Lesson 1

Today's topics

- Practicalities
- Decentralised Systems
- Blockchain theory
- Cryptography
- Solana Architecture
- Consensus

> ### Introduction
>
> > ### Course Plan
> >
> > Week 1 - Introduction to Blockchain, Solana and Rust
> > Week 2 - Rust / Solana development / token program
> > Week 3 - Anchor framework
> > Week 4 - Solana Program Library / Security

Practical Details

All lessons will be conducted online.
The usual format will usually be 45 mins of theory followed by 45 mins practical
You will be able to work in teams

How to ask questions ?

We have channels for questions

- Sli.do : link
- Discord channel

Guidelines:

- Post your questions in these channels instead of asking individuals.
- Include context in your questions to ensure they are clear and understandable.

- Check existing topics before posting on Sli.do and upvote those you're interested in.

How do practicals work ?

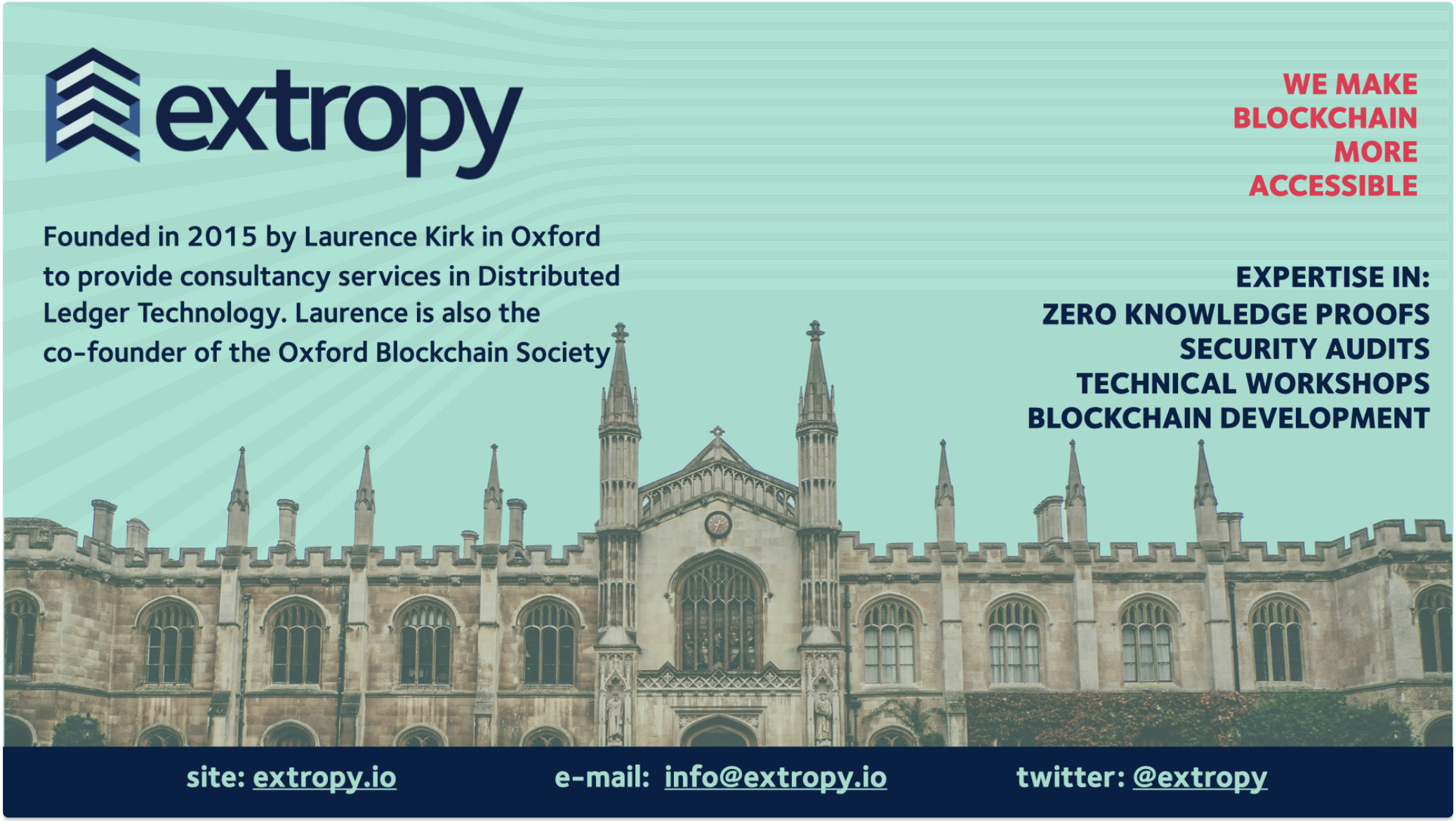
The lessons will typically be split 50/50 into theory and practical

During the practical half of the lesson you can work on exercises and ask questions in the support channel

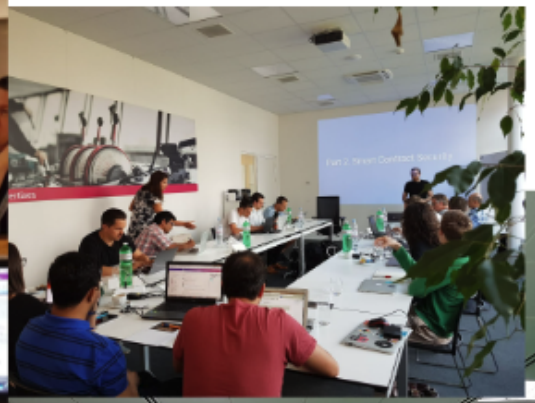
You do not need to submit the homeworks, we suggest you put your answers into a repo.
We will review the exercises once most students have finished them

---

About us


extropy
WE MAKE
BLOCKCHAIN
MORE
ACCESSIBLE
Founded in 2015 by Laurence Kirk in Oxford
to provide consultancy services in Distributed
Ledger Technology. Laurence is also the
co-founder of the Oxford Blockchain Society
EXPERTISE IN:
ZERO KNOWLEDGE PROOFS
SECURITY AUDITS
TECHNICAL WORKSHOPS
BLOCKCHAIN DEVELOPMENT
site: extropy.io
e-mail: info@extropy.io
twitter: @extropy

Running workshops and hackathons since 2017



Decentralised Systems

Problems with centralised systems

Monetary System

- Bank closure / insufficient capital reserves
- greek debt crisis in 2015 ? banks closed and people lost savings, insurance schemes meant nothing, lead to an increase in Bitcoin use in Greece
- Availability of banks
- Inflation - money supply controlled by central authority
- Merchant accounts may be shut down
- Control of money for political reasons - wikileaks funding shutdown

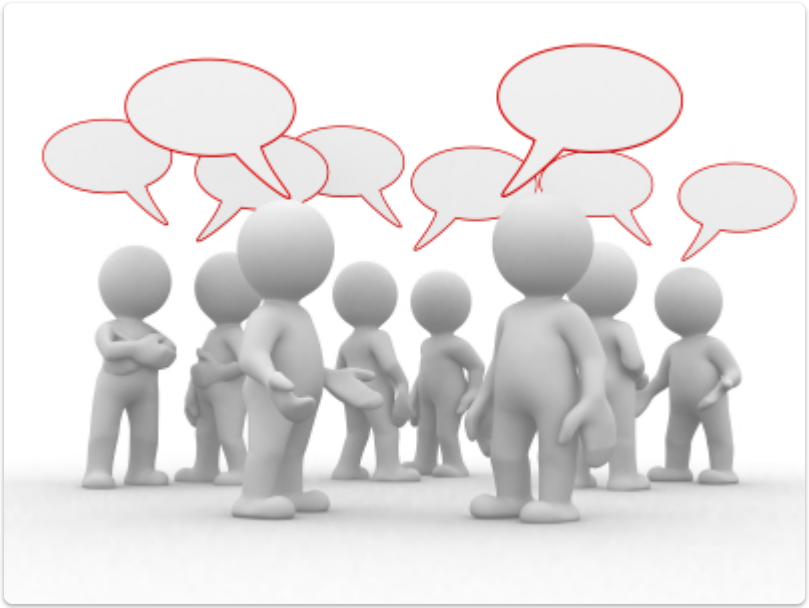
There are layers of access control built into our banking systems to prevent fraudulent transactions, effectively security is achieved by closing the network.

Goals of decentralisation

- Participation
- Diversity
- Conflict resolution
- Flexibility
- Moving power to the edge (user)

Introduction to Blockchain

Gossip network



**

Shared public ledger

Cryptography

These components give the blockchain

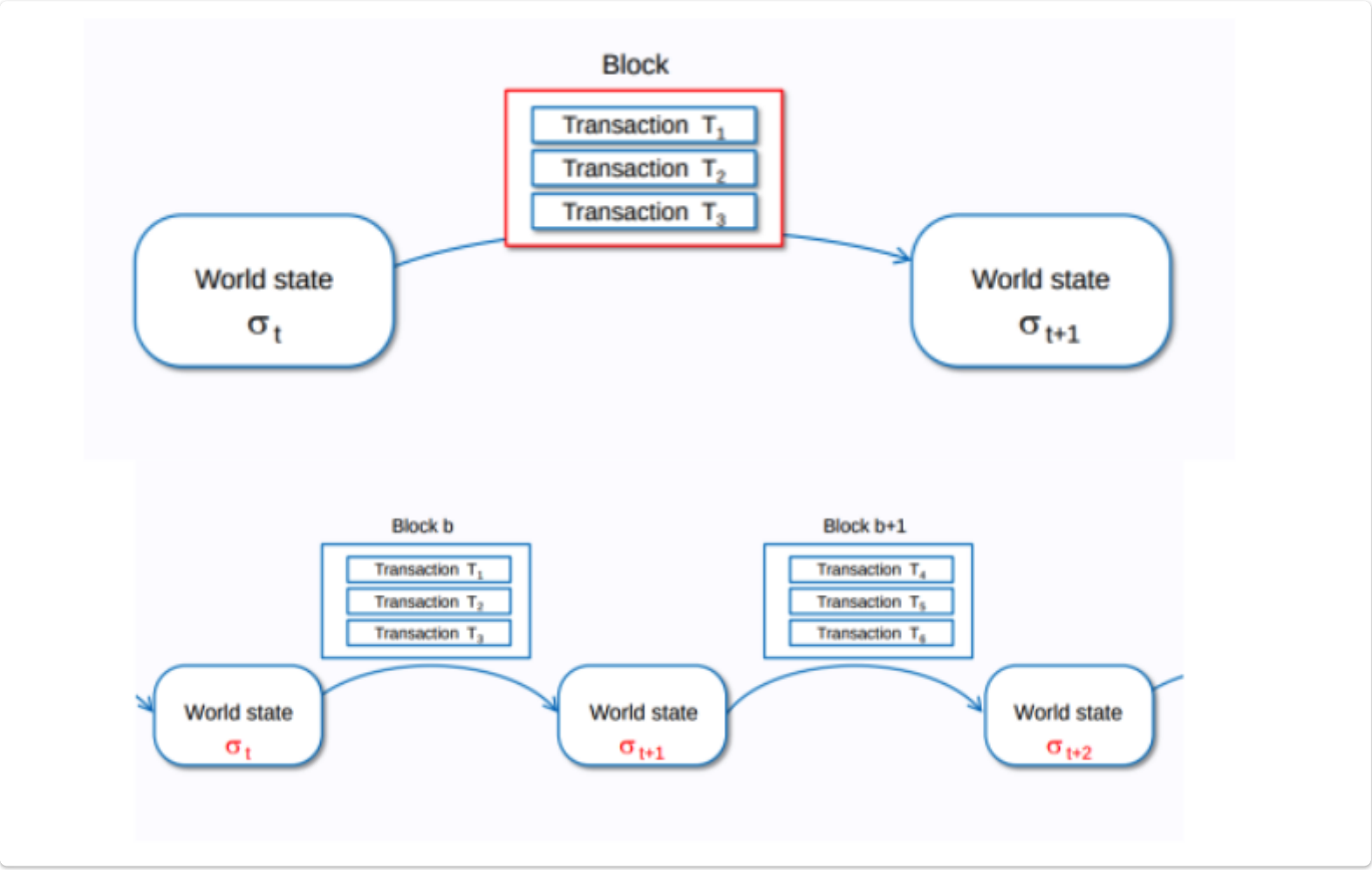
- Transparency and verifiable state based on consensus
- Resilience
- Censorship resistance
- Tamper proof interactions

Blockchain components in more detail

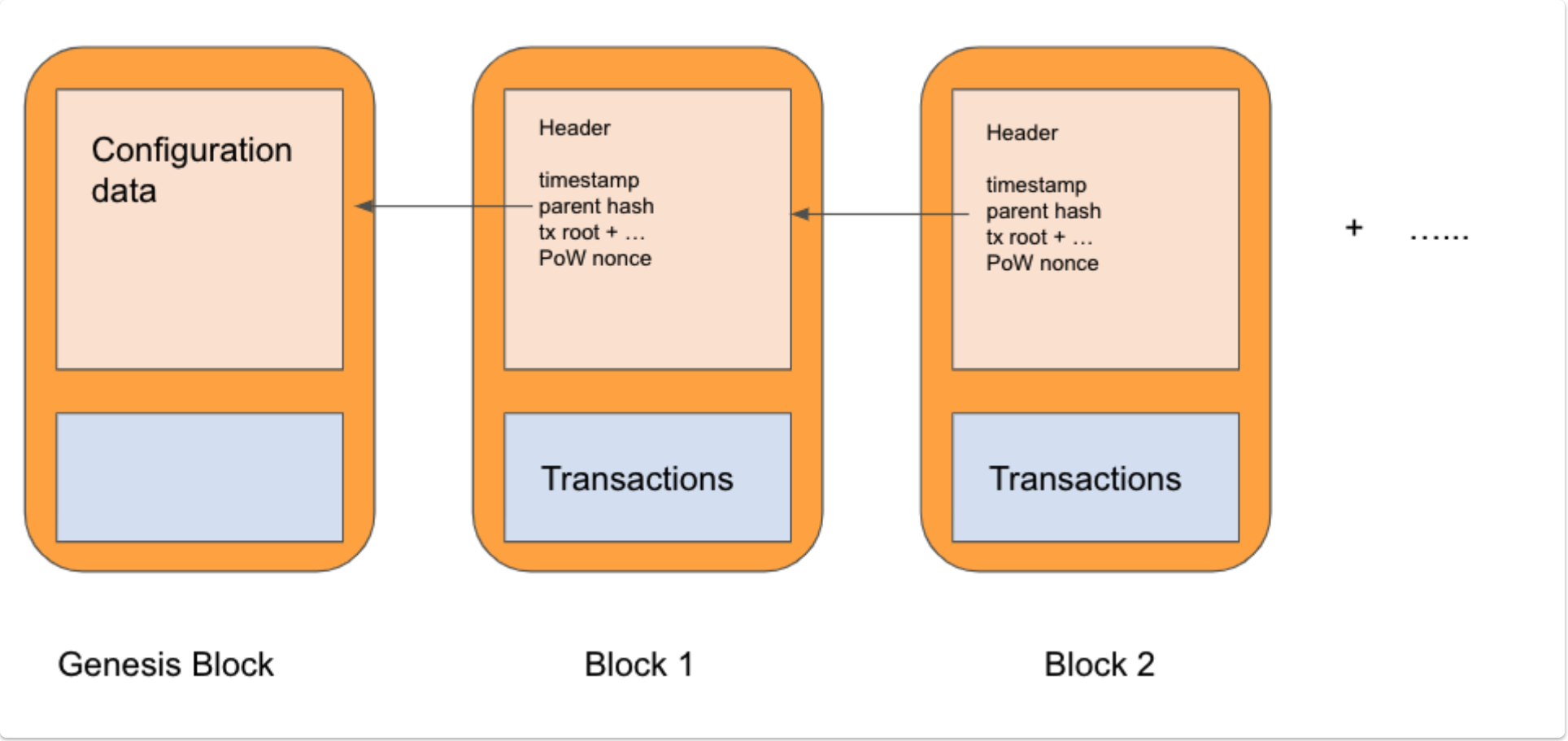
- A peer-to-peer (P2P) network connecting participants and propagating transactions and blocks of verified transactions, based on a standardized "gossip" protocol
- Messages, in the form of transactions, representing state transitions
- A set of consensus rules, governing what constitutes a transaction and what makes for a valid state transition
- A state machine that processes transactions according to the consensus rules
- A chain of cryptographically secured blocks that acts as a journal of all the verified and accepted state transitions
- A consensus algorithm that decentralizes control over the blockchain, by forcing participants to cooperate in the enforcement of the consensus rules

- A game-theoretically sound incentivization scheme to economically secure the state machine in an open environment
- One or more open source software implementations of the above ("clients")

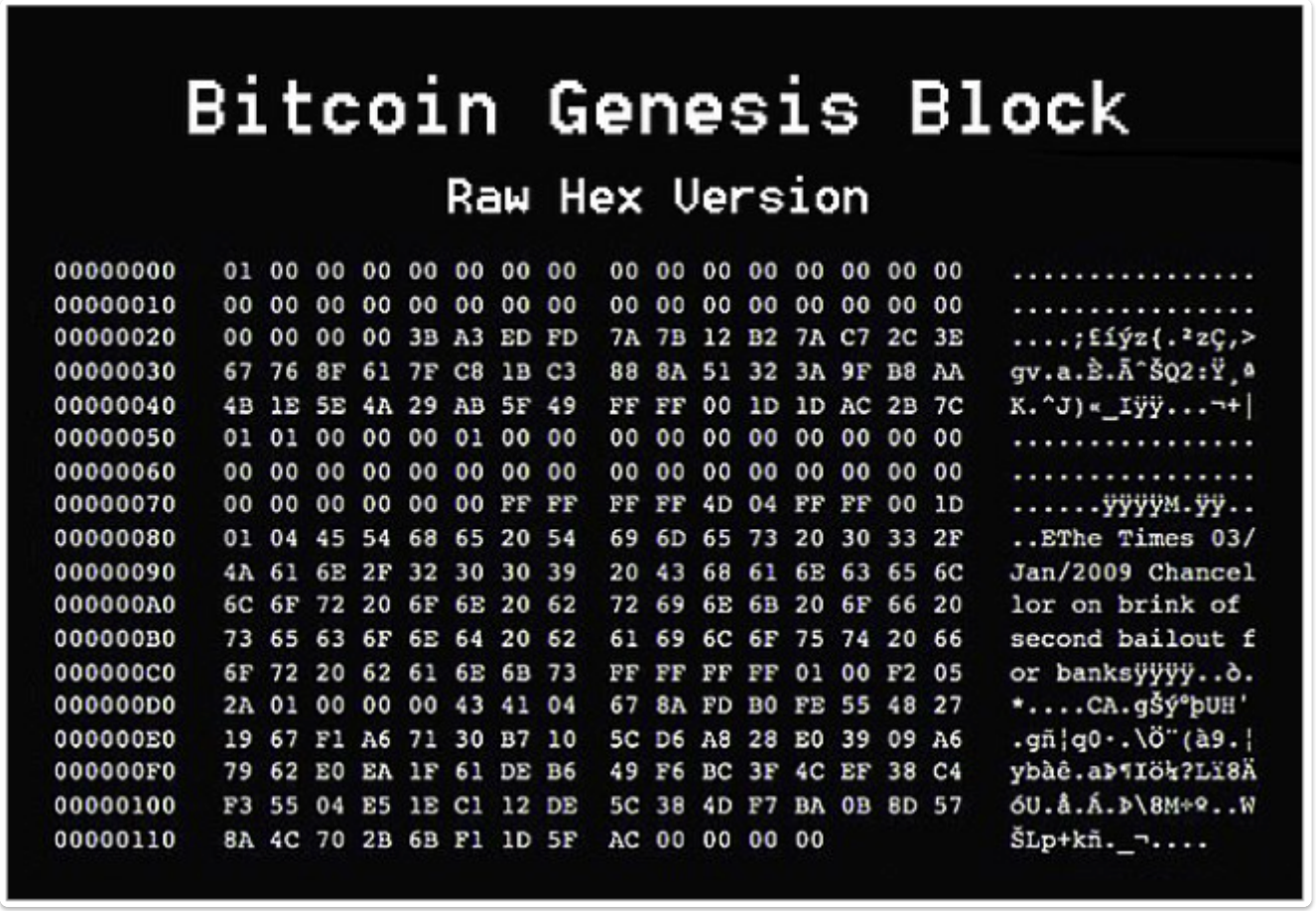
Blockchain as a state machine in Bitcoin



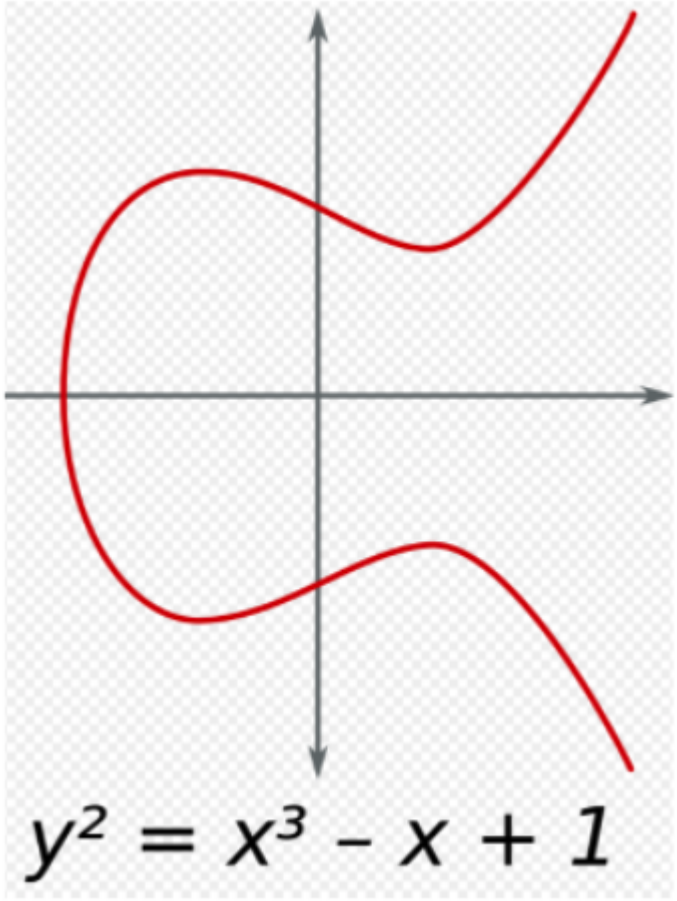
General Blockchain Structure for example Bitcoin



Genesis Block - the starting block


Bitcoin Genesis Block
Raw Hex Version
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;£íýz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_Iÿÿ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D ......ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ò.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠý°þUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ¦q0·.\Ö¨(à9.¦
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybàê.aÞ¶Iö¼?Lï8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.å.Á.Þ\8M÷º..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ._¬....

Key Cryptography - Elliptic curves



Solana uses EdDSA (Edwards-curve Digital Signature Algorithm)

It uses the curve25519 curve.
Elliptic curves have a shorter key length for the same level of security as RSA

Keys and addresses

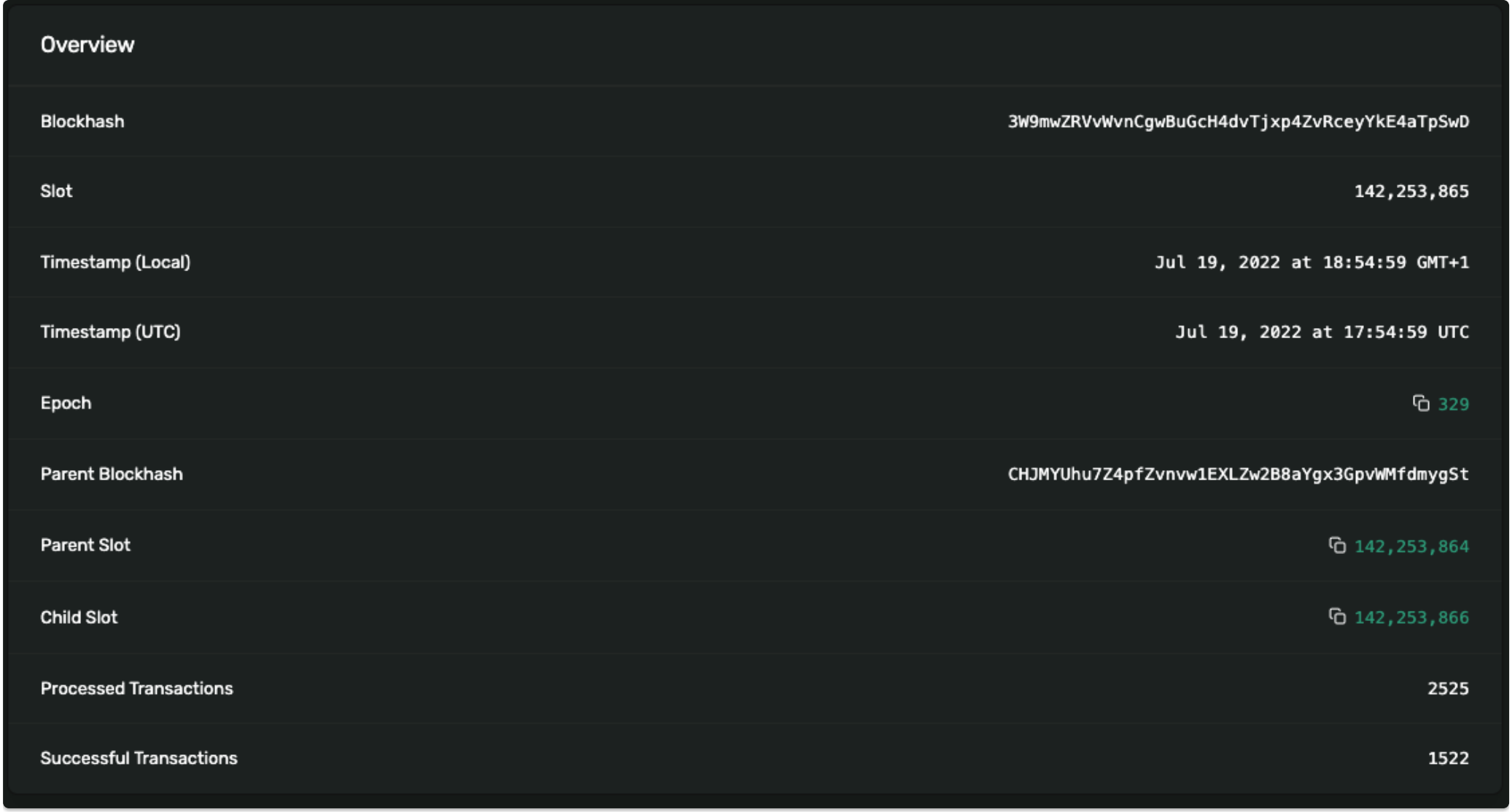
The key may be

- an ed25519 public key
- a program-derived account address (32 byte value from the ed25519 curve)
- a hash of an ed25519 public key with a 32 character string

Solana Architecture

Solana Blocks

In Solana the concept is a little different, but we still gather transactions together with some meta data.

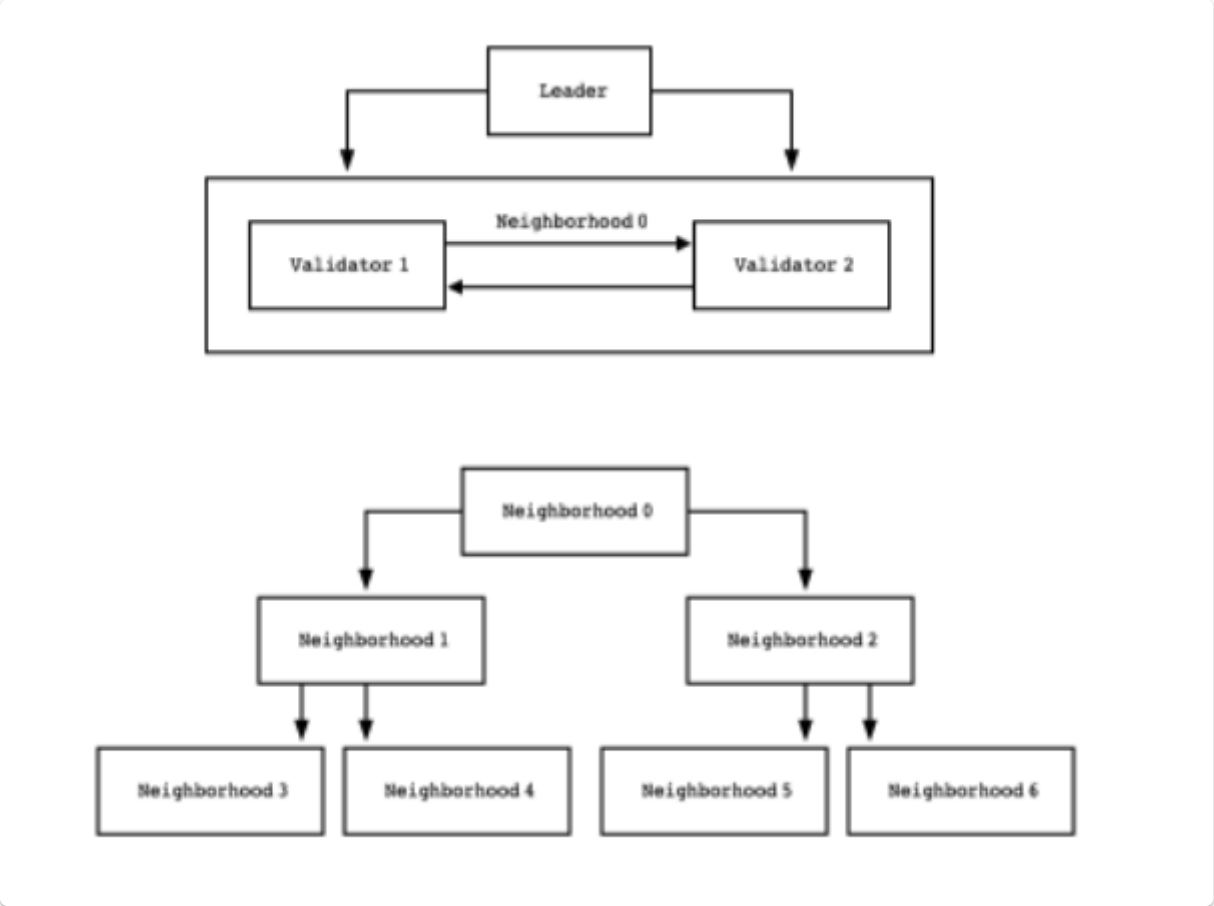


Each block is 10MB, blocks are proposed roughly every 800ms,

Solana Network

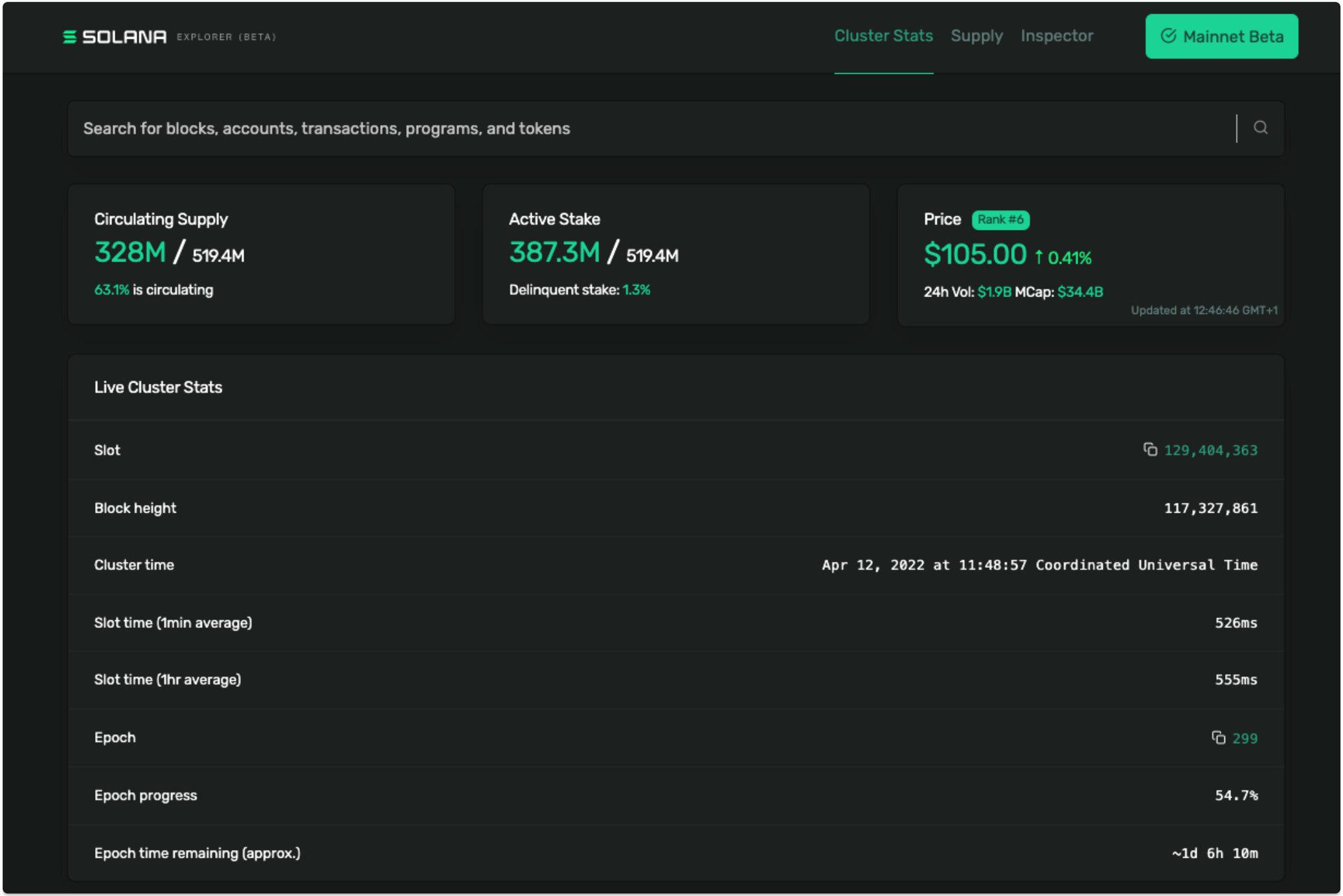
A Solana cluster is a set of validators working together to serve client transactions and maintain the integrity of the ledger. Many clusters

may coexist. When two clusters share a common genesis block, they attempt to converge. Otherwise, they simply ignore the existence of the other. Transactions sent to the wrong one are quietly rejected.

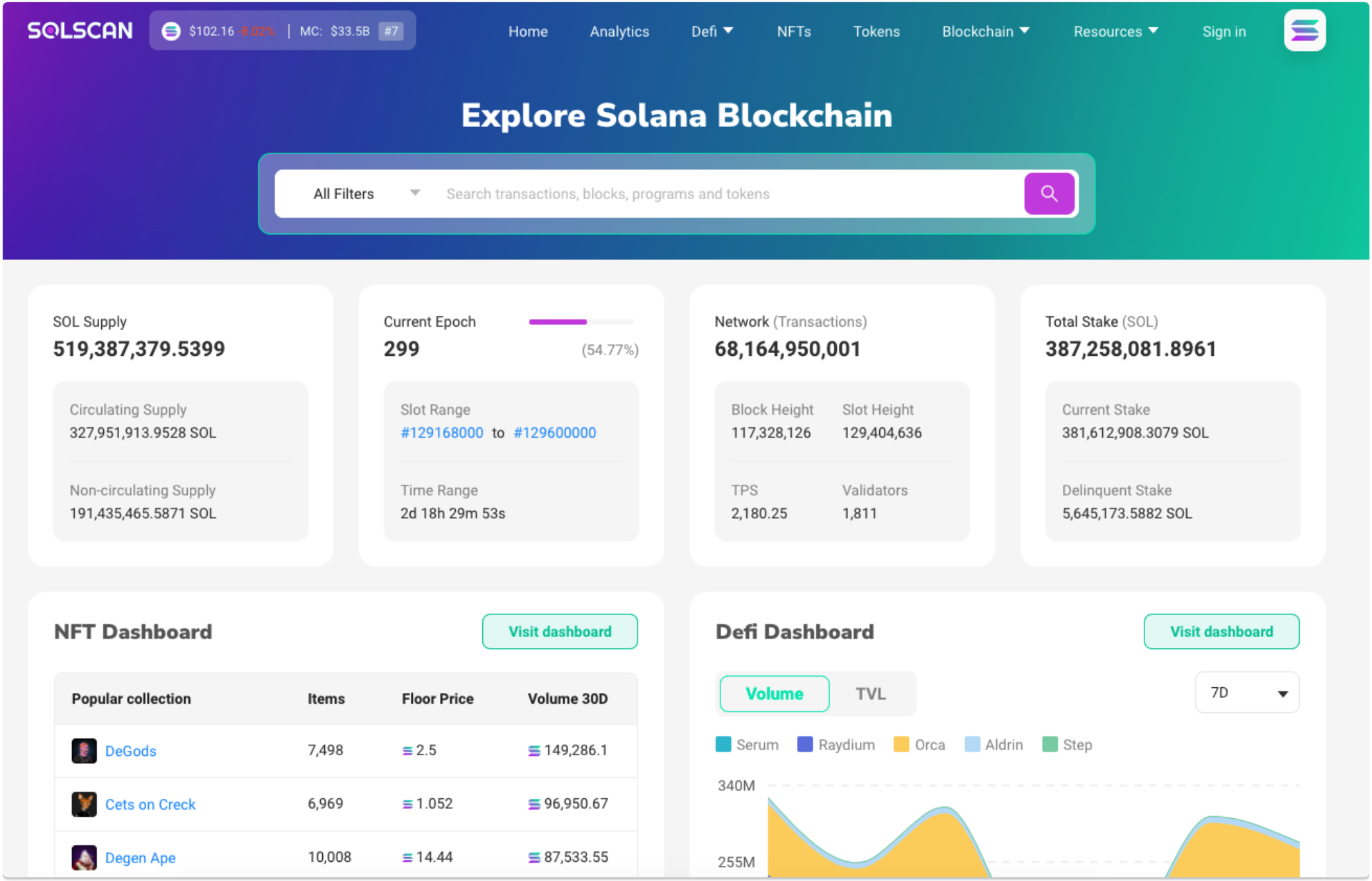


Block Explorers

Solana Explorer



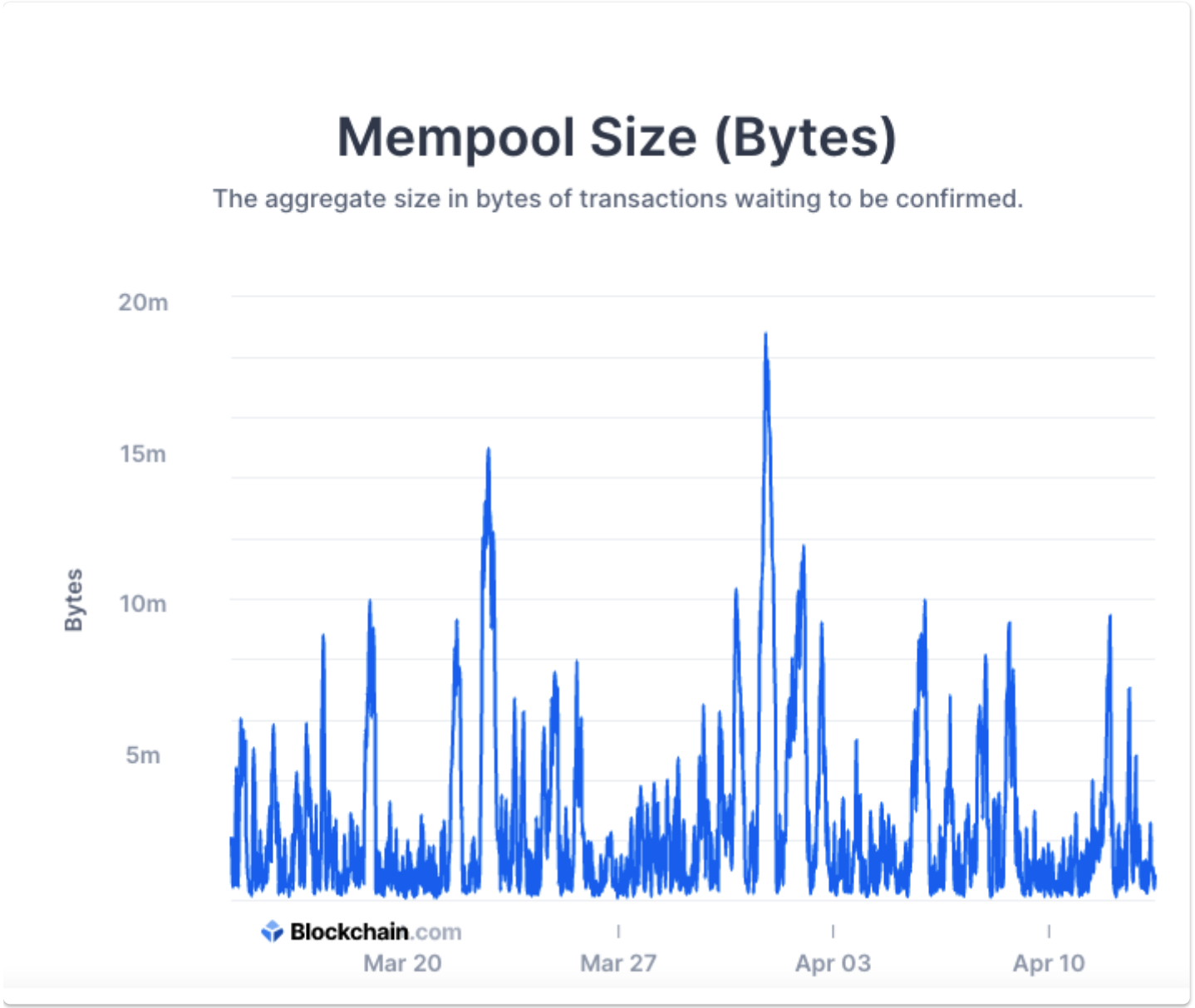
Solscan


SOLSCAN
$102.16 -8.02% | MC: $33.5B #7
Home
Analytics
Defi
NFTs
Tokens
Blockchain
Resources
Sign in
Explore Solana Blockchain
All Filters
Search transactions, blocks, programs and tokens
SOL Supply
519,387,379.5399
Circulating Supply
327,951,913.9528 SOL
Non-circulating Supply
191,435,465.5871 SOL
Current Epoch
299
(54.77%)
Slot Range
#129168000 to #129600000
Time Range
2d 18h 29m 53s
Network (Transactions)
68,164,950,001
Block Height
117,328,126
Slot Height
129,404,636
TPS
2,180.25
Validators
1,811
Total Stake (SOL)
387,258,081.8961
Current Stake
381,612,908.3079 SOL
Delinquent Stake
5,645,173.5882 SOL
NFT Dashboard
Visit dashboard
Popular collection
Items
Floor Price
Volume 30D
DeGods
7,498
2.5
149,286.1
Cets on Creck
6,969
1.052
96,950.67
Degen Ape
10,008
14.44
87,533.55
Defi Dashboard
Visit dashboard
Volume
TVL
7D
Serum
Raydium
Orca
Aldrin
Step
340M
255M

Solana Beach

The mempool (pending transactions) and Gulfstream

Mempool size in Bitcoin



From Gulfstream docs

"Mempools in Ethereum and Bitcoin are propagated between random nodes in peer-to-peer fashion using a gossip protocol. Nodes in the network periodically construct a bloom filter representing a local mempool and request any transactions that do not match that filter (along with a few others such as a minimal fee) from other nodes on the network. Propagation of a single transaction to the rest of the network will take at least log(N) steps, consumes bandwidth, memory and computational resources required to filter it."

Gulfstream

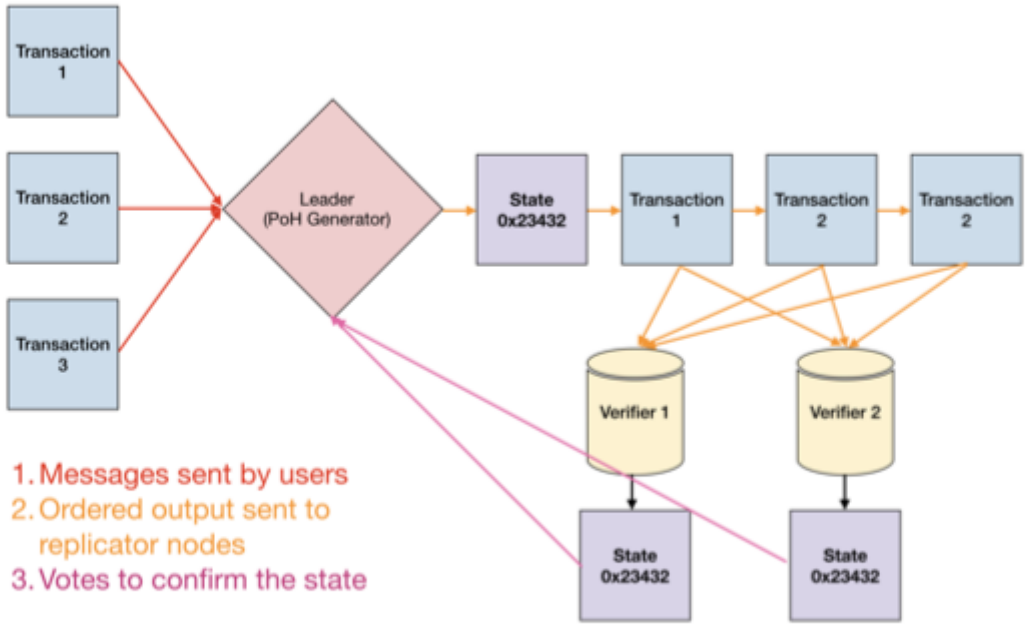


Figure 1: Transaction flow throughout the network.

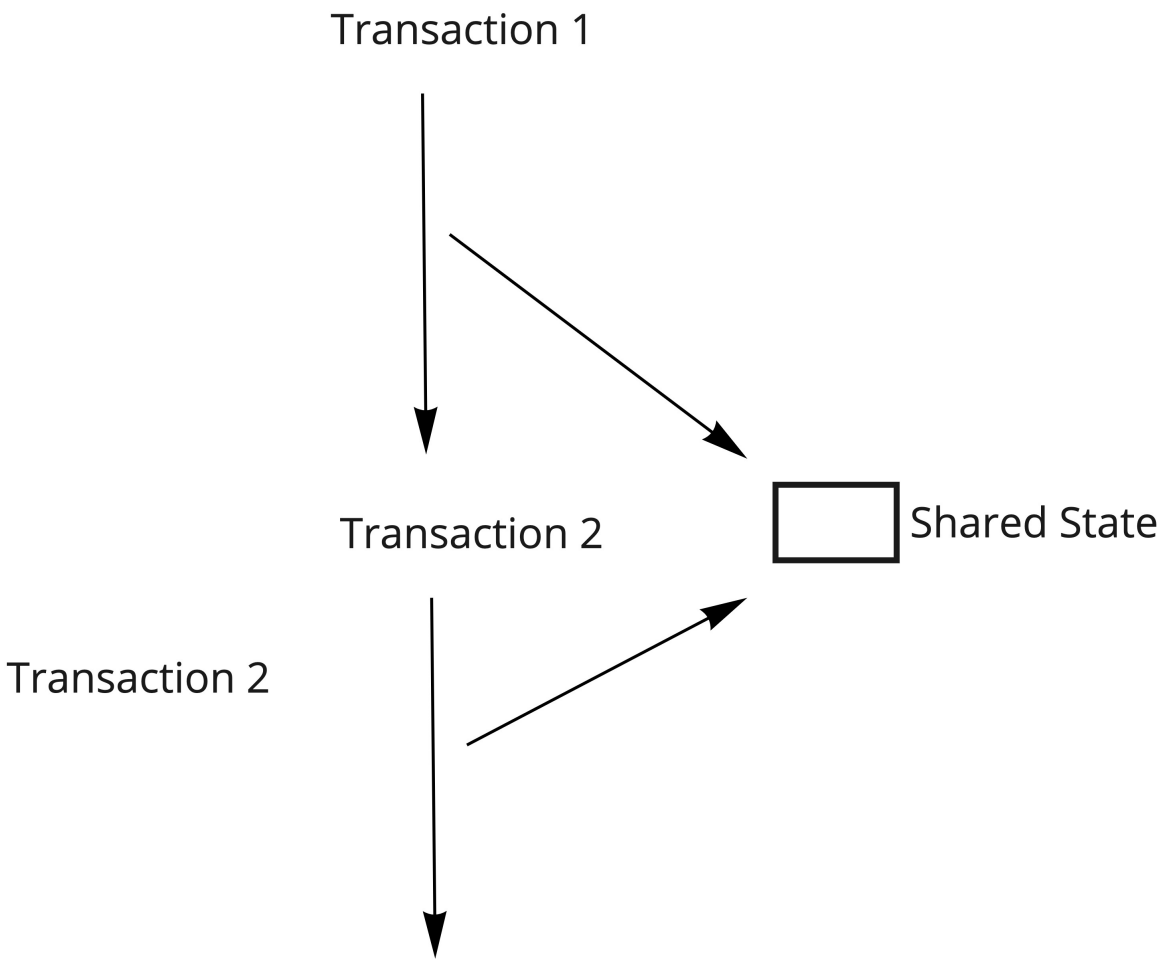
Since every validator knows the order of upcoming leaders, clients and validators forward transactions to the expected leader ahead of time. This allows validators to execute transactions ahead of time, reduce confirmation times, switch leaders faster, and reduce the memory pressure on validators from the unconfirmed transaction pool. This

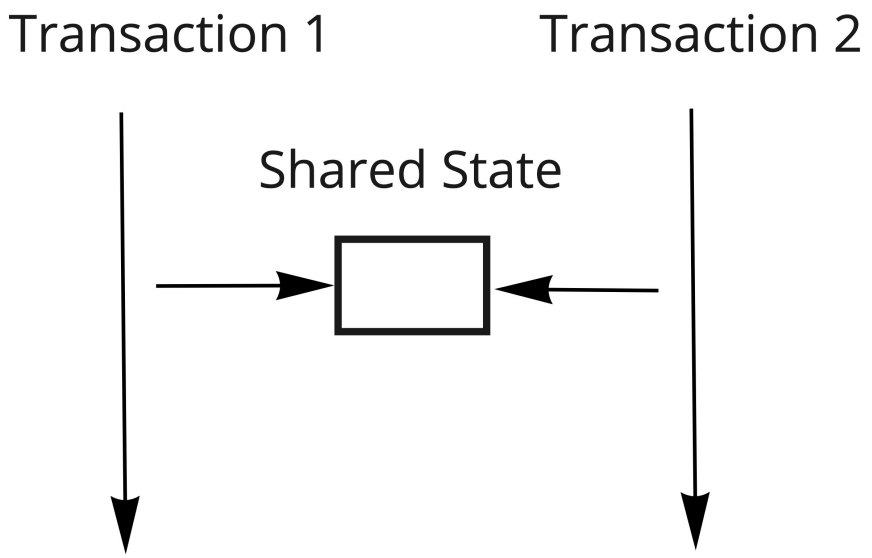
solution is not possible in networks that have a non-deterministic leader

Transactions reference recent blockhash and the transaction is valid only in the children of the referenced block, and is only valid for about 32 blocks.
Assuming block times of 800 ms, that equates to 24 seconds.

Once a transaction is forwarded to any validator, the validator forwards it to one of the upcoming leaders. Clients can subscribe to transaction confirmations from validators. Clients know that a block-hash expires in a finite period of time, or the transaction is confirmed by the network.
This allows clients to sign transactions that are guaranteed to execute or fail. Once the network moves past the rollback point such that the blockhash the transaction reference has expired, clients have a guarantee that the transaction is now invalid and will never be executed on chain.

Concurrency and Throughput





How can we improve performance ?

- lets add more threads / cores / do more in parallel

  or
- lets keep everything single threaded

In Ethereum processing of contracts is single threaded

Solana has introduced a way to process programs in parallel

Transaction	Updates
1	Account A
2	Account B
3	Account A
4	Account C

Consensus in distributed systems

- how can participants agree on the state of the system ?

Byzantine fault tolerance (BFT) is the dependability of a fault-tolerant computer system to such conditions where components may fail and there is imperfect information on whether a component has failed.

Why do we need consensus ?

“The double spending problem is a potential flaw in a cryptocurrency or other digital cash scheme whereby the same single digital token can be spent more than once, and this is possible because a digital token consists of a digital file that can be duplicated or falsified.”

[Paper]

Synchronisation in Distributed Systems

There is a general difficulty with agreeing on time / sequences in distributed systems

In Bitcoin and Ethereum there is no clock available, and participants in the system are given the ability to decide on the sequence of transactions, by mining a block.

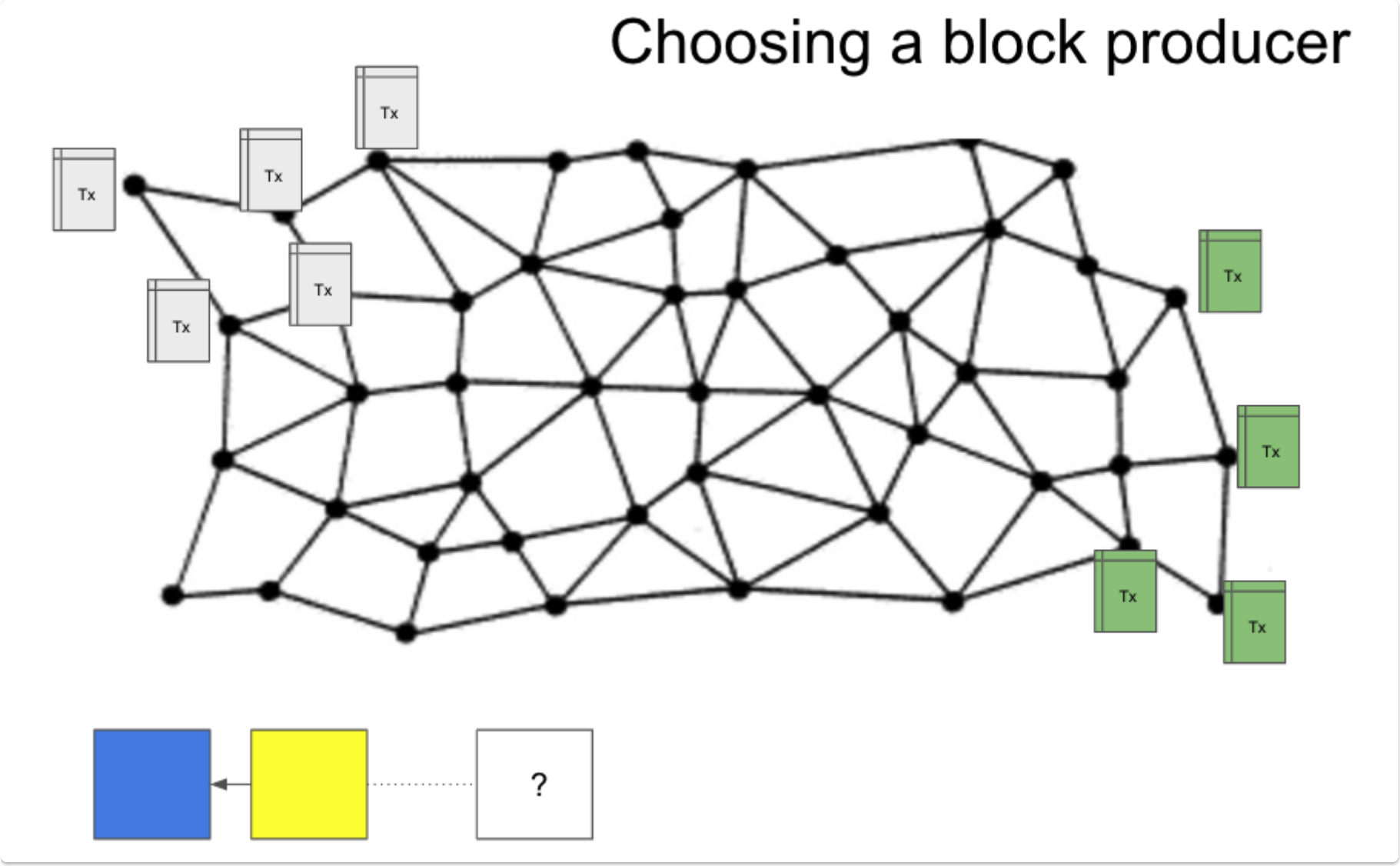
The big innovation from Solana was Proof of History which gives us a verifiable ordering to events

- Proof of Work uses economic incentives to give an ordering of blocks
- Hadera hashgraph uses a median of supplied timestamps

There are 2 Parts to Consensus mechanisms

- Choosing a block producer / leader
- Agreeing on which blocks (transactions) form the canonical chain

For blockchains in general



Typically we allow a block producer to

- choose transactions to be included
- decide on the ordering of transactions

Choosing a leader / block producer

We want this to be 'fair' and difficult to abuse.
PoW uses a race / lottery to solve a puzzle
PoS (DPoS) uses different methods, but often a VRF to assign a time slot to a potential block producer.

One potential problem is liveness

- what if no producer is chosen ?
- what if the chosen block producer fails to produce a block ?

Having a reliable source of time can safely solve timeout issues.

Some Implementations of Sybil / Consensus Mechansisms

- Practical Byzantine Fault Tolerance (pBFT) Castro and Liskov 1999
- Nakamoto Consensus (PoW) 2008

Now there are many “Proof of ....
Stake / Authority / Burn / Elapsed Time / Spacetime ....”
Solana - Proof of History / Tower Consensus (BFT)

Proof of Stake

There are many implementations of PoS - Ethereum , Mina, NXT ...

Common features

- Potential block producers have to submit a stake of the native crypto currency to be eligible
- The current block producer is chosen at random, the probability of being chosen will depend on the amount of stake offered.

- If the block producer behaves maliciously they lose some or all of their stake

Ethereum PoS

Ethereum now uses PoS as a means of choosing a block proposer.

- Slots are assigned to producers who have deposited a stake

The consensus mechanism has two parts

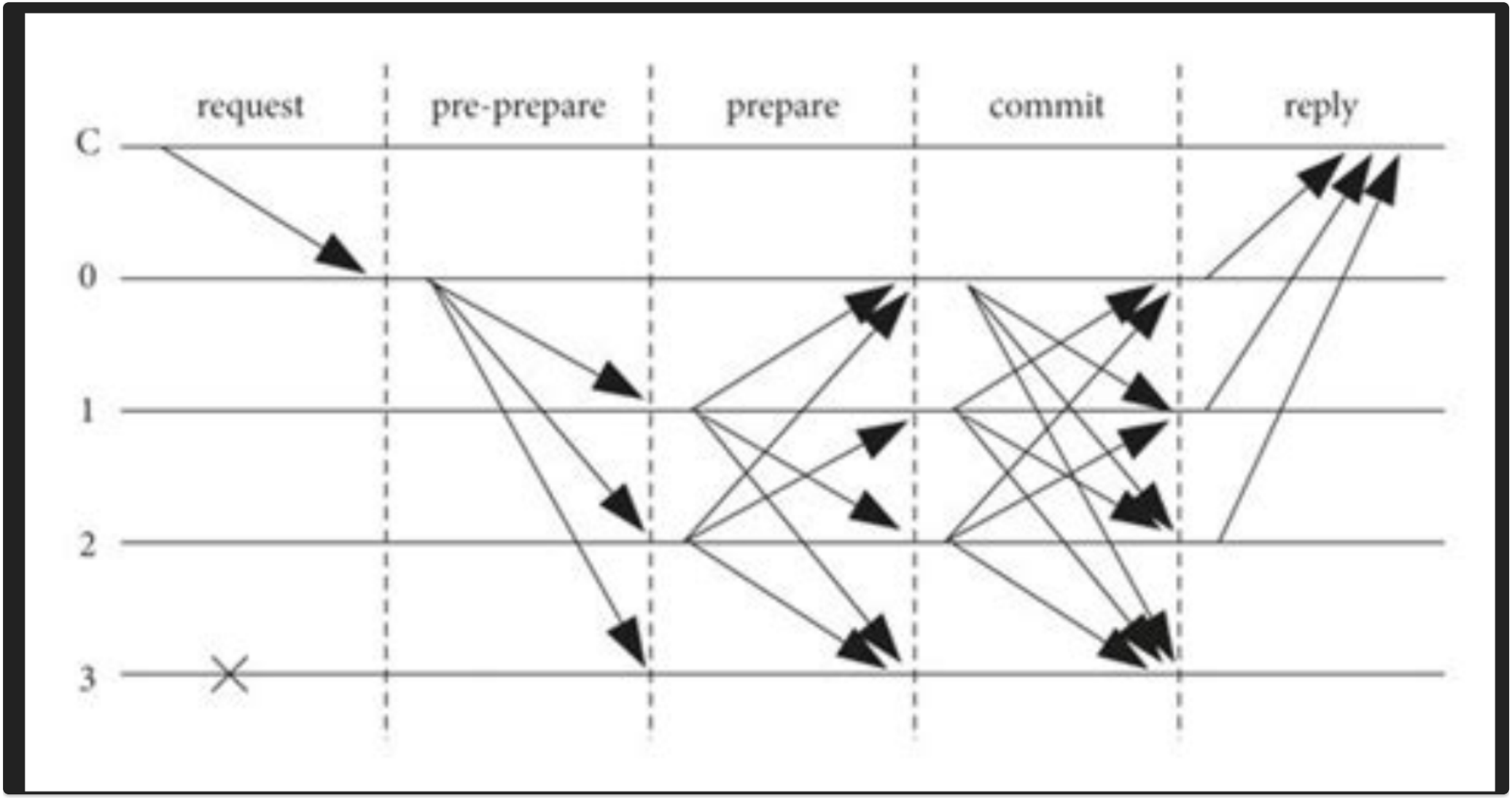
- LMD-GHOST – which adds new blocks and decides what the head of the chain is
- Casper FFG which makes the final decision on which blocks are and are not a part of the chain.

Sui

Narwhal and Bullshark, Sui's Mempool and Consensus Engines
There is a splitting of concerns that you don't get with other mechanisms

- ensuring the availability of data submitted to consensus = Narwhal
- agreeing on a specific ordering of this data = Bullshark

pBFT - Practical Byzantine Fault Tolerance



pBFT requires 3f+1 nodes in the system, where f is the maximum number of faulty nodes that the system can tolerate.

> Therefore, for the group of nodes to make any decision, approval from 2f+1 nodes is required.
