The Technology Behind Solana

Eric Anderson
Student at Ontario Tech University
Oshawa, Canada
eric.anderson1@ontariotechu.net

Abstract – Throughout this paper there are multiple topics discussed. To start off the innovations of Solana will be talked about. This includes Proof of History, Practical Byzantine Fault Toleration, Turbine, Gulf Stream, Sealevel, Pipeline, Cloudbreak and Archivers. Then the paper will move onto the applications of Solana, which will cover Serum and Star Atlas. Finally, we will cover the advantages and downsides of Solana.

Index Terms – Archivers, Blockchain, Cloudbreak, Cryptocurrency, Gulf Stream, Pipeline, Practical Byzantine Fault Toleration, Proof of History, Proof of Stake, Sealevel, Serum, Solana, Star Atlas, Turbine

I. INTRODUCTION

In November 2017 Solana was born, although not a cryptocurrency yet it started its journey on becoming one of the biggest ones in the world. So, if the cryptocurrency did not quite exist yet what happened in 2017? Well Anatoly Yakovenko published his whitepaper on Proof of History, which will be covered later on in the paper. As you will read Proof of History is the core of how Solana works. Proof of History allowed a system that was 10,000 times faster without any additional modifications. At this point with the help of Greg Fitzgerald, Anatoly implemented Solana in rust and called it Loom [11].

On February 13th 2018 the first open-source implementation of Anatoly's white paper began under the name Silk. Just fifteen days later Greg released the first demonstration of Silk verifying ten thousand transactions in just over half a second. Shortly after this Anatoly, Greg, Stephen Akridge and three others co-founded Loom. Not too long after though Ethereum had a project called Loom, so the team rebranded to the name today, Solana. This name came from a beach called Solana where Anatoly, Greg and Stephen lived while working for Qualcomm [11].

Since 2018 Solana has only improved and become more popular. In 2021 the interest in Solana on google has increased by 350%. Solana has also been ranked in the top ten cryptocurrencies. "Several factors are fueling Solana's value, with the venture into non-fungible tokens (NFTs) emerging as the possible top reason. The interest in the asset follows the publication of the Degenerate Apes NFT collection. The publication became the center of attention for creators and token holders in the asset ecosystem. The hype around Solana also comes after the network unveiled the "global Solana hackathon". The competition that runs until early October seeks to inspire innovators to create and develop blockchain-based games, art, and collectibles alongside decentralized lending platforms built on the Solana blockchain." [13]

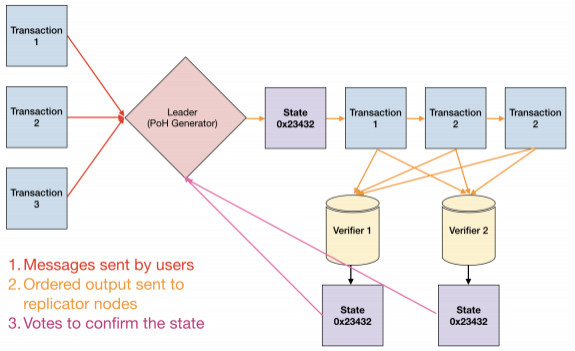
So, with such a rapidly growing cryptocurrency it is useful to understand how Solana functions. Solana has made many innovations in the crypto space which will be the focus of this paper. Those innovations would be Proof of History, Practical Byzantine Fault Toleration, Turbine, Gulf Stream, Sealevel, Pipeline, Cloudbreak and Archivers. It is also important to cover what Solana is being used for, as well as what some of its ups and downsides are.

II. TECHNOLOGY

A. Overview of How Solana Works

Before discussing the technologies Solana uses it is important to talk about how its network functions. A Solana network can be broken down into a leader and verifiers. These verifiers and leader possess the same hardware capabilities, and as such only differ in a logical sense. In this network there can only be one leader but any node can become the leader. Any node selected to become a leader is done through Proof of Stake (POS) elections. When an election is required the validation node with the largest voting power is selected. In the event of a tie though the node with the highest public key address is selected as a leader. The Solana network also has a fail safe where a secondary node can be elected to take over from the leader in the event of its failure [6]. Now with an understanding of how a leader is elected let's finally dive into how the Solana network actually functions. First transactions made by users are sent to the leader. This leader then will sequence these message transactions with the use of Proof of History (POH). POH will be discussed later on in this section. With the transactions organized the leader executes them on the current state in the RAM. Next the lender publishes the transactions and signature of the final state to the

verification nodes. Once here, the verification nodes can execute the transaction like the leader with their copies of the state. If the signatures of state match the leaders than it will count as a vote in Solana's consensus algorithm [21]. When the network receives at least two-thirds of the network in votes it is said that the network has reached consensus on a transaction [6].



[21]

B. Proof of History

An important part of the Solana network is its POH algorithm. With it, the network can have a high throughput rate because the times of the transactions can be easily tracked. Therefore, allowing the network to easily keep transactions in order [21]. This tracking works with the use of a cryptographically secure function like sha256. So, when a transaction is made and added to the sequence, they are hashed with the previous transaction's hash. This way, one cannot guess the hashes of the upcoming hashes as you need the entire sequence to calculate the next hash. In addition, during the hashing process data can be appended to the previous transaction's hash to further increase integrity of the sequence [6].

PoH Sequence

Index	Operation	Output Hash
1	sha256("any random starting value")	`hash1`
2	sha256(`hash1`)	`hash2`
3	sha256(`hash2`)	`hash3`

[6]

The Solana network also supports the horizontal scaling of POH. This means that more than one POH generator can exist. Solana achieves this by mixing the sequence state between generators without splitting. As a result of the horizontal scaling all the participating generators are needed to reconstruct the events in the system. By scaling the system can handle more events, but it is at a cost towards real time accuracy [6].

PoH Generator A			PoH Generator B		
Index	Hash	Data	Index	Hash	Data
1	`hash1a`		1	`hash1b`	
2	`hash2a`	`hash1b`	2	`hash2b`	`hash1a`
3	`hash3a`		3	`hash3b`	
4	`hash4a`		4	`hash4b`	

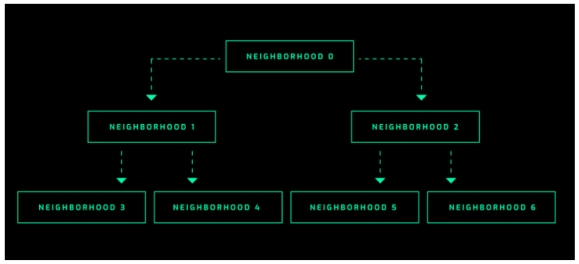
[6]

C. Practical Byzantine Fault Toleration

With PBFT, network consensus can occur without having large messaging overhead and latency [21]. The implementation of Solana's PBFT requires the use of its POH function, as it is used as a global source of time before consensus. Due to the structure of the Solana ledger PBFT time-outs can be directly recorded on it. In practice PBFT can be broken down into two concepts. When a validation node votes on a POH hash the system guarantees that the node can only vote on hashes that are children of its last vote for at least X hashes. Also, the time-out for previous votes double. This means as more blocks are added to the ledger the time it would take to rollback to a block exponentially increases. As such, the more blocks that are added the higher chance old blocks are confirmed. Once a POH hash is confirmed it can no longer be rolled back [7].

D. Turbine

Solana's Turbine is a solution to the scalability trilemma. The trilemma is, increasing the number of nodes in a network increases bandwidth but the propagation time to all nodes grows. So, with out any technology implementation, like Turbine, a block would need to be transmitted to all the nodes in the network. Turbine solves this in a few ways. For one it uses UDP to transmit individual packets through a random network path. It also breaks blocks into 64KB packets and sends them to different validator nodes. Finally, it also groups nodes into a tree of neighborhoods. As a result, packets can be sent to each neighborhood and then propagated to each node in that neighborhood [8].



[8]

E. Gulf Stream

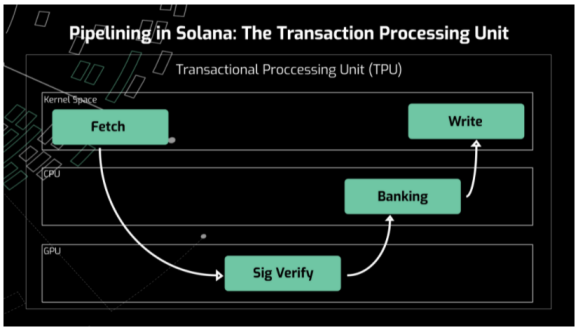
Gulf Stream is Solana's solution to achieve a high-performance adversarial network. In Solana Gulf Stream is what manages mempools. A mempool is a set of transactions that have been submitted but not processed yet. With Solana's technology a mempool of 100,000 can be executed in seconds. This is achieved by pushing transaction caching and forwarding to the edge of the network. Due to the Solana network design every node knows the order of the upcoming leaders, clients and validators. As such, transactions can be forwarded to the expected leader ahead of time. This has the by-product of reduce confirmation times, faster leader switching and lower pressure on the memory from validators from the mempools. For this to work though the Solana network must have a deterministic leader, which it does [3].

F. Sealevel

Unlike other runtimes, Solana has built one that can process tens of thousands of smart contracts in parallel. The high efficiency is the result of two things. The first being that all available cores on validators are used. Secondly, it is because transactions describe the states they will read or write while executing. Thus, non-overlapping and state sharing transactions can execute concurrently [5].

G. Pipeline

To be an efficient network Solana must quickly form consensus, validate massive blocks of transactions and replicate those transactions across the network. To do this, the process of transaction validation uses pipelining. Keeping the network cards, CPU cores and GPU cores busy all the time is important so Solana introduced a four stage Transaction Processing Unit (TPU) in software. In the network the TPU "progresses through Data Fetching at the kernel level, Signature Verification at the GPU level, Banking at the CPU level, and Writing at the kernel space. By the time the TPU starts to send blocks out to the validators, it's already fetched in the next set of packets, verified their signatures, and begun crediting tokens." [4] As a result of this the TPU can process 50,000 transactions simultaneously, and this can all be done with a computer for under $5000 [4].



[4]

H. Cloudbreak

Solana accounts are totally random cryptographic public keys. An account wallet will have many Account addresses that are completely unrelated to other addresses. As a result of no locality between accounts it is improbable, they will be started close together in memory. A single transaction will need to read two accounts and write to one, so an inefficient database can be a huge bottleneck. The solution to this problem is to have a database perform concurrent reads and writes.

Cloudbreak allows these concurrent reads and writes to occur. In this technology memory-mapped files are leveraged. These file's bytes are mapped into a virtual address space. Once done the mapped file behaves like traditional memory. Cloudbreak also leverages CPUs and operating systems, as the former is great at prefetching memory that is accessed sequentially, and the latter is good at handling sequential page faults. As such, the accounts data structure is broken up as follows.

1. Indices of accounts and forks are stored in RAM.
2. Accounts are stored in memory-mapped files up to 4MB in size.
3. Memory maps only stores accounts from a single proposed fork.
4. Maps are randomly distributed across many SSDs.
5. Copy-on-write semantics are used.
6. Writes are appended to a random memory map for the same fork.

7. Indices are updated after each write is completed.

Solana's technology allows for the benefits of sequential reads and writes. This result is a database the horizontally scales really well. The last thing that Cloudbreak does that is really good is it performs garbage collection. When forks become finalized beyond rollback and accounts are updated old versions get removed and memory is relinquished [20].

I. Archivers

At full capacity the Solana network generates 4 petabytes of data a year. It is not feasible for every node to store all that data as it would limit network membership to a few large centralized systems. Archivers have very low hardware requirements and are not consensus participants. The Solana Replicator network functions as follows. “Archivers must signal to the network that they have X bytes of space available for storing data. On some frequency, the network divides the ledger history into pieces to target some replication rate and fault tolerance based on the number of Replicator identities and total available storage of Archivers.” [1] Once the Archiver data assignments have been made, each Archiver downloads their data from consensus validators [1].

IV. APPLICATIONS

A. Serum

Solana has a wide range of applications. One of which is Serum. Serum is a decentralized exchange (DEX) that is built on the Solana blockchain. As such it comes with all the benefits, like low transaction costs and great transaction speeds [9]. Serum uses a decentralized orderbook that allows them to match buyers and sellers. This orderbook is run with the use of smart contracts. In addition, Serum has the benefit of having cross-chain support; which means that tokens built on other platforms can still be traded with Serum. Also, other decentralized finance projects can use its liquidity [20].

When a trader goes to buy or sell cryptocurrencies from liquidity pools, users have full control of their orders. So, users can choose the price they want to buy and sell their assets at. During a trade Serum has a fee associated with it. This fee is in Serum’s currency, SRM, and the tokens are removed from circulation at the end of a transaction. Cross chain swaps work by using collateral; when a swap occurs, the users sent money to a smart contract. If the swap is successful the money is returned to the users. In the event of a dispute the contract determines the correct user by checking the ledger. In the event there is wrong doing the correct user is sent their assists back plus part of the other user’s collateral [20].

B. Star Atlas

Another example of Solana’s applications is Star Atlas. This application of Solana is very unique as it is combining blockchain mechanics with game mechanics [9]. Star Atlas’ gaming model is called Play-To-Earn. This model incentivises gamers to play the game [17]. With blockchain games like Star Atlas have players earn cryptocurrencies based on the time and effort they put into the game. Most Play-To-Earn games require an initial investment, but users can make their money back in a couple months [15].

As far as the actual game goes, it is based in 2620 and three factions must fight for resources, territory and political power. The three factions are the MUD (humankind), ONI (consortium of alien races) and Ustur Sector (sentient androids). Players of the game are citizens and can explore space, search for resources and influence the outcome of galactic conflicts between factions. As a result, players earn real-life rewards for their efforts [15].

V. CONCLUSION

Solana is and innovative and useful cryptocurrency with many applications. With its technical innovations it is a scalable and fast crypto currency. With the use of technologies like Proof of History, Practical Byzantine Fault Toleration, Turbine, Gulf Stream, Sealevel, Pipeline, Cloudbreak and Archivers Solana is able to achieve transaction speeds of 50,000 transactions per second. Also, once Solana grows more it could be capable of 700,000 transactions per second. With all this speed this cryptocurrency has many applications. One of which is a decentralized exchange called Serum. Another application was a game called Star Atlas that combines blockchain mechanics with it. Solana is still in its infancy, but it has some good technology behind it and hopefully it will continue to grow over the next few years.

VI. FEEDBACK

When looking at Solana I see many advantages and disadvantages. Overall, I think Solana

is still in its infancy and needs some time to grow. Although it seems like it has a high chance of becoming an even more dominant currency in the future. When looking at Solana's benefits there are a few key areas to look at, although there are more. These areas are the networks scalability, low barrier of entry for validators and its environmental friendliness.

With the use of Solana's technologies like POH, Turbine and Cloudbreak the network can currently process 50,000 transactions per second; but as a result of the network's scalability, it potentially could get up to 700,000 transactions per second [10].

In addition, validators have relatively low technology requirements, really only costing the amount of a high-end gaming PC. The example requirements from Solana are as follows.

Component	Example	Estimated Costs
GPU	2x 2080Ti	$2500
OS/Ledger Storage	Samsung 860 Evo 2TB	$370
Accounts storage	2x Samsung 970 Pro M.2 512GB	$340
RAM	32 GB	$300
Motherboard	AMD x399	$400
CPU	AMD Threadripper 2920x	$650
Case		$100
Power supply	EVGA 1600W	$300
Network	> 500 mbps	

As you can see the component recommendations are still consumer grade making the entry for validators easier [19].

Also, compared to other cryptocurrencies Solana uses POS instead of Proof of Work (POW). This has the result of being better for the environment. With POW computers need to work hard to solve mathematical problems to protect the network integrity, which uses a lot of electricity. Solana on the other hand with POS, nodes need to stake SOL tokens to protect the network. Although this still uses power it is significantly less than POW [16]. Like any good thing though there are some downsides.

One of these issues is Solana does not have a lot of transparency. For cryptocurrencies it is normal to release a roadmap so that potential users and investors can see where the currency is planned to go. Solana is not like this though; they do not see the current value of it. This in the dark strategy, definitely would make investing in Solana riskier [12].

Solana also seems to have a lack of investment. There are many organizations using and supporting the currency but not many putting money into it. As a result of this they are falling short in providing value to their users [12].

Finally, Solana centralization is still relatively high. The "Solana Foundation is the only entity developing core nodes on the blockchain. This means Solana has a central point of control that reduces the network's overall decentralization" [18]. This higher centralization increases the hacking risk [14].

REFERENCES

[1] A. Yakovenko, "Archivers - Solana's solution to petabytes of blockchain data storage," *Medium*, 18-Jul-2019. [Online]. Available: https://medium.com/solana-labs/replicators-solanas-solution-to-petabytes-of-blockchain-data-storage-ef79db053fa1. [Accessed: 07-Nov-2021].

[2] A. Yakovenko, "Cloudbreak - Solana's horizontally scaled state architecture," *Medium*, 23-Jul-2019. [Online]. Available: https://medium.com/solana-labs/cloudbreak-solanas-horizontally-scaled-state-architecture-9a86679dcbb1. [Accessed: 07-Nov-2021].

[3] A. Yakovenko, "Gulf Stream: Solana's mempool-less transaction forwarding protocol," *Medium*, 20-Jul-2019. [Online]. Available: https://medium.com/solana-labs/gulf-stream-solanas-mempool-less-transaction-forwarding-protocol-d342e72186ad. [Accessed: 07-Nov-2021].

[4] A. Yakovenko, "Pipelining in Solana: The Transaction Processing Unit," *Medium*, 09-Sep-2019. [Online]. Available: https://medium.com/solana-labs/pipelining-in-solana-the-transaction-processing-unit-2bb01dbd2d8f. [Accessed: 07-Nov-2021].

[5] A. Yakovenko, "Sealevel - parallel processing thousands of smart contracts," *Medium*, 09-Sep-2019. [Online]. Available: https://medium.com/solana-labs/sealevel-parallel-processing-thousands-of-smart-contracts-d814b378192. [Accessed: 07-Nov-2021].

[6] A. Yakovenko, “Solana: A new architecture for a high performance blockchain.” [Online]. Available: https://solana.com/solana-whitepaper.pdf. [Accessed: 07-Nov-2021].

[7] A. Yakovenko, “Tower BFT: Solana's high performance implementation of PBFT,” *Medium*, 17-Jul-2019. [Online]. Available: https://medium.com/solana-labs/tower-bft-solanas-high-performance-implementation-of-pbft-464725911e79. [Accessed: 07-Nov-2021].

[8] A. Yakovenko, “Turbine - Solana's block propagation protocol solves the scalability trilemma,” *Medium*, 11-Jul-2019. [Online]. Available: https://medium.com/solana-labs/turbine-solanas-block-propagation-protocol-solves-the-scalability-trilemma-2ddba46a51db. [Accessed: 07-Nov-2021].

[9] G. Schout, “The Top 10 Solana Projects,” *Medium*, 11AD. [Online]. Available: https://medium.com/stakin/the-top-10-solana-projects-ea9f52020219. [Accessed: 07-Nov-2021].

[10] H. Maishera, “What is Solana – one of Ethereum's major rivals,” *Yahoo! Finance*, 27-Oct-2021. [Online]. Available: https://finance.yahoo.com/news/solana-one-ethereum-major-rivals-044511895.html. [Accessed: 07-Nov-2021].

[11] “History: Solana Docs,” *Solana Documentation*. [Online]. Available: https://docs.solana.com/history. [Accessed: 07-Nov-2021].

[12] IamKingCliff, “Not sure about Solana,” *Medium*, 16AD. [Online]. Available: https://medium.com/nerd-for-tech/not-sure-about-solana-24cebf37717e. [Accessed: 07-Nov-2021].

[13] J. Baltrusaitis, “Global interest in Solana on google rockets by over 350% year-to-date,” *Finbold*, 03-Sep-2021. [Online]. Available: https://finbold.com/global-interest-in-solana-on-google-rockets-by-over-350-year-to-date/. [Accessed: 07-Nov-2021].

[14] K. Arora, “Centralized and decentralized cryptocurrency exchanges,” *Analytics Steps*, 06-Aug-2021. [Online]. Available: https://www.analyticssteps.com/blogs/centralized-and-decentralized-cryptocurrency-exchanges. [Accessed: 07-Nov-2021].

[15] “Play to earn Blockchain Games,” *Sequence*, 28-Jul-2021. [Online]. Available: https://www.uxsequence.io/learn/article/blockchain-gaming-and-play-to-earn/. [Accessed: 07-Nov-2021].

[16] S. Schroeder, “Solana: What you need to know about the skyrocketing cryptocurrency,” *Mashable*, 09-Sep-2021. [Online]. Available: https://mashable.com/article/what-is-solana. [Accessed: 07-Nov-2021].

[17] “Star atlas: A complete guide,” *Sequence*, 31-Aug-2021. [Online]. Available: https://www.uxsequence.io/learn/article/star-atlas-a-complete-guide/. [Accessed: 07-Nov-2021].

[18] T. Craig, “How decentralized is Solana?,” *Crypto Briefing*, 16-Oct-2021. [Online]. Available: https://cryptobriefing.com/how-decentralized-is-solana/. [Accessed: 07-Nov-2021].

[19] “Validation stake delegation: Solana docs,” *Solana Docs Blog RSS*. [Online]. Available: https://docs.solana.com/implemented-proposals/ed_overview/ed_validation_client_economics/ed_vce_validation_stake_delegation. [Accessed: 07-Nov-2021].

[20] “What is serum? (SRM): SRM Coin,” *Kraken*. [Online]. Available: https://www.kraken.com/learn/what-is-serum-srm. [Accessed: 07-Nov-2021].

[21] “What is Solana (SOL)?,” *Genesis Block*. [Online]. Available: https://genesisblockhk.com/what-is-solana/#How-Does-Solana-Work. [Accessed: 07-Nov-2021].