< Project Highlights >

Secure and Interoperable Systems

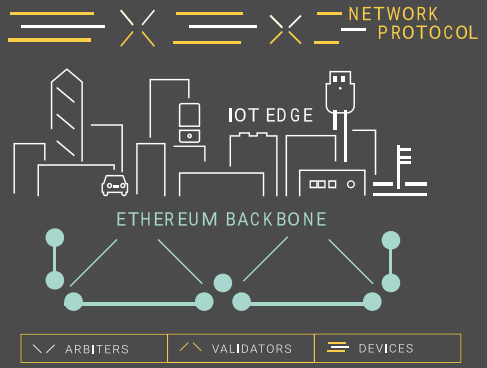
An industry report estimates that the IoT industry could have a total economic impact of $3.9 trillion to $11.1 trillion per year in 2025, with up to 40% of the value locked in interoperability problems. To tackle this issue at the operating system level, weeveOS will be the first lightweight IoT-Blockchain operating system. It runs on commodity IoT hardware, supports the ARM Trustzone extension, and contains several data protocol and blockchain primitives that allow devices to discover and transact in a secure fashion.

IoT-Enabled Marketplaces

When networks of devices achieve sufficient trustworthiness and low transaction costs, new types of trade among devices can occur at staggering volumes. Weeve provides the base building blocks for these marketplaces, including membership standards and secure protocols. These IoT-enabled marketplaces enable groundbreaking efficiencies across sectors spanning manufacturing, agriculture, and transportation.

Weeve Network Protocol

Trust is an important factor in marketplaces, and it is necessary to maintain high standards to ensure safety for all participants. Without safety, no transactions occur. Therefore, the Weeve Network Protocol combines incentive elements of staking, attestations, and verification to bootstrap trust. The network protocol implements tunable incentives that reward good behaviors and punish bad ones.



Staking Utility

WEEV token aims to ensure all devices meet the desired membership standards and incentivize curators to provide quality data. To achieve this aim, Weeve's network protocol requires participants to stake WEEV tokens when registering.

DEVICES/ MARKTPLACES/ REGISTRIES

Device registry is a membership standard that a device needs to fulfil, which implicitly serves the purpose of assessing the quality of the data. All devices must be listed on device registries in order to participate in the marketplace. Participants must stake WEEV tokens to apply for listing, which could be challenged by other token holders. If the device is "good" and accepted on the list, the device owner keeps the staked tokens, and may withdraw the stake when leaving the registry. In any case a challenge is lost, the staked tokens are forfeited and divided as a reward amongst token holders who participated the challenge.

Network Governance

WEEV token holders are able to self govern registries and marketplaces if they are outlined in the registry and marketplace guidelines. WEEV token holders could vote for proposals of relevant membership standards and revise them over time. By deploying the WEEV token, we empower the actual users of standards to determine the future state of their own standards. In contrast with the large catch-all international standards bodies of today, Weeve network participants will enjoy shorter feedback cycles for proposals and group deliberations, and standard emergence will occur in smaller fast-moving marketplaces.

< Token Highlights >

Reward or Penalty Mechanism

The Weeve network market mechanism design ensures an equilibrium between key players and important market forces is reached, such that each Weeve player will pursue a utility-maximizing strategy.

The Weeve network mechanism follows a trigger strategy: Players supporting the stability of the network get rewarded, while players defecting the network are punished. The reward mechanism clearly incentivises players to join the network, trade their data and contribute their knowledge and services to the stability of the network. Without suitable incentive mechanisms the network will starve, and marketplaces will not foster due to marginal and unimportant supply and demand. On the other hand, the punishment mechanism combats network destabilisation strategies. Destabilizing player strategies of Weeve network participants are disincentivized and result in negative payoffs. The WEEV token is the unit of value in all transaction to settle value - positive or negative payoffs as per participants actions.

Secure IoT Communication Protocol

PROBLEM

Companies are very keen on fast production cycles and ignore important considerations to protect their users. This results in IoT communications plagued with serious security flaws.

SOLUTION

Our TEE-MQTTS protocol extends the widespread MQTT protocol with new cryptographic protections. It is more lightweight than MQTT over TLS, and provides support for Trusted Execution Environments (TEE). The result is higher security, scalability, and efficiency.

BENEFITS

Optimize IoT communication
Reduce battery life
Reduce network bandwidth
Reduce operator costs due to decreased communication rounds

Secure IoT Wallet

PROBLEM

Cryptoasset wallets are typically designed for general-purpose computers and not IoT device firmware. Therefore, use of existing wallets with IoT devices results in clumsy, error-prone, and inefficient implementations.

SOLUTION

Weeve's secure IoT wallet integrates directly into device firmware, stores standardized smart contract templates, custodies device-specific credentials, and supports advanced device-specific functionality such as Trusted Execution Environments (TEE). It will be provided for free to improve the baseline quality of devices that handle cryptoassets.

BENEFITS

Shield cryptographic keys on the IoT device against software attacks
Shield cryptographic algorithms (e.g. ECDSA) against software attacks
Prevent authorization of non history-dependent smart contract transactions

Signed Data and Execution

PROBLEM

Most receivers of IoT device data have no guarantees of origin, reliability, or identity.

SOLUTION

Weeve's security protocols include the ability to sign entire programs and their output data to add stronger guarantees around data sourcing.

BENEFITS

Cryptographically assess the quality of device data and act as a basis of pricing
Reduce incidence of data forgery
Increase data integrity and richness of metadata

< Product Highlights >

IoT-to-Blockchain Operating System

PROBLEM

Transaction on the blockchain is limited by processing power, storage, and physical security concerns.

SOLUTION

Weeve's lightweight operating system runs on commodity IoT hardware providing additional security guarantees at the firmware level. It also has support for the ARM Trustzone extension, which parallels the Intel SGX architecture and is more geared towards IoT devices.

BENEFITS

Resist software attacks (e.g. buffer overflows, return-oriented programing)
Isolate security-sensitive data, task and protocols from the rest of operating system (e.g. Trusted Storage for wallet keys)

CURRENT STATE

Alpha released in github:
https://github.com/weeveiot/weeveos