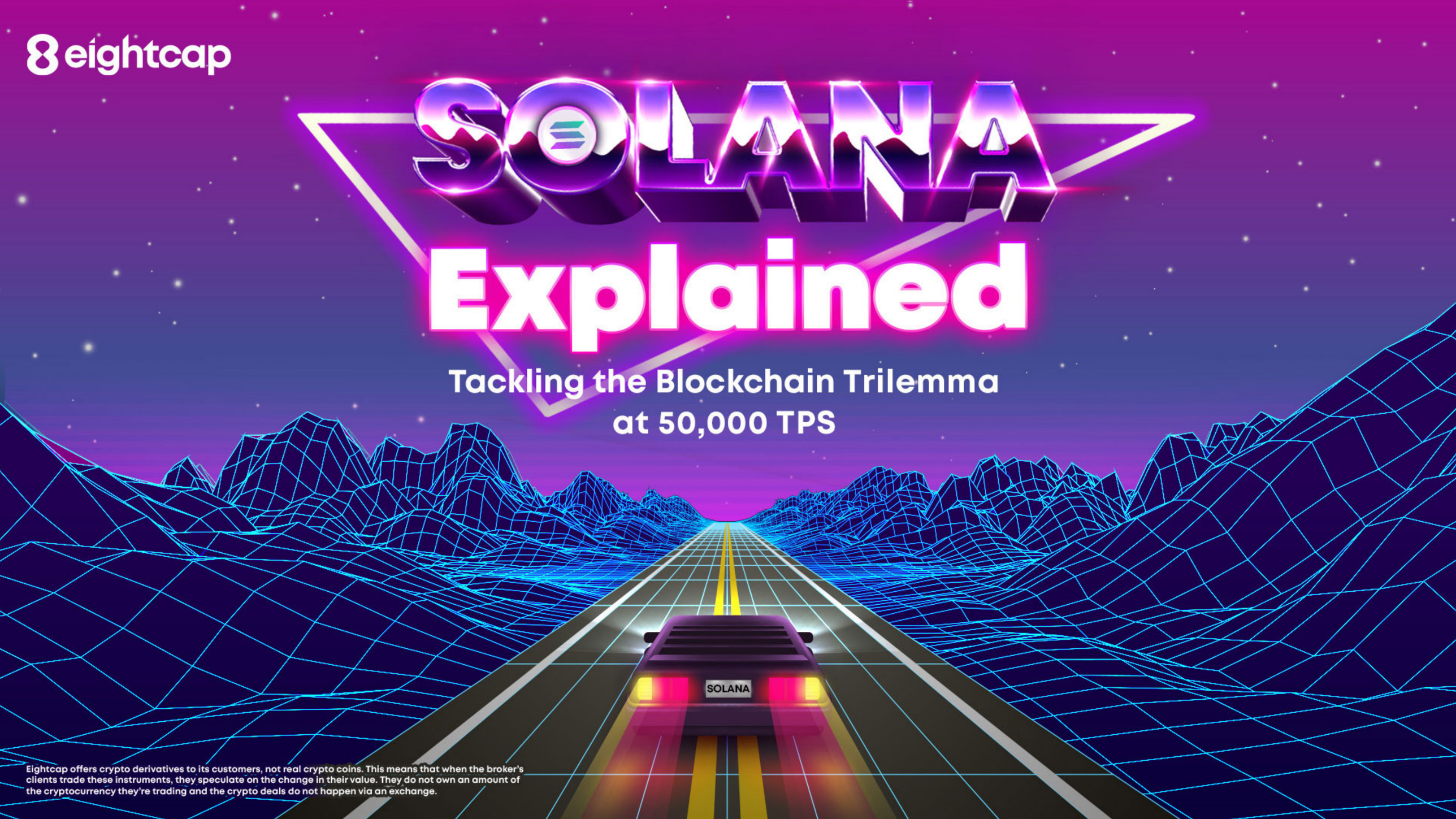
eightcap

SOLANA Explained

Tackling the Blockchain Trilemma at 50,000 TPS



eightcap

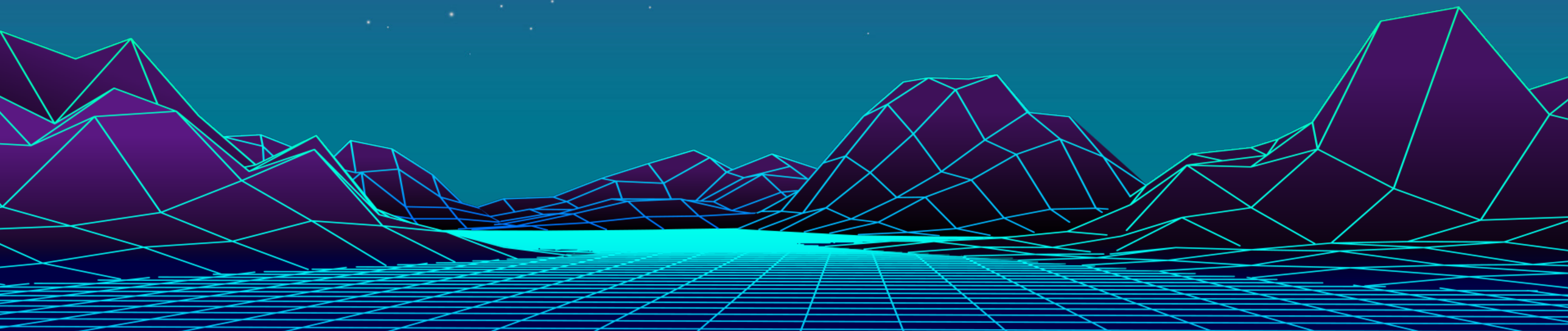
Summary

Solana is a web-scale blockchain network whose goal is to tackle the issue of scalability while remaining decentralized and secure. It does that through a set of protocols and other technologies that form its hybrid consensus mechanism. Solana's cryptocurrency, SOL, successfully claimed its place among the top 10 cryptocurrencies in 2021. Let's have an in-depth look at both its foundations and the premises that might make it the next big thing in the crypto ecosystem.

eightcap

Intro

How fast does a cryptocurrency have to be so it can replace fiat money entirely? As decentralized and secure as blockchain networks are, they don't always manage to provide timely clear answers to this question. Block time, or the time needed to validate a block and approve the tokens on it, allow for transactions to take place. Transactions, on the other hand, are counted in seconds. Even for Bitcoin and Ethereum whose numbers, when analyzed up close, show 3-7 TPS for the biggest crypto on the planet and 15-25 TPS for the runner-up.



eightcap

Intro

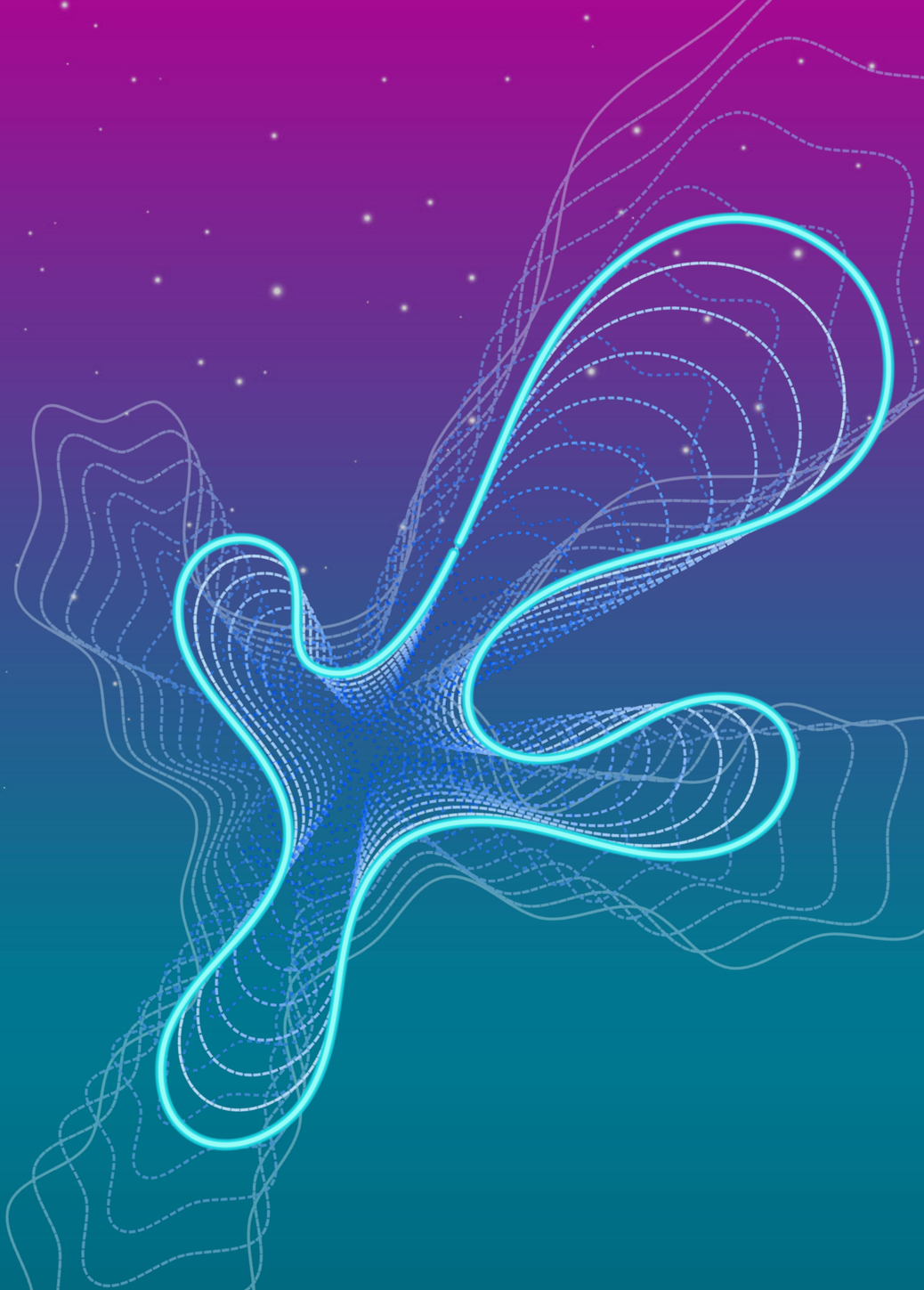
Solana, whose cryptocurrency, SOL, is sitting in the top five list by market cap, at $75,551,713,011, has an answer. **It is 50,000 TPS and counting – something possible only due to its consensus approach.** It makes use of what's called a proof-of-history method, based on the proof-of-stake consensus mechanism utilized by networks like Cardano. Having a cryptocurrency reach five digits in transactions per second exceeds Visa or Mastercard's 188 billion and 118 billion transactions per year, or approximately 6,000-8,000 TPS. That being the case, how much of a difference do those few thousand TPS matter in today's world where transaction numbers climb year after year? Let's find out.

eightcap

From Qualcomm to Loom and Solana

Solana's beginning dates back to November of 2017 when its creator, Anatoly Yakovenko, published the whitepaper that set the foundations for the future blockchain. His analysis of network synchronization for the purpose of keeping time between computers from different networks was put forth as the guiding motive behind proof-of-history that enables **10,000 times faster transactions.**

Yakovenko's experience with internal systems clock synchronization came from his work in Qualcomm, Mesosphere, and Dropbox. Seeing as even Bitcoin and Ethereum are struggling to produce results better than 15-45 transactions per second, it is understandable why centralized options like Mastercard and Visa are still the main go-to for global payments. That's still a field where cryptocurrencies are losing, although they offer many other beneficial features.

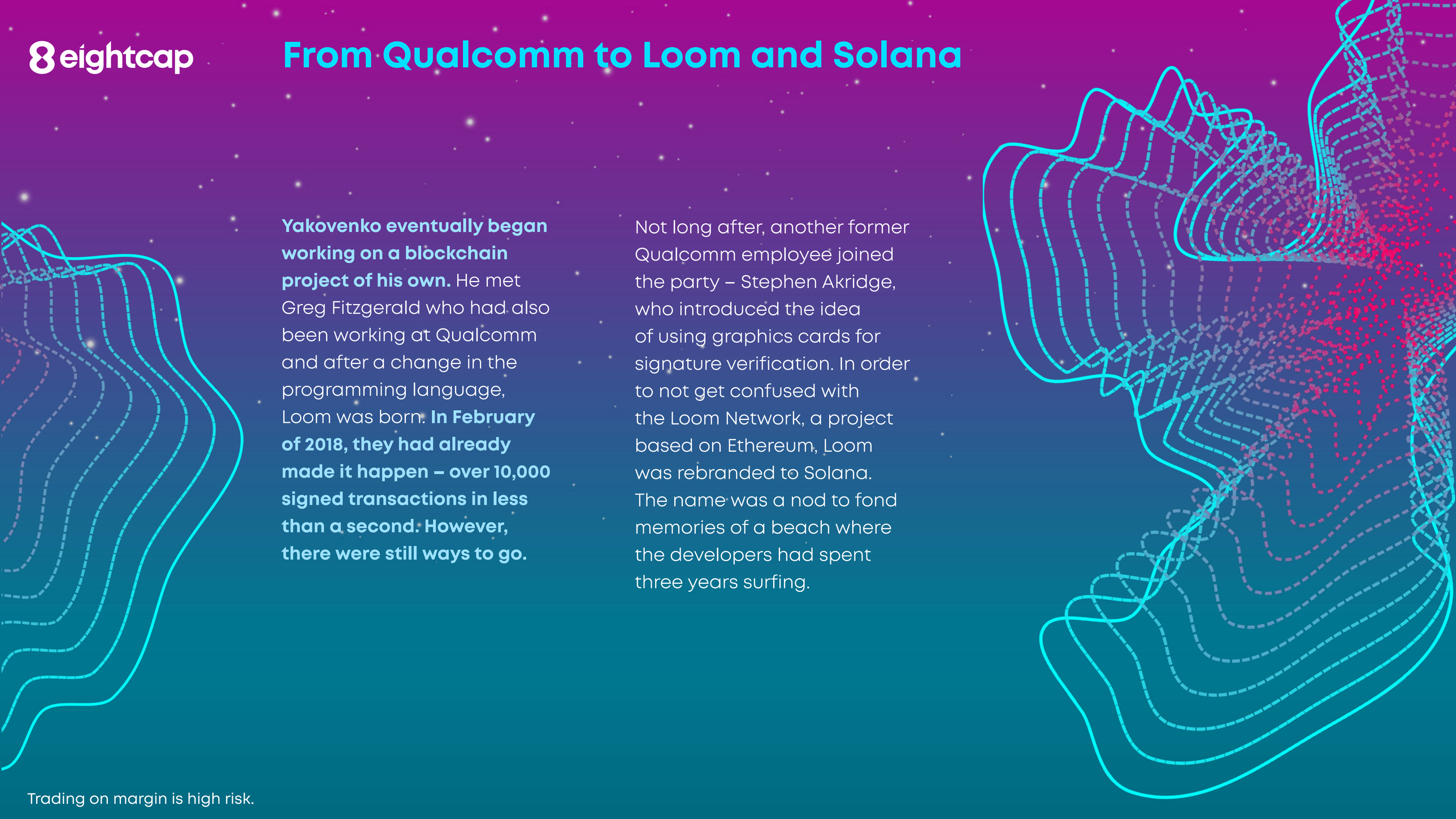


eightcap

From Qualcomm to Loom and Solana

Yakovenko eventually began working on a blockchain project of his own. He met Greg Fitzgerald who had also been working at Qualcomm and after a change in the programming language, Loom was born. **In February of 2018, they had already made it happen – over 10,000 signed transactions in less than a second. However, there were still ways to go.**

Not long after, another former Qualcomm employee joined the party – Stephen Akridge, who introduced the idea of using graphics cards for signature verification. In order to not get confused with the Loom Network, a project based on Ethereum, Loom was rebranded to Solana. The name was a nod to fond memories of a beach where the developers had spent three years surfing.



From Qualcomm to Loom and Solana

Around the start of the second half of 2018, the team began working on a larger network of nodes that would make it possible to verify even more transactions per second. In December, they had reached an average of 200,000 TPS with periodical spikes of over 500,000. Later on, the project opened up to supporting more on-chain programs and programming languages, all between the safe walls of BPF (Berkeley Packet Filter), used for network traffic analysis and data transferring.

Currently, Solana Labs are the heart of the blockchain represented by Yakovenko and his team. In fact, that's the initial fundraising organization that managed to receive funding of $20 million during 2019 and another $1.76 million during its public token sale of 2020. Nowadays, the non-profit organization, Solana Foundation, works on community growth and fund development.

eightcap

The Blockchain Trilemma

Blockchain technology pertains to our online activities and can extend to real-life applications. From transactions to credential validations, there is a place for everything digital that requires the secure transfer of data. Most commonly, such data would be trading and investing funds, purchases, be they of products, services, or virtually anything. Once the data is processed, it is stored on a distributed database that maintains this shared list of information in the form of blocks. Each one of them is encrypted and carries the history of all its predecessors, passing it down the chain. Thus, a blockchain is born.

However, it usually comes with the downside of having to choose between making it two of the three variants at most – decentralization, security, and scalability. Most cryptocurrencies and blockchain networks choose to go with security and decentralization before anything else – this is where

The Blockchain Trilemma

we have the most famous players like Bitcoin, Ethereum, Cardano, Dogecoin, Shiba Inu, and others. We also have those that choose to be scalable and secure at the cost of decentralization – such is the case with Ripple, Hyperledger, EOS, Stellar, etc. And finally, there is the group that relies on decentralized scalability without providing proven secure means of verifying transactions – some examples include Vechain, Nano, and IOTA.

While Ethereum's Eth2 upgrade slated for 2022 is set to make the network more scalable than ever, **at this time, Solana is about the only option that covers all three elements of the trilemma.** To be precise, the real roadblock was the scalability, or the time it took networks to reach a consensus between validators of a block. As a result of the hybrid consensus algorithm of PoH and PoS, the usual number of 15 transactions per second or less can be upscaled to 50,000 and under the right circumstances, many times over.

eightcap

Why it's important that crypto-currecies are as fast as fiat currencies

For cryptocurrencies, scalability has always been a field in which even Bitcoin and Ethereum do not excel. Thus far, there have been several potential solutions proposed to overcome this problem.

One of them is batch payments as one transaction. A practical example – payroll payments to 1000 employees would be sent through Bitcoin as a single transaction. That way, employees' wallets would receive the allocated funds and the employer's wallet would be the only one to make this single transaction. A benefit of batch transactions is that the time it would take would be shorter, the transaction size would be smaller and therefore, the fees associated would not be as high either. This system is useful for one-to-many transactions, including bill-paying amongst others. However, if we were to take the earlier example of payroll, with a single transaction being used for multiple recipients, all of

Why it's important that crypto-currencies are as fast as fiat currencies

them would be able to view the transaction records and therefore, everyone else's wallets. Consequently, it would be possible to deduce who got how much and as a privacy concern, this is not an ideal approach.

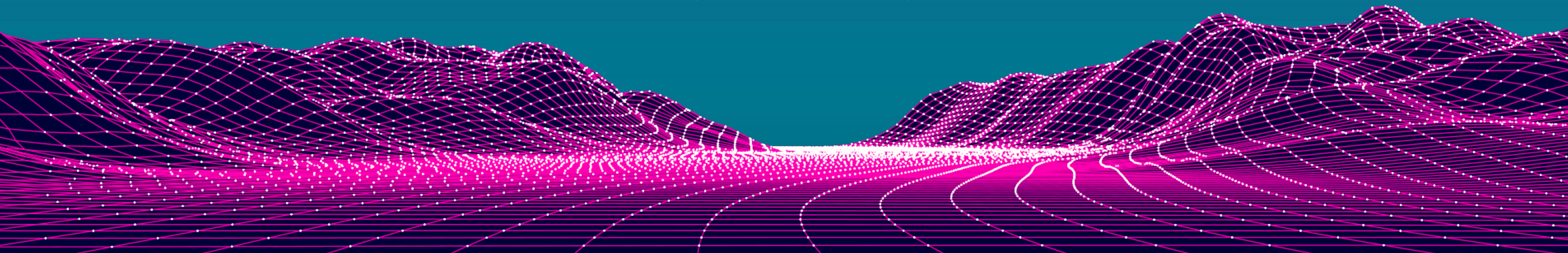
Another method is the Lightning Network that tackles this issue by offering safe and instant transactions without fees, but it works only on Bitcoin-core-based blockchains like Dogecoin, Litecoin, Bitcoin Cash, etc. Bitcoin Cash itself is also an option that increases the transactions per second performed but it's even more limited, as there is no way to make use of it outside the Bitcoin Cash platform itself.

On the other hand, Solana is built from the ground up with the idea that tens of thousands of transactions per second are the bare minimum. Not a bad idea for accommodating the world with a viable blockchain solution to this problem. Its scalability is only limited by the hardware being used – GPU, CPU, memory, and bandwidth. What's more, Solana nodes

Why it's important that crypto-currencies are as fast as fiat currencies

can be hosted in pretty much every mainstream data center, including AWS, Azure, and Google Cloud. They are not just for show either. Their networks are soon to be connected via undersea fiber optic cables that run across the world. As a result, they excel in performance, stability, and resources. Let's take AWS VPC's 4.9 Gbps/sec internet speed – while using Solana, in theory, it's possible to reach 3.5 million TPS.

Even so, centralized networks are not as reliable – Azure's minute-long outage can sometimes extend to several hours and even Google can have several outages in a month. That's where a decentralized system like Solana's can come in handy. Although it requires a hefty investment of around $5000 to build a proper rig and an acceptable internet connection, based on the Speedtest Global Index and Speedtest website, it's possible to reach several million TPS. Understandably, when you can have this kind of scalability, institutions working with billions of transactions can sleep sound knowing their business wouldn't be obstructed by the blockchain transaction speed. At this time, though, given that only about 3,000 transactions on average are performed each second, it is safe to say that the network will need quite a push to come close to such numbers.



eightcap

Proof-of-history & tackling the trilemma

Now that we know that bandwidth is the answer to the blockchain trilemma, or more precisely, the scalability trilemma, we can dive deeper into how Solana's proof-of-history attempts to change that.

Using proof-of-history based on the proof-of-stake consensus, a trustless source of time can be established for the whole network. Doing so, the network remains decentralized. At the same time, the blockchain record of activities is permanently stored and the chronological storage is facilitated.

Moreover, since PoH acts as the primary instrument to ensure node synchrony, it works alongside the proof-of-stake consensus and turns the consensus algorithm into a hybrid. While the proof-of-work consensus relies on raw processing power and the proof-of-stake algorithm – on stake holding, the proof-of-history method requires proof of historical events. It creates a historical record serving as proof that an event took place at a specific moment in time.

eightcap

Proof-of-history & tackling the trilemma

Validators do not have to “talk” to each other to confirm that an event took place so that a block can be safely formed. Instead, each validator’s clock is maintained by the SHA-256 encoding of the passage of time in a sequential-hashing VDF (verifiable delay function). Basically, confirmation occurs by checking if everyone’s clocks are running on time and if all events are equally recorded.

Reliance on local computer clocks and timeouts between state transitions beyond the VDF is unnecessary when following this approach. Nodes begin this state transition as soon as they receive the message that says a portion of the VDF has been generated. The method of data transmission happens through the Turbine propagation protocol that helps make the final step towards getting rid of the trilemma.

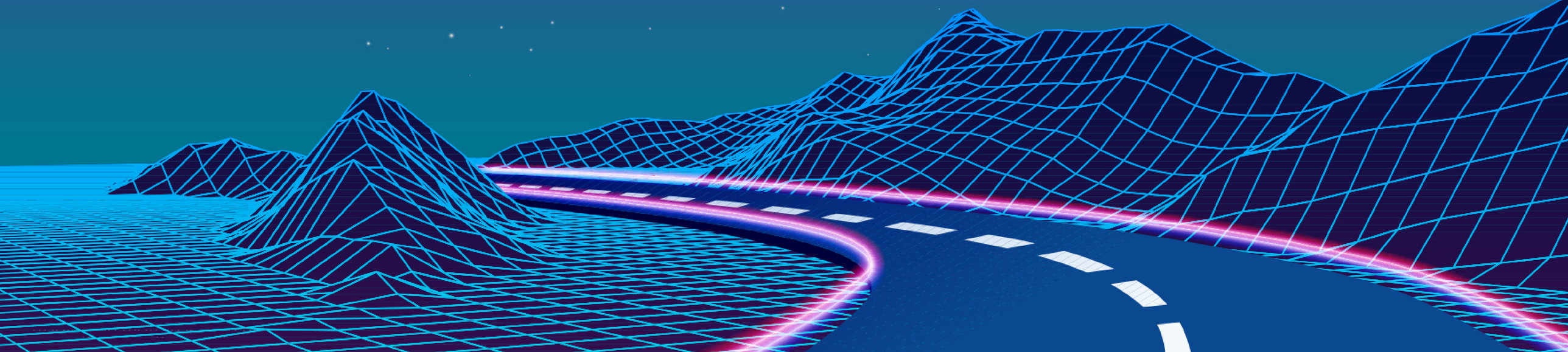
Proof-of-history & tackling the trilemma

A data propagation technique/protocol serves a specific purpose. BitTorrent uses TCP (Transmission Control Protocol) to offer host-to-host communication for transfer of large files to large groups of people. MediaFLO, which Yakovenko worked on, improved multicast over wireless networks efficiency by utilizing data propagation protocols on the physical layer, i.e. through specific devices. Solana, on the other hand, takes that to the next level.

High-performance blockchains transfer large amounts of data to a large number of peers, but they need longer time frames to do that. Validators work in groups and the leader needs to transmit a block of a given size. Let's say 20,000 validators take part in validating a block of 128 MB in size, which is made up of 500,000 transactions of 250 bytes. The leader would have to transmit 128 MB of data 20,000 times so that the block validation is complete. Bandwidth is the key to accommodating this number of connections.

Proof-of-history & tackling the trilemma

Borrowing from BitTorrent's TCP technology, Turbine, Solana's block propagation protocol, has the leader break the block into packets of up to 64 KB in size. They then transmit those to validator "neighborhoods", or just small groups of validators – in this case, 2,000. In turn, each validator retransmits their packet to another group of peers. In the end, each neighborhood expands further. Depending on the network, this can reach numbers such as 40,000 validators in just two hops, equal to around 200 milliseconds if each link is 100ms on average. This process becomes more complex as we speak and Solana's testnet shows it live on a limited number of nodes to save costs.



eightcap

The Solana Network

In addition to PoH and Turbine – two core features to the Solana network, there are six more. Each of them acts as a layer to make the network function correctly. If we were to think as the ones discussed thus far as the skeleton of the network that provides scalability, the rest are the bones, organs, and blood that give it life, keeping it decentralized and secure.

Solana has taken the Practical Byzantine Fault Tolerance (PBFT), used to prevent software errors and malicious attacks, and optimized it. After PoH's function as a kind of cryptographic clock has been performed, the Tower BFT algorithm takes over and essentially serves as the synchronized clock allowing for consensus to take place without considerable cost or delay.

The Solana Network

Gulf Stream – the mempool-less transaction forwarding protocol, serves as the management board. Generally, mempools are submitted transactions awaiting processing by the network. Those can be seen live for networks like Bitcoin and Ethereum and can range from a few hundred thousand to a few million. Solana breaks the cycle by having validators forward transactions to the upcoming leader so that they are processed faster. As a result, leaders change faster and there is not that much strain for validators. The 50,000 TPS is achieved thanks to this protocol's seamless integration.

Sealevel is the parallel smart contracts run-time, or the reason why Solana is able to use parallel blockchain transactions. It comes at the cost of every core of CPUs, SSDs and GPUs a validator needs to manage tens of thousands of smart contracts at a given time. After all, when you have scalability, you might as well allocate all the power you have, right?

eightcap

The Solana Network

Pipelining is the process through which the network's validation mechanism is optimized, regardless of the CPU design. A sequence of input data is assigned to the relevant hardware components and consequently, transaction data is verified and duplicated throughout the nodes. Very useful when there are several stages of processing data with separate hardware.

Cloudbreak is the database with all the accounts that can be stored on a scalable platform like Solana. It uses a horizontal scaling data structure that enables it to read and write across the network simultaneously.

Archivers is a network of nodes that stores data coming in from the validators. Ledger data can accumulate fast, and it isn't difficult for blockchain networks to produce 4 petabytes at 1 Gbps. Storing such enormous amounts of data can lead to centralization if things are not managed well. Utilizing a distributed ledger storage, Solana periodically verifies the correct data is being stored through nodes in the form of personal computers or even laptops.

eightcap

Solana has potential for scaling up, but it's a game of timing

Nowadays, being a decentralized and secure blockchain has become a standard that many skilled teams meet when developing their projects. However, being scalable without moving towards centralization or risking data being exposed seems to pose a challenge related to the consensus mechanism of a network.

Solana's idea to getting around this is by taking the proof-of-stake algorithm and building on it with proof-of-history. By moving away from local computer clocks, it employs a method of using a synchronized clock that allows validation at breakneck speed. This is achievable by utilizing 8 technologies that have become the building blocks of the network.

eightcap

Solana has potential for scaling up, but it's a game of timing

Projects on the network are growing in number and ambition. However, it is still early for Solana to supersede the top currencies.

Over time, though, it certainly shows the potential to turn into a leading, if not the leading blockchain network. Nevertheless, with other networks looking for a viable option to solve this potential issue, time is of the essence, as Solana's fast transaction speed is currently the main appeal it has. Whatever lies beyond for Solana and how it affects SOL's price in the future, traders who want to see it through will have to be on the lookout.

Bibliography Index

PAGE 3
https://www.investopedia.com/terms/b/block-time-cryptocurrency.asp
https://blog.tezro.com/cryptocurrency-transaction-speeds/

PAGE 4

https://coinmarketcap.com/currencies/solana/
https://www.statista.com/statistics/261327/number-of-per-card-credit-card-transactions-worldwide-by-brand-as-of-2011/

PAGE 5
https://docs.solana.com/history
https://solana.com/solana-whitepaper.pdf

PAGE 7
https://docs.solana.com/developing/on-chain-programs/overview
https://medium.com/solana-labs/announcing-the-formation-of-the-solana-foundation-afde417afd73

PAGE 8
https://en.wikipedia.org/wiki/Blockchain
https://medium.com/yardcouch-com/solana-everything-you-need-to-know-about-the-ethereum-killer-e34c18f17d22

PAGE 9
https://www.cnbc.com/2021/10/28/what-to-know-about-ethereum-altair-upgrade-and-proof-of-stake.html

PAGE 10
https://towardsdata__science.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44
https://bitcointechtalk.com/saving-up-to-80-on-bitcoin-transaction-fees-by-batching-payments-4147ab7009fb

PAGE 12
https://www.theregister.com/2020/04/08/azure_devops_outage/
https://www.datacenterdynamics.com/en/news/google-cloud-suffers-brief-outage-bringing-down-gmail-snapchat-and-nest/
https://www.speedtest.net/global-index#mobile
https://explorer.solana.com/

PAGE 13
https://medium.com/solana-labs/how-solanas-proof-of-history-is-a-huge-advancement-for-block-time-178899c89723

PAGE 14
https://crypto.iacr.org/2018/slides/28858.pdf
https://solana.com/news/turbine---solana-s-block-propagation-protocol-solves-the-scalability-trilemma

PAGE 15
https://www.bittorrentvpn.com/udp-vs-tcp-protocols/
https://en.wikipedia.org/wiki/MediaFLO

PAGE 16
https://testnet.solana.com/

PAGE 17
https://pmg.csail.mit.edu/~castro/osdi99_html/osdi99.html

PAGE 18
https://medium.com/solana-labs/gulf-stream-solanas-mempool-less-transaction-forwarding-protocol-d342e72186ad
https://www.blockchain.com/charts/mempool-size
https://etherscan.io/chart/pendingtx
https://medium.com/solana-labs/sealevel-parallel-processing-thousands-of-smart-contracts-d814b378192

PAGE 19
https://medium.com/solana-labs/pipelining-in-solana-the-transaction-processing-unit-2bb01dbd2d8f
https://medium.com/solana-labs/cloudbreak-solanas-horizontally-scaled-state-architecture-9a86679dcbb1
https://solana.com/news/archivers---solana-s-solution-to-petabytes-of-blockchain-data-storage

PAGE 21
https://www.solana.news/sol-projects