Smart Shards - Self-governed trusted Sharding Smart Home

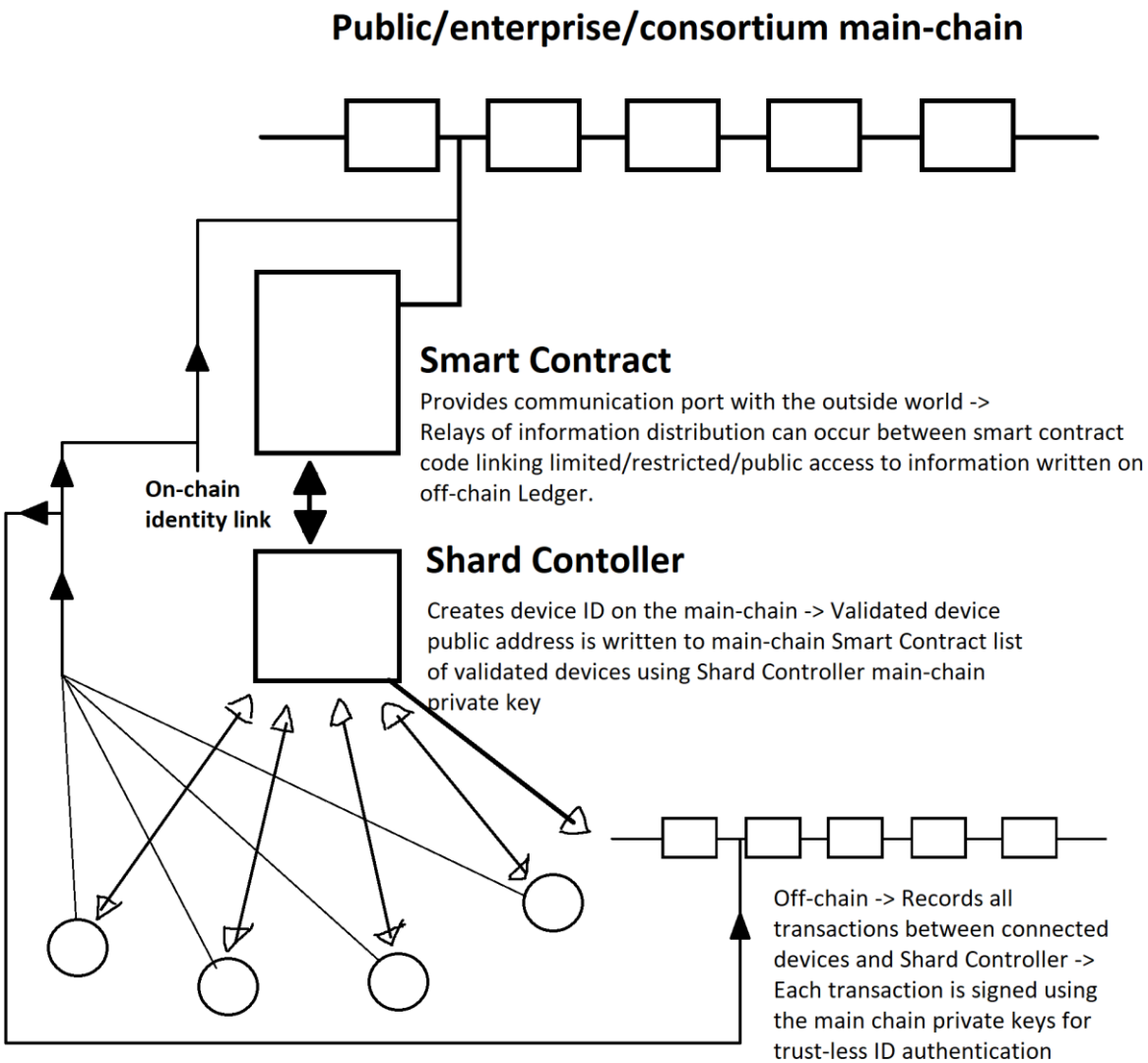
Off-chain second-layer solution for secure IoT-device identity validation, secure communication, and record keeping. By linking a Smart Home Shard with a Smart Contract on any Public/Private DLT-Platform, you open the door to many features of the future of IoT Smart Homes. This off-chain solution provides unlimited transaction throughput, opt-in for on-chain finality, and minimum transaction fee gas spending.

Most modern homes are using indoor Wi-Fi connection to link devices; anything from their phone, TV, Security alarm, Laptop, iPad, smart fridge, smart thermostat, lights, speakers, etc. Our devices are communication and transmitting more and more information as IoT emerge. Distributed Ledger Technology can be leveraged for multiple purposes around Smart Homes and IoT. A smart home can benefit from secure communication between devices, and protection from outside intrusion by validating device-identities on-chain. All devices are validated by the home owner using incorruptible cryptographic signatures. The governance of the Ledger of validated addresses and historical transactions between the validated devices. The governance is taken care of by the home itself. Connected devices in the home (computers, phones, tv) which are under-utilizing their CPU/GPU validate transactions made between validated devices. Unused storage is leveraged to store the Ledger, as the transaction record and address list is only of validated devices, ledger size and computational work required are minimal; no on-chain transactions between nodes. IoT devices only require internet connection, capacity to transmit, and holding a private key (same key as for on-chain validated identity) for signing transactions.

Example: A Smart Thermostat can transmit a message/transaction -> Your phone is listening for transactions -> it will pick up the transactions -> on-chain validate identity -> write the transaction to the second-layer Ledger

Devices limited by storage and computational work can leverage other devices in the home by transmitting data to be stored, or to perform computational work using the data. Shard Controllers can launch the message on-chain for trusted timestamps, to sell the data, or transmit it to a supervising manufacturer.

This solution provides a Shard Smart Home owner with a more secure network and Smart Home solution. It opens the door to interconnectivity and machine economy through IoT. Any Shard operator can leverage a private chain, while being connected to a public/private main-chain. A main-chain operator could be a manufacturer of any smart device, or a consortium of manufacturers. It could also be a public chain providing trust-less governance and global access.


Public/enterprise/consortium main-chain
Smart Contract
Provides communication port with the outside world -> Relays of information distribution can occur between smart contract code linking limited/restricted/public access to information written on off-chain Ledger.
On-chain identity link
Shard Contoller
Creates device ID on the main-chain -> Validated device public address is written to main-chain Smart Contract list of validated devices using Shard Controller main-chain private key
Off-chain -> Records all transactions between connected devices and Shard Controller -> Each transaction is signed using the main chain private keys for trust-less ID authentication
Second chain has no blocktime, consensus mechanism, or confirmation times. Transaction throughput is unlimited as Shard Controllers are the sole upholder of consensus

Users

As the entire off-chain is run by the buyer of the Smart Home product or system, only the on-chain identity validation will imply minimal transaction fee costs. Any manufacturer of a can offer a simple extension to their Wi-Fi connected device. The manufacturer can validate the identity of each manufactured device, and home owners can simply add the on-chain identity of a device to their Shard Controller list or add the manufacturer as a trusted actor -> Nearby devices from trusted manufacturer may automatically connect to the Wi-Fi. Any home owner wishing to improve their network security, can do so by only allowing validated devices to connect to the Wi-Fi. Each purchased device can have its entire supply chain on a manifest linked to a Manufacturer Smart Contract. A home owner can know with absolute certainty that the product is from the trusted manufacturer, and that the production has met expected criteria for production and shipping. At 0 cost for the enterprise, a device may have the home owner be in control of all IoT units while securely and incorruptibly transmitting data back to the Enterprise for analysis. The service can be leveraged using just one type of Smart Home product;

Use case for one connected product: Smart Thermostat writes in-house and outside temperature data to the Shard Controller's Ledger & the on-chain Ledger.
Example: In my home, I have Smart Thermostats which are centrally controlled by the manufacturers. My home is freezing cold during the winter, I have called them to have them increase the heat, but they won't, they are saying that the in-house temperature is correct. I know they are wrong. If I had a Shard Controller, I could verify this temperature on my own, and prove to the manufacturers that they are wrong. The enterprise in turn can have a cost-free distributed database of temperature data run by all the connected Smart Home devices. They also get incorruptibly performance data from their products.

Use case for multiple connected products: A single manufacturer can validate the identity of two different devices and create instructions for cross-product communication. A home owner who already owns a Smart Thermostat, now purchasing a Smart Fridge from the same OR a different manufacturer, can have these two automatically communicate and adjust settings according to the other trusted device communication.
Example: Since my home is freezing, my fridge will likely require less cooling to remain cold. A trusted Smart Thermostat can send a secure message to the Smart Fridge. It is verified by its on-chain identity from the manufacturer, and the trusted device list of the Shard Controller; the Smart Fridge can trust the temperature information and make adjustments according to the information. This can securely be done cross-manufacturers as it only requires general communication rules. Manufacturer A can build interaction protocols for products from Manufacturer B.