Empowering the Economy of Things

weeve. network

Token Paper (Part 3/4)

The weeve Network Protocol & Token Model

The Weeve Network Protocol and Token Model*

Sidd Bhasin and Sebastian Gajek

weeve.network

Abstract

It is an indisputable fact that data has tremendous value when tokenized and used in a network to support the mechanics and principles of an economy. The Weeve network empowers the economy of things by introducing a commercialisation layer between (IoT) devices and the Blockchain. In the Weeve network, machines (or "Weeves" thereof) index, process, tokenize and trade harvested data against digital data assets, among them are most notably cryptocoins.

Weeve envisions public or private marketplaces for any form of digital assets ranging from geo-data to electricity or delivery status, where data producers and consumers (resp., buyers and sellers) come together, escrow their supply and demand, and exchange their digital assets for agreed upon prices.

To establish network stability in presence of rational players not necessarily following a fair game strategy, the network utilises a cryptoeconomic incentive mechanism design. To participate in the game (and thus the network), the players stake a token to vouch for their actions. In case of network instability (e.g., dispute, unfair exchange, infringement) the community can challenge the stake. The Weeve network is designed to penalize unfair strategies through stake sacrifices, and reward honest strategies through fee mechanisms.

Keywords: game theory, cryptoeconomics, fair exchange, stake-based mechanism design, rational players, machine-to-machine economies

*For releases of the Weeve network protocol please go to to `https://github.com/weeveiot/weevenetwork`

Contents

1 Introduction

1.1 Motivation

Internet-of-things (IoT) devices are approaching critical mass, and today we lack the necessary interoperability, data rights, and security infrastructures to fully enable new markets and paradigm shifts. Gartner estimates as many as 8 billion IoT devices connected in 2017, and some predict as many as 28 billion IoT devices by 2021. Reports suggest $4-11 trillion a year in new economic value by 2025.

Blockchain will enable the creation of new digital economies. In fact, it is a stepping stone to a fully automated commercialization of data between devices, empowering what we call the Economy of Things (EoT). In an Economy of Things, IoT devices on behalf of their owners (private individuals, enterprises, or any legal entity) offer their data through concepts known as first-price or second-price marketplaces and other IoT devices or entities consume the data in exchange of crypto coins or related digital assets (e.g., trade geo-data for temperature-data). Imagine, for example, a solar panel selling excess energy to an electric vehicle which requires some charge in exchange for crypto coins. The solar panel equipped with an ammeter could measure the current consumption and instruct an electric relay to shut the electricity when the negotiated amount of energy has been delivered. This use-case is just one of the many examples demonstrating the versatility of *tokenizable data* applications, and its implications for transforming digital economies.

1.2 Challenges

Before we can arrive at an Economy of Things (see Fig. 1), and before data can be made economically useful and exchangeable, a fundamental problem must be solved:

> How can we enable a *trustless*[1] network in which (anonymous) entities follow marketplace principles, namely escrow supply and demand for a fair price?

Data quality and integrity have the most significant impact on successful IoT operations. Computers have bugs and unexpected failures all the time. IoT devices - now harvesting valuable data (digital assets) - are nothing more than lean, lightweight computers connected to the Internet. Much care must be taken that devices do not offer data they do not own or that is simply false for the sake of a better price. Devices are frequently miscalibrated, and unethical vendors have incentives to tamper with results. Use of incorrect information often results in worse outcomes than using no information. Without guarantees of (cryptographic) device identity, data origin and integrity, for example, very few prospective data buyers would have sufficient confidence to freely exchange on a data-centric marketplace, as the relation to the ownership is ambiguous.

[1] By trustless we mean a fully decentralized, self-sustainable network where the players mutually distrust each others.

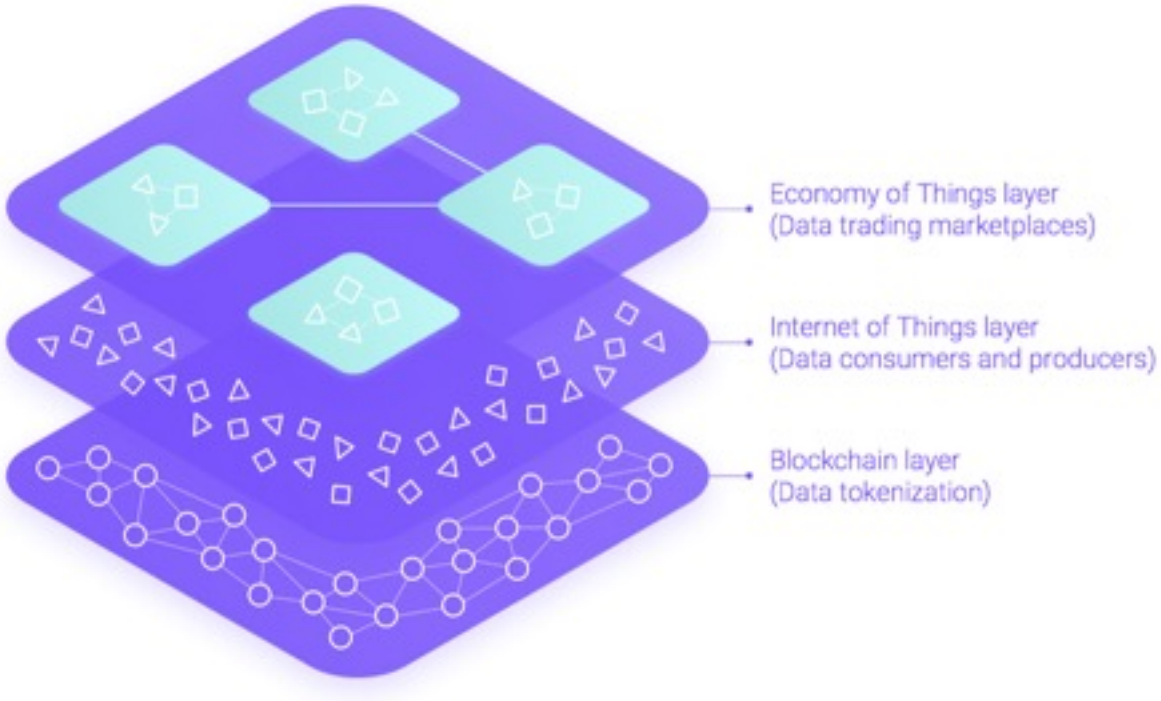

Figure 1: Layered Perspective of the Economy of Things. IoT Producers and Consumers interconnected to the Blockchain form Data Marketplaces.

A related problem is the lacking agreement on standards for devices. The IoT ecosystem—though the buzz has been in the air for many years—is still immature. We observe a technological omnishambles of IoT sensor chipsets, Operating Systems or communication protocols, leaving IoT designers with innumerable choices in the technology zoo. These difficulties make it hard for both marketplace operators and participants to assess the reliability and trustworthiness of the device and its qualified provisioning of data. Data, much like any other commodity, receives its value based on the the source of its origin. For the marketplace to truly attach a value to data (or a stream thereof), we need to understand the journey it took to get from sensor to marketplace. The higher the chance of this data being tampered with, the less we can trust it, thus value it. These are factors we use to attach value to any commodity and we need to take the factors for digital assets as well into account.

1.3 Weeve's Cryptoeconomic Token Mechanism in a Nutshell

In multi-player networks the parties pursuit different strategies to maximize their utility. In fact, when financial incentives are given, we must cope with unfair players. For example, infringement may occur. Counterfeit data producers may fake real producers thereby gaming the system to their advantage. Any form of plagiarism, brand counterfeiting or patent violation may occur cultivating black markets. Problems like the above are intrinsic to a multi-player network with financial interests.

In order to build a stable network that incentivizes all parties to act fairly and maintain the honest state of the system, one needs an intrigue mechanism design. To this end, the Weeve network leverages *principles of cryptoeconomics*—one of the astonishing ingenuities of contemporary Blockchain technologies. The Weeve network builds marketplace applications and related services for device registration, asset validation, and dispute resolution on top of a Blockchain. The underlying blockchain gives us (i) a unit of value that can be used to create incentives and penalties, and (ii) occasionally a toolkit with which we can design conditional logic in the form of "smart contracts." Entangled with the Blockchain the Weeve network creates a system of incentives that rewards the curation of marketplaces with high-quality data.

In a nutshell, marketplace curators stake tokens as a collateral to the quality of data supply and demand. The Weeve network protocol allows marketplace participants to challenge the marketplace curators by token holders, and in case of loosing the challenge, the deposit is forfeited and divided up as a reward amongst token holders who participated in the challenge process. The Weeve network protocol applies a similar mechanism design to incentivize device owners to attain a high membership standard, making sure the provided data is of economic value (and not a fake data stream). To participate in a marketplace, device owners have to be listed on device registries. Each registry stands for a membership standard, which the device needs to fulfil. Implicitly a registry in the Weeve network serves the purpose of assessing the quality of the data. Candidates must make a deposit denominated in the registrys intrinsic token to be considered for listing. Token holders may challenge the device. If the device is "good" and accepted on the list, the device owner keeps her deposit, and may withdraw it should it desire to leave the registry.

The rationality behind these incentive mechanisms is that devices not meeting the desired membership standards, not generating truthful data, or not following the network etiquette, will avoid a registry application, as this leads to financial loss. Further, marketplace curators are incentivised to provide real supply and demand of quality data, ensure a price equilibrium for suppliers and demanders, and counteract infrigement. Otherwise, they risk the loss of their stake.

2 Weeve Network

Weeve's vision is to empower the Economy of Things where IoT machines (or weeves thereof) index, process and trade harvested data against digital assets, most notably crypto coins. We envision public or private marketplaces for any form of digital asset ranging from geo-data to electricity or delivery status, where data producers and consumers (resp., buyers and sellers) come together, escrow their supply and demand, and fairly exchange their digital assets for agreed upon prices.

2.1 Network Design Goals

The Weeve network aims to establish inter-device trust and cultivate emergent standards to enable the creation of hiqh-quality marketplaces for fair trade of valuable assets between IoT devices.

2.1.1 Quality of Data

The primary goal for the network is to ensure the quality of data on the marketplace. Data quality can be quantified through the reputation and authenticity of the entity generating the data, measures monitoring and safeguarding the harvesting, processing and transportation of the data, or the validation through trusted third parties or a democratically voted quorum. All the quantification mechanisms serve the sole purpose of data attestation, and are an essential tool to the determination of the value and price of data. One of the primary obstacles to mass EoT adoption is the attestation of data. By removing this obstacle, Weeve will enable an Economy of Things dependent on reliable and correct information. By linking devices to attestations of properties such as device ownership, inspection history, and live automated testing results, the network brings the security of service-level agreements. With assurances against fraud in place, market safety improves, allowing participants to confidently transact digitally-represented assets.

2.1.2 Network Stability

When dealing with economics, we must assume players in the Weeve network have perfect rationality[2]. That is, they always act in a way that maximizes their utility and are capable of arbitrarily complex deductions towards this end. Note that a rational player must not necessarily act with a strategy towards the wellfare of the network. In fact, a rational player is selfish, plays unfair, and does not hesitate from betraying its peers. These actions are critical to the network, as they distabilize the network. If the network is not stable, supply and demand will not come up: Buyers will not be prevented from buying fake or overpriced data, and sellers will lack the justification to demand for higher prices.

The Weeve network implements a mechanism design to stipulate a form of equilibrium. In an equilibrium, every player of the network will select a utility-maximizing strategy. The idea underlying 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 with their knowledge and services to the stability of the network. Note that without incentive mechanisms, the network will be subject to unimportant supply and demand, and experience rapid decreases in network activity. On the other hand, the punishment mechanism combats network destabilisation strategies. Destabilizing player strategies in

[2]In contrast to human beings who act sometimes irrationally, the Weeve network consists of machines mostly executing a computational mechanism design. As the mechanism is implemented as a protocol and hardcoded in the device, irrational deviation is unlikely to happen.

Weeve network makes sure participants are disincentivized and result in negative payoffs if they do so.

2.1.3 Decentralized Community-Governed Standards

For a wide-spread utilisation of the network, we must assume that various players irrespective of their underlying technologies (at least in the initial stage of network bootstrapping) connect to the network. By allowing marketplace owners to set the interoperability and credibility standards, the marketplace can self-regulate in a decentralized manner. Technological innovation frequently outpaces regulatory frameworks, so the ability for flexible, community-driven standards is extremely important. IoT devices like any computing device are manufactured by many companies for all different kinds of reasons. In order to allow unrelated companies to build devices that have interoperability, they must follow the same standards and procedures. By (cryptographically) securing these standards, device operators have an economic incentive to follow the same standard so competitive devices can be listed on the same marketplace. Governance is used to decide relevant membership standards and to revise them over time. By further empowering the actual users of standards to determine the future state of their own standards, Weeve network participants will enjoy shorter feedback cycles for proposals, group deliberations, and implementations, as standards emergence would occur in smaller fast-moving marketplaces as opposed to the large catch-all international standards bodies of today. As a positive side-effect, the flexible and contemporary adoption of standards contributes to the gradual increase of the data quality and network stability.

2.1.4 Conflict Resolution

Disputes are a common scenario in trade economies. Consider, for example, a dispute between a buyer and seller where the buyer claims they have not obtained the good and service as contracted. When it comes to dispute resolution, there are three basic types. The goal of mediation is for a neutral third party to help disputants come to consensus on their own. Rather than imposing a solution, mediation works with the conflicting sides to explore the interests underlying their positions. In arbitration, a neutral third party serves as a judge who is responsible for resolving the dispute.[3] The arbitrator analyzes the relevant evidence, then renders a binding decision. The most familiar type of dispute resolution, litigation typically involves a defendant facing off against a plaintiff before either a judge or a judge and jury. The judge or the jury is responsible for weighing the evidence and making a ruling.

Weeve network participants will take advantage of arbitrators for dispute resolution, in case an automated consensus is unreachable, for example, a dispute resolution protocol. We remark that dispute resolution can occur with aid of litigation as well. Blockchain technologies provide an appealing infrastructure to implement distributed litigation and the Weeve network will leave this possibility open for future work.

[3] e.g. `https://jury.online/arbitration`

2.1.5 Blockchain-Agnosticism and Micro-Economy Interoperability

In the spirit of real-world economies, the economy of things constitutes in fact various micro-economy, each being the space for a particular asset. For example, we will witness the fostering of micro-econonomies for tokenized energy. Other micro-economies will deal with geo-data. What the micro-economies distinguishes are the requirements on the choice of the blockchain technology in terms of throughput, scalability, or transaction costs. For example, an energy speed trading micro-economy demands high throughput and low transactions costs from the underlying blockchain in an permission-less environment, while a toll payment setting might already work with an enterprise blockchain. The point to stress here is that *use cases define the right choice of the blockchain*. They vary from case to case. To prevent a limitation of the Weeve network, a goal is blockchain agnosticism: Micro-economies determined by the marketplaces they comprise support the Blockchain technology that suits best the use case, its customers or legal and technical requirements. In the Weeve network, each micro-economy will support its own blockchain technology, running on top of the marketplaces.

Blockchain agnosticism implicitly gives raise to and necessites a second sub-goal. When micro-economies arise it is essential to support cross-economy interaction. A car paying tolls will want to pay for the charging of energy as well. To broaden the application of the Weeve network, micro-economies and the affiliated marketplaces need to connect, interact, and bridge the token barrier through interoperable interfaces. The latter property makes the Weeve network approach interoperable with other blockchain-enabled networks and their own token models and protocols. The tremendous advantage here is that cross-network applications and services are integratable.

2.2 Network Participants and Node Curators

At a high level, we consider a finite set of nodes $N = \{1, ..., n\}$ who are connected to the network (or graph). A network is a pair (N, g), where g is a set on the nodes. Let g denote one of the standard ways networks are represented: by their adjacency matrices as well as by listing the pairs of nodes that are connected. Each node represents a player (or set thereof) in the network who owns, controls or curates the node.

2.2.1 Nodes

Each node in the Weeve network abstracts one of the following basic functions illustrated in Fig. 2:

Device Node is the source and/or recipient of digital assets. In the most simple form, a device node is an Internet of Thing with the purpose of supplying or demanding assets. In general, it is any computing device offering resources to or demanding resources from the Weeve network. Sometimes we will refer to sellers as devices supplying assets, and to buyers as devices demanding assets. An asset is any form of tokenizable data with potential value.

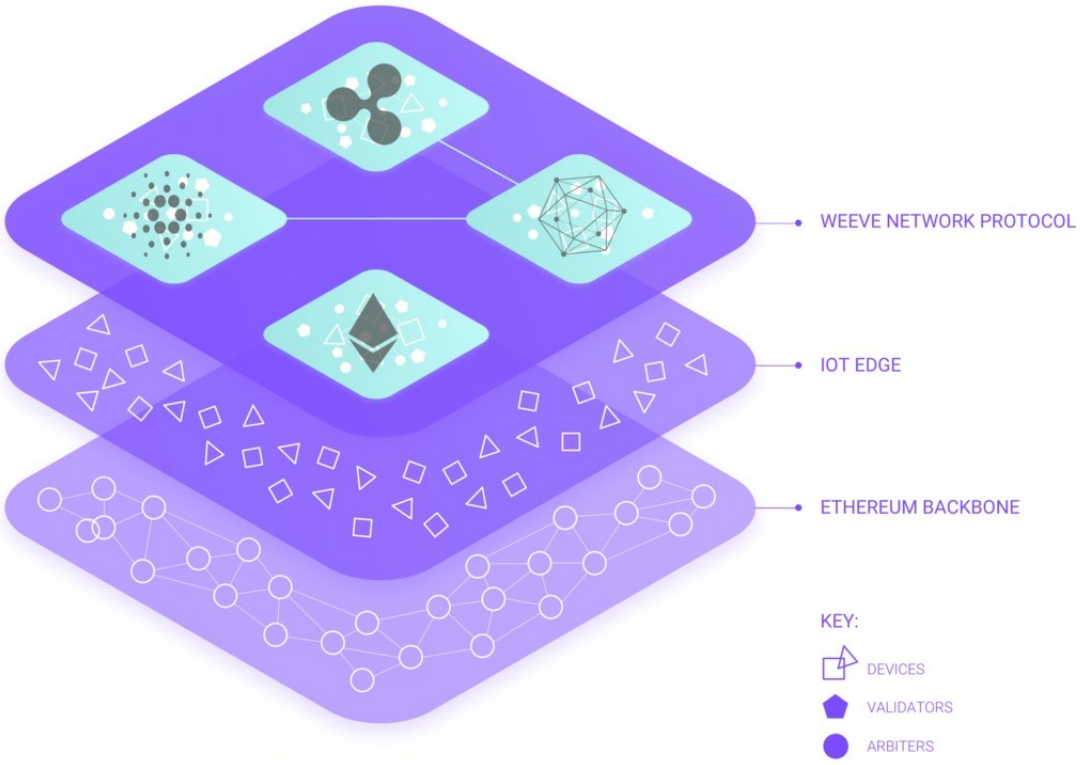

Figure 2: Weeve Network Model in the Context of the Economy of Things. Micro-Economies consist of Marketplaces, IoT devices, Registries, Arbiters and Validators. Each Micro-Economy may use its own (permission-based or -less) Blockchain technology and the Economies interoperate through Bridge Technologies.

Registry Node manages device ownerships and properties. Te function in the Weeve network is to enable the identification and classification of devices. A registry is a listing of devices conforming to certain membership standards which assert criteria such as device identity, device owner identity, compatible protocols, transaction strategies, and device capabilities.

Marketplace Node is a gateway to economic activity. A market is a medium that allows buyers and sellers of a specific good or service to interact in order to facilitate an exchange. The goods and services in the Weeve network primarily center around tokenized data.

Validation Node has a verifying function in the Weeve network. The task of a validation node is to support device registry and marketplace nodes in the device classification. Validation nodes are auditors that do assess and certify device properties in correspondence of membership standards. They scrutinise the device's marketplace suitability.

Arbitration Node serves the purpose of dispute resolution in the Weeve network.

We remark that we leave open to amend in future the network with additional functions. See Section 5 for some initial ideas.

2.2.2 Curators and Governance

Nodes cover essential functionalities of the Weeve network. In practice, each of the above nodes is owned, curated and orchestrated by a physical or legal entity. The entity may be a private person, an enterprise, a government, a non-profit organisation or any subset thereof. An entity may not only be implemented through actions taken by the legal person, but also through a smart contract, Web server or any other programmable interface. The flexible approach allows for a spectrum between full centralization and full decentralization: enterprises may wish to fully control their nodes while communities or consortiums may desire a more equitable approach. Details of the governance system are left to the implementation of the node, subject to the agreement of the curator(s) of the node. For ease of presentation, we assume the Weeve network consist of the following primary curators, summarized in Fig. 3:

Registry owners operate device registries and define a community standard to assess the reputation of device owners and the criteria supporting the listing of their devices. Those criteria may range from soft facts like deposit amount, history of previous registries, reputation of the device manufacturer to hard facts like a unique cryptographic ID, support for hardware/software with high-security guarantees, such as for this purpose developed weeveOS[4]. They also define the criteria for banning a device from the registry as well as a protocol for solving disputes with aid of validators and arbiters.

[4] `http://www.github.com/Weeveiot/WeeveOS`

Device Owner: Transact on the network for a fee.

Registry Owner: Propose and maintain acceptable registry rules, such as membership standards, registry fees, and validation criteria and arbitration policies.

Marketplace Owner: Propose and curate acceptable subscription rules, such as device standards, registry fees, validation criteria and arbitration policies.

Validator: Assess and enforce membership standards for a fee.

Arbiter: Resolve disputes for a fee.

Figure 3: Summary of the Key Players in the Weeve Network

Device owners wish to use the Weeve network by joining device registries being a prerequisite for marketplace participation. A registry is a means to look up the properties of a device and relate the device to its owner. To join device registries, device owners must ensure that their devices meet the membership standards put forth by each desired registry. To become listed, a validator appointed by the registry needs to evaluate the membership suitability.

Marketplace owners curate marketplaces. Similar to registry owners, they define the define the quality standard of the assets traded through the marketplace. To this end, they define the criteria supporting the listing of devices and the evaluation of the asset devices supply and demand. They also define the standards for dropping devices off the marketplace, and the set of eligible arbiters to solve disputes between devices or competing marketplaces. Apart from the device management, marketplace curators agree upon the parameters to setup the market, including for example, the type of tradabale data, the pricing mechanism, the fee model subject to their business model (e.g., per device, per transaction) and the payment method.

Validators are appointed by device registries and check for adherence to membership standards. Their role is to ensure only devices that are trusted and of high quality can transact in marketplaces. The Weeve network delegates the appointment of validators and their processes to the registry owners.

Arbiters adjudicate disputes which inevitably arise in distributed networks. Device registries or marketplaces authorize arbiters to resolve disputes on specific transaction types, and in the case of inter-registry transaction types, all registries involved must have a common set of arbiters for that transaction type to support disputation.

It is worth mentioning that network curators range from single private persons to any alliance of legal entities. Specifically, in some cases a single entity may take different curator roles. For instance, a car manufacturer may not only curate cars, it may also run a registry for the cars. This way, car manafacturer can register to different marketplaces, such as parking

lots owned by different operators, as long as the cars meet the marketplace membership standards. We refer the reader to the use case paper for additional discussions [1].

3 Weeve Network Protocol and Token

3.1 Mechanism Design

Mechanism design is a field of economics dedicated to the study of mechanisms to (dis)/incentivize actions. Blockchains bring home the idea that through cryptography and properly-aligned incentives we can design secure consensus protocols. However, Blockchains have by far a higher meaning, whose utility for designing (security) protocols and applications has not been explored to its full magnitude and purpose. The Weeve network considers Blockchain as a base layer protocol which not only provides the technological basis for transferring coins from one account to another, or more generally, speaking to store an entry in a fully distributed, permission-less database, but also readily provides an infrastructure for incentive-based protocols.

3.1.1 The Principles of Token-Curated Decisions

A Blockchain underlies the idea that tokens have utility and the increase of token quantity is widely accepted as reward whereas the decrease of token quantity is seen as a penalty. One can use the reward mechanism to incentivize "good" actions and the punishment mechanism to disincentivize "bad" moves. Although simple in its execution this mechanism lays the foundation for *cryptoeconomic incentive designs*, among them being proof-of-stake based consensus protocols like Casper apparently the most prominent applications. The key idea can be described as follows: Players stake tokens to backup their actions and the protocol allows to challenge the player's action (and thus her stake). A bit more concrete, the protocol consists of locking the stake, announcing the challenge, and initiating a community voting where each voter pays for a vote in the number of tokens proportional to the stake. The winning voters share the reward proportional to the stake of the losing voters.

3.1.2 Quadratic Voting and Why a Majority Stake Holder does not Rule the Network

The previously described (voting) protocol is an example for a token-curated majority decision. The norm of one-person-one-vote with majority rule treats token holders fairly by giving everyone an equal chance to influence outcomes. However, in some decision problems a majority rule is not the right choice as it may notoriously result in tyranny of the majority. Some voters may not be able to participate in the protocol, as they cannot afford the number of suppositional tokens. Specifically, when the wealth expressed in tokens is unequally distributed, a large number of token holders who care only a little about an outcome prevail over a minority that cares passionately, resulting in a reduction of aggregate welfare.

Quadratic voting is the most important idea for law and public policy that has emerged from economics in (at least) the last ten years. Each voter can buy votes for, or against a proposal, by paying tokens the square the number of votes that he or she buys. The stake is then returned to voters on a per capita basis. Weyl and Lalley prove that the collective decision rapidly approximates efficiency as the number of voters increases [2]. Weyl further proves that quadratic voting is quite robust to collusion, fraud, and irrational voter behaviorsome properties majority voting does not provide [4].

The Weeve network considers quadratic voting (or variants thereof like cubic or exponential voting) as an essential tool in token-curated decisions, specifically in economies where a uniform token distribution is improbable. This is the situation when stake holders like enterprises or industry alliances hold a significant amount of the stake; in the most extreme case they hold more than 51% of the total token supply of the voters.

Curators of the Weeve network are left with the choice of selecting the voting rule that best suits their community and their understanding of a democratic decision process in order to avoid a tyranny and a meaningless voting outcome.

3.1.3 Incentivizing the Generation of High-Quality Data

The Weeve network aims to encourage device owners to manage their devices with much care and diligence. Devices are the source of the Weeve network. Recall, they are the producers and consumers of digital assets and the engine of supply and demand. Device owners have a intrinsic incentive to join the Weeve network: Producers are interested in profit-making whereas consumers are looking for assets. Marketplaces address these motivations in exemplary manner. To facilitate the operation of marketplaces and generate data traction, the Weeve network is comprised of marketplaces with different asset topics (e.g. geo-data, temperature), data quality and requirements that the devices need to fulfil in order to par.

The axiom of the Weeve network is that device owners need to register their devices with a device registry meeting the membership standard of the marketplace. Note that when the device is listed on a registry, it may connect to all marketplaces supporting the registry standards or a subset thereof. The design decision here is to facilitate the enablement of cross-marketplace device interconnection. Devices shall access and interact with marketplaces having similar standards. This makes the whole concept more general and powerful.

Device owners thus desire the consideration to be listed on high-quality registries. They are allowed participation in high-quality marketplaces where digital assets are expected to be traded at a higher price in contrast to low-quality marketplaces. To become a member of a registry, device owners take part in a token-curated decision. That is, they stake tokens, per device, subject to the membership standard and registry policy.

Validators take part in the voting and it is up to the registry policy to nominate validators. Depending on the type of the registry, validators can range from distinguished entities to any token holder including the registry owners. Validators have the purpose to test the device's compliance with the registry's membership standard. Their incentive to engage in token-curated decision is twofold. First, they receive a fee from the voting, which amounts to the share of the forfeited deposit. Second, validators desire to keep demand for the token

they hold high, as this increases its price. This happens if validators assure a stable network with high-quality registries and devices.

Device owners will not apply to a registry if they believe they will be rejected, as this would result in a financial loss for them. In case of rejection, its deposit is forfeited and divided up as a reward amongst token holders who participated in the challenge process. If they are accepted, their deposit is locked, but may be withdrawn at any time the device owner wishes to leave the registry.

3.1.4 Incentivizing High-Standard Device Registries

Device registries play a crucial role in the network. Much emphasis was put in the mechanism design of the Weeve network to cultivate meaningful device registries, as a registry with (many) bad devices harms network stability.

For the creation of registries, owners are asked to deposit a stake proportional to the number of registered devices. In general, any token holder can cast a registry. As high-quality registries require a significant amount of tokens, registries are firstly, an instrument for enterprises or alliances of token holders. As in larger interest groups decisions are made in a democratic way, the expectation is that the majority of registry owners will outnumber bad curators. To further motivate the owners to orchestrate "good" registries, their stake is used as a collateral in token-curated decisions.

Registry owners can be challenged by marketplaces entangled with the registry in case there is evidence for a membership standard violation. In its simplest form, a membership violation happens when a registered device turns out to produce counterfeited data. In practice, marketplace owners have to specify more general violation terms. Further token holders, including registry owners, may announce to challenge other registries. The rationality here is to prevent any form of infringement. Suppose any form of device or data plagiarism, such as brand theft, trademark counterfeiting, and patent violation occurs caused by a "bad" registry. The ability to challenge the registry disincentivizes owners of the counterfeit registry, as this would result in a financial loss of their stake.

It remains to reason why curating a registry is appealing, as owners may risk to lose their stake. Registry owners set the bar when it comes to the enforcement of membership standards through the acceptance and rejection of device applications. Their incentive is to contribute to the quality of the Weeve network, as this keeps demand for the token they hold high and increases its price.

3.1.5 Incentivizing the Curation of Fair Marketplaces

Given the fact that marketplaces earn a fee for every successful trade of digital asset, subject to the marketplaces business model, the opportunity of revenue is an obvious motivation to manage and orchestrate marketplaces. To operate a marketplace, marketplace owners stake a deposit. The stake is a safety deposit and used in a token-curated decision to incentivize the owners to ensure fair trade. Devices exchanging digital assets may challenge the marketplace in case of dispute. A malign marketplace may emulate the availability of

Incentives: The WEEV token encourages positive network actions.

- Device owners stake tokens to register a device on the device registry
- Registry owners stake tokens to create a new device registry
- Marketplace owners stake tokens to create a new marketplace
- Used for payment of fees to validators and arbiters

Disincentives: The WEEV token discourages defecting network actions.

- Collateral to punish offending devices exploiting network resources
- Collateral to punish offending device registries degrading the quality of the network
- Collateral to punish marketplaces conducting any form of infridgement

Figure 4: Overview of the WEEV token rationalities

high-quality data, but in fact, offer low-quality data from devices not meeting the proposed membership standard. Likewise, a bad marketplace may not maximize the utility of supplier and demanders, resulting in a non-justified price for the traded asset. In this case, the device or device owners may announce a challenge against the marketplace using its stake as collateral.

It is important to note that staked tokens are locked and unusable during the staked period even for the Weeve network. The protocol will not allow any entity to use these tokens even the Weeve network. In order for anyone to gain access to these collateral tokens, one would need to buy 51 percent of the 1 billion tokens in circulation and gain access to the protocol, this being a highly improbable scenario (Section 3.1.2). The reason it is highly improbable is once the other users on the network know that an intentional centralization of the Weeve network is taking place (which can be easily done through a virtual public announcement), there would be no incentive to remain on the network. In such a scenario, all honest users would unlock their stake, switch to the forked network, which would become the new Weeve network, and thus, render the original network worthless. If there would be no users on the centralized dishonest network, the incentive for any entity to gain access to the protocol would be close to 0. In essence, any dominating player would be spending a lot of Weeve tokens to gain control of a potentially useless network as once it has gained majority access, the honest system would just switch to a forked one, rendering the whole initiative useless in the first place.

3.1.6 Weeve Token and its Necessity

The Weeve token (WEEV) is the native token of the Weeve network and necessary for the operation of the network protocol. It has a fixed supply with no built-in burning functionality. Its main functions are summarized in Fig. 4. The WEEV token is necessary to the network so

that participants are held accountable for their actions and therefore aligned in the long-term. A network with high quality participants and authentic transactions has higher intrinsic value, and this should be reflected in the tokens value, and vice versa. If, for instance, Ether were used instead of WEEV, then the Ether network value would likely vastly overshadow that of the Weeve network. This would mean that there would no longer be long-term incentive for participants to actively improve their own network, and no long-term incentive for participants to prevent the destruction of their own network through negative activities such as speculation. Put in other words, Ether or any related token does not reflect the dynamics of the Weeve network. There might be situations where fluctuations of the Ether price are completely orthogonal to the performance of the Weeve network. The WEEV token decouples from the fluctuations and gives token holders a fair and reliable tool to assess the value of the network.

3.2 Weeve Network Protocol

The Weeve network protocol, see Fig 5, specifies the high-level participation of nodes on the Weeve network and the integration of third party services. Each device registry and marketplace owner stakes the WEEV token as collateral. The enforced rule of thumb is that the more value the owners wish to conduct, the more collateral is required as a safety deposit subject to validation and arbitration (details follow). Each function in the protocol attempts to increase interoperability, create trust, or both. To increase interoperability, the protocol specifies membership standards, transaction types, listing of devices, listing of transaction history, and the brokering of new transactions. These components provide enough information and tools to negotiate a shared transaction type, commit the new transaction type, and initiate transaction requests with responses.

For bootstrapping trust, the protocol specifies validation guidelines, access to activity logs, listings of validators, and dispute resolution mechanisms. These items allow registries to provide reasonable guarantees that the transactions will be genuine and free of errors.

The Weeve network protocol does not aim to solve data fraud directly; it simply allows individuals and marketplaces to agree on what defines trustworthiness and where to draw the line.

3.2.1 Membership Standards

Specification of membership standards should prioritize:

- Human-friendly specifications and reasoning
- Standard general structure and sections
- Accessibility for relevant parties
- Technical details for conforming implementations when applicable, such data structures
- Simple formatting

- Updated author contact
- Dates, times, and document update history

Due to the overwhelming number of possible device registry types, no single best format for specification of membership standards is currently known, but one or more workable standards should emerge as experience is gained. Conversations with prospective IoT partners across industries have revealed wildly different requirements for membership standards, adding further credence to the IoT interoperability dilemma. For this matter, it is best to avoid overprescription in the face of uncertainty.

Digital documents containing membership standards for a registry may be quite large, such as when containing attachments for technical details and specifications with embedded data tables. Therefore, membership standards should be housed off-chain with on-chain entanglement, such as on an IPFS[5] cluster or a decentralized, immutable storage provider.

Changes to a registry standards must be legitimized by the device registrys governance criteria and immutably logged for registry members and marketplace members to review. A similar set of standards should be applied by marketplace creators. It should be restated that membership standards will vary drastically depending on specific device registries and marketplace creators; a device registry for connected tea kettles does not require the same intense membership standards as a registry for military equipment.

3.2.2 Validation and Arbitration Guidelines

As companion documents to the membership standards, validation and arbitration guidelines are provided by registry and marketplace owners as assessment tools for validators and arbiters that have been appointed. Validation guidelines, which may be seen as an auditing standard, serve as the contract of work between the registry/marketplace and its validators, outlining such agreements as automated assessments (e.g. through a remote attestation protocol [3]), manual assessments (like inspecting the hardware), timelines, acceptance criteria, and dispute resolution for validators. Once a device has initiated its request to a marketplace, these validation guidelines serve as a source. A similar mechanism purposes the arbitrations guidelines as well. They essentially allow to specify the arbiter in case of a dispute and make use of function interfaces similar to that of validators.

These guidelines should be similar in structure to the U.S.-based FedRAMP Program assessment templates[6] and guidelines, which are for example used by the U.S. Federal Government to provide the industry with a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Additionally, the programs website provides a list of authorized assessors, just as each device registry maintains lists of appointed validators. Validation guidelines should prioritize:

- Human-friendly guidelines and reasoning

[5] `https://ipfs.io/`

[6] `https://www.fedramp.gov/templates/`

- Machine-referenceable document anchor points to support automated checking and digital reporting formats
- Accessibility for validators and arbiters
- Technical details for conforming implementations when applicable, including source code or third-party services used for assessment
- Machine-referenceable document anchor points to support automated checking and digital reporting formats
- Checklists and grading rubrics for desired validations
- Qualitative and quantitative feedback including overall alignment with membership standards, notable strengths and weaknesses, applicant history with respect to membership standards
- Updated author contact information
- Dates, times, and document update history

3.2.3 Activity Logs

Registry and marketplace owners are encouraged to keep transaction activity logs for events that occur on the registry and marketplace. Arbiters may wish to access a subset of activity logs to resolve disputes with the relevant data. If an arbiter attempts to resolve a dispute and the transaction activity logs of one party are missing, the arbiter is likely to rule in favor of the party presenting evidence. Therefore, marketplace owners are inclined to keep good records to improve their dispute outcomes.

Specifically marketplace owners may wish to check the relevant transactions activity logs of their transacting parties to ensure consistency and correctness of transaction histories or device validations. These are also helpful in a challenge phase when assessing the trustfulness of a device. Activity logs should be at least filterable by:

- Dates
- Activity Type
- Participant IDs

It is strongly encouraged that the following events produce detailed log entries:

- Governance changes
- Change proposals and references
- Voting outcomes

- Transactions
- Changes to membership standards
- Changes to validation guidelines
- Changes to transaction types
- Changes to device listing
- Changes to device metadata

In some situations or countries, privacy of activity logs may be relevant. In which case, the Weeve network will suggest privacy enhancing technologies, such as multi-party computation or functional encryption, to comply with the data privacy regulations.

3.2.4 Transaction Types

Registry and marketplace owners will have the ability to specify transaction types via RFC-style documents, libraries, and example code. These transaction libraries should log relevant data for dispute and arbitration purposes in the activity log. This requirement enables arbiters to have the relevant facts when determining case outcomes, and is essential for a safe marketplace.

Membership standards may include requirements that further foster device interoperability, such as device URIs, transaction-specific protocol support, service endpoints, data storage providers, data measure units, and more. These requirements serve as the foundation that enable cross-device exchange, be it simply raw data or more complex transactions such as auctions, price negotiations, and advanced querying capabilities. Membership standards give transaction types a basis on which to depend.

For determining transport layers in transaction types, device registries are encouraged to utilize the MQTTS protocol[7], specifically designed by the Weeve team, which supports base IoT secure device communications such as addressing, session management, data transfer, and confirmation. For determining payment layers in transaction types, device registries are encourage to utilize fair exchange protocols[8], which support supply-demand escrow, price negotiation, and delivery acknowledgment. Other service layers may added to the transaction types in the same vein.

Per transaction type, the registry and marketplace owners may specify parameters related to the arbitration process, wherein one or more parties dispute a transaction and require a resolution. These parameters include, but are not limited to:

- Dispute time windows
- Minimum and maximum dispute amounts

[7] cf. Section 2.2, `http://papers.Weeve.network/Weeve_whitepaper.pdf`
[8] cf. Section 2.5, `http://papers.Weeve.network/Weeve_whitepaper.pdf`

- Resolution guidelines
- Arbiter selection guidelines
- Choice of modular arbitration system

3.2.5 Transactions

Every transaction must have a unique transaction identifier, a unique device identity, a transaction type, and corresponding transaction metadata recorded and authenticated or attested on-chain. This requirement ensures that, in the case of disputes and arbitrations, transactions are considered as atomic, and are accompanied with the best-possible data about the transactions, and their participants, and the way they interacted that led to the dispute. Transactions without on-chain records will not enjoy full protections from the Weeve network in the event of a dispute.

3.2.6 Metadata Interfaces

Metadata for devices and transactions can and should be represented in a variety of formats, including JSON, XMLS, wire protocols, and binary blobs depending on its use case. For example, metadata formats used for high-frequency trading machines may require far more compact data packing than formats used for highway toll booths. Therefore, it is unreasonable to require any particular metadata representation format. However, for sake of interoperability, there must be at least one common way to access these metadata. Therefore, the registry and marketplace will require basic listing, filtering, creation, and access functionalities to be made available to smart contracts. These requirements will initially be implemented as an interface specification for smart contracts, and they will incorporate authentication and authorization components as well.

3.3 Weeve Protocol Interface

A Weeve node may be implemented using a variety of underlying technologies, from centralized servers ran by traditional enterprise companies to fully-decentralized smart contracts governed by a community of IoT device enthusiasts. This flexibility allows many groups of diverse people to trade, whether they are large corporate entities, or very involved individuals. A smart contract implements the protocol interfaces which satisfies several function signature requirements, as described at a high level in the sections below (Fig. 5).

In short, each node must implement functions that support:

- Staking and unstaking to the Weeve network smart contract (Staking and unstaking would be at multiple levels, i.e. registry, marketplace etc. for devices wishing to take part in the Weeve network)
- Retrieving membership standards

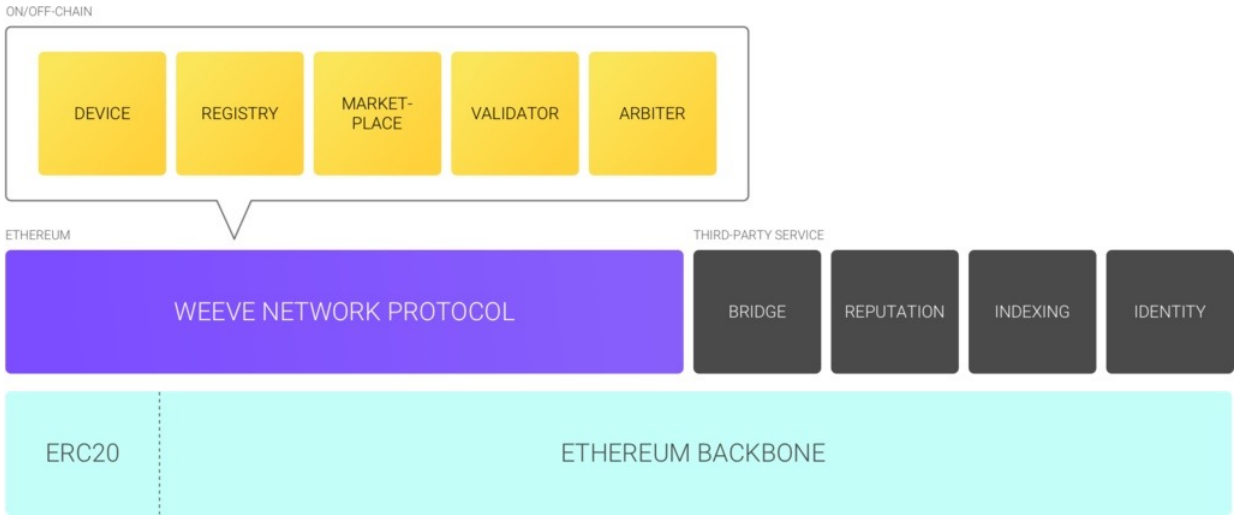

Figure 5: Weeve Protocol Interfaces: High-Level Overview and Extensions to Third Party Services like indexing, reputation system, identity management and other (bridged) Networks

- Retrieving validation guidelines
- Retrieving supported transaction types
- Querying activity logs
- Listing devices and metadata
- Listing transaction history and metadata
- Listing validators (Registries & Marketplaces)
- Listing arbiters (Registries & Marketplaces)

3.3.1 Listing and Delisting

Prospective owners may stake a significant amount of the WEEV token, proportional to their anticipated desired transaction volumes, number of devices listed etc. (mechanism is left open for now to let the system have flexibility) to create a new device registries and marketplaces, respectively. As part of the creation process, the stake must be placed through the device registry (resp. marketplace) containing at least one initializing device conforming to the membership standards, in demonstration that the standards are indeed attainable. Recall, we need stakes from registry owners to prevent offence between registries. Using game theory incentive mechanisms, no registry creator would have the incentive to game the system or take it away from its honest state without facing the risk of losing its stake and being recognised in the system as dishonest. This mechanism of staking is deeply embedded

in the system at all levels, ranging from registry creation, marketplace creation to device listing in registries and marketplaces.

If the initializing device is delisted with no other valid devices on the registry, the device registry (resp. marketplace) stake is freed, and the owner may then destroy the registry (resp. marketplace) by withdrawing the stake. The Weeve network may eventually implement a garbage collection process whereby registries and marketplaces are required to pass simple liveness checks to remain in good standing. The initializing device has no special status on the registry (reps. marketplace) past serving as the initial demonstration of attainable membership standards. These staking and demonstration measures are intended to discourage the creation of low-quality nodes on the Weeve network, and to facilitate their removal.

Initially, all new registries will be subject to approval by the network-elected validators members of the Weeve foundation to protect the nascent ecosystem from pollution, but the projects long-term goal is decentralized community-driven governance, possibly mimicking the applicant-challenge systems of certain nodes themselves.

3.3.2 Retrieving Membership Standards

A node must be able to access the membership standards of other registries. Therefore, any node must support querying from the network. In the implementation of the interface, the function returns signed membership standards in order to authenticate sensitive data.

3.3.3 Retrieving Validation Guidelines

Just as with membership standards, a node must also be able to access validation and arbitration guidelines of other registries/marketplaces. In the implementation of the interface, the function is passed a signed registry and device origins to allow any appropriate restrictions on returned validation/arbitration guidelines as to protect sensitive data.

3.3.4 Retrieving Supported Transaction Types

During registry creation, the registry owners may specify the types of transactions the registry supports, including per-transaction-type protocol details such as calling conventions, timing, price calculations, relevant data structures, and delivery requirements. These transaction types must be made available for listing via an interface implementation and may be protected with permission controls.

3.3.5 Query Activity Logs

Activity logs are an avenue for device registries and market places to provide transparency to prospective marketplace creators. By providing an interface that exposes validation records and governance history, a prospective marketplace may have more certainty that a device within the device registry will deliver as promised.

3.3.6 Listing Devices and Metadata

Devices and their metadata may be made available upon request. The device listing function in the smart contract is used by registries and marketplaces to find other devices. All queries may be authenticated and authorized by each device registrys security system.

3.3.7 Listing Transactions and Metadata

Transactions and their metadata may be made available upon request. The transaction listing function in the smart contract is used by other devices to check historic transactions and reference other ones. All queries may be authenticated and authorized by each device registrys security system.

3.3.8 Listing Validators

Registry owners may appoint validators to fulfill the validation criteria for membership standards. This may be a combination of automated and manual tasks. An interface must be exposed to provide a list of active validators.

3.3.9 Listing Arbiters

Registry and marketplace owners may appoint arbiters recognized as a fair and independent third party to resolve disputes. An interface must be exposed to provide a list of active arbiters. These lists contain metadata such as account information, and they are used to authenticate and authorize arbiters to view certain activity logs across Device Registries. This serves the purpose of dispute resolution.

4 Disputes and Arbitrations

Arbitration becomes necessary when at least one party of a transaction opens a dispute. The dispute initialization should automatically collate all relevant transaction details stored on or off-chain, and collect additional data from the transacting parties as necessary. Disputes over human-originating transactions must receive different treatment than disputes over machine-originating transactions. For example, dispute resolution for millions of millisecond-paced device transactions may require aggregation, analysis, and deliberation by human agents, similar to e-discovery processes undergone by enterprises in litigation.

For example, in a marketplace for electric vehicles seeking charging stations, the membership standards may require the electric vehicles to take snapshots of the vehiclebattery charge, mileage, tyre pressure, etc. This data might be used to determine if an electric vehicle received the full amount of charge it was granted, with corroborating evidence against tampering. This way, arbiters are fully equipped with the best information available to come to a decision.

4.1 He Said, She Said

As in existing multisided platforms, a reputation system may be utilized to help resolve disputes in the event of differing unsubstantiated accounts of an event. Reputation systems are out of scope for the Weeve network Protocol, but are possible and encouraged per device registry or across them.

4.2 Storage

Initially, each device registry and marketplace will provide facilities to access, store, and manage data structures for purposes of disputes and arbitrations. In the long term, support will be implemented for decentralized registries of validators and arbiters that may cross validate to similar domain, or rely on a decentralized service that provides validator management (kleros, delphi, etc.).

4.3 Third-Party Services

Several projects in the blockchain ecosystem are already working on open and fair systems for adjudication, including Delphi and Kleros, and effort has been made during smart contract implementation to support full compatibility with these pluggable arbitration services at the behest of the registry and marketplace owners. Many of these services still require the legitimate appointment of fair arbiters, so in these cases, arbiter selection shall remain the responsibility of the owners. Additionally, variables related to arbitration such as dispute time window, dispute minimum and maximum amounts, and arbiter fees are already set by the owners in the transaction types.

4.4 Cross-Registry Arbitration

For arbitration across multiple registries, arbiters certified by all participating registries and marketplaces for specific transaction types may be permitted to arbitrate corresponding disputes for a fee. In the future, we may imagine multiple arbiters each representing their registrys interests to come to consensus, not unlike claims adjusters of today.

5 Auxiliary and Future Functionality

Just as application layers reside on top of session layers in the OSI model, important services to ensure network stability may exist using primitives provided by the Weeve network protocol. The following sections describe features that are **not** part of the Weeve network protocol, but are deeply interconnected and we consider their integration as a viable enrichment of the network in future.

5.1 Listings of Device Registries and Marketplaces

Device registries and marketplaces may be listed on the Weeve platform and eventually tagged with attributes such as geography, registry type, and publicly-available membership standards. Assessment and approval of listings may initially include all staked device registries that opt in, but in the long term, the final say on this activity should be left to the community. It is possible to use a device registry to contain membership of other registries, but this recursive structure is complex and deemed out of scope for the initial smart contract implementations. These listings will become available to the relevant parties through a website maintained by the Weeve platform, and eventually also through dApps as ecosystems such as Blockstack[9] reach maturity. Sign-in via cryptocurrency wallet will be supported, as to allow permissioned access to listings of device registries.

5.2 Reputation Systems

Reputation systems ensure market safety by letting marketplace participants know with whom they are transacting. They are important constructs that do much to enable new forms of trade. Therefore, the Weeve network may provide building blocks for the participants to access reputation systems on top of the protocol.

For example, marketplaces driven by human participants will require user interfaces to fully communicate the semantics of a reputation for humans to make better decisions. On the other hand, near fully-automated marketplaces where devices engage in high-frequency trades may use statistical methods to analyze data for algorithmic updates of reputations and automatically rank desirable trading partners without human intervention.

5.3 Intra-Blockchain Transactions ("Bridge")

Blockchains technology is nascent, and there may be many competing blockchains that serve as infrastructure for protocols. The first iteration of the Weeve network will be built on the Ethereum blockchain, but it must adapt to future evolutions or competitors that provide de-facto underlying foundations. Therefore, it is important to take a flexible approach that is reasonably agnostic to the underlying blockchain implementation, as recommended by the notable projects PolkaDot, Telegram, and Blockstack.

To achieve blockchain interoperability across transactions and registries, a marketplace may require its members to adhere to standard specifications of URIs that can represent device registries across different blockchains. Transactions may be forwarded across different blockchains using relay technologies which are rapidly reaching maturity and mass adoption. The primary benefit to the network is the ability to utilize the unique advantages of specific blockchains, such as high-throughput processing or guarantees of anonymity.

[9] `https://blockstack.org/`

5.4 Identity and Management

Identities play a fundamental role in any network. They provide authenticity and enable accountability of the owner. For example, multiple devices may be owned by a single entity. Suppose they tokenize and monetize data, then their earnings shall be transferred to the wallet of the owner. Vice versa, when a device runs short in tokens, the owner of that device shall recharge its device.

Despite the fact that all devices have their own identity and thus their own wallet to engage in the Economy of Things, they are managed by a single entity. Identity management functionalities are an interesting augmentation of the Weeve network that third-party projects like uPort[10] already provide.

6 Conclusion

The IoT industry today suffers from expensive interoperability and security problems. The Weeve network aims to solve this by providing the community with high-quality open-source software including the the WeeveOS—an IoT-to-Blockchain Operating System secure by design—and the Weeve marketplace curation platform. The WEEV token enables a marketplace built on these primitives, open to any participants in the world, and flexible enough to meet the demands of both traditional chain-of-command enterprise companies and proponents of a decentralized future for IoT devices.

With its protocol, the Weeve network tackles tough interoperability and trust problems using membership standards, validation guidelines, and transaction types. The underlying blockchain infrastructure bridges the gap between untrusted parties, and the WEEV token can incentivize safe inter-device trading activity. The Weeve network will enable a decentralized future in which new markets for inter-device transactions will spawn through emergent order at the will of its community.

References

[1] S. Bhasin and S. Gajek. Weeve network protocol: Use cases, 2018.

[2] S. Lalley and E. G. Weyl. Quadratic voting: How mechanism design can radicalize democracy. In *American Economic Association Papers and Proceedings,*, volume 1, 2018.

[3] A. Seshadri, A. Perrig, L. van Doorn, and P. K. Khosla. SWATT: software-based attestation for embedded devices. In *2004 IEEE Symposium on Security and Privacy (S&P 2004), 9-12 May 2004, Berkeley, CA, USA*, page 272. IEEE Computer Society, 2004.

[4] E. G. Weyl. The robustness of quadratic voting. *Public Choice, Forthcoming*, 2016.

[10] `https://www.uport.me/`