Week 2

The Stellar Consensus Protocol and its Position on the Blockchain Generations

Stellar Technical Academy

UNIC | DLRC

Stellar

Session 2: Agenda

1. Prominent Consensus Protocols and the Stellar Consensus Protocol
2. Deep Dive into the Stellar DEX
3. Blockchain Generations and the Stellar Blockchain Network
4. The Blockchain Trilemma and How Stellar addresses it
5. Smart Contracts on Stellar
6. Conclusion

Session 2: Objectives

In the second week of the Stellar Technical Academy, you will:

- ✓ Learn about the Stellar Consensus Protocol (SCP), the Stellar Decentralized Exchange (SDEX) and how they contribute to the purpose of Stellar.
- ✓ Learn about Blockchain generations. You will understand why and how blockchain started, how it has evolved, where it is heading and what blockchain generation Stellar belongs to.
- ✓ Discover about the famous blockchain trilemma and how Stellar addresses it.

1. Prominent Consensus Protocols and the Stellar Consensus Protocol

Prominent Consensus Protocols and the Stellar Consensus Protocol

Introduction

- So, consensus protocols form the backbone of blockchain by helping all the nodes in the network verify the transactions.
- A consensus protocol represents a mechanism which ensures that every new block that is added to the blockchain is the one and only version of the truth and that it, also, is verified and agreed upon by all the nodes in the current blockchain.
- Nevertheless, blockchain encapsulates a great number of consensus protocols, which come in many variations.
- We are going to have a look in some of the most famous consensus protocols, namely:
  - Proof-of-Work (PoW)
  - Proof-of-Stake (PoS)
  - Practical Byzantine Fault Tolerance (PBFT)
  - Federated Byzantine Agreement (FBA)
  - Stellar Consensus Protocol (SCP)

Prominent Consensus Protocols and the Stellar Consensus Protocol

Criteria of the Consensus Protocols

- Consensus protocols can be categorized according to their properties, and while some consensus protocols can co-exist with others this is impossible.

- These properties are:
  - **Fault Tolerance:** signifies that a system can survive the failure of a validator at any point. Basically all consensus protocols choose this as one of their three properties.
  - **Safety:** signifies a guarantee that something bad, like an accidental fork, will never happen. This means that if the network cannot agree on the ledger, it will not fork and the validators will not create two different ledgers. Instead, the network will stop making progress. You'll manually have to go in and figure out what is going on.
  - **Liveness:** signifies a guarantee that the network will always close a ledger to be live, responsive, and accepting future transactions. This means that validators may diverge on different ledgers, causing an accidental fork. Network participants won't know which ledger the network will ultimately decide to take, exposing the network to double-spend risks. Obviously, a protocol can not achieve both safety and liveness.
  - **Open or closed membership:** signifies whether participation in consensus must be approved by a central authority (closed membership) or participation and withdrawal can be achieved without any central authorization.
  - **Low latency:** refers to the case where a system is able to reach an agreement within minimal time.
  - **Asymptotic security:** refers to the case where no amount of computing power can overtake the network.

Proof-of-Work (PoW) Consensus Protocol

- It is one of the first consensus protocols used in the blockchain and it is designed for permissionless public ledgers.
- The algorithm of the consensus solves a computational, cryptographic puzzle of finding a random integer, called ‘nonce’, that leads to hashes with a specified number of leading zeros in order to create new blocks in the blockchain.
- This process is known as ‘mining’ and it uses computational resources from the systems in the node to reach consensus.
- Accordingly, nodes that engage in mining are known as ‘miners’.
- The blocks are represented in a linear structure and each block represents a group of transactions.
- Every transaction is validated and signed using the public and private key assigned to each user.
- It is the consensus protocol that Bitcoin and Ethereum are currently using, even though Ethereum is currently working on adopting the Proof-of Stake (PoS) consensus.

Proof-of-Stake (PoS) Consensus Protocol

- Proof-of-Stake (PoS) is an enhanced version of the PoW protocol.
- Contrary to the PoW consensus protocol, PoS does not require investing in expensive hardware, that consumes a vast amount of energy to solve a complex computational puzzle.
- Instead, validators are picked and assigned with a block and they invest in the tokens of the blockchain protocol by locking up some of their tokens as a stake.
- Basically, the validators validate a block by placing a bet on it, if they discover a new block which they think can be added to the chain.
- If the validators succeed in validating the transaction, then they get a reward proportionate to their bets and their stake increases accordingly.
- Next, a validator is chosen to generate a new block based on their new economic stake in the network.
- This way, PoS incentivizes good behavior and penalizes bad behavior.

Practical Byzantine Fault Tolerance (PBFT) Consensus Protocol

- The Practical Byzantine Fault Tolerance (PBFT) consensus protocol is an optimized version of the Byzantine Fault Tolerance (BFT) consensus protocol.
- Applying the Byzantine Fault Tolerance (BFT) consensus protocol enables a distributed network to reach consensus, even when some of the nodes in the network fail to respond or respond with incorrect information.
- The Byzantine Fault Tolerance (BFT) consensus protocol is responsible for protecting the system against any drop out of the nodes or any failures to respond with correct information, by promoting collective decision making and reducing the influence of faulty/malicious nodes.
- **How does the system decide what amount of faulty/malicious nodes is acceptable?**
- Leslie Lamport has proved that *"if we have 3m+1 correctly working processors, a consensus can be reached if at most m processors are faulty"*.
- This way, the BFT consensus protocol helps the correctly working nodes in the network reach consensus on their values, addressing the problem that is called the Byzantine General's Problem.

Practical Byzantine Fault Tolerance (PBFT) Consensus Protocol

- PBFT is more “practical” in a sense that it works in asynchronous environments, like the Internet, and provides a practical Byzantine machine replication that works even when malicious nodes are operating in the system.
- However, a PBFT consensus can be reached if the condition that the maximum number of faulty/ malicious nodes must not be greater than or equal to one-third of the total nodes of the system is true.
- The nodes in a system that applies the PBFT consensus protocol are sequentially ordered, with one node being the primary and the rest of them being the secondary nodes.
- The primary node receives a request from the client and shares the request with all the secondary nodes.
- The nodes perform the service requested and send back a reply to the client.
- Then, the request (the validation of a block) is possible if (m+1) nodes agree on the same decision, where m is the maximum number of the faulty/malicious nodes allowed.

Federated Byzantine Agreement (FBA) Consensus Protocol

- The Federated Byzantine Agreement (FBA) is a consensus protocol suitable for worldwide consensus, where each participant knows of others it considers important and it uses nodes, quorum slices and quorums.

- A node waits for the vast majority of those it considers important to agree on a transaction before considering the transaction settled. In turn, those important nodes do not agree to the transaction until the nodes they consider important agree as well, and so on. Eventually, a sufficient amount of quorum slices agrees to a transaction and it becomes unattainable for attackers to roll it back and the transaction is considered settled.

- The set of important nodes that are needed to reach to an agreement are the quorum slices and, the agreement, once it is reached and final, is the quorum.

Stellar Consensus Protocol (SCP)

- The Stellar Consensus Protocol (SCP) is an evolution of the Federated Byzantine Agreement (FBA) consensus protocol.

- More specifically, the SCP distinguishes itself from the FBA consensus protocol by enabling open membership: while other protocols that apply the FBA have a determined membership list (closed membership), Stellar uses open membership and is the first Byzantine Agreement protocol that gives each node maximum freedom in choosing which combinations of other participants to trust.

But how does the Stellar Consensus Protocol (SCP) work?

- In a similar way to the FBA consensus protocol, the SCP uses ballots, a series of attempts to reach consensus. The ballot-synchronization protocol ensures that nodes stay on the same ballot for increasing periods of time, until the ballots are effectively synchronous.

- Although the process can not be terminated until ballots are synchronous, two synchronous ballots, in which faulty members of well-behaved nodes' slices do not interfere, are enough for the SCP to terminate, i.e., to come to an agreement.

- Moreover, the balloting protocol specifies the actions taken during each ballot: first, it's the *prepare phase*, where nodes try to determine a value to propose that does not contradict any previous decisions. Then, it's the *commit phase,* where nodes attempt to make a decision on the prepared value.

Stellar Consensus Protocol (SCP)

How does the Stellar Consensus Protocol contribute to the Stellar Blockchain?

- As we have seen earlier in this week's material, the Stellar Consensus Protocol (SCP) is closely tied to the Stellar Core.
- Also, as mentioned before, Stellar Core is the backbone of the Stellar network, since it consists of all the nodes, where each one of its nodes keeps the current state (or the ledger).
- Of course, the current state is replicated on each of these Stellar Core nodes.

But how can we be sure that the current state is replicated correctly in all the nodes?

- Enter the Stellar Consensus Protocol, complementing the function of the Stellar Core in a vital way; it ensures that all these replications of the current state in the nodes are the same, meaning that all the nodes of the network produce exactly the same result (consensus).
- So, the Stellar Consensus Protocol ensures that all Stellar cores apply the same transactions.

Prominent Consensus Protocols and the Stellar Consensus Protocol

Comparing the Consensus Protocols

	Fault Tolerance	Safety	Liveness	Open Membership	Low Latency	Asymptotic Security
PoW	✓		✓	✓		
PoS	✓		✓	✓	maybe	maybe
PBFT	✓	✓			✓	
FBA/ SCP	✓	✓		✓	✓	✓

2. Deep Dive into the Stellar DEX

Introduction to the Stellar Decentralized Exchange (DEX)

What are Decentralized Exchanges (DEXs)?

- Decentralized exchanges, also known as DEXs, are peer-to-peer marketplaces that facilitate cryptocurrency traders to make transactions directly.
- In essence, this means that the cryptocurrency traders are able to make transactions without handing over management of their funds to an intermediary or custodian.
- DEXs were created in order to remove the requirement for any authority to oversee and authorize trades performed within a specific exchange, giving its users the advantage of keeping control of their wallet's private keys.
- This way, users can immediately access their crypto balances after logging into the DEX with their private key.
- Over recent years, many popular decentralized exchanges have been built on top of leading blockchains that support smart contracts.
- They are built on top of layer 1protocols, meaning that they are built directly on the blockchain.

Introduction to the Stellar Decentralized Exchange (DEX)

How do DEXs work?

- Each time a trade occurs in a DEX, there also incurs a transaction fee along with the trading fee. In essence, traders interact with smart contracts on the blockchain to use DEXs.
- In general, there are three main types of decentralized exchanges:
  - Automated market makers
  - Order books DEXs and
  - DEX aggregators.

Picture by https://cointelegraph.com/

Introduction to the Stellar Decentralized Exchange (DEX)

How does the Stellar DEX work?

- The Stellar network acts as a decentralized exchange (DEX), that allows us to trade and convert assets on the network.
- The Stellar ledger stores both balances held by user accounts and orders that user accounts make to buy or sell assets.
- More specifically, Stellar's decentralized ledger is like a database that can not only store account balances and payments, but it can also store **sell** orders, **buy** orders and **matchmaking** orders.
- All these offers come to represent a global order book on a decentralized exchange, or DEX for short.
- However, the best way to understand the Stellar DEX is to compare it to the centralized exchanges and the DEXs built on Ethereum.

Introduction to the Stellar Decentralized Exchange (DEX)

Understanding Stellar's DEX

	Stellar's DEXs	Centralized Exchanges	Ethereum's DEXs
What about private key possession?	You are in control of your private keys and in control of your money.	They store private keys on central servers, having a history of being attacked.	They store your funds in smart contracts, also with a history of being attacked.
Is the order book stored on-ledger or off-ledger?	Stellar has an order book and offer matching built in at the protocol level. So, on-ledger offers are a simple addition to the decentralized database.	A large amount of trust is placed in centralized exchanges and the servers they store orders on. So, you can be locked out or the server can go down and you will not be able to place your order.	Due to long transaction times and too few transactions per second, buy and sell offers stored in the Ethereum blockchain get backed up, forcing many Ethereum DEXs to store order books and match orders off-ledger on one server.
Once an order is matched with another compatible order, does the trade execute in the network with tokens truly being swapped?	The trade actually occurs on ledger.	The private key holding the newly traded tokens is stored on the centralized server.	The trade actually occurs on ledger.

Introduction to the Stellar Decentralized Exchange (DEX)

Understanding Stellar's DEX

	Stellar's DEXs	Centralized Exchanges	Ethereum's DEXs
What is the cost of each exchange?	The Stellar DEX only costs 100 stroops per operation, a very small amount – merely fractions of a cent.	Most centralized exchanges charge a substantial fee for purchases.	Ethereum DEXs also take a cut on top of the Ethereum network fee for a transaction.
What is the transaction speed for each exchange?	Stellar's 5 second ledger closing time makes it likely the fastest DEX out there.	Centralized exchanges are incredibly fast at around 1 second	Ethereum DEXs experience the same lag that all transactions on Ethereum do, currently at around 3 minutes.

3. Blockchain Generations and the Stellar Blockchain Network

Blockchain Generations and the Stellar Blockchain Network

Milestones of Blockchain

- **1991:** Stuart Haber and W Scott Stornetta describe for the first time a cryptographically secured chain of blocks, aiming to implement a system where document timestamps could not be tampered with.
- **1998:** Computer scientist and cryptographer Nick Szabo introduces a mechanism named ‘bit gold’, for decentralized virtual currency. Although his theory was never implemented, it is considered to be “a direct precursor to the Bitcoin Architecture”.
- **2000:** Stefan Konst publishes his theory of cryptographically secured chains, along with concrete ideas for its implementation. In to this theory, the corners of any graph, according to the edges existing between them, are linked together using cryptographic methods. This prevents unauthorized entities from manipulating or removing corners or edges unnoticed from the graph.
- **2008:** the developers with the pseudonymous Satoshi Nakamoto, using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party, re-design blockchain and release a white paper establishing the model for a blockchain.
- **2009:** the developers with the pseudonymous Satoshi Nakamoto implement the design as a core component of the cryptocurrency ‘Bitcoin’, making blockchain technology’s first public debut.
- **2014:** blockchain technology is separated from the currency. Its potential for other financial and interorganisational transactions is being explored and Blockchain 2.0 is born, referring to applications beyond currency. Ethereum blockchain emerges, introducing computer programs into the blocks, representing financial instruments such as bonds, known as smart contracts.

Blockchain Generations and the Stellar Blockchain Network

Blockchain 1.0 – Digital Currency

- The first generation of blockchain, Blockchain 1.0, introduced digital currencies and is directly linked to the emergence of Bitcoin.
- More specifically, it is characterised by:
  - the underlying technology platform that consists of mining, hashing and public ledgers
  - the overlying protocol, which refers to the use of transaction enabling software and
  - the overall digital currency, whether this is Bitcoin per se, or any other digital coins/tokens.
- However, Satoshi Nakamoto, the pseudonymous developer(s) of Bitcoin were the first that conceptualized the notion of blockchain, by outlining it in the Bitcoin white paper.
- The system was mainly created in order to:
  - Reduce transaction fees for online purchases
  - Introduce greater anonymity than credit cards, since accounts are pseudonymous and the protocol is designed to encourage the use of a new account (public address) for each transaction
  - Introduce decentralisation, since digital currencies do not rely on a third-party, and
  - Protect against inflation, since Bitcoin uses cryptography that guarantees a relatively fixed money supply.
- Bitcoin is blockchain technology's first real use case, and that's why these two terms often go hand-in-hand.

Blockchain Generations and the Stellar Blockchain Network

Blockchain 2.0 – Digital Economy

- While Blockchain 1.0 was in action, the blockchain community started thinking that the technology could possibly do a lot more that just allowing to send and receive coins and trade anonymously.
- So, the era of Blockchain 2.0 emerged.
- Blockchain 2.0 is associated with a wide variety of economic and financial applications, that exist beyond simple payments, transfers and transactions.
- More specifically, this blockchain generation adheres to applications that include traditional banking instruments, such as loans and mortgages, as well as complex financial instruments like titles, contracts and other assets and properties that can be monetized.
- The highlight of the Blockchain 2.0 generation is the advent of smart contracts.
- Typically, contracts are managed between two separate entities, possibly with other entities supervising the oversight process. However, smart contracts are self-managing on a blockchain, thus enabling true decentralisation.
- Basically, smart contracts are computer programs that automatically execute, when a pre-configured condition among the participating entities is met.

Blockchain Generations and the Stellar Blockchain Network

Blockchain 2.0 – Digital Economy

- Nowadays, the technology of smart contracts is directly linked to Ethereum.
- Ethereum is the most well-known platform that first introduced and ran smart contracts.
- Improvements with Blockchain 2.0 resulted in Ethereum behaving less like a cryptocurrency (unlike Blockchain 1.0 – Bitcoin) and more like an entire digital ecosystem that other cryptocurrency projects can operate on.
- Imagine that: similarly to some applications that are built on iOS, there are decentralized apps (dApps) that are built on Ethereum.
- **Stellar belongs to Blockchain 2.0, the Digital Economy.**
- The Stellar Development Foundation is currently working on its very own native smart contract.
- Moreover, as you will discover in the following weeks, Stellar not only accommodates simple payments and transfers, but supports many financial applications as well, such as loans, mortgages, titles etc.
- We are going to dive deeper into the various applications and use cases of Stellar in the coming weeks.

Blockchain Generations and the Stellar Blockchain Network

Blockchain 3.0 – Digital Society

- Blockchain 3.0 is going to shape our everyday lives, since the term refers to a vast amount and kinds of applications.
- However, what is remarkable here is that the next generation blockchain does not involve money, currency, commerce, financial markets and other economic activities.
- It refers to applications that include art, health, science, identity, governance, education, public goods and other aspects of culture and communication.
- Some of the most promising applications of Blockchain 3.0 are:
    - Smart cities, which involve horizontally cumulative elements such as smart governance, smart mobility, smart resources etc.
    - Internet of Things (IoT), which refers to e-business applications.
    - Large-scale data management in electronic medical records (EMR) systems.
    - Creation of digital identity, that unbanked individuals can benefit from by gaining access to bank accounts, loans and other financial services that were previously inaccessible to them.
    - And so on …

Blockchain Generations and the Stellar Blockchain Network

Blockchain 3.0 – Digital Society

- Additionally, Blockchain 3.0 tackles two problems that beset both of the previous blockchain generations:
  - Scalability
  - Interoperability
- The problem of scalability is a major issue that Bitcoin is facing and refers to troubled processing times and bottlenecking.
- **What is bottlenecking?**
- Imagine that there is a pizza and a class of 10 people and everybody gets their slice. Then suddenly, 10 more people arrive that need to get a slice, but the size of the pizza remains the same. This leads to everyone waiting much longer to get their slice and also get a smaller portion.
- Now, in blockchain, imagine that too many people are trying to transact simultaneously. This leads to delays in the transactions – which is not sustainable for the financial system – and to higher gas fees, which leads to the possibility of exclusion.
- **How does Blockchain 3.0 make scalability feasible?**
- 'Third-gen' blockchain projects are designed with scalability in mind. So, their technology automatically resolves issues of scaling, by bringing 'more pizza' when needed, so that no one has to wait for a "slice".

Blockchain Generations and the Stellar Blockchain Network

Blockchain 3.0 – Digital Society

- As previously mentioned, interoperability is another problem the other two blockchain generations face.
- **What does the interoperability problem refer to?**
- It is a known fact that in the first iterations of blockchain, the chains can not interact with each other. Think like trying to charge an iPhone with a Samsung charger – not compatible.
- However, the digital society relies on systems collaborating with each other, where information and data can be shared across platforms and it automatically solves the interoperability problem.
- Currently, there are third-gen projects like Cardano and Polkadot, that have introduced interoperability functions into their blockchain.

4. The Blockchain Trilemma and How Stellar addresses it

The Blockchain Trilemma and How Stellar addresses it

Decentralisation, Scalability, Security

- The Blockchain Trilemma is a concept first coined by Vitalik Buterin and it addresses the underlying problem blockchain is facing, being the incapability to efficiently balance between decentralisation, scalability and security.
- **Decentralisation**
- As you have already seen from Week 1, decentralisation is the backbone of blockchain.
- While in traditional finance, the system is entirely centralized, decentralized systems empower permissionless ownership, where decisions are made by consensus: transactions are approved by a group of nodes as opposed to an individual node.
- Moreover, once these transactions are verified by consensus, they can not be altered.
- However, from pure decentralisation inherently emerges a ‘speed of transactions’ trade-off.
- For example, if a consensus comes along with multiple confirmations, it makes sense that it takes longer for a transaction to be approved by a consensus, than to be approved by a centralized entity.
- So, the question that arises here is:

“How can we achieve speed, without compromising consensus?”

The Blockchain Trilemma and How Stellar addresses it

Decentralisation, Scalability, Security

- **What is Stellar's position on the decentralisation of the blockchain?**
- Stellar is 'decentralized to the core' and has proven it theoretically and concretely.
- More specifically, as we mentioned in the previous lesson, the Stellar Consensus Protocol (SCP) is based on the Federated Byzantine Agreement (FBA) Consensus Protocol, which allows decentralized, autonomous computing networks to reach a consensus outcome on some decision.
- However, in the recent past, Stellar proved in practice that it really is a decentralized network.
- On April 2021, the Stellar Development Foundation's validator nodes, along with several nodes run by others in the ecosystem, temporarily stopped processing ledgers, and the SDF public Horizon instance stopped ingesting them.
- This led to a brief period of time, when it was impossible to serve requests or submit transactions to the network.
- While the Stellar Development Foundation (SDF) engineers started investigating and addressing the problem right away, there is a rather notable thing that happened; despite all the validators that had stopped working, there were still enough validators available to securely process transactions,
- This means that no matter the damage, the Stellar network still remained online, which is exactly how decentralized networks should operate.
- You can read more about this Stellar network downtime incident in Stellar's blogpost.

The Blockchain Trilemma and How Stellar addresses it

Decentralisation, Scalability, Security

- **Scalability**
- Scalability is where the issue really lies.
- Like any other network, a blockchain should be able to support the influx of users that troop in when it gets popular and manage high transaction volumes, if it wants to achieve mass adoption.
- Although scalability doesn't come off as important as decentralisation and security, it is critical for the network's vitality and competitiveness because it represents the point up to where blockchains can compete with traditional financial systems.
- A typical example of a blockchain network that struggles to handle scalability is Ethereum.
- Thanks to Ethereum first implementing smart contracts and being the main go-to source for Non-Fungible-Token (NFT) marketplaces and Decentralized Finance (DeFi) protocols, its scalability has suffered.
- Ethereum hasn't been able to handle the load of transactions leading to imposing extremely high gas fees, where the higher the gas fee, the more likely it is for a transaction to be prioritized.
- So, the question that arises here is:

"What is the maximum number of transactions a blockchain protocol can efficiently handle?"

The Blockchain Trilemma and How Stellar addresses it

Decentralisation, Scalability, Security

- **What's Stellar's position on the scalability of the blockchain?**
- As indicated in the 2022 Stellar Roadmap, the Stellar Development Foundation is aiming at increasing the network's scalability, as one of the three strategic blocks it concentrates on.
- More specifically, Stellar is planning on increasing its scalability in order to be able to accommodate use cases that require high transaction volumes and more throughput, as measured in transactions per second.
- In general, by increasing scalability, Stellar wants to offer more ways and opportunities for the community to participate in the ecosystem, through core optimisations.

The Blockchain Trilemma and How Stellar addresses it

Decentralisation, Scalability, Security

- **Security**
- Security isn't a new concept, since it is required in the traditional financial systems too.
- The term encompasses all of a blockchain's defence mechanisms against threats and malicious actors who might attempt to somehow take advantage of other computers on the blockchain.
- It is obvious that for the majority of crypto projects, they have been mainly focused on decentralisation and scalability, leaving security behind, since a barrage of high-profile hacks of exchanges and manipulation of vulnerabilities in source code has occurred.
- Although blockchain is inherently secure, it is not completely immune to hackers.
- As we have mentioned in Week 1, if a hacker is able to secure control of more than half of the network, they are able to alter a blockchain and manipulate transactions (the '51% attack').
- The more nodes a blockchain has, the more secure it is.
- Along with decentralisation, security is a core component for blockchains and necessary to remain competitive in today's industry.
- So, the question that arises here is:

"How can a system really prevent and diminish malicious actor that manipulate the system?"

The Blockchain Trilemma and How Stellar addresses it

Decentralisation, Scalability, Security

- **What is Stellar's position on the security of the blockchain?**
- Stellar has proven that it values security as a pillar of its network, since, as we have seen in the previous week, the Stellar Consensus Protocol (SCP) favours safety over liveness.
- Stellar's consensus algorithm ensures security in the transactions, in the sense that a block of transactions can never produce different results for different participants.
- Moreover, when it comes to tackling the infamous '51% attacks', the network is made in a way such that the cost of compromising Stellar validators is somewhat under the control of their administrators; SCP is responsive to high-assurance implementations, such as using hardware security modules to prevent a validator from signing contradictory messages.

The Blockchain Trilemma and How Stellar addresses it

Decentralisation, Scalability, Security

- Even though it is possible that many people aren't aware of the 'Blockchain Trilemma' and what the term means, they definitely are aware of the problems it represents, e.g., Bitcoin users experience extremely slow transaction speed and Ethereum users pay higher gas fees.
- It is important to keep in mind that the term 'Blockchain Trilemma' is just a way to conceptualize the problem and, under no circumstances, does it imply that all of its three aspects can not be achieved at the same network.
- However, there is no concrete blockchain network that has succeeded in incorporating all three features.
- In the future, if projects are able to successfully solve the trilemma, we could be looking at new levels of blockchain adoption.
- **How does Stellar ultimately address the blockchain trilemma?**
- Undoubtably, Stellar embodies decentralisation; the transactions are approved by a group of nodes as opposed to an individual node, once these transactions are verified by consensus, they can not be altered and Stellar Development Foundation is working on developing its native smart contract.
- Moreover, with the Stellar Consensus Protocol (SCP) favouring safety over liveness, it is obvious that it attaches great importance on securing a network where the transactions are safe.
- In regards to scalability, Stellar has already started working more extensively on it, as part of its 2022 roadmap.

5. Smart Contracts on Stellar

Comparison of Smart Contracts

Stellar Native Smart Contract

- Entering 2022, the Stellar Development Foundation released its roadmap, which includes developing its very own native smart contract.
- More specifically, the SDF plans on conducting thorough research and managing code development along with the Stellar community, in order to build a smart contract implementation this year.
- As Stellar is an open-source network, the SDF smart contract is something that must be built with the contribution of Stellar's engaged ecosystem of developers, in order for Stellar to keep developing in a way that reflects its community.
- You can find more about the Stellar's 2022 roadmap here.
- Also, you can jump on the Stellar discord in order to learn more about the current status of the smart contracts journey.

6. Conclusion

Conclusion

Key Learnings

- The Federated Byzantine agreement, is the basis of the Stellar Consensus Protocol. The essential innovation compared to the FBA is that with the SCP, not every transaction is subject to a consensus by vote (‘quorum’) in the whole network, but a validation for which a smaller part is sufficient, which the participant concerned is free to choose (the so-called ‘quorum slice’). The expectation is that, over time, particularly trustworthy nodes will emerge in the network that become intersections of diverse quora and form so-called quorum intersections - nodes on a meta-level of relative trust that stabilize the network even against strong deviations and errors such as hacker attacks.

- Decentralized exchanges, also known as DEXs, are peer-to-peer marketplaces that facilitate cryptocurrency traders to make transactions directly, without handing over management of their funds to an intermediary or custodian.

- There are three different blockchain generations; the ‘digital currency’, which was introduced with bitcoin, the ‘digital economy’, where the use of smart contracts became established and ‘digital society’, where blockchain applications will be widely adapted in our everyday lives. Stellar belongs to the ‘digital economy’ generation and is currently developing its native smart contract.

- The blockchain trilemma means that only two out of three constraints in a decentralized network can be reached. Therefore, the blockchain developer must decide which of one the features they will sacrifice.

References

References

1. https://www.stellar.org/learn/blockchain-basics
2. https://www.lumenauts.com/lessons/stellar-consensus-protocol
3. https://cointelegraph.com/defi-101/what-are-decentralized-exchanges-and-how-do-dexs-work
4. https://developers.stellar.org/docs/glossary/decentralized-exchange/
5. https://www.investopedia.com/tech/blockchain-technologys-three-generations/
6. https://www.ledger.com/academy/blockchain/web-3-the-three-blockchain-generations
7. https://cutt.ly/4OHRH4I
8. https://finance.yahoo.com/news/layer-two-solutions-help-solve-144306678.html#:~:text=Essentially%2C%20the%20blockchain%20trilemma%20is,many%20computers%20in%20their%20network
9. https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3
10. https://www.ledger.com/academy/what-is-the-blockchain-trilemma
11. https://medium.com/interstellar/understanding-the-stellar-consensus-protocol-423409aad32e#:~:text=The%20Stellar%20Consensus%20Protocol%20was,consensus%20outcome%20on%20some%20decision.
12. https://stellar.org/blog/decentralized-to-the-core?locale=en
13. https://www.stellar.org/roadmap?locale=en

Questions?

Contact Us: Stellar Developers Discord

Twitter: @StellarOrg

UNIC | DLRC

Stellar