Blockchains, blockweaves, and the decentralised revolution

•••

Sam Williams, Archain CEO

My background

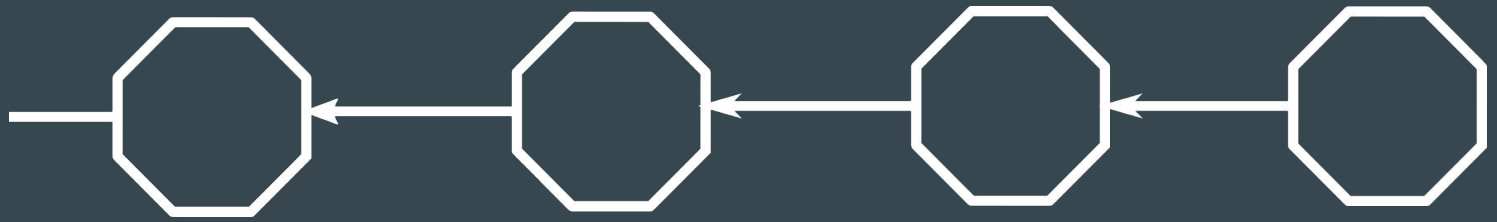
- CEO of the Archain project
  - A decentralised, permanent archive for the internet
  - https://www.archain.org
- Erlang/distribution specialisation
- PhD candidate
  - Developed HydrOS, a distributed operating system, written in Erlang
  - http://hydros-project.org

Presentation summary

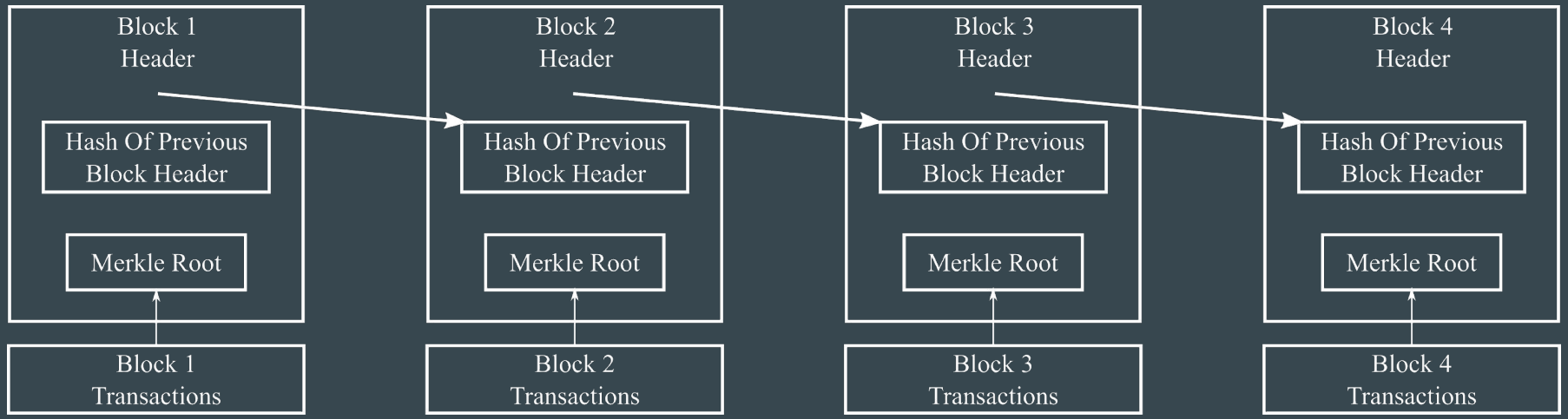
- Blockchains & blockweaves
  - Their similarities & differences
- The Archain project - an open, immutable, decentralised archive
  - Potential effects of the Archain
  - Building Archain
    - Erlang's role
    - Testing the Archain network
- A new model for decentralised application design
  - Archain app competition

Blockchain Basics: What are blockchains?

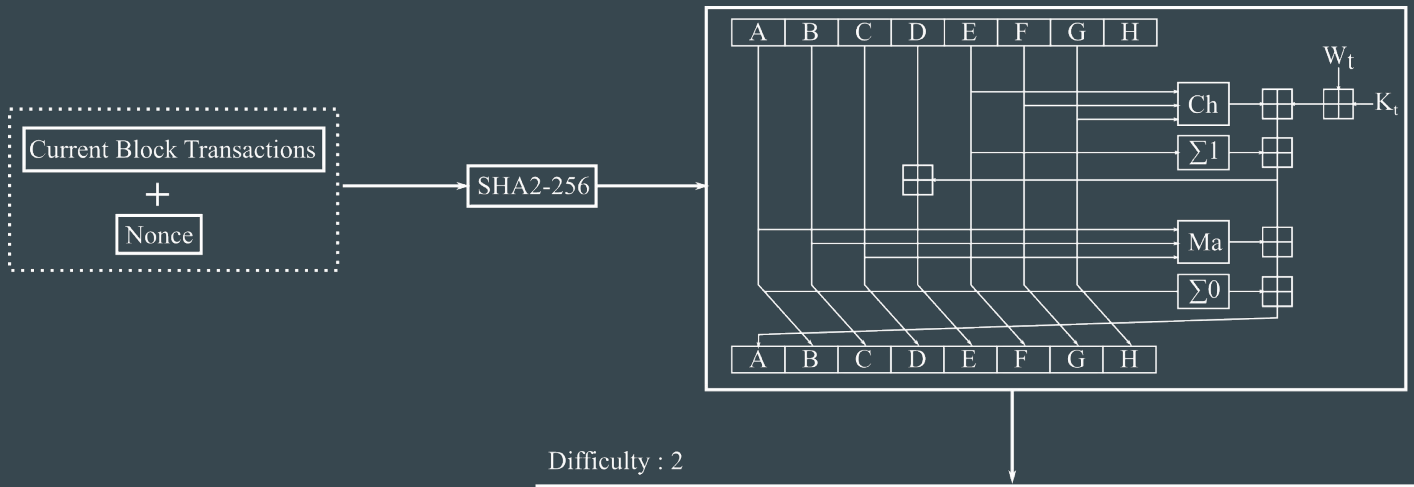
- Hosted on a peer to peer network.
- A decentralised system for negotiating and storing transactions
- Records (‘blocks’) are comprised of transactions
- Blocks are linked and secured by cryptography
- Blocks are added by participating in a ‘Proof of Work’ system
    - ‘Miners’ generate random chunks of data and hash them with an ‘open’ block, looking for a result with a certain number of preceding zeros



Blockchain Basics: What are blockchains?



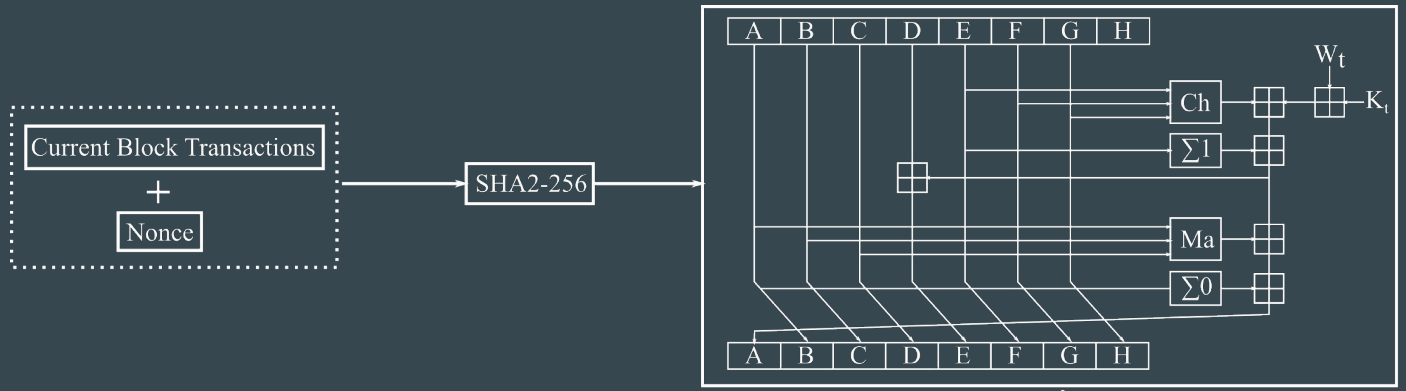
Blockchain Basics: Proof of Work (easy)



Difficulty : 2

D9E8AC5114B738AB359D8EBBF95AC6EEA05070E2DF9B9113606F6CCE118C775D
C03B4127EB7EF10C9D725408352C5215292BA7159A63B41A6A712EEB6AF5F858
AD00A93FF34A39E70260A0D41951AA3DCB1E4147480844A5D8796C70834D5CFC
945E4893567554E68F6F28D5652917269341A5F3D295A16B7C708C9BFD95DC5D ✓

Blockchain Basics: Proof of Work (hard)



Difficulty : 4

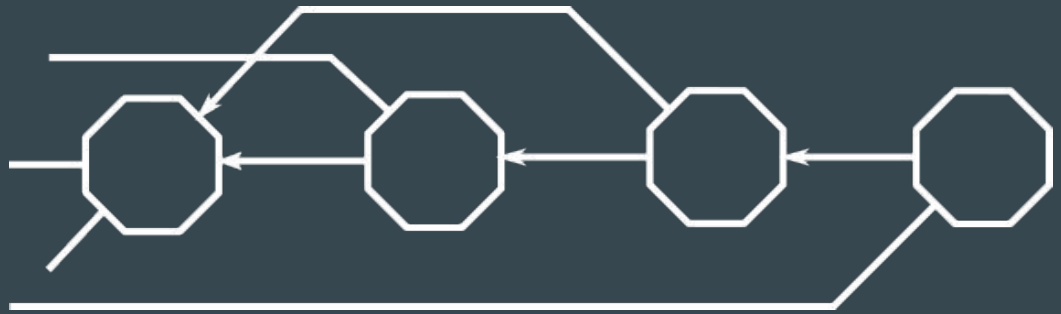
D9E8AC5114B738AB359D8EBBF95AC6EEA05070E2DF9B9113606F6CCE118C775D
C03B4127EB7EF10C9D725408352C5215292BA7159A63B41A6A712EEB6AF5F858
AD00A93FF34A39E70260A0D41951AA3DCB1E4147480844A5D8796C70834D5CFC
945E4893567554E68F6F28D5652917269341A5F3D295A16B7C708C9BFD95DC5D
53C234E5E8472B6AC51C1AE1CAB3FE06FAD053BEB8EBFD8977B010655BFDD3C3
F14B4987904BCB5814E4459A057ED4D20F58A633152288A761214DCD28780B56
8F8EEA956D0EA50D6442FDAB213326F75BB6F584268B0795AD452FAA85DB5F9D
962363262646163663330323163663233353538316439623865666633386362616330366 2 ✓

Blockchain Basics: Why are blockchains important?

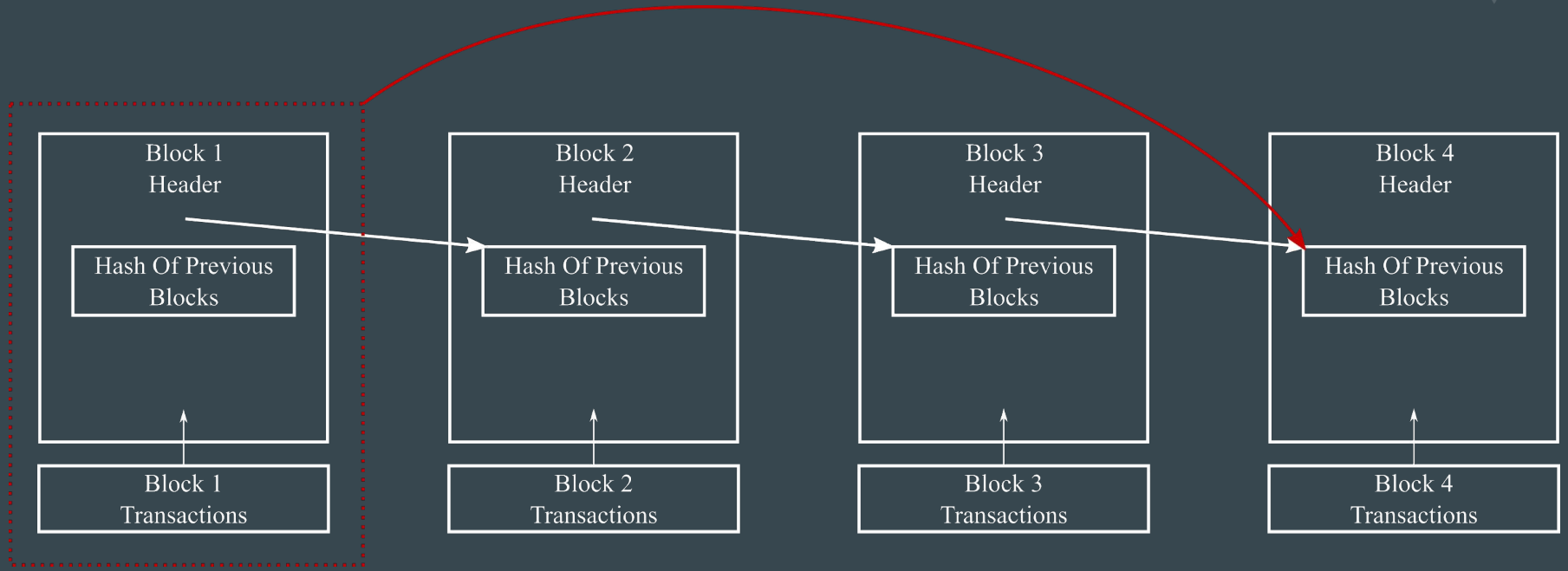
- Transactions can be made without any kind of centralised authority
- Transactions are cryptographically verifiable at all times
  - Monetary system secured by cryptography, not trust
- Examples of use:
  - Bitcoin - for value transfer
  - Ethereum - for smart contracts

Blockweave Basics: What are blockweaves?

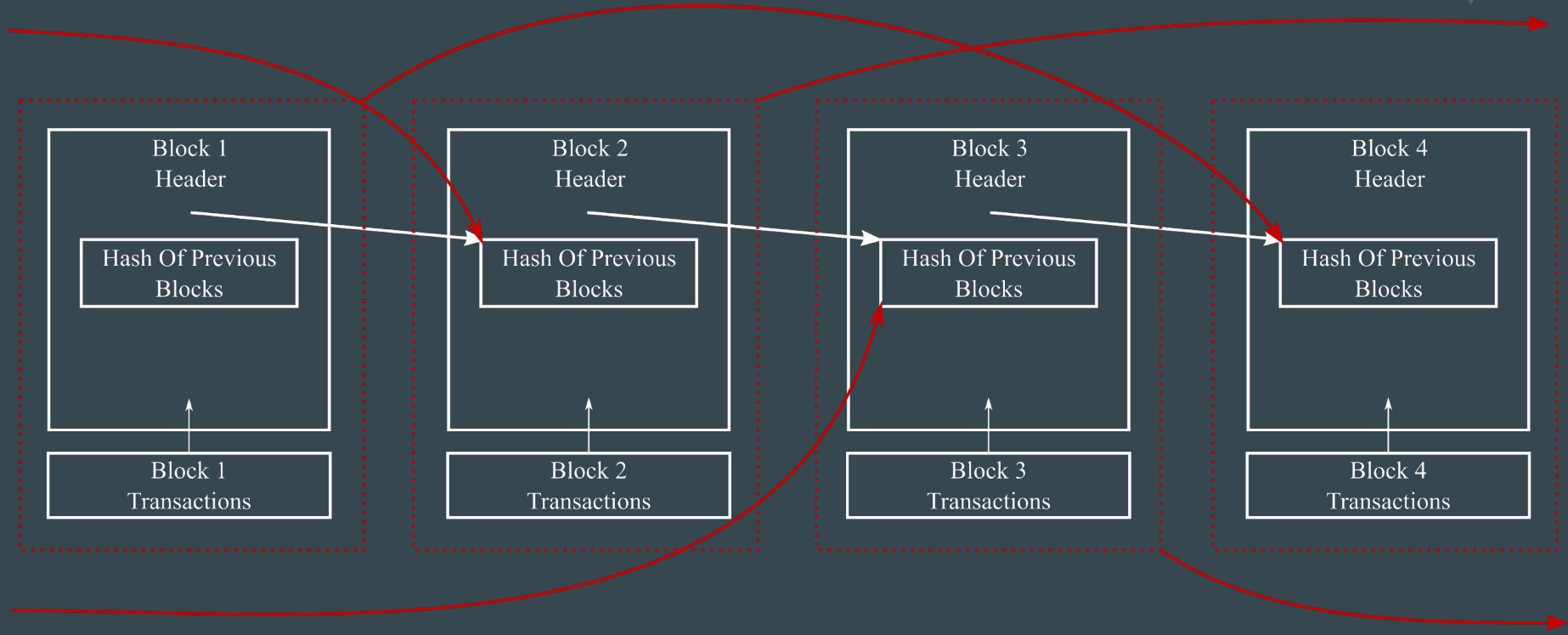
- Sharding
  - A blockweave is a blockchain that shards
- Proof of Access
  - Built on top of typical Proof of Work algorithms
  - Replaces most ‘useless’ work with **useful** storage
  - Maintains PoW security guarantees
- Distributed storage
  - Evenly-distributed & self-organising storage by miners



Blockweave Basics: What are blockweaves?



Blockweave Basics: What are blockweaves?



Blockweave Basics: Why are blockweaves better?

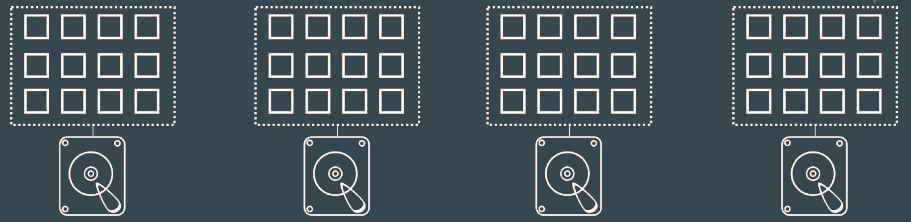
- Sharding
  - Store data directly on the blockweave
  - Allows for huge scaling potential
- Convenience for miners
  - Miners can instantly join the network and mine almost immediately
  - Download just a few blocks to start, instead of >200GB
- Consensus
  - Datastructure can be split among many machines on the network
  - Allowing for consensus and storage to be achieved for much larger pieces of information

Blockweave Basics: Why are blockweaves better?

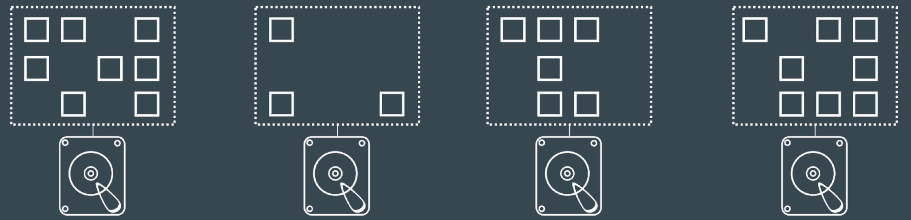
- Recall blocks
  - Blockweaves include a recall block (as well as the previous block) with every newly-mined block
  - Recall blocks are pseudo-randomly generated at the time of mining the previous block
  - This incentivises miners to store existing parts of the weave, allowing them to earn rewards by mining new blocks
- Storage distribution
  - Miners incentivised to prioritise blocks stored by few others
  - Doing so lowers their hashing power requirements
  - At a network level, this naturally creates an evenly-spread and self-organising storage of blocks

Blockweave Basics: Why are blockweaves better?

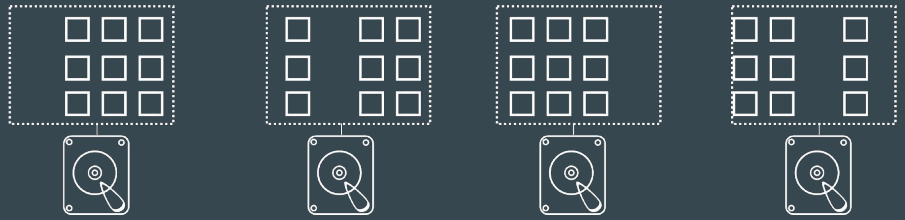
Blockchain



Blockweave
(before self-organisation)



Blockweave
(after self-organisation)



About the Archain project

- A decentralised, permanent archive for the internet
- Built on a shardable blockweave cryptocurrency
- Able to scale to huge sizes
- Cryptographic verification at the points of archiving, storage, and retrieval

Internet archive on the Archain

- Hand-curated record of human history
  - Cryptographically secured on a geographically distributed hard-drive
- Protects the information record
  - Against being lost, damaged, or altered (accidentally or intentionally)
  - Beyond both censorship and natural disaster
    - E.g. Fire at the Internet Archive storage facility
- More than *just* an archive - users will be able to ‘step through’ versions of the webpages as they existed at different points in time
- Archived pages maintain existing addresses
  - Allowing hyperlinks to be maintained
- Solves the problem of the ‘Orwellian memory hole’

Building the Archain project

- Blockweave datastructure
  - Sharding allows for true scaling of the distributed network
- Verification of content
  - Algorithm ensuring clients & miners reach a consensus on webpage content before archiving
- Erlang
  - Automatic distribution of processes
    - Rapid development of prototype network
    - Running large-scale test networks in realistic conditions inside one machine
  - Networking model
    - Message passing and networking treated identically

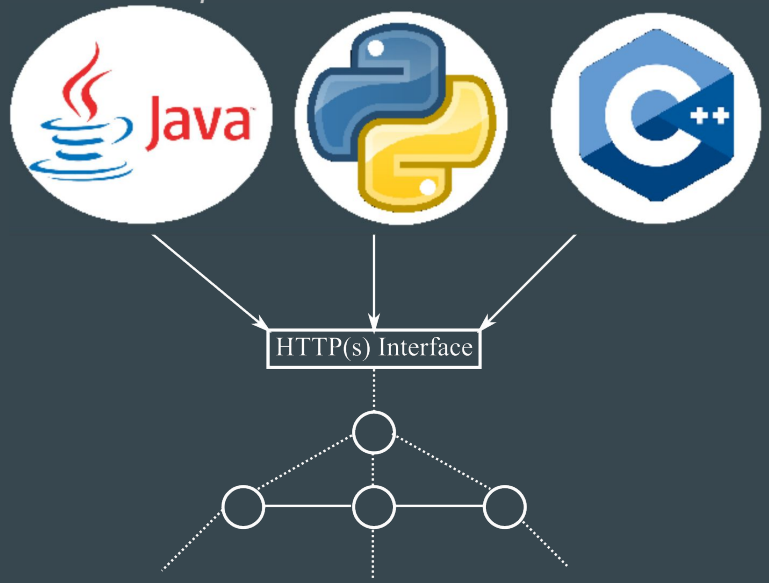
Building the Archain project: Testing the network

- Never-Off Very Large Network Simulator (NO-VLNS)
  - Framework for running massive (1000+ nodes) simulated networks
  - Realistic conditions, latency, packet loss, and network failure
  - Full client simulation

- Tiny Network Tests (TNT)
  - Extreme bug isolation
  - No automatic mining
  - We can create and test highly unusual situations with strong consistency

Apps on the Archain

- Creating a new model for decentralised, permanence-based applications
- Distributed storage
  - Archain apps utilise the blockweave for distributed *storage*
  - Traditional blockchain apps use blockchains for distributed *computation*
- Develop apps in any programming language
  - Via a simple RESTful HTTP or Erlang interface
- Monitor network messages
- Some possible applications:
  - Automated trading
  - Brand management
  - Decentralised social media



The Archain App Development Competition

- Launched on 3rd of November 2017, closes on 3rd August 2018
- Purposes of the competition:
  - Kick-start the Archain app development community
  - Encourage innovative uses of the Archain network & unique blockweave technology
  - Promote the Archain app development ecosystem, by providing developers with small and large volumes of AR to fuel their apps
- Prizes & rewards
  - First prize of 125k AR, two runner up prizes of 62.5k for the best applications submitted
  - Developers are also competing for $10,000 in investment from the Archain project
  - Plus, all entrants will receive 100 AR for participating!
- Details of requirements & rules can be found on the Archain Medium blog

Questions?

“He who controls the past controls the future, who controls the present controls the past”

- Orwell, 1984.