QUANTUM 1NET™

LIGHTPAPER

Introducing

QCoin

Table of Contents:

Problems with existing Blockchains

Blockchains have demonstrated great promise of utility over several fields including “Internet of Everything” (IoE), finance, governance, identity management, service decentralization and asset-tracking.

We have seen a number of blockchain and crypto projects reach significant milestones. Some are functional and open such as Bitcoin while others provide strong privacy like Zcash and Monero.

Others are designed to fulfill requirements of enterprise and operate in private.

However, despite the technological promise, we have yet to see significant real-world deployment of present technology.

We have identified six key weaknesses in current blockchain technology stacks.

Security

Quantum Hacking is coming, blockchain and cryptocurrencies needs to be ready, as failing to do so will set back the decentralization development for a decade.

Scalability

Existing blockchain technology doesn't have the capacity to run the amount of transactions necessary to fulfill the promise of a decentralized world.

Governance

Existing blockchain governance is focused on proof of work vs proof of stake, incorrectly rewarding the few at the expense of the many.

Develop

DApp creation is limited by the lack of integration opportunity, which exists because there is no scalability and immutability makes most services impossible to deploy as an DApp.

Deployment

Because of the lack of scalability, interoperability, and developability, end consumer use cases are not realized and deployed. Blockchain has not yet bridged the gap from core technology to actual deployments, and mostly remains theoretical rather than practical.

Quantum1Net is a Decentralized Service Platform.

Quantum1Net allows any Internet service, be it AirBnB, Google or Amazon, to become decentralized and provide their users with the security and privacy they need, while still maintaining the quality of service.

Taking the concept of Dapps and expanding it in to fully Decentralized Services, so anything can become decentralized.

At a high level, here are the problems we are solving:

1.Security (Quantum Computer Enhanced Hacking protection)
2.Privacy (Your data is Your data)
3.Scalability (Incentives, Embedded chains, Sharding)
4.Multi-Service (Not DApps)
5.Simplicity (Easy, to install and use)

Multi-Service

We are looking at a future filled with P2P transactions and decentralized services.

Current decentralized solutions are DApps, that are service specific and unique, and are immutable, so not usable for any service that needs to be able to be updated and dynamic.

What we need is a platform that is easy to use and that can fill the world with diverse decentralized services that can interoperate just like the centralized Internet to today.

Quantum1Net is design to enable Services to be decentralized with a click of a button, through our seamless deployment system.

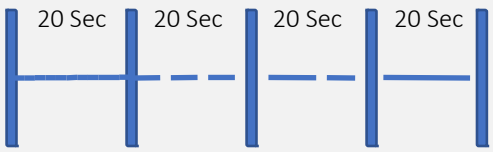
Thereby solving the existing problem and creating a truly trustless platform and ecosystem that will develop and thrive.

Scalability

Currently transactions are processed one-by-one on network nodes, creating a bottleneck as more transactions try to make their way through the network.

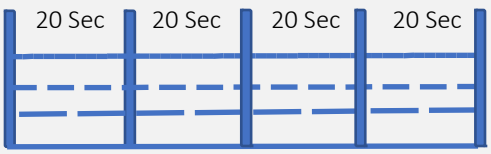
Quantum1Net creates the ability to run several embedded chains, each processing multiple transactions in parallel, which allows networks to obtain infinite scalability.

Current Method:
Single Transactions



Because transactions have to be processed one-by-one by each node, there is a limit to network scalability.

New Method:
Multiple Embedded Transactions



Our tests indicate that Yggdrasil can process up to around 100000 TPS. By creating embedded chains, we can multiply this so that Quantum1Net can securely process hundreds of times more.

*Simplified drawings

Hacking affects blockchain in 4 major areas
1. Mining
2. Transactions
3. Historical chain
4. Extract Private key Seed from Public Key

There is a huge difference between the First Gen Cryptos and Second Gen Blockchain,
Gen One [BitCoin, LiteCoin, BitCoin Cash, BitCoin Gold …]
Gen Two [Ethereum, Waves, NEO, Tezos ….],
when it comes to security, this due to the fact that the first generation blockchains have the account states hardcoded in the transactions as opposed to the second generation where account states are calculated by the node processing the blocks.

On mining both Gen 1 and Gen 2 have similar problems, that finding the correct nonce is a lot easier for a Quantum Computer then it is for a Binary Computer There would be a need to implement a Quantum Safe Block Signature like the XMSS (https://datatracker.ietf.org/doc/rfc8391).

On Transactions, we have "the first node that you send the transaction to can replace the change address with whatever they want, recover the private key from your public key, and forge your signature."
Most Gen Two Chains can change to a one-time key function without a need to move everything into a new chain, however for the Gen One chains it is not that simple and the chains will need to be hard forked.

The historical chain should be safe as it has been spread to enough nodes to be secure. 51% attack should not make a difference with a Quantum Computer or not, but still a problem that Yggrdasil solves by micro and macro signing and pseudo-random assignment of nodes.

The ability of quantum computers to extract private keys from public keys
https://www.linkedin.com/pulse/quantum-computing-blockchain-killer-samuel-falkon
is a huge problem.

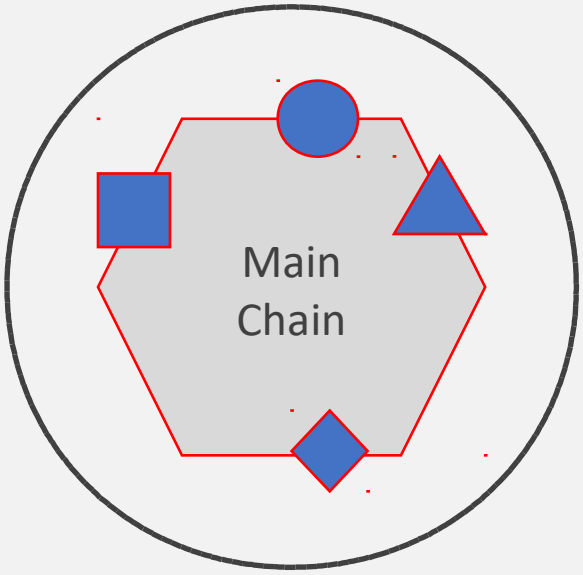
Quantum1Nets solutions:
The Yggdrasil blockchain uses XMSS as block signature,
One-Time-Keys,
XMSS makes the historical chain secure and the built in sharding with oracle nodes make it possible to add additional security on the historical chain, as needed,
Extract private keys is solved by One-Time-Keys.

The Breakdown

Quantum1Net is a Decentralized multi-service Platform.

Quantum1Net's Yggdrasil Blockchain consists of a main chain that can embed multi chains in parallel so that transactions can be spread out across the chains, allowing many more to be processed in the same period of time.

Quantum1Net ensures that each of these blockchains remains secure and that any dealings between them are faithfully executed. Specialized chains called bridges can be created to link independent chains.



Main chain
Coordinates consensus and transaction delivery between chains

Embedded chains
Private chains which gather and process service specific transactions

Bridge
Link to embedded chains with their own service specific consensus

Node Roles

Validators

Secure the main chain by POW and POS, validating proofs from other nodes and participating in consensus with other validating nodes.

Nomination for minting

Secure the relay chain by selecting good validators, PoW and staking QCoins.

Oracles

Maintain a universal state of Main and Embedded Chains They also monitor the network and can prove bad behavior to validators.

A New Core

In a Decentralized Internet, our services, identities and our data is our own – safely secure from hacking and prying eyes. we believe that the Internet can and should be completely decentralized, to limit opportunities for bad actors. Call it what you want, Web3, Internet 2.0, Blockchain 3.0. **We call it a better Internet.**

QCoin is built to bridge the development of the future Internet and the current Internet by providing an easy way to transform existing centralized services to decentralized.

Qcoin and Quantum1Net enables an internet where blockchain provides trust-free transactions via the mainchain, or with private service specific chains with focus on scalability, governance and interoperability.

What will you decentralize with Quantum1Net?

Technical

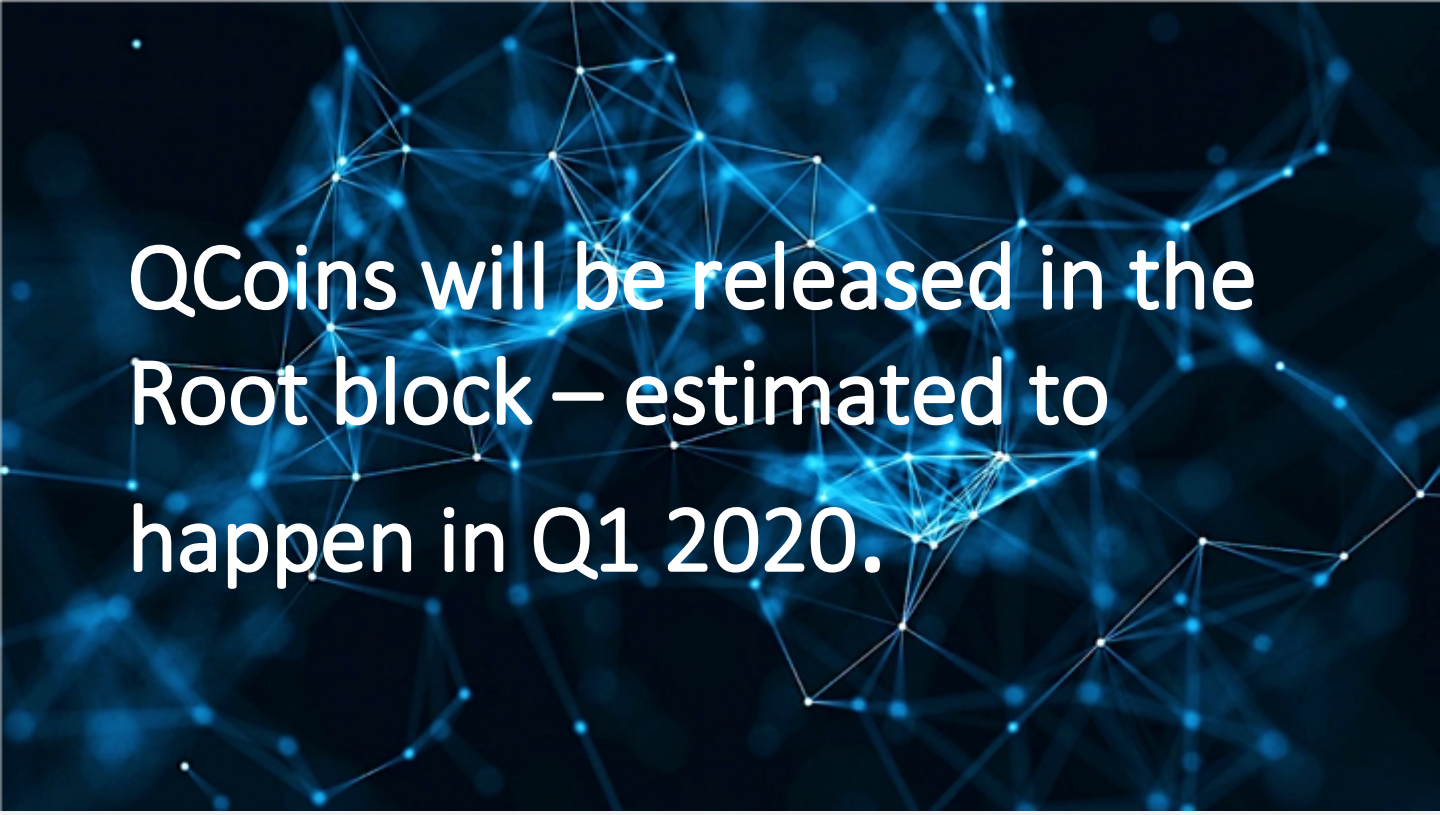
Links White Papers

Blockchain

Quantum security

Key Exchange

Links Video



QCoins will be released in the Root block – estimated to happen in Q1 2020.

The sale is a discounted at start sales, so by ordering early and locking in your QCoins early you get the best price.

The pre-testnet order price is $0.05. = 90% discount

The testnet phase1 order price is $0.10. = 80% discount

The testnet phase2 order price is $0.15. = 70% discount

The testnet phase3 order price is $0.25. = 50% discount

The MainNet release order price is $0.50.

The sales closes once the orders received for the entire 40 million QCoins.

The QCoin

Speed of Transactions

Micro and Macro signatures and parallel nomination of signing nodes, creates un-president speed of transaction.

Governance

Quantum1Net Node Holders have complete control over the protocol. All privileges, which on other platforms are exclusive to miners, will be given to the relay nodes participants (Node Holders), including managing exceptional events such as protocol upgrades and fixes.

Operation

Game theory incentivizes token holders to behave in honest ways. Data transport is used as Work in PoW so data in needs to match data out on all nodes, Good actors are rewarded by this mechanism whilst bad actors will lose their stake in the network. This ensures the network stays secure.

Embedding

New embedded chains are added by seed transactions. Outdated or non-useful embedded chains are removed by setting the seed transactions state to void.

Roadmap

Quantum1Net's Root Block will launch in Q1 2020. Here's how we plan to get there:

Block Signing mechanism
Using Rx/Tx of all nodes and Micro/Macro consensus mechanism.
The mechanism allows the proof of misbehavior for the dismissal of malicious validators.

Parallelized decentralized minting candidate selection mechanism
Each chain nominates and uses its own signing nodes allowing multiple independent items to be agreed upon under a single series based upon subjective reception of the partial set of validator statements. Used as an input to the finalization mechanism.

Proof of Work
The Work preformed by nodes in Quantum1Net is useful work in the sense that Transmitted data (Tx) and Received data (Rx) is registered as work and used for consensus

Proof of Stake
Extending the consensus mechanism into Proof of Stake territory; this module includes staking tokens, and is one further deterrent for bad actors.

Networking subsystem
This is the means by which a peer network is formed and maintained. By using our extensive knowledge about Internet networking and P2P communications Quantum1Net have developed an unique inhouse Peer network.

State Machine implementation
This will include an integration with the embedded chains, allowing embedded chains to gain consensus without its own internal consensus mechanism.

Transaction processing subsystem
An evolution of quantum1net and QCoin, this will allow for transactions to be sent, received and propagated. It includes the designs of transaction queuing and optimized transaction routing on the network layer.

Peer-routing subsystem
This introduces more specifics into the Data-Channels behavior. Multi-hop, Network location clustering are all features of this sub-system.

Service Manifests
Decentralized service maintenance is solved

Quantum1Net was created to decentralize the Internet, to nurture and help technologies and services in the fields of decentralized solutions.

The QCoin is the Utility of Qantum1Net, and creates cross-border scaling, global payments, and is the Driver of the quantum safe peer2peer data-channels in Quantum1Net.

More information:
quantum1net.com
info@quantum1net.com

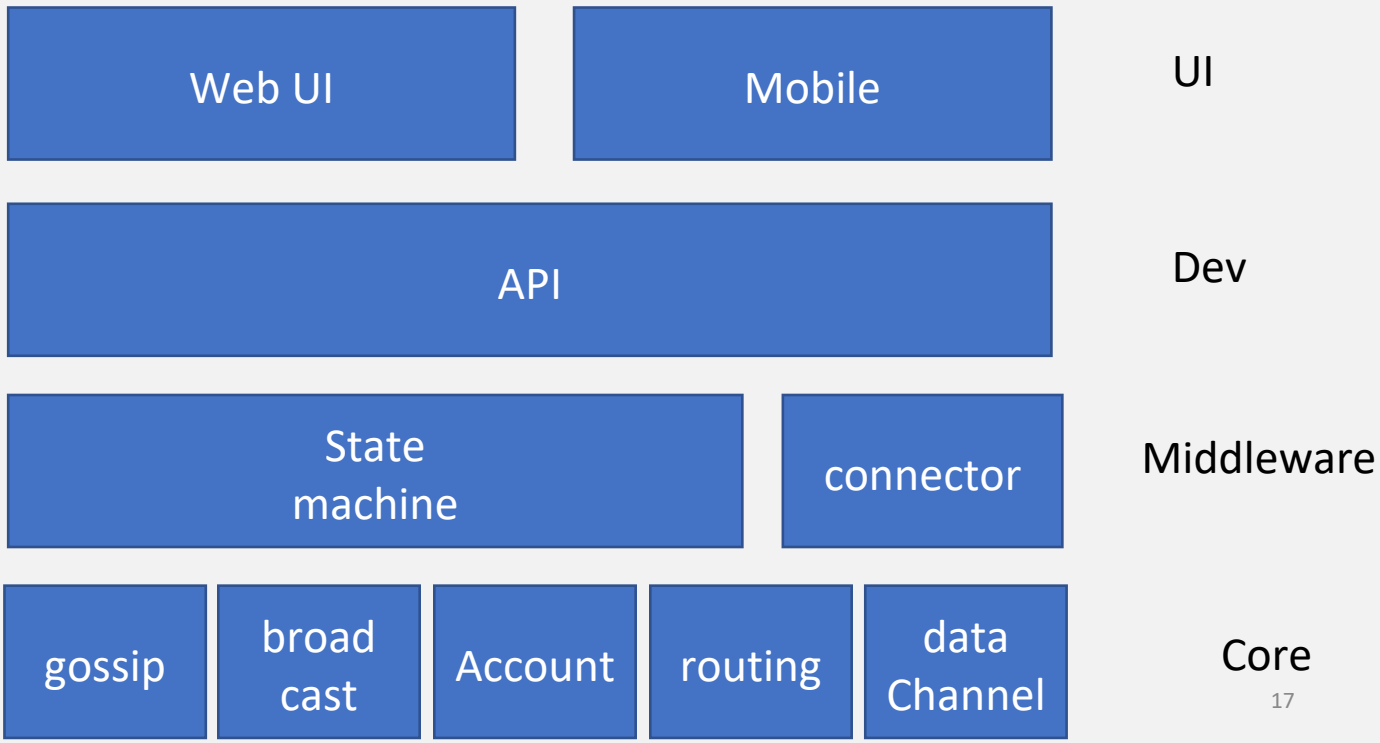
The Future of Quantum1Net:
Quantum1Net seeks to fund or otherwise assist in the development and deployment of services aligned with it's mission: Decentralize the Internet

The Development

Quantum1Net is developing the QCoin and the Peer-Network inhouse.

Founded in 2017, the team consists of 10 top professionals who are experts in peer and Mesh Networking, Cryptography, Embedded systems and distributed computing.

Quantum1Net is creating the most advanced blockchain based platform that will be able to decentralize any present or future Internet service.



Further Reading

https://quantum1net.com