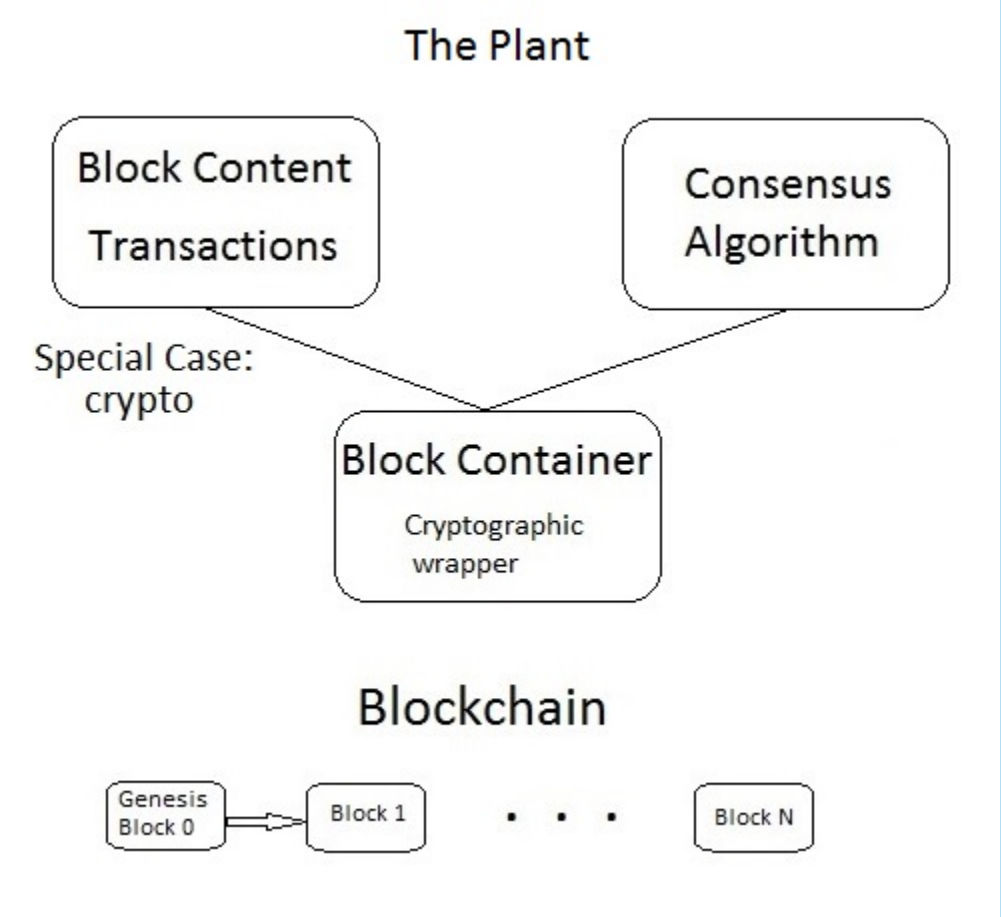
Blockchain Consensus Models

Stephen Swift
© openstreetVR Systems, Inc.
81st ISO JPEG Workshop
October 16th, 2018
Vancouver, BC

Blockchain Structure

- Block content
- Block container
- Consensus model



Consensus Models

- Proof of Work - POW
- Proof of Stake - POS
- Proof of Activity (Hybrid POW/POS)
- Proof of Authority (Byzantine Fault Tolerant variant)
- Proof of Burn
- Proof of Validation
- Proof of Existence
- Proof of Importance
- Ripple Consensus Protocol
- Stellar Consensus Protocol (SCP)
- Others

How to compare different consensus models
The Kramer List of ideal consensus

- Near infinite scalability - >1,000,000 tps
- Near infinite decentralisation - > 10,000 miners
- Low energy use - > 10,000 times less than Bitcoin mining
- Near instant transaction latency - < 3 seconds
- Permissionless and trustless
- Zero Fees (or almost zero)

Generations of consensus models

- Proof of Work (POW) – 1st Generation - Bitcoin
- Proof of Stack (POS) – 2nd Generation - Peercoin
- Hybrids – 3rd Generation - NEO (PoW with PoS)
- New Models – 4th Generation
  - Red Belly - (PBFT)
  - Holochain - (Edge blockchain)
  - Hashgraph - (Something completely new)
  - PoM - (RBFT)

Comparison of 1st, 2nd and 3rd generation blockchains

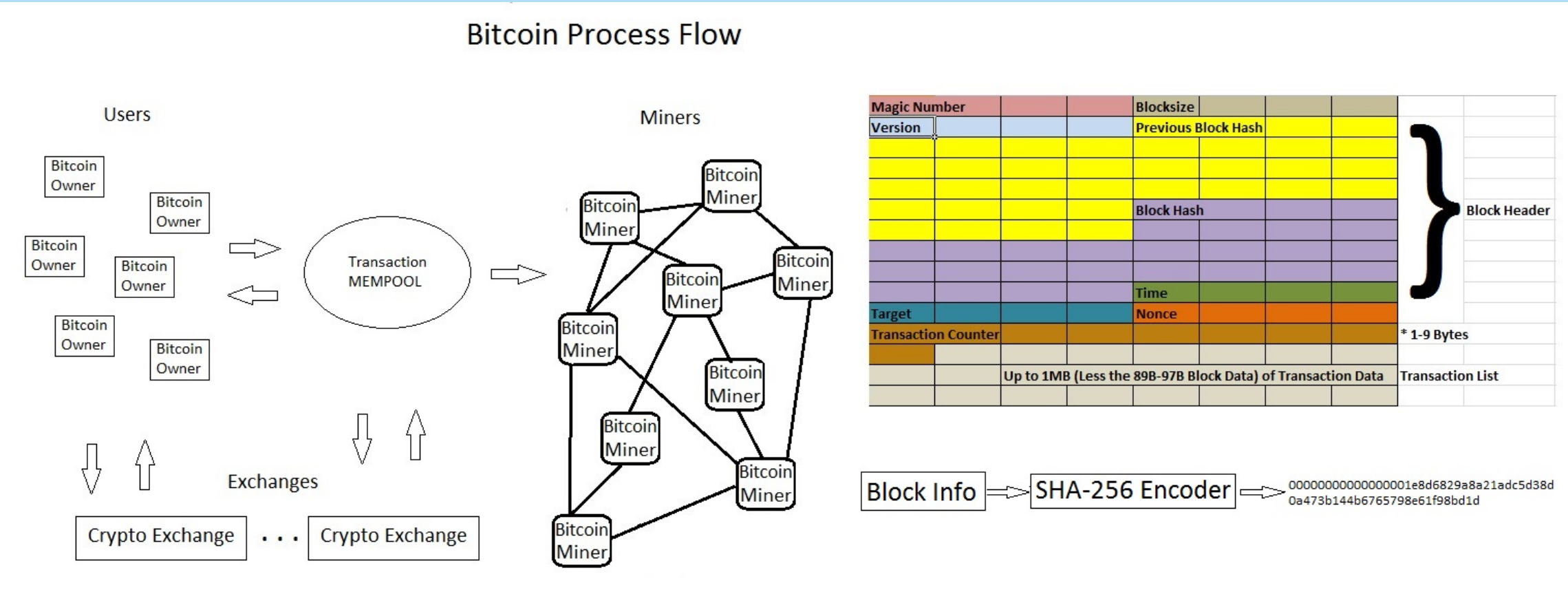
- Bitcoin
- Ethereum
- EOS
- NEO
- IOTA

There are over 2600 cryptocurrencies with the vast majority being ERC-20 Smart Contracts on Ethereum

Bitcoin Consensus Model

- Proof of Work
- Created in 2009 - first financial transaction occurring on May 22, 2010
- 12.5 new Bitcoin created every 10 minutes – current market cap $114 billion
- Highly decentralized with over 7,000 bitcoin miners around the world – concentration in China
- Solves a SHA-256 cryptographic puzzle for block generation (ASIC heavy) through brute force hash calculation
- Bitcoin mining consumes 22 terawatts – almost the same as Ireland
- 3-7 TPS – Layer 2 Lightning Network allows off chain transactions
- Permissionless, trustless and decentralized
- Several hard forks - Bitcoin Cash, Bitcoin Gold, Litecoin, etc.
- 17 million bitcoins have been mined – 4 million to go – last one in 2140
- Transactions on bitcoin blockchain are buy/sell requests

Bitcoin Consensus and Transaction Flow



Ethereum

- Proof of Work (migrating to Proof of Stack over the next few years)
- Proposed in 2013 – went live July 30, 2015
- 3 new Ether created every 15 seconds – current market cap $21 billion
- Eco-power friendly
- Highly decentralized with over 25,000 nodes
- Solves an Ethash cryptographic puzzle which is memory intensive (no ASIC)
- Allows developers to build and deploy decentralized applications
- 15 TPS – Sharding and Plasma could allow 1,000,000 TPS
- Permissionless, trustless and decentralized
- No coin hard cap
- Transactions on Ethereum blockchain are smart contracts

EOS

- Platform for decentralized applications (Dapps)
- Created mid 2017 and officially went live January 31, 2018
- Consensus over events rather than consensus over state
- Block production every 3 seconds
- Platform does not charge micropayments – left to Dapps
- Theoretically could scale to 1,000,000 TPS
- Largest ICO to date $4.7 billion – current market cap $4.9 billion

For more information:

https://eos.io/

NEO

- Referred to as China's Ethereum
- Launched in 2014
- Block generated every 15-20 seconds – 2 million blocks/year - $1 billion market cap
- NEO holders paid in GAS – type of dividend
- Platform to digitize assets using digital identity and smart contracts to self-manage digital assets
- Focused on allowing businesses to manage smart contracts effectively, safely and legally
- Two-tiered consensus based on PoS to enable voting and delegated BFT
- Capable of 10,000 tps
- Digital identity based on X.509
- Governance has voting and dividends making it a security

- For more information:

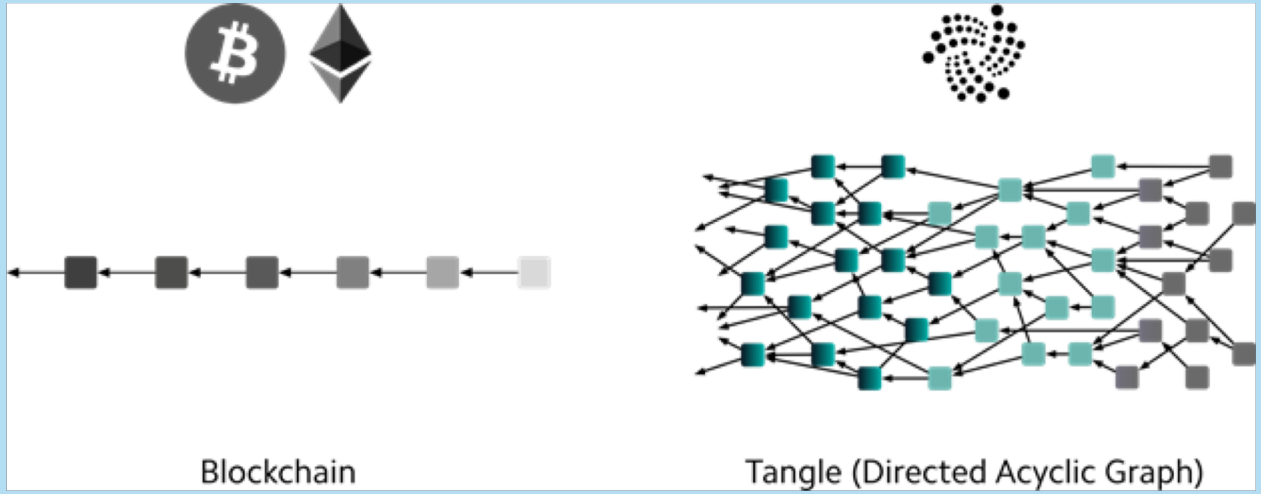
  https://neo.org/

IOTA

- Lean Proof of Work
- Created in 2015 – no mining, fixed supply
- DLT for the Internet of Things – pseudo blockchain called the Tangle
- Secure, scalable and feeless transaction settlement layer
- Uses a DAG (directed acyclic graph) rather than blockchain called Tangle
- Transactions can occur simultaneously, asynchronously and continuously
- Pay-it-forward fee-free consensus process - $1.4 billion market cap
- Transaction rate grows as validations grow
- Potential for massive tps growth
- Microsoft, Deutsche Telekom and Fujitsu collaboration

For more information:

https://www.iota.org/



4rd Generation consensus models

- Red Belly
- Holochain
- Hashgraph
- OVR PoM

Red Belly

- Developed by the Concurrent Systems Research Group at the University of Sydney
- Fork free
- Deterministic Byzantine consensus using a weak coordinator
- In 2017 demonstrated >660K TPS in single data center exceeding VISA's 56K TPS
- Sept 26th demonstrated >30K TPS with 3 second latency using 1000 virtual machines in 14 different AWS data center around the world
- For private and consortium blockchains
- Promising consensus model

For more information:

Redbellyblockchain.io

Holochain

- Fully distributed peer-to-peer network – not blockchain
- Although a DLT it is considered a post-blockchain ledger
- Agent centric - no centralized blockchain – every agent has it’s own blockchain
- Public chain - $148 million market cap
- Pushes chain from center to the edge
- Distributed Hash Table
- Distributed validation called Proof of Service – user gets paid by helping another user
- Gossips for Immunesystem
- Membranes
- Proof of service – history of apps running on a agent

For more information:

https://holochain.org/

HashGraph

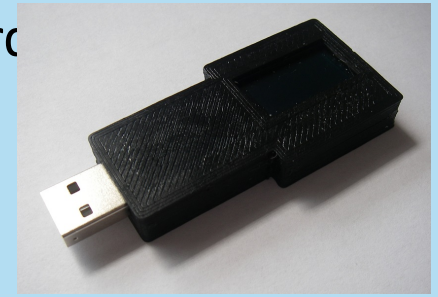
- Virtual voting algorithm combined with gossip protocol
- Alternative to blockchain – but supports DLT
- TPS >100K/sec
- 30 computers reached 50K TPS globally dispersed with 3 second latency
- Popular with large financial institutions – raised $100 million
- Not a public crytocurrency
- Over 200 ambassadors running 80 meetups worldwide with 5000 attendees.
- Joined the Trusted IoT Alliance

For more information:

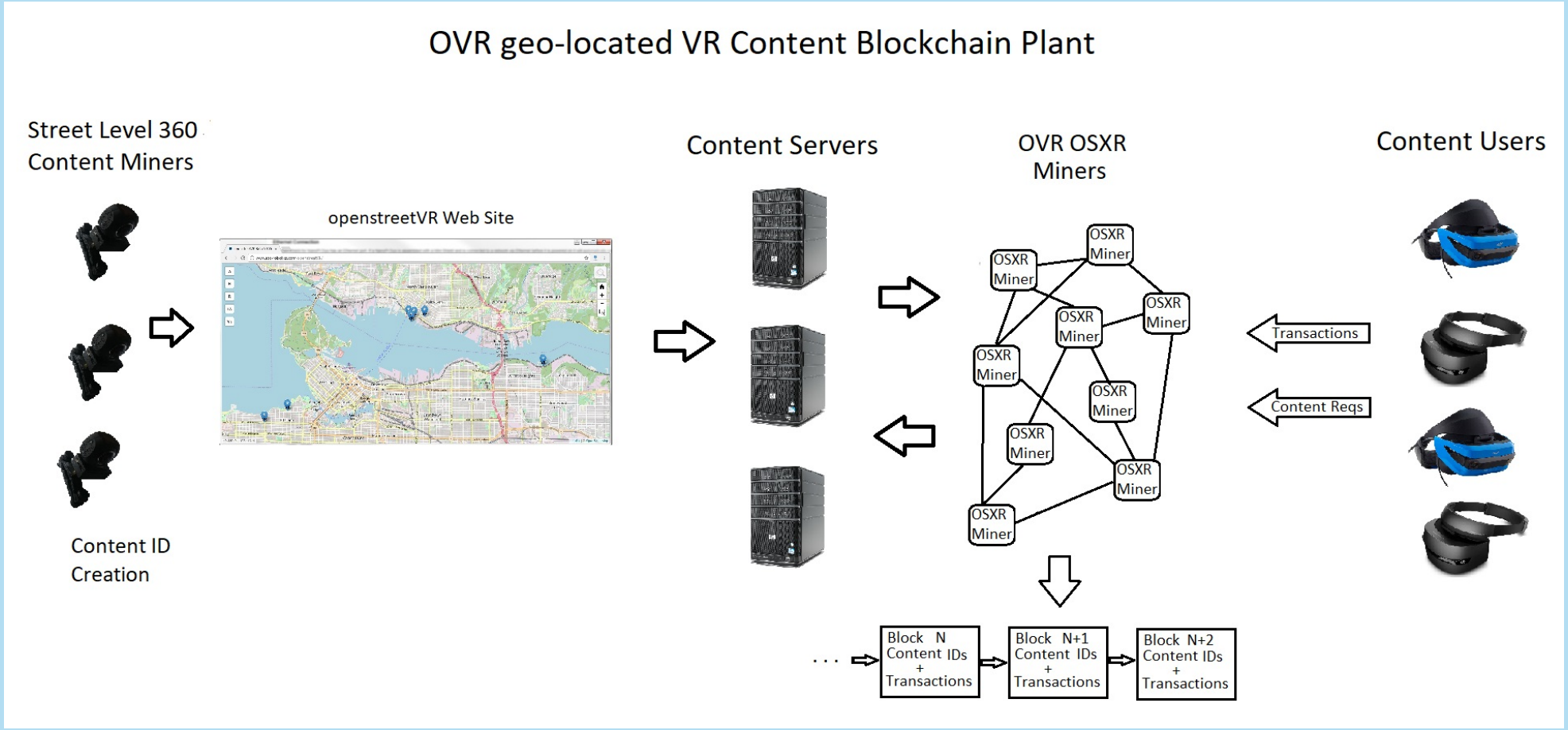
https://www.hedera.com/

Proof of Merit Consensus

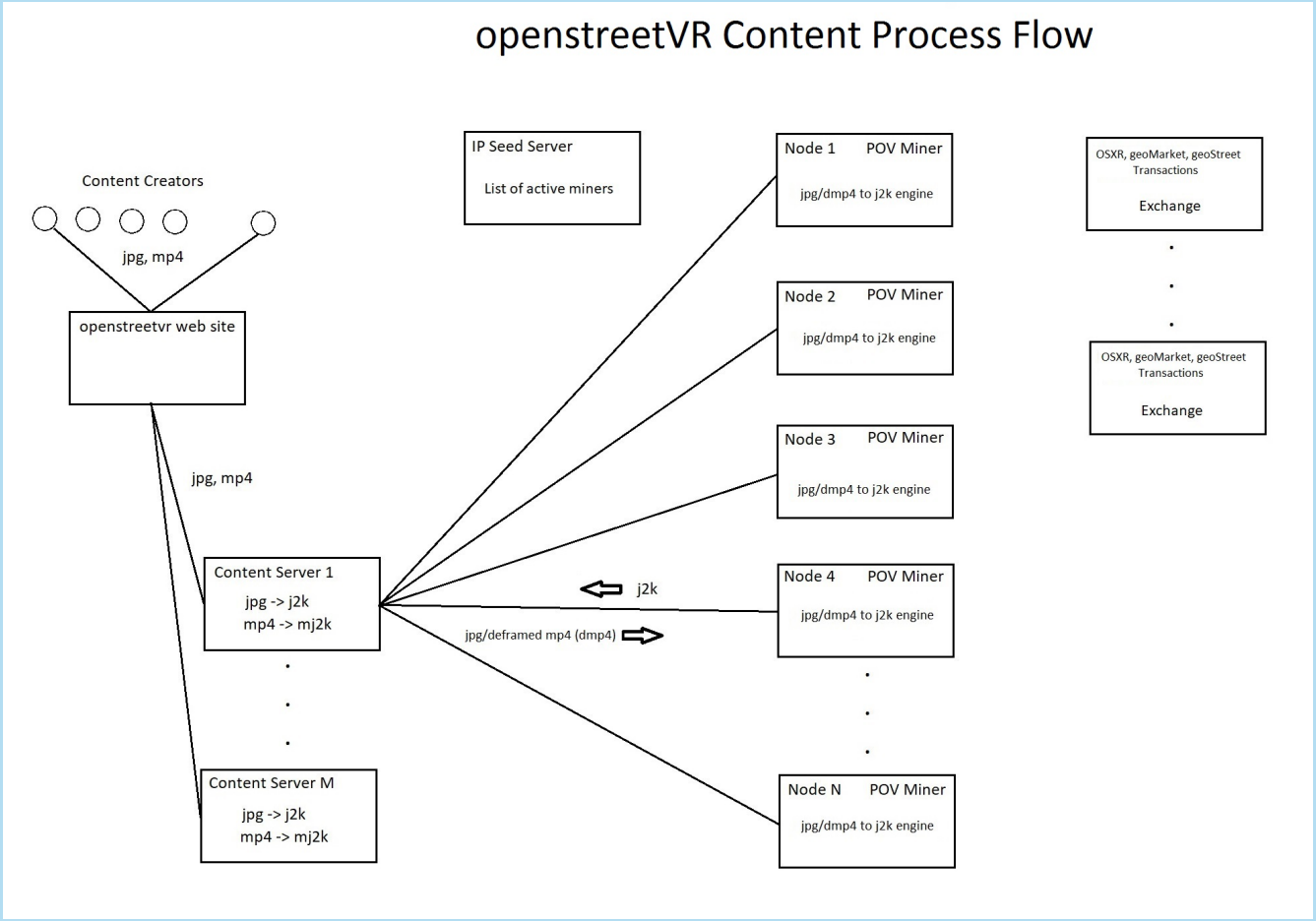
- Based on a decentralized Randomized Byzantine Fault Tolerance with no coord
- Each miner has a dedicated Thermal Hardware Random Number Generator (HRNG) with a dedicated challenge/response Cryptographic Element (CE)
- Highly scalable, decentralized, low latency, eco-power friendly
- Enrollment process to vote – must do some useful work – merit work
- All voting is randomized by HRNG with equal access – no staking
- Expected to achieve > 30K TPS in closed 80 core HPC platform with room to grow
- 3-4 second latency
- Still under development - not publicly available – beta before year end
- Mainnet in Q1/Q2 2019
- Purpose built for openstreetVR and tightly integrated with it

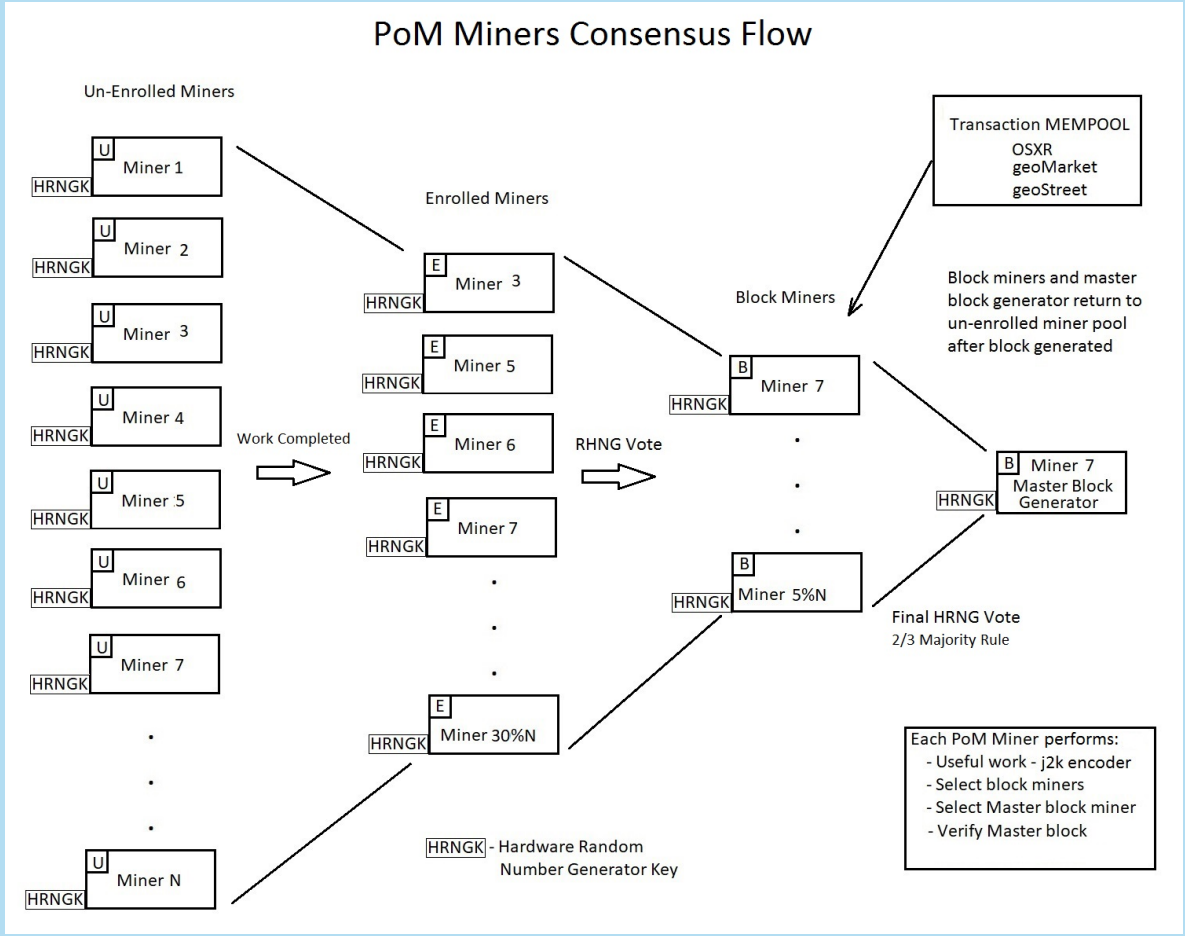


openstreetVR content flow



PoM Consensus flow





PoM used by openstreetVR (OVR)

- Immersive street level 360 content web site with app-less VR immersion using Edge browser with a Windows Mixed Reality Headset 1440x1440
- Display 360 images using JPEG2000 ROI, JPIP (Part 9) – 10-15K images
- Token/coin based: geoStreet, geoMarket, OSXR
- Content servers and miners
- Uses Babylon.js framework
- Hardware Wallet - OVRStick
- PoM consensus

www.openstreetvr.com

Effective FOV of Windows Mixed Reality Headset 10K Image

JPEG2000 Region of Interest (ROI) image extraction mode reduces the amount of content that must be transferred to the client viewer from the server dramatically increasing throughput. On the image on the right a small fraction of the total image is actually seen in the headset.

Blockchain patent landscape

- From 2011 to 2015 86 patents were filed
- In 2017 over 600 patents were filed
- To day over 2000 patents have been filled – pace is picking up
- China filed more than half of all blockchain patents in 2017
- Largest blockchain patent portfolio is held by Alibaba followed by IBM
- The next batch of filers are financial institutions
- Walmart has growing blockchain patent inventory

Clearly a lot of focus and activity in this area

Ideal Consensus model

- Should rate highly on the Kramer List
- Patent neutral
  - OK if patented as long as FRAND'd
  - Intellectual Property Rights (IPR) should be crystal clear
  - Submarine patent free – application patents
- Royalty free – look at the effect MPEG LA is having
- Non-fungible – Meets regulatory compliance

Importance of Standards Bodies

From a report issued by Standards Australia - "Roadmap for Blockchain Standards - March 2017"

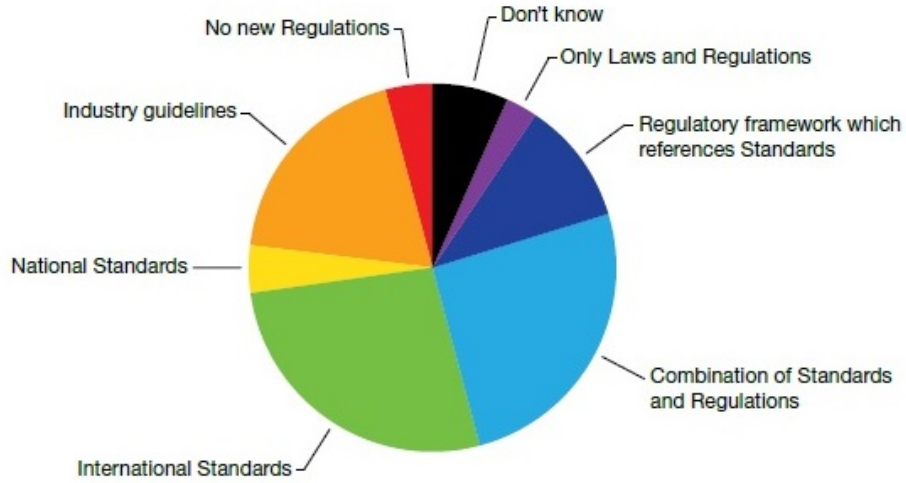
Blockchain Issues

The survey allowed participants to consider the optimal standards and regulatory framework to support the roll out of blockchain technologies. More than 88% of respondents suggested that either national standards, international standards or a mixture of standards and regulation are required to support an appropriate co-regulatory framework for blockchain-related industries. Less than 3% of respondents believed that laws and regulation alone would be sufficient.

The respondents also highlighted a number of blockchain issues that could be addressed through the development of appropriate standards. These include but are not limited to privacy, security, governance, terminology, interoperability and risk.

https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx

The optimum standards and regulatory framework to ensure we are fostering innovation and entrepreneurism



More than 88% of respondents indicate a role for standards in supporting the roll out of blockchain technologies. Source: Blockchain survey, Standards Australia analysis

ISO JPEG Blockchain Workshop
Consensus Models

Contact Stephen Swift for additional information.
kalmantech@yahoo.com

Thank you

If any content in this presentation is subject to copyright and/or require attribution please advise.