system designed to make transactions faster on the blockchain. The Lightning Network would also bring advantages such as: less dependency on miners, micropayment friendly, multi-signature friendly, reduced blockchain load, and decreased waiting time.

Future development (continued)

- Stellar also aims to improve through hardening: ensuring the network remains resilient and secure as improvements are made.
- The team wants to make Stellar more decentralized and easier to run a full validator by reducing the overhead of running a node. They are also aiming to improve how the network's health is monitored, and the way nodes exchange data by revisiting characteristics of the P2P code.

Token economics



- Lumens (XLM) are the native asset of the Stellar network. They contribute to the ability to move money around the world and help conduct transactions between different currencies quickly and securely.
- The Stellar network launched with 100 billion XLM and has a fixed inflation rate of 1% per year. Each transaction on the network has a fee of 0.00001 Lumens, designed to prevent DoS attacks where a malicious actor is spamming the network with transactions.
- All accounts on the network are required to hold a minimum balance of 0.5 Lumens. The requirement is designed to declutter the ledger by eliminating abandoned accounts, ensuring that all accounts are likely to have utility on the network.

Team and advisors

Jed McCaleb

Co-Founder and Lead Developer

Jed created eDonkey2000 early in his career, which eventually became one of the largest file-sharing networks. He then created Mt. Gox, the first major bitcoin exchange, and was a Co-Founder of Ripple in 2011 before creating the Stellar protocol and development foundation.

Nicolas Barry

CTO

Nicolas previously helped build large scale systems at Microsoft and Salesforce and holds a MS in Computer Science and Mathematics.

David Mazieres

Chief Scientist

David is a professor of Computer Science at Stanford University, where he leads the Secure Computer Systems Group. His research interests are Operating Systems and Distributed Systems with a focus on security.

Strengths

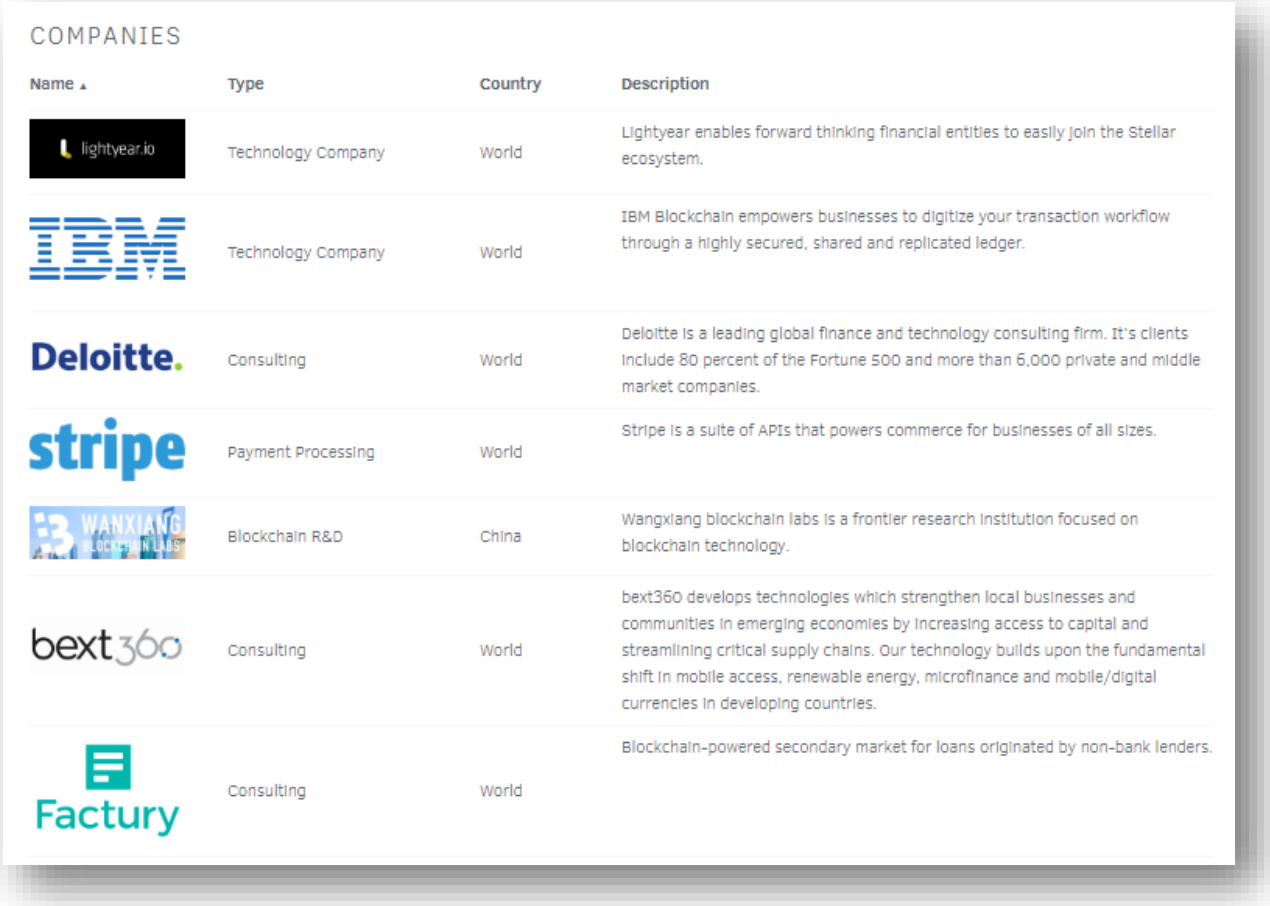
- Project maturity – Stellar is among the oldest and most mature blockchain projects. They have been working for over 4 years on their mission, while the majority of projects in the space have started in the past 1-3 years.
- Jed McCaleb, Co-Founder of Stellar, has been in the bitcoin/blockchain space since 2011 and is very well respected across the industry. He has assembled a strong core team and they are advised by well-known leaders in the tech industry.
- Stellar has abstained from the hype-based marketing many projects used during the ICO bubble, instead focusing on building out their technology and community. As quoted from their 2018 roadmap update, "For those of you hoping for splashy partnership announcements, that's not our goal here. Also, at a philosophical level, we believe that applauding our nth partner is less important than ensuring our existing partnerships are successful."

Strengths (continued)

- The SCP has advantages over traditional proof of work. It has a low computational power requirement, meaning less impact on the environment and low barrier to entry. It also has a high transaction throughput.
- Stellar has made it easy and secure to create a token on the network and launch an ICO. With faster transaction times and smaller fees, it could compete as an ICO platform in the future.
- Stellar specializes in payment transactions and features such as cross-currency transactions have valuable real world use cases.

Strengths (continued)

- Stellar has a growing list of company partnerships, bringing on 37 new partners in 2017 alone. They are working with large tech companies such as IBM, who announced they successfully used the public Stellar blockchain to settle cross border fiat transaction in near real-time. This milestone validated Stellar's use case and proved that established tech companies are willing to adopt it.



COMPANIES

Name ▲	Type	Country	Description
lightyear.io	Technology Company	World	Lightyear enables forward thinking financial entities to easily join the Stellar ecosystem.
IBM	Technology Company	World	IBM Blockchain empowers businesses to digitize your transaction workflow through a highly secured, shared and replicated ledger.
Deloitte.	Consulting	World	Deloitte is a leading global finance and technology consulting firm. It's clients include 80 percent of the Fortune 500 and more than 6,000 private and middle market companies.
stripe	Payment Processing	World	Stripe is a suite of APIs that powers commerce for businesses of all sizes.
WANXIANG BLOCKCHAIN LABS	Blockchain R&D	China	Wangxiang blockchain labs is a frontier research institution focused on blockchain technology.
bext360	Consulting	World	bext360 develops technologies which strengthen local businesses and communities in emerging economies by increasing access to capital and streamlining critical supply chains. Our technology builds upon the fundamental shift in mobile access, renewable energy, microfinance and mobile/digital currencies in developing countries.
Factury	Consulting	World	Blockchain-powered secondary market for loans originated by non-bank lenders.

Weaknesses

- Low percentage of total supply is circulating – at the genesis of the Stellar Network, 100 billion lumens (XLM) were created as specified in the protocol. As part of its custodial mandate, SDF was entrusted to oversee that the vast majority, 95 billion, of the lumens are distributed to the world. Only 5% of which have a lock up period of 5 years. As such, SDF can unlock a lot of the XLMs held by them, which can dramatically increase the circulating supply of XLM and dilute its holders.
    - 5% or 4.75 billion XLMs are held by SDF to support operational costs. In order to provide market stability to lumens, SDF founders and Stripe have agreed not to sell any of the lumens initially received for at least five years, i.e. until 2019.
    - As of August 2018, SDF had distributed 8.14 billion XLMs, or 43.4% of the current circulating supply.

Weaknesses (continued)

- Inflation of XLM is something that needs to be considered as well.
    - Every year, there is a 1% inflation rate. Note that the inflation rate is based on the total supply (or 104.2 billion) rather than circulating supply (18.8 billion). Using the numbers as of August 2018, the inflation rate is 5.3% of the circulating supply – not a low amount.
- There are no block rewards to node operators as transaction fees do not flow to them. As such, there is minimal incentive to become a network validator. Hence, there are very few nodes compared to networks such as Ethereum.

Weaknesses (continued)

- Smart contracts on Stellar are not Turing complete and are less flexible than smart contracts on Ethereum or other platforms. However, one could also argue that being Turing incomplete also makes Stellar less vulnerable to attacks than Ethereum.
- There is a lot of competition in the money transfer/payment platform industry, including Ripple, which is the third largest cryptocurrency by market cap as of writing and has been around longer.

Our conclusion

Overall Rating: B

- Stellar is one of the more mature projects in the blockchain space. The team is very accomplished and advised by established names in the tech industry.
- The Stellar Consensus Protocol is a promising approach that tackles many of the issues facing other consensus mechanisms. It achieves consensus in a quick manner while allowing for cheap transactions without scarifying too much in network security and decentralization, in our opinion.
- On the business development front, Stellar has already made a significant impact in the cross-border payments industry and will continue to do so. The platform also doubles as a token creation/ICO platform, which is another area that could bring significant value to the network.

Our conclusion (continued)

Overall Rating: B

- Despite the solid fundamentals, the token economy does not provide strong assurance that XLM holders are rewarded because SDF controls the vast majority of total supply, most of which are unlocked. Users would need to trust SDF not to flood the market with excess supply of XLMs.
- Being mostly a coin used for payments, XLM suffers from high velocity in that users don't hold the coin for a long duration. For example, in the cross border transactions that IBM is testing, XLMs are acquired and then immediately sold and converted into another currency once transferred, in order to avoid the fluctuation in XLM price.
- Therefore, if the quantity theory of money (MV = PQ) holds true for cryptocurrency valuation, the network value (M) of XLM would suffer if the velocity (V, the number of times that an average coin changes hands in a given time period) is high.

CrushCrypto