



QUANTUM1NET  
Decentralized Service Platform



## MISSION

To create a low powered (Green) decentralized and fully autonomous P2P Private Network solution on Blockchain with advanced routing and traffic sharing, self sustaining through its own crypto-economy





## OUR GOAL

Create a secure, fast and efficient network environment based on decentralization, to transform key transactional markets like VPN, Online Banking, Managed File transfer, CDN, cyber security.



## OUR CONSENSUS

By using Proof-of-Contributing-Work instead of Proof-of-Work, we focus on rewarding the support of the network based on data transactions and therefore have no power wasting Mining and can instead Mint the QCoins



## THE PROBLEM?

The Internet-of-Everything is already happening, with Smart Cities, sensor systems and smart clothing, but the problems with large scale centralized networks and data transmissions becomes even bigger as we add more and more devices, and if security and/or privacy is compromised at a centralized point the whole network is compromised.



## OUR SOLUTION

Internet-of-Everything needs a new solution, with Resilience, Predictability, Transparency, Immutability, Interoperability, Consensus, Security, and Eco-Friendly.

All this is achieved in a decentralized private network in two layers, the first layer is a Quantum Computer Enhanced Hacking protected data transmission layer, the second layer is based on blockchain and is the “receipt” and consensus layer of the Private Network.

## Q1N MINTING NOT MINING

Q1N is a Blockchain driven Service Platform empowering the crypto economy and supported entirely by its users.

To transmit data over the transaction network, you either have to have coins in your wallet, or the receiving node accepts “collect” by extracting coins from the receivers wallet. Thereby the nodes supporting the Q1N Ecosystem generate passive income for the node owner.

Revenue nodes may be deployed by anyone. Nodes will generate income by relaying transactions over the internet, with the only requirement being that you own a QCoin that is then added to the wallet of the node.



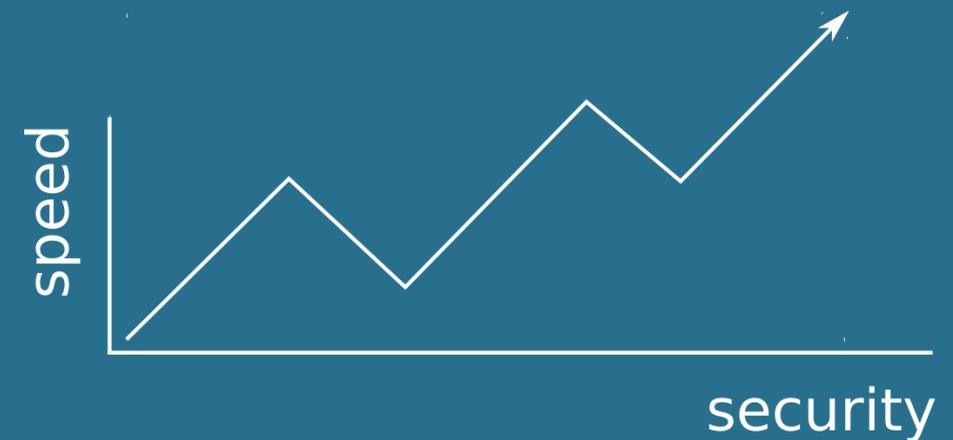
## RELAYERS MINT COINS AS THEY SUPPORT THE NETWORK

### USE TO EARN - EARN TO USE

By using Proof-of-Contributing-Work instead of Proof-of-Work, we focus on rewarding the support of our network without the massive use of energy intensive Mining. Instead of Mining we efficiently Mint QCoins in our Q1N transactional process. Simply Much More Output For Much Less Input.

Vastly increasing the security, speed, and number of transactions while significantly reducing the energy consumption to do so.

By being able to mint more currency as the Economy grows the blockchain is future proof and scalable in a way no other crypto currency is



# THE VALUE PROPOSITION:



# Quantum1Net BENEFITS

## GREEN

- Low power by optimized Quantum Safe security based patent pending
- Low power by using light weight layered hashing with angled offset by layer
- Low power by Proof-of-Contributing-Work not Proof of Work

## EFFICIENT

- Fast transactions by layered signing of blocks, Micro signing and Macro signing
- Fast transactions by Geo-located micro signing
- Fast transactions by Macro signing only on global level
- Fast transactions by built as a Mesh of secure End2End tunnels
- Fast transactions by tunneling with optimized routing based on ASn Mapping

## SECURE

- Secure transactions by Quantum Safe End2End encryption
- Secure signing by Quantum Safe Layered hashing
- Secure storage by Quantum Safe Elliptic curve Encryption



Green Tech



Quantum Safe



High Speed

## The Quantum1Net Overlaying Network

All people, computers, devices, or objects currently within the network is connected One-Time-Connection (“OTC”) that is both dynamic and transient existing only for the time it is required.

By design the Q1N OTC is invisible to all other participants on the Internet and Quantum encrypted making it impossible to either intercept or read the data being transmitted within it.

The Q1N Network enables any point or points within the Internet-of-Everything to be uniquely and securely connected over the top of the existing network infrastructure.



FROM YOU TO ANYONE OR ANYTHING

## Domains on Quantum1Net

The Quantum1Net Vanity name / Domain Registry so that any HTTP or HTTPS service can become Quantum Safe, by being on Quantum1Net, we like to call it HTTPQS. Any Service node can add a Vanity Name to their wallet similar to a Web URL.

## Blockchain in Blockchain (BinB)

With Embedded Blockchains, being incorporated in Quantum1Net, private data can be added to the system without slowing down transaction speeds, solving problems with

- IoE Data access
- End2End Letters Of Credit
- Serial Numbers & RFID Tags
- Property Registration
- Health Care
- Pharmaceuticals



# Service Manifests

## Making Decentralized Multi-Service Platform Reality

In a fully decentralized system there is no central point to control, manage and maintain deployed multiple services, so each existing Distributed system is built around one service and is dedicated to run the service.

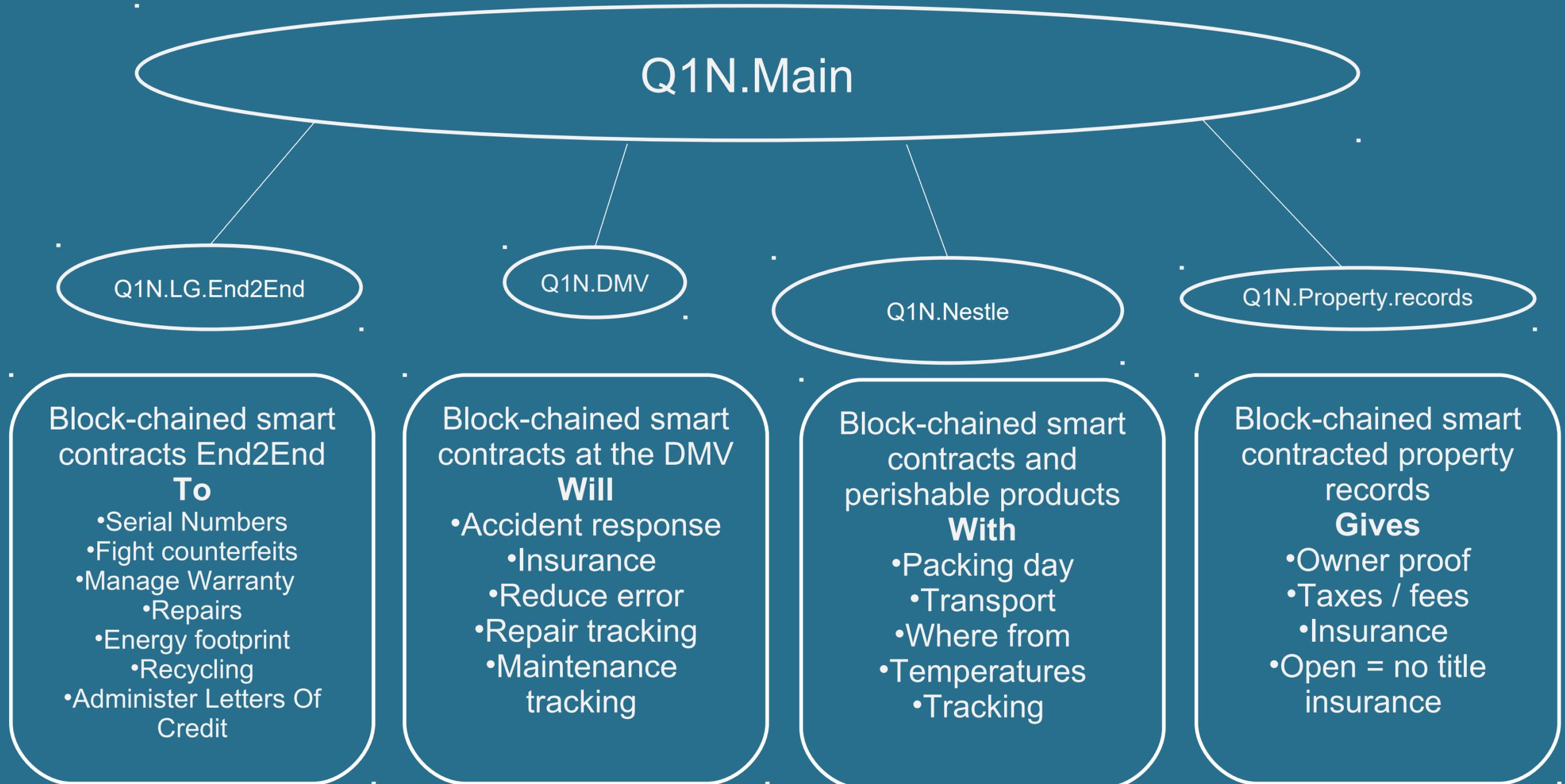
You can use the approach of “smart contracts”, and make the solution immutable and release it in the wild to never be changed. That approach do not fit most services, as it is hugely limiting.

So to solve this, Quantum1Net has developed the Service Manifest, that describes permissions and policies of a specific Service and makes it possible for multiple Services to run on the same decentralized, distributed system.

- Device control
- Node choice (Use specific nodes)
- Policies by service and by user
- Generate child Manifest as needed



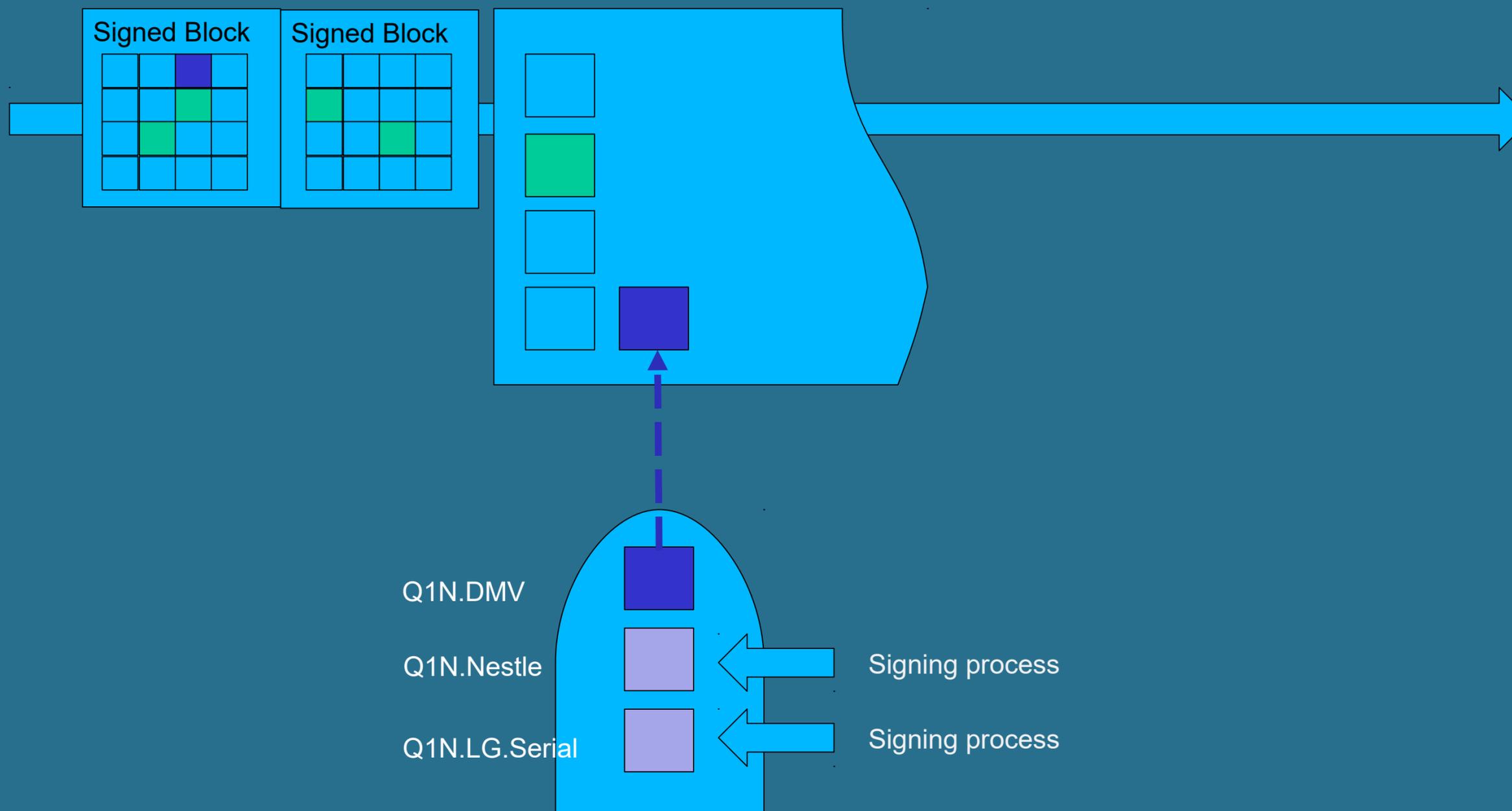
# Blockchain in Blockchain (BinB)



BLOCKCHAIN IN BLOCKCHAIN

# Blockchain in Blockchain

- Transmission
- Monetary
- BinB signed
- BinB unsigned





QUANTUM  
1NET™

# DPN (Decentralized Private Network)

## The Uniqueness of Q1N DPN:

- There are no centralized servers
- The Nodes are and define the network
- All connections are End2End encrypted
- All payload data is Quantum Safe
- Exit points can be random bounced or chosen by geographic area
- There are no logs kept anywhere in the system
- Uses HTTP and HTTPS ports to negotiate tunnels through firewalls
- No ugly fine print in user agreement, no logs no data saved, period!
- Works on restricted networks

# GhostWire (Decentralized Web Hosting)

## The Uniqueness of Q1N GhostWire:

- There are no centralized servers
- The Nodes are and define the network
- All connections are End2End encrypted
- All payload data is Quantum Safe
- Exit points can be random bounced or chosen by geographic area
- There are no logs kept anywhere in the system
- Uses HTTP and HTTPS ports to negotiate tunnels through firewalls
- No ugly fine print in user agreement, no logs no data saved, period!
- Works on restricted networks

## DezComp (Decentralized Computing)

### The Uniqueness of Q1N DezComp:

- There is no centralized computers to listen in on
- There are no centralized computers to hack
- By breaking computations in to smaller pieces and have multiple machines working on them we gain efficiency
- Distributed systems are much more cost effective compared to very large centralized systems
- Since users can have a node in multiple geographical locations, distributed systems allow the traffic to hit a node that's closest, resulting in low latency and better performance

## Power sharing for EV's

In one embodiment Quantum1Net is used as a Private Network with a Cryptocurrency to run a electrical charging pole systems where anyone can in a simple way add charging opportunities for EV's and become a part the Ecosystem.

The Cryptocurrency is used as the barrier to setup charging poles is lowered and therefore the solution will have an easier time gaining traction.

The cryptocurrency coin is use to pay for use of charging poles and generates coins for owners of the charging poles, renewable energy and non renewable energy poles can be identified and have different payment structures.

By storing data as Locating and Power use, the blockchain data can also be used to learn the optimal routes and best charging rutines.

## Smart Home

The biggest caveat with smart homes is the security solutions, the risk of intruders gaining access to the house through the smart system is a real risk, or even worse steal private data about the inhabitants, but high security raises the barrier of entry as just adding a new person as a weekend visitor, can need a support person to make a house call.

When running on blockchain, smart home devices become immutable and therefore safe from cyber attacks. This means that hackers cannot access your home or the data collected by your IoT devices. Additionally, with a blockchain-powered smart home system, you can securely enable other parties to access specific areas and devices without giving them access to everything.

It is all about combining Security and Flexibility.

# Smart City

## Governance:

Real Estate Land Titles ,Welfare Benefit Tracking, e-residency,

## Healthcare:

Healthcare Record Management, Patient-Related Outcome Measures (PROMs)

## Energy:

Self-Sufficient Microgrid, Supply Chain/Public Safety Supply Chain Tracking

## Smart Cities and the Internet of Things (IoT)

Smart Cities are going use of IoT-based solutions for a wide variety of purposes such as law enforcement, asset tracking, utility meters, streetlights, vehicles, and drone registration. Blockchain technology is a good choice for IoT management for several reasons. Blockchain's decentralized peer-to-peer architecture is resilient and better able to handle the large volume of IoT enabled devices compared to a hub and spoke centralized architectures. Infrastructure failures would be less catastrophic because a decentralized network is highly fault tolerant. IoT devices would be guided by smart contracts to other functioning peer nodes. IoT device digital signatures kept on a blockchain would authenticate the device, helping mitigate or prevent cyberattacks, and IoT device activity logs would leave an evidence trail for auditing and diagnostic purposes. Blockchain consensus could monitor and insure IoT software patch integrity while smart contracts determine when patches are applied so that rollouts occur in an orderly manner.