The RDDL Network

The physical trust stack for web3

Tom Fürstner

Release 1.3 (2022.06.01)

Table of Contents

1. Abstract

Ever since the first Industrial Revolution, machines have been accelerating the evolution of economic activity, becoming indispensable drivers of progress. While many concomitant technological advancements supported the creation of the **Machine Economy**, each new industrial revolution that transformed it was underpinned by a **key technological enabler**. We argue that **blockchain** plays the same transforming role for the 4^{th} Industrial Revolution that steam, electricity and computers have played for the previous three respectively.

However, for blockchain to be truly transformative, it requires **common standards, common protocols and common processes** that are **mass-adopted within the current and the future Machine Economy**. Over the last decade, blockchain has been embraced at an unprecedented pace in the financial services. Yet, just as the **internet** today is much bigger than **email**, blockchain technology is much more than **decentralized money alone**. Offering machines **unique, incorruptible identities, equipping them with all the necessary tools to communicate and transact securely and autonomously via smart contracts and within incentive networks** will enable hyper-innovative economic models with the mandate to radically change the Machine Economy. To date, blockchain in the machine world has only seen minimal developments. *Even the largest protocols are lacking effective machine onboarding mechanisms or infrastructure.*

The RDDL Network is a blockchain-based protocol, using a **unique Proof of Productivity (PoP)** consensus mechanism that proves identity, data accuracy and utilization for all types of machines. These proofs lead to a robust network from which network participants can launch their own circular micro-economies, and therefore democratize not only their financing mechanisms, but also their ability to properly reward/ incentivize participants of their own economies. The potential applications of the Network are many, varied and highly consequential**, ranging from empowering blockchain technology to interact effectively with industrial machines, creating new investor classes by enabling crowdfunding into specific economies via tokens (which can be swapped in/out of parallel economies), to tokenizing and monetizing machine utilization data, to influencing human energy-consumption behaviors or driving a green new deal agenda**. In this way machine owners, institutional or private investors and consumers can all participate in micro-economies together. Ultimately, these new economies can focus on efficiencies not yet realized using standard technology, such as smart contracts, automated consensus-driven decisions, token distribution & swapping, and removal of intermediaries.

The RDDL Network will provide the **common infrastructure** that will become **foundational across blockchains and industries**, allowing **machines** to participate **directly and autonomously in the economic models** that are emerging with increasing web3 adoption, directly **accelerating** the 4^{th} Industrial revolution, and **laying the bricks for the next major transformation of the Machine Economy.**

Doing so, the RDDL Network and its corresponding Protocol will unlock the next level of potential that lies dormant within our existing, centralized machine-economic models:

- Through tokenization, **unlocking the liquidity** that machines absorb
- Offering financial products such as **loans or micro-investment products** linked to this liquidity
- Develop the **machine data economy** which can accelerate the emergence of smart cities, smart factories, smart supply chains, etc
- Change **production and supply chain patterns**, optimising utilisation and reducing transaction costs
- Accelerate the **adoption of renewable energy** by financing the costs associated with deploying renewable energy generating infrastructure and fully tracing energy patterns
- Advancing up **pay-per-use services** via machines and tokens
- Introducing machine-centric **NFT** propositions and services based around digital twins

With this paper the RDDL Network team aims to provide an overview of the possibilities that lie ahead and the next steps that it will be undertaking. The team explains in detail **the unique physical trust stack for web3 that it has developed** and that is already being used by its industrial partners, and lays out a proposal for a protocol including the tokenomic design to grow the wide adoption of this new crypto-hardware enabled physical trust layer. This paper should be seen as a discussion paper that will encourage the formation of a community around the proposal for a Physical Trust Layer and help challenge and improve the different technical areas covered within this text.

2. The Case for a Physical Trust Layer for the Machine Economy

Since their emergence over a decade ago, blockchain technologies have been providing a real-life solution to the challenge of trust in decentralised systems and networks. While the initial focus of blockchain was on applications in the finance sector, the maturity of these technologies within the **physical world** - including sectors such as **mobility, renewable energy, supply chains, manufacturing, and agriculture,** to name but a few - has been, thus far, underwhelming. Blockchain has the potential to be even more impactful by combining **cyber and physical systems through integration** with Layer 1 infrastructure such as Bitcoin **and Ethereum, and subsequently, any other blockchain layers that are built upon these.**

The hardware, systems, and infrastructure to enable this integration is what the RDDL Network refers to as the Physical Trust Layer

The Machine Economy that is enabled through the Physical Trust Layer and corresponding infrastructure will **drive greater adoption of blockchain in all areas of the global economy** and will accelerate the development of web3 in a mutually reinforcing way.

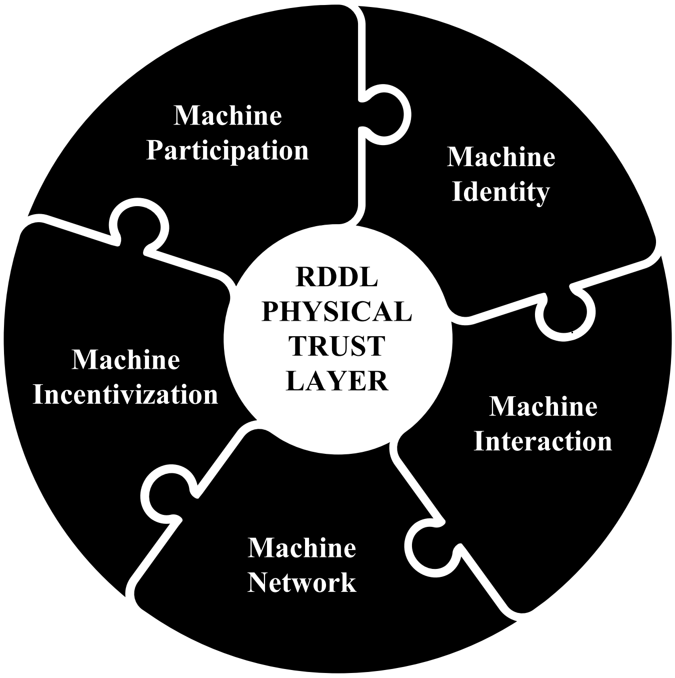
A strong case example for the Physical Trust Layer is in the **automotive industry**. Typical automobiles can have more than 100 built-in sensors permanently monitoring speed, engine temperature and braking processes, and collecting a variety of other data. These same vehicles generate around 25 gigabytes of data every hour. Autonomous vehicles will generate even more – up to 3,600 gigabytes of data per hour. Extracting this value creates several challenges. The obvious one is that the amount of data cannot be processed efficiently with centralized backends. Data must be pre-processed and analysed while only the insight gets transferred to backend systems (for instance, using **AI** computing at the edge). Embedding these mechanisms into web3 workflows necessitates the implementation of machine identities via decentralized identities (DID) and corresponding self-sovereign identities (SSI) to establish **digital twins on the RDDL Network**. Using smart contracts, execution of workflows will be used for automation of regulatory guidance. Reporting and monitoring of required data, the checking of compliances, and approval processes will become foundation of the data made available to data marketplaces in new economies. All the above can only happen with blockchain based hardware infrastructure and the introduction of token economic networks such as the RDDL Network built around its unique **Tracker Wallet** Hardware (TW) and the Physical Trust Layer that these create.

Even though the possibilities appear endless, to date, the RDDL Network is **the only initiative** tackling these problems holistically and proposing **the end-to-end infrastructure** to facilitate the onboarding of all machines into this token economy paradigm.

3. The RDDL Network Design Logic

The fundamental logic underpinning the RDDL Network proposition can be summarised by the five core pillars outlined below:

Figure 1: Fundamental RDDL Network Design Logic



3.1. Machine Participation

The Machine Economy includes industrial machines only, vehicles, machines used in manufacturing or the production of other machines, IoT devices, energy generation facilities (primarily renewable, i.e., solar panels or turbines), batteries, industrial and household robots.

In the current state of the Machine Economy, signals that machines are emitting are can often not be captured fully are lost within the business use cases where the machines are deployed or sometimes simply ignored. Understanding these signals, capturing them for verification, and proving their usefulness without creating data overloads are foundational components to enable the participation of machines in web3 economic models.

As such, each machine that participates in the RDDL Network will constitute a node, taking on several potential roles within this network. Turning a machine into a network node and operating such nodes will be incentivized through RDDL token rewards.

To participate in the RDDL Network, every machine must be extended with a **Tracker Wallet** hardware component built around an ARM 64bit server based on Cortex A5xx architecture as carrier board with the following hardware extensions. The RDDL Network greatly facilitates this process through. Note, there are also hardware servers running independently from any machine. On this hardware, a software stack consisting of software drivers, libraries, protocols and APIs have to be operated.

Table 1: RDDL Network Hardware and Software Prerequisites

Hardware Prerequisites	Software Prerequisites
Network component	Web Server
RF communication component	Wallet API & crypto primitives
Controller area network component	CAN and CAN dbc libraries
Wallet component	Network & modem drivers
Data storage component	Power meter API
Power meter component	Planetmint instance

3.2. Machine Identity

One of the main challenges to enable machines to participate directly in the blockchain economy is the ability to allocate these machines **with a fully secure, incorruptible, blockchain ready identity**. Beyond this, there are several other technology challenges present including connectivity, scalability, energy consumption, and data privacy. To tackle these challenges, the RDDL Network has created state-of-the art **Physical Trust Hardware equipping** the machine with all the necessary tools and capabilities to become an active participant in the envisioned Machine Economy.

These include:

- Secure device layer, Tracker Wallets that integrate hardware wallets, trusted gateways, HSM, secure tags, secure elements
- Secure industrial protocol layer - Confidential CANdbc and CAN FD, ASAM, FlexRay, LIN, TCN, et al.
- AI and Policy Layer – smart, trusted and confidential computing

As all RDDL Network devices include hardware wallet capabilities, including secure elements, all of them are represented by private key- / public key-derived identities. Keys do not have to be brokered to the devices or exchanged between the devices. Instead, they get created and derived via key derivation methods. **The secrets within the secure element never get exposed**. This offers better security than any kind of key exchange mechanism.

3.3. Machine Transactions

All machines connected through the Physical Trust stack and validated in the RDDL Network will be able to send and receive signals and information from and to other machines.

Through the **Physical Trust Layer**, any **machine that fulfils a set of criteria** will receive a hard- and software stack to bring standardized signal data to the web3 economy and generate inputs to data markets in different ways.

This will include:

- Sharing the signal data to existing and emerging data markets and/or other data protocols
- Creation of staking or investment products related to the economic value of the machine
- Validating the output of other machines

3.4. Machine Network

The network will be responsible with providing signed and certified signal data, certifying that machines are working (consuming energy; sending/receiving data streams, etc.), and validating transactions sent by other machines.

The new infrastructure capabilities provided are designed to link a variety of ledgers in a decentralized yet hierarchical fashion, ensuring the integrity of the data gathered. The network design also provides **a secure way to implement oracles as necessary feature for integrating legacy infrastructure and gathering data from available databases** to make it available for blockchain computations, and to securely import trustworthy data from the physical world of machines and sensors.

3.5. Machine Incentivisation

The purpose of the RDDL Network is to enable and incentivise the largest possible number of machines to join the machine economy and unlock the value that lies within these machines. The higher the number of machines that act as nodes in the network, the greater the value of the network. This value will be reflected by the RDDL Token, the network's Governance and Incentive Token. Each machine added to the network can be rewarded with tokens in exchange for participation in the network.

4. The RDDL Physical Trust Layer

The Physical Trust Layer is only becoming possible now as the Bitcoin ecosystem has further evolved with functional additions to its scripting layer via extending its op-codes called Taproot, and with the progress made on second layer and side-chain networks like Liquid and Rootstock. The RDDL network is built on top of these innovations. With these innovations, Bitcoin closes the gap in contractual expressiveness to Ethereum while not giving up its robust and resilient code base. Bitcoin revolutionized the possibilities of the monetary system and ways to manage digital assets. With the extended capabilities of Bitcoin and its side-chains the RDDL Network enables the Bitcoin protocol and its side-chains to manage physical assets the very same way. Bridging back the blockchain world to the world of physical assets, especially machines opens up completely new ways to set up self-driven machine economies thanks to IoT smart contracts, trust anchors, digital twins, machine DIDs, tokenized machines as DeFi collateral, certificate and green bond markets, green power purchase agreements and many more.

The services and applications offered by the Physical Trust Layer are enabled by a multi-token system, including the primary **RDDL Token** (the governance and incentive token) and RDDL Network participant-defined **Asset Tokens** (created by users of the protocol). Machine owners who hold the RDDL Token can generate Asset Tokens, separate, unique, asset-derived tokens (initially, as stable coins) via the services of the RDDL Network. The Asset token enables DeFi based business models for all network participants and turns the machine network into a DAO and the individual machines into Token Economy assets. The value of the Asset Tokens is equivalent to the contribution of the machine owners and operators to the network, offering a stable pricing mechanism for the web3 services built around machine utility. This multi-token design is the basis for creating bridges to any other existing or emerging blockchain projects and creating new token economies based on the underlying assets that have joined the RDDL Network.

4.1. Secure and Trusted Hardware

The **lowest level of the Physical Trust Layer is constituted by the Tracker Wallet technology** built around hardware security modules, secure elements, smart card technology (ISO-7816) and secure hardware enclaves. These hardware devices and components are designed exclusively to work within the Physical Trust Layer and allow for a diverse set of form factors. These hardware wallets act as versatile trusted gateways using Intel's Software Guard Extension architecture as the central processor, to FPGA-extended ARM Cortex M4 units, to RISC-V based microcontroller platforms used for secure field bus systems. The Physical Trust Layer will be integrated into existing industrial hardware as the RDDL Network evolves i.e.: **smart meters and loggers, material and data analytic machines, car data loggers and gateways, smart sensors and actuator systems, valve systems measuring material throughput etc.**

The same technology is used for trust-devices which manage the machine data and configuration access according to user role models. This limits only skilled and trusted operators and traders to configure or change hardware components and contract logic, especially threshold values and data structures that trigger transactions within the RDDL Network.

All devices have unique attributes verifying a device identity and a list of associated device identities that they are allowed to interact and transact with. All inter-device communications are hardened and rely on this device identity's attestation to a blockchain.

Machines use the secure hardware described in this paper (i.e. 3.2) to prove their identities, to assure the provenance of their data and to protect their data while traveling between devices and services. This element is essential when pairing machine identities with the identities of other devices to allow peer-to-peer encrypted communication, transactions, interactions, and governance. A distinction needs to be made between an ordinary blockchain and a domain-specific, i.e. secure, federated industrial blockchain, where access and user role models need to be defined and governed through clear policies. Given the nature of the RDDL Network as a foundational layer representing real world assets in web3, the secure hardware is indispensable in achieving the required levels of security.

The operators not only configure the devices but define which data are of relevance and which algorithms should operate on them to reduce the payload that is going to be sent to blockchain services to trigger smart contract logics and settlements - smart, AI-driven edge computing.

4.2. Confidential Signal Data

To fully exploit the data that comes from a variety of machines, relevant machine signals must be harmonized. They must speak a **"common language"** that unifies any kind of economically meaningful machine signal. For this purpose, **Layer 0x00 uses parts of the Controller Area Network (CAN) specification, specifically CAN DBC, the CAN-bus database: its structure and syntax define precisely the signal**, its value range, its encoding scheme etc.

CAN DBC, also called CANdb, is a protocol derived from the automotive industry. With the ubiquity of the Controller Area Network standard, from automotive to aerospace industries, CANdb is a perfect, universal signal description language, even for domains that are not initially CAN-bus-driven.

The guarantee of **data provenance, signal integrity, relevance and value consistency** to trigger smart contracts serves several network purposes. Realtime auditing and *track & trace* of machine data is possible, reporting of machine capacity and productivity readings can happen fully automatically. Products derived from a machine capacity together with smart contracts allow the autonomous setup and execution of conventional (bonds, loans, options, etc) and decentralized financial instruments (staking, voting, flash loans, etc.)

The Physical Trust Layer solves significant **challenges of token-curated registries, data markets, compute-to-data initiatives and similar ongoing efforts that have only partially been successful to date**. All signals are harmonized concerning their structure and syntax. Therefore, it becomes significantly easier to run Big Data and AI analytics on such signals and data. As the signal data are always encrypted, the data sovereignty of individual persons, companies and institutions stays untouched. Even when data is aggregated to bigger, common data pools, the Physical Trust Layer brings the **efficiency and trust required by data markets to be impactful and relevant**.

4.3. Hardened Communication Channels

Communication within the RDDL Network is hardened. All data and signals within the Physical Trust Layer stay encrypted over their entire lifetime. The encryption and decryption keys, also called blinding keys, are derived from the key material securing the machines' hardware wallets and their identities. Everything follows a machine-identity-address-wallet scheme as blinding keys are nothing else but another hierarchical, deterministic derivation of seeds and base keys forming blockchain addresses and machine identities. The very same secret that is used to enable automated settlement of machine transactions gets used to protect a machine's identity, its data and its signals.

Address identities are pre-attested/ pre-provisioned to machines**, secure EEPROMS inside the machines**, the ledgers, the data, the signals, the algorithms and finally the cloud services and applications monetizing the whole system. In other words, the secure element creates a secret on its own hardware, a secret that is never exposed to the world, which cannot be exported, read, or written. Only the public key derived from the secret is made public.

Any communication inside the **networks happens between a quorum of devices which protect each other which increases the overall reliability of the network**. There is no doubt within the whole RDDL Network which entities are allowed to talk to exactly which other entities, which code sequences are allowed to be operated on which devices, which data are to be allowed to be read by whom etc.

4.4. The Secure Cloud and the Secure Hardware Enclaves

The machines, their data, their attributes and their signals are **constantly transferred, stored and analyzed at a cloud backend.** The cloud services are implemented on **CPUs with strictly segregated memories.** In the specific case, within hardware enclaves by Intel using its processor series supporting the software guard extension (SGX), by ARM using its TrustZone enclave technology and by AMD's secure encrypted virtualization (SEV).

The focus of the most recent **Physical Trust Layer enclave technology is on a containerized implementation of Intel's SGX.** Following a data-to-compute principle promoted by the **Ocean Protocol,** the transferred machine data and the algorithms operating on them are processed within these enclaves. The control of the individual enclaves **stays with the party which owns the data sovereignty**.

Access to the enclave is only possible with the right key material. This allows a granular access to the data. It is then up to the data owner to decide to give full or partial access to all data, or only to the right to use specific algorithms on the data, to pool the data or to keep this completely separated and segregated.

Considering that the mentioned data markets are **curated by tokens**, the cloud backend also serves as **a data and token custodian**. With the custodian function as a service, the enclaves turn into highly scalable and powerful **hardware wallets** managing machine data as financial assets.

5. The RDDL Network Blockchain Architecture

5.1. Principles

The RDDL Network is a machine-to-machine token network built around interconnected Tracker Wallets and designed with adherence to the technological path laid down by the Bitcoin network. Its reward mechanism is built around the Proof of productivity (PoP) consensus mechanism. The proof defines the constraints of when and where tokens are minted and subsequently rewarded to machine owners. RDDL Token Minting takes place exclusively when participating machines can give proof that they were productive according to the purpose of the machine network. A machine has fulfilled the network's purpose when it **creates signal data**, **attests them to a blockchain** and when it **produces or consumes energy**.

Any machine becomes a member of the network when it can prove its existence to the network. Therefore, the machine must become directly addressable through the Tracking Wallet Represented and protected by a seed/mnemonic phrase inside a hierarchical deterministic **hardware wallet**, the node starts to answer mathematical questions from the network according to its key material. This material consists of a private-public key pair. While the public key is used to attest the machine and its attributes to the blockchain, the private key stays unknown to the world, securely inside the Tracking Wallet. The private key is then used to sign messages received from and sent to the network, to derive other keys to sign transactions, trigger smart contracts, encrypt and decrypt its own payload and to 'harden' the communication with the network and other nodes aka machines.

5.2. Node Structure

The RDDL Network is composed of full nodes and Light Nodes. Essentially, machines that participate in the network, equipped with the relevant Tracking Wallet become Light Nodes and are directly involved in the Proof or Productivity Consensus. A Federation of Full Nodes with some broader technological requirements will ensure the Tendermint Core consensus and attestation to the blockchain.

Full Nodes store the full transaction history, Light Nodes only the transaction of relevance for the associated machine, its data and attributes. Full Nodes also act as validators and as Proof of Productivity coordinators, hence, full nodes validate all the transactions within the RDDL Network.

Both Full Nodes and Light Nodes are connected over a secure network, not the open internet, and are built around similar hard- and software stacks. Every node is acting as a hierarchical deterministic hardware wallet. Therefore, managing its own key material, signing its own transactions, and securing its own payload.

5.3. Tracking Wallets

To participate in the RDDL Network blockchain, each machine will need to be allocated with a Tracking Wallet, a hardware wallet that also acts as a trusted gateway. While the generic characteristics of these devices have been presented earlier in this paper, the specific requirements are laid out below.

The Tracking Wallets are mining devices and Light Nodes built around an ARM 64-bit architecture on top of NXP's i.MX8 series of chipsets. The new family, which is based on up to six 64-bit ARMv8-A technology processor cores and includes a HiFi 4 DSP, LPDDR4 and DDR4 memory support as well as dual Gigabit Ethernet with audio video bridging (AVB) capability, is designed to advance automotive dashboard graphics such as instrument clusters, infotainment visuals, heads-up displays, rear-seat screens and more. Capable of driving four HD screens with independent content or a 4K screen, the new devices introduced today include:

Table 2: RDDL Network Hardware Wallet CPU Requirements

MX 8QuadMax which integrates:	**MX 8QuadPlus which integrates:**	**MX 8Quad which integrates:**
two ARM Cortex®-A72 cores	one ARM Cortex-A72 core	four Cortex-A53 cores
four Cortex-A53 cores	four Cortex-A53 cores	two Cortex-M4F cores
two Cortex-M4F cores	two Cortex-M4F cores	two GC7000LiteXS/VX GPUs
two GC7000XS/VX GPUs	two GC7000LiteXS/VX GPUs	

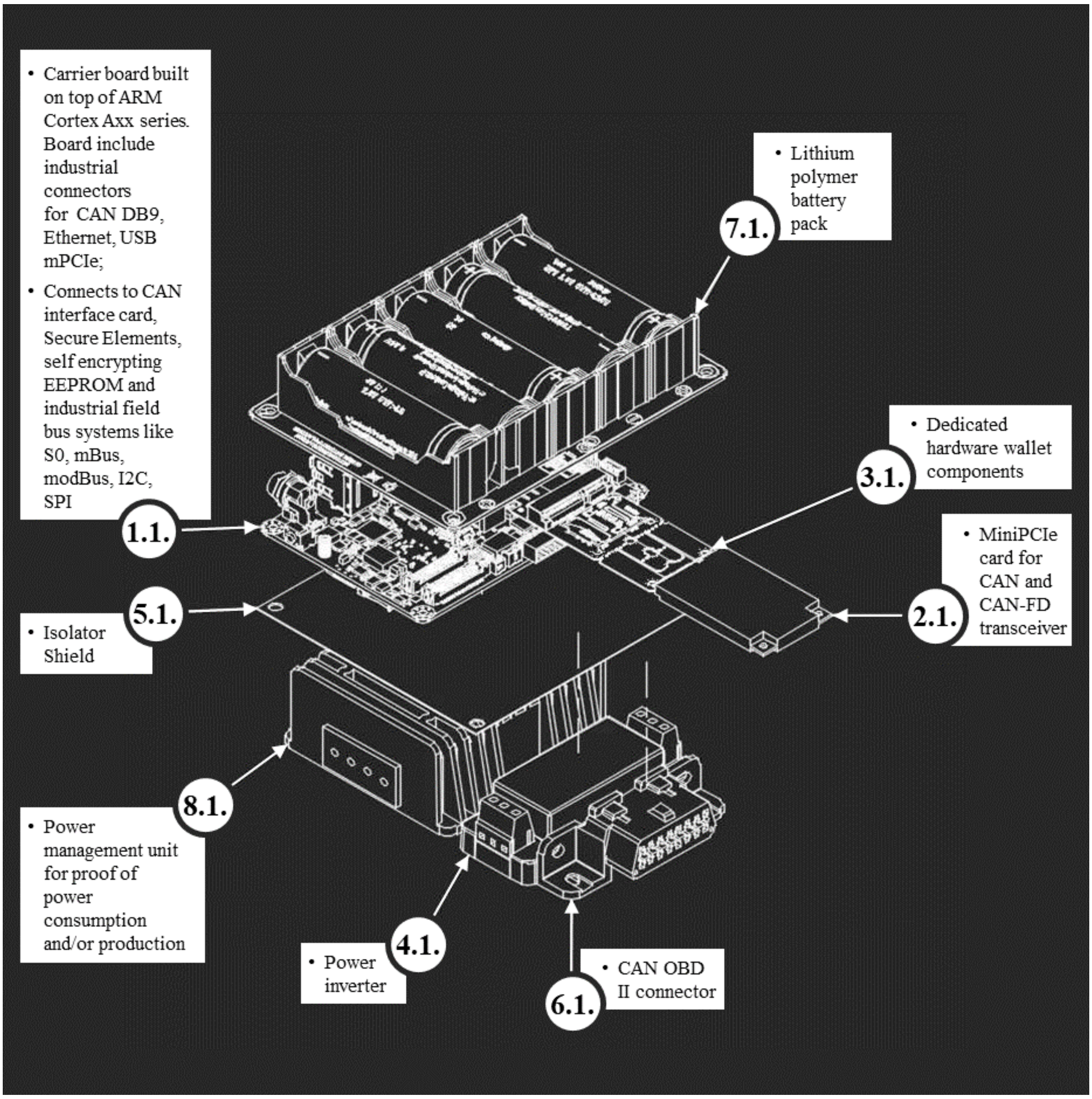
These are the ideal chipsets for diverse IoT and industry 4.0 use cases. This architecture combines powerful 64-bit ARM processors with GPU and MCU capabilities. Using these chipsets allows for general purpose programming, number and cycle intensive algorithm computation and I/O (input, output, sensor, actuator) driven computation.

MX8 chips are built with support for Android, Linux, FreeRTOS, QNX, Green Hills, and Dornerworks XEN, multiple temperature grades including automotive AEC-Q100 grade 3 (-40° to 125°C Tj), industrial (-40° to 105° C Tj), and consumer (-20° to 105° C Tj), and are fully supported on NXP's 10 and 15-year Longevity Program.

Relying on these chipsets allows the RDDL Network to drive fast, scalable and resilient industrial grade hardware wallets but also certifiable devices, which is of uttermost importance within industrial setups. Otherwise mining hardware like wallet systems could not be seriously embeddable into contemporary automobile architectures, industrial processes, or the renewable energy sector.

Like their "smaller brothers" Ledger, Trezor, Coldcardwallet, etc. the RDDL Network Tracking Wallets rely on trusted and confidential computing architectures, memory segregation, secure elements and secure enclave technology.

Figure 2: Tracking Wallet Conceptual Design



5.4. Blockchains in Blockchain

The RDDL Network is not only a machine's network but also a network of multiple blockchain components aligned and adapted to achieve optimal performance for the Physical Trust Layer & Protocol, with potential to facilitate on-ramp function and bridges to other blockchains.

5.4.1. Role of Planetmint

A core component of the RDDL Network is **Planetmint,** a metadata storage solution chosen to manage large scale, high throughput data and identity and orchestrate governance tasks within the network. Planetmint is a web3 data storage solution that grew out of the BigchainDB and IPDB projects as a necessity to address the challenge to store metadata and linked data on a blockchain. Especially within the context of industrial blockchain applications, data storage is **as important as value settlement, smart contracts and management of key material**. Similarly to IPFS, another web3 data storage system, data is stored in a decentralised way. Differently to IPFS, this is performed in a highly scalable In Memory data and application service system called Tarantool, where the sharded database instances are “consensing” the data stored via the Tendermint consensus algorithms. For industrial machines and participants in the RDDL Network there is strong requirement for clarity around where data are stored. Planetmint always gives a guarantee of data availability and data provenance. With IPFS data are stored in chunks locally, in the cache of the peers of the decentralized IPFS network, who must request data files first. Once the data disappears from the local cache there is no further guarantee that there are still enough chunks available at the peers to recreate the data. Beside that it is not known where exactly the chunks are stored. To avoid these pitfalls the RDDL network relies on the Tarantool - Tendermint combination.

Planetmint uses a strictly sandboxed version of the Lua Virtual Machine (VM) as smart contract language which is fully compliant with Ethereum VM (EVM). The application services within Tarantool are also modelled and implemented as Lua VM code. This enables Planetmint to address issues associated with scaling, payload and/or data constraints transaction throughput better than other chains without compromising security.

Planetmint has further developed the concept of crypto-conditions, originally implemented by Ripple as part of the Interledger Protocol - one of the first inter-blockchain settlement projects. Therein, smart contracts are modelled as “conditions” and “fulfilments”.

- Conditions are logical gates that evaluate and validate cryptographical primitives like signatures, hash digests, or synthetic primitives consisting of a series of Bitcoin or Ethereum op-codes.
- Fulfilments are connecting logical gates into a circuit structure and deliver the input data to evaluate the result of the circuit.

In essence, Planetmint replaces smart contract logic with a smart and flexible signature scheme. The benefit of this approach is that logical gates and circuits can emulate any virtual machine and accordingly will be capable to bridge different blockchains on the level of the op-codes of their virtual machines.

The functions of smart signatures as application services together with the metadata and linked data repositories enable Planetmint to also act as an oracle service, because it can store at the same time blockchain “consensed” data and data independent from the blockchain.

Planetmint’s versatile application services are also used to control all Liquid Network related transactions and the RDDL network’s inherent Proof of Productivity (PoP).

Planetmint facilitates a set of core transactions:

Table 3: Planetmint core transaction types

1. Create transaction	5. Burn transaction	9. Issuer multisig transaction
2. Transfer transaction	6. Voting Transaction	-- In the future --
3. Compose transaction	7. Validator election transaction	10. Staking
4. Decompose transaction	8. Challenge transactions	11. Inter blockchain transaction

5.4.2. Role of the Liquid Network

Liquid was designed as a sidechain to the Bitcoin network to address scaling issues and data throughput problems.

The Liquid blockchain can operate as a standalone blockchain or be pegged to another as a sidechain, enabling assets to be verifiably transferred between two different blockchains. Liquid allows the issue of multiple different types of assets on a single blockchain, opening up many new use cases for implementation.

This capability to issue, reissue and burn tokens representing individual assets make Liquid essential to the RDDL Layer 0x00's machine tokenization strategy. Every machine or its output can be turned into a deliberate number of tokens which then represents either the machine, ownership right, usage rights, attesting specific attributes or certificates.

The capabilities of the Liquid Network as a global financial instrument to self-issue assets and to hold them in self custody, in combination with the Tracking Wallet enabled deep integration into the cloud custody of the Physical Trust Layer is what unlocks the key DeFi functionalities that the RDDL Network is enabling.

5.4.3. Role of Celestia

The RDDL Physical Trust Layer will use Celestia's proof of data availability for generic and distributed peg-in functionality between the RDDL Token and the various Asset Tokens (see **Section 7.3** for details). The core idea of Celestia is to decouple transaction execution (and validity) from the consensus layer, so that the consensus is only responsible for a) ordering transactions and b) guaranteeing their data availability. For the RDDL Network it will not be possible to run the machine connected hardware wallets as full nodes. The hardware wallets are neither built nor intended to serve as full nodes. Therefore, a Light Node approach is necessary. The different machines will also differ in their requirements for consensus, metadata, transaction and message types. With its consensus nodes, storage nodes and Light Nodes, Celestia offers the perfect architecture for the RDDL Network.

The table below offers an overview of the major open source blockchain components play an active role in the RDDL Network's overall functional design.

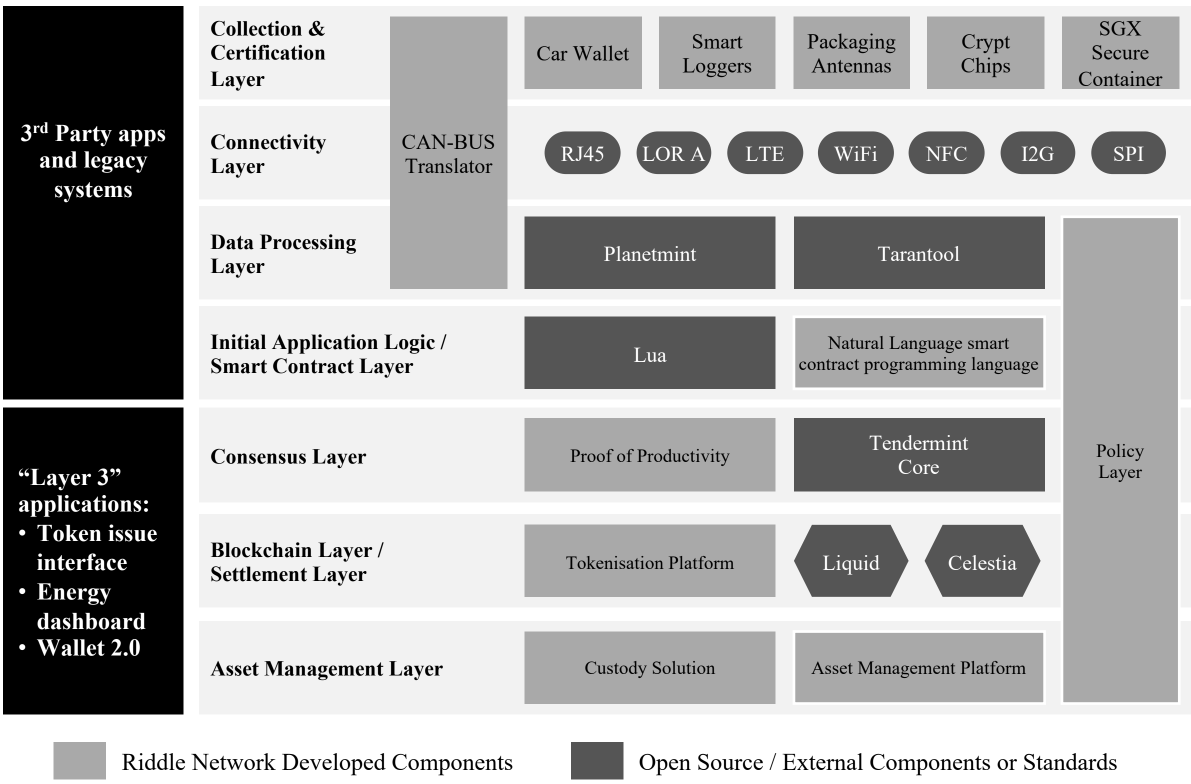
Table 4: RDDL Network External Blockchain Components

	Planetmint (Blockchain Governance and Orchestration Layer)				**Liquid Network** (Tokenisation & Settlemetn Layer)
	Tendermint (Consensus Layer)	**Celestia** (Data Availability Layer)	**Tarantool** (Data Storage Layer)	**Lua** (Smart Contract Scripting Language)	
Overview	Tendermint is a low-level protocol comprised of two main pieces: a blockchain consensus engine and a generic application interface. Baked into Tendermint's consensus algorithm is the fundamental concept of Byzantine Fault Tolerance (BFT). In essence, Tendermint is open source software for securely and consistently replicating an application on many machines. Tendermint works even if up to 1/3 of machines fail in arbitrary ways.	Celestia - at its center is the core mathematical primitive that makes sharding secure: data availability proofs using erasure codes. Using this primitive directly, rather than through sharding, allows the Celestia data availability layer to have the scaling of sharded blockchains for block verification.	Tarantool is an integration of a Lua application server and a database management system. The DBMS was originally developed as an in-memory NoSQL DBMS, and later it was extended with a disk storage engine option. Tarantool's in-memory engine is lock-free. It uses cooperative multitasking to handle thousands of connections simultaneously. There is a fixed number of independent execution threads and they do not share state.	Lua is a powerful, efficient, lightweight, embeddable scripting language. It has a simple procedural syntax with a powerful data description structure. Lua supports a variety of programming methods: procedural programming, object-oriented programming, functional programming.	The Liquid Network is a Bitcoin layer-2 solution enabling the fast, confidential settlement and issuance of digital assets, such as stablecoins, security tokens, and other financial instruments, on top of the Bitcoin timechain. It facilitates the transfer of assets to and from the Bitcoin mainchain via a two-way peg. The amount of BTC circulating on a sidechain is always verifiably equal to the amount of BTC "locked" on the Bitcoin mainchain.
Role played in RDDL Protocol	Tendermint provides the underlying logic for the RDDL Network Block creation. Tendermint uses validator nodes - 20 or 50 or anything in between, involved in the consensus mechanism itself. Tendermint allows for non-Validator nodes, nodes that receive the result of the consensus and help the creation of a new block, the RDDL Network Light Nodes.	The RDDL Physical Trust Layerwill use Celestia's proof of data availability for generic and distributed peg-in functionality. The core idea of Celestia is to decouple transaction execution (and validity) from the consensus layer, so that the consensus is only responsible for a) ordering transactions and b) guaranteeing their data availability. Celestia's tech stack helps the RDDL Protocol to address essential challenges such as scalability, speed and reduction of infrastructure costs. It also offers an ideal mix of full and light node capabilities.	Within the RDDL Network, Tarantool's disk-based storage engine exploits the advantage of single-threaded requests and hence avoid unnecessary synchronization overhead. Tarantool also supports secondary indexes, asynchronous replication, and some SQL operations.	Lua can been used in many industrial applications with an emphasis on embedded systems. Lua is a fast language engine with small footprint. It has a simple and well documented API that allows strong integration with code written in other languages. A fundamental concept in the design of Lua is to provide meta-mechanisms for implementing features, instead of providing a host of features directly in the language. Lua is small, adding Lua to any RDDL Network application does not bloat it.	The capabilities of the Liquid Network as a global financial instrument to self-issue assets and to hold them in self custody, in combination with the hardware wallet enabled deep integration into the cloud custody of the Physical Trust Layer is what unlocks the key DeFi functionalities that the RDDL Network is enabling.

5.5. End-to-End Architecture

Historically, a significant number of blockchain stacks (i.e. Bitcoin) have had a monolithic design. In other words, each blockchain stack is a single program that handles all the concerns of a decentralized ledger, including P2P connectivity, broadcasting of transactions, consensus on the most recent block, account balances, user-level permissions, etc. Using a monolithic architecture can make it difficult to reuse components of the code and attempts to do so result in complex maintenance procedures for forks of the codebase. Another problem with monolithic design is that it limits the blockchain to the language of the blockchain stack (or vice versa). The RDDL Network approach is to decouple the consensus engine and P2P layers from the details of the application state of the blockchain and use the optimal set of components within each blockchain layer, whether these were developed internally by the RDDL Team or externally by other open-source projects. The diagram below presents an overview of the *initial* end-to-end architecture.

Figure 3: RDDL Network End-to-End Blockchain Architecture



6. The RDDL Network Proof of Productivity and Consensus Mechanisms

Most of the transactions that happen in the RDDL Network are attesting to and creating assets and their attributes. Therefore, create, transfer, compose and decompose transactions dominate the network payloads. Many single transactions get collected into a block, which then gets written into the blockchain. Planetmint facilitates this process through its short block creation time. A new block on the RDDL Network will be created every minute, compared to one every 10 minutes for Bitcoin.

The RDDL Network uses "***Proof of Productivity***" to ensure that the machines themselves become the anchors of trust, allowing for the highest level of network security by making machines prove their identity and the fact that they are running at appropriate capacity (or not). A machine has fulfilled the network's purpose when it creates data, when it produces or consumes energy, and when this is attested to the blockchain. The consensus mechanism used to achieve this is ***Tendermint Core*** within the broader Planetmint Ecosystem.

6.1. Proof of Productivity (PoP) challenge process

PoP attests two facts:

1. That a machine was active by giving proof to its kWH production or consumption for the most recent block epoch.
2. That a machine produced and attested data against the blockchain during the most recent block epoch.

To ensure this is the case, a **Challenge Process** is initiated.

At the end of an epoch, the RDDL Network activates a daemon process inside of Planetmint to create a challenge transaction. The validator initiating/creating the last transaction for an epoch also triggers the challenge creation.

Following a **round-robin** or **lottery principle** the next **challenger** and **challengee** are being defined out of all actively connected Light Nodes of the RDDL Network, and hence are available for token rewards. The same validator (a RDDL full node) then messages the challenger to create a challenge. Thus messaged, the challeng er node then pings the challenged node and requests the most recent kWH- and data-availability-proof. The challenged Light Node will then send the requested data from its local data storage to the challenger node. The challenger node will then compare the received data with the data attested to the last block on the RDDL Network.

In case the data are the same, the challenge is fulfilled successfully. **The challenger Light Node creates a challenge transaction and transfers it to the full node that has requested the challenge**. Then the challenge transaction is sent to the Planetmint network to be validated and "consented"; rewards are granted. **In case the consensus mechanism also validates the challenge it gets written together with the most recent block to the blockchain.**

Subsequently, an issuer transaction is being created.

6.2. Issuer Transaction

The **RDDL Tokens** are continuously issued and re-issued on the Liquid Network. The re-issue transaction of tokens happens according to the reward schedule, reward mechanics and challenge system created by the validator node that triggered the challenge. This full node creates an issuer transaction. The issue transaction must be successfully co-signed by **at least 6 full nodes** (as opposed to Light Nodes participating in the challenge process), **according to the Tendermint Core consensus mechanism,** then it will be sent to the Liquid Network for settlement. Only when this Liquid transaction gets settled, the Issuer transaction also gets written to the Planetmint network. The multisig scheme follows a 6 out of 15 signatories logic.

6.3. Tendermint Consensus Mechanism

From Cosmos White Paper:

> Tendermint is a partially synchronous BFT consensus protocol derived from the DLS consensus algorithm. Tendermint is notable for its simplicity, performance, and fork-accountability. The protocol requires a fixed known set of validators, where each validator is identified by their public key. Validators attempt to come to consensus on one block at a time, where a block is a list of transactions. Voting for consensus on a block proceeds in rounds. Each round has a round-leader, or proposer, who proposes a block. The validators then vote, in stages, on whether to accept the proposed block or move on to the next round. The proposer for a round is chosen deterministically from the ordered list of validators, in proportion to their voting power.
>
> Tendermint's security derives from its use of optimal Byzantine fault-tolerance via super-majority ($>\frac{2}{3}$) voting and a locking mechanism. Together, they ensure that:
>
> $\geq\frac{1}{3}$ voting power must be Byzantine to cause a violation of safety, where more than two values are committed.
>
> if any set of validators ever succeeds in violating safety, or even attempts to do so, they can be identified by the protocol. This includes both voting for conflicting blocks and broadcasting unjustified votes.
>
> Despite its strong guarantees, Tendermint provides exceptional performance. In benchmarks of 64 nodes distributed across 7 datacenters on 5 continents, on commodity cloud instances, Tendermint consensus can process thousands of transactions per second, with commit latencies on the order of one to two seconds. Notably, performance of well over a thousand transactions per second is maintained even in harsh adversarial conditions, with validators crashing or broadcasting maliciously crafted votes

7. The RDDL Network's Token Economics

7.1. The RDDL Token

The guiding principle of the RDDL Network's **token economic design** is to enable, encourage and authorise the largest possible number of machines to join the blockchain economy and unlock the value that lies within this network of machines. The higher the number of machines that act as nodes in the network, the greater the value of the network. These dynamics are incentivized through the **RDDL Token**. As such, the price of the RDDL Token will float and will be driven by the long-term utility of the network along with crypto market dynamics.

Simultaneously, the **RDDL Token** is also the transactional token that facilitates operations on the RDDL Network. All machines, applications, programmes and other services that are or will be linked with the RDDL Network require computing power, storage, management, etc and the RDDL **Token is a form of payment for network participants** to execute their requested operations on the network.

Once tokens become available token holders can start to consume network services and utilities. The **RDDL Network** resembles a meta-network with its capability to function as a platform to create other tokens and token-networks. The RDDL Network not just delivers the functionality of token creation, but also additional services to create data markets, data-to-compute services, micro-investment platform services, trusted hardware and computing services, custody services, certificate markets, hardware licensing and subscription services and more products.It also facilitates the onramp of industrial machine tokens into other web3 protocols.

Classic blockchain servings offered will be:

1. Token creation
2. Token swapping
3. Token custody
4. Token staking
5. Governance services like voting and staking
6. Operations of full and Light Nodes
7. Validation services
8. Rewards, Grants and inventive services
9. Fee rewards

7.2. The RDDL Token Disbursement Mechanics

The RDDL Network will release 2.1 Billion RDDL Tokens over a period of 35 years. The token reward schedule for participating nodes is well aligned with the block creation schedule. The reward schedule is designed and will execute on a fixed time period similar to the Bitcoin network, using a halving schedule and fixed amount of total tokens. Hence, the amount of tokens to be issued for a certain period of time is fixed.

There will be a halving period every seven years, equivalent to five breakthrough technology innovation cycles. Given the industrial DNA of the RDDL Network, aligning it to major innovation cycles is essential in keeping the network at the edge of innovative thinking.

Table 5: Token Distribution by Cycle

Cycle	Period	Tokens Distributed
Cycle 1	Years 1 - 7	1,005 M
Cycle 2	Years 8 - 14	525 M
Cycle 3	Years 15 - 21	262 M
Cycle 4	Years 22 - 28	132 M
Cycle 5	Years 29 - 35	66 M

Block creation and rewarding happens according to the RDDL Network's capability every minute.

The RDDL Network anticipates a block creation every minute. Each 7 year cycle is formed of ~3.7 Million minutes. **This means that the RDDL Network will be issuing about 286 Tokens every minute for the first 7 years**.

7.3. The Asset Tokens

One of the core purposes of using the RDDL Network is ultimately to create new, machine token economies. This is where the inherent capability of the RDDL Network **to issue seamless, interchangeable Asset Tokens** plays a key differentiating role.

Per strict definition, machines are non-fungible. However, by tokenizing them, i.e. digitising them as assets, turning them into a digital twin, issuing attributes and claims on top of them, machines become re-fungible. As the tokens representing them can be bought, sold or exchanged. The versatility of the token which can represent the whole asset as such, fractional ownership, fractional drawing and utility rights, access and usage rights, claims and certificates of any kind, proof of provenance, proof of non-hazardous materials, enable a broad portfolio of new business developments around machines, otherwise not possible.

A token/ set of tokens can only be issued against an asset around the value and a narrative that real world value lies behind the asset/machine that is tokenized. To do this, metadata needs to be uploaded: i.e. a link to a contract, insurance certificate, etc: proof that it exists in the real world and it is valuable.

7.3.1. The Relationship between the RDDL Token and the Asset Tokens

This tokenisation of industrial machines and infrastructure happens via tokenising the machine as asset or service. The tokenised asset will be implemented as a stable coin and is to be evaluated in a standardised manner. The amount of this contribution is considered when a machine is rewarded during the Proof of Productivity (PoP) challenge. The asset and service value of data and signals of a private car will be very different to the contribution by a solar power plant. The reward mechanism considers these differences by using a multiplication factor used on the block reward. This multiplication factor is implemented around the **logarithm to the base 10** to keep the additional incentive in range.

The function to calculate the RDDL Token reward multiplier is defined as follows:

Reward(x) = 1+log_10(x)/100

*with x being the value of the data/machine.

For example:

A private car owner tokenizes the CAN bus signals of his car, valued with 100 EUR. The function to calculate the reward multiplier is defined as:

Reward(100) = 1+log_10(100)/100

Accordingly, the car owner will be rewarded with a share of the reward 286 * 1.02 equals 291.72 token reward.

A different example, i.e. a citizen solar power plant tokenises a micro investment scheme valued at 3,000,000 EUR. The multiplication factor would be:

Reward(3,000,000) = 1+log_10(3,000,000)/100

Accordingly, the citizen power plant will be rewarded with a share of the reward 286 multiplied by 1.064 equals a 304.304 token reward.

The intention of the RDDL Network remains to **keep the influx of additional RDDL tokens into its token economy steady**. Therefore, the network controls the periodicity of the PoP challenge. In case that during several minutes, substantially more tokens were mined than the 286 ones, the network may pause any new block rewarding to balance out any previous imbalances.

To enable this dynamic, **watchmen-controlled escrow accounts will be required**. The challenge that arises is how to manage them collectively and in a distributed fashion. The inflow and outflow of units inside the escrow account influences the creation or destructions of coins inside the Liquid network. In case that the escrow accounts are under centralized control, the whole system turns into a centralized one which is against the fundamental principles underpinning the RDDL Physical Trust Stack.

There the management of the escrow accounts must be controlled by a collective of wallet accounts. The Liquid Network uses a Bitcoin multi-signature contract to protect the peg-in relation of bitcoin and L-btc (Liquid Bitcoin). However, this mechanism stays restricted to Bitcoin, exclusively.

Therefore, the **RDDL Network attempts to create a more versatile peg-in mechanism, including any token of interest,** independent of its core structure and technology, especially independent of its consensus mechanism guaranteeing finality of transactions. The sidechain ambitions around Ethereum came up with optimistic and zero-knowledge rollups to tackle the same challenge. Consequently, this raises the question whether rollups can also be turned into a generic watchmen function for Liquid. In case yes, the decentralized management of the escrow accounts securing the Liquid token peg-in can be assured. **The RDDL Network will use Celestia's Proof of Data availability to ensure the optimal peg-in mechanism**.

7.4. Ramp-up and Reward Split

The network will require initial liquidity to start and economic activity. To achieve this there will be a defined ramp up phase during which the block reward will be higher before decreasing over the period of a year. According to the PoP, every block reward will be divided between several stake holding institutions, which guarantee operations and availability of the network.

The stakeholders will be consisting of:

Table 6: Token Allocation

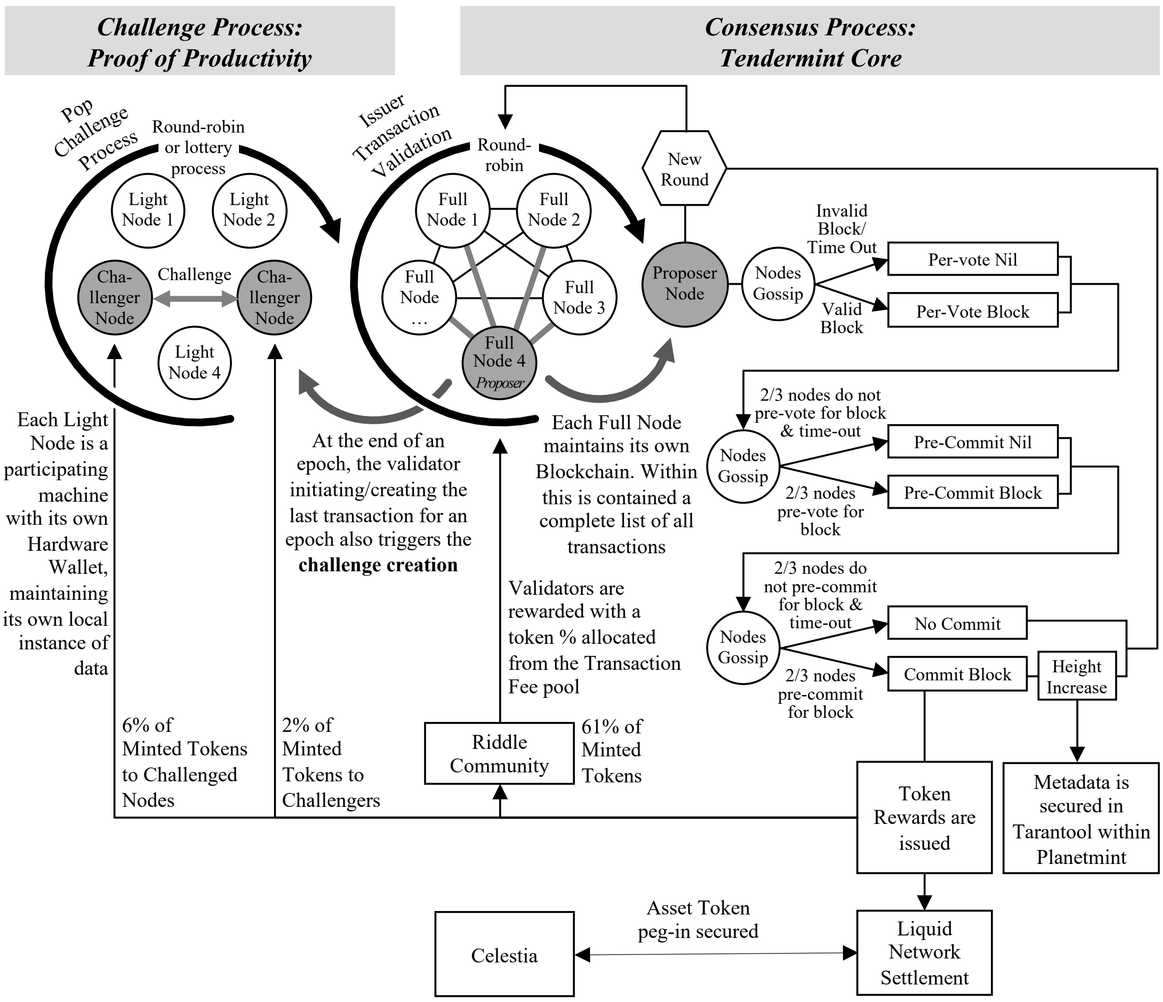
Stakeholder	% of all Tokens Allocated
Challenger machine	2%
Challenged machine	6%
Foundation (Treasury, Team, Core developers, early shareholders)	19%
Community	61%
Strategic partners and infrastructure enablers	2%
Investors	10%

The token reward schedule for participating nodes is well aligned with the block creation schedule. The reward schedule is designed and will execute on a fixed time period similar to the Bitcoin network, using a halving schedule and fixed amount of total tokens. Hence, the volume of tokens to be issued for a certain period is fixed. Additionally, it is part of the reward design to decide whether tokens get issued with every block or e.g.: with every 10th or 60th block created. In the case of the RDDL Network, the reward schedule will follow the block creation design of Planetmint, with the block interval comprising an epoch every 60th block. When an epoch ends, a challenge transaction is created and therefore token rewards are generated. According to the success of the challenge transaction a token issuing transaction will take place (or not).

The issue transaction will result in:

1. Reissuing RDDL tokens on the Liquid network to the RDDL issuer wallet.
2. Splitting the token reward according to the token reward mechanics and subsequently transferring the tokens to the correct beneficiary wallets.

Figure 4: RDDL Network End-to-End Consensus Mechanisms



8. References

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008 3.1, 7, https://bitcoin.org/bitcoin.pdf

A.Haleem A.Allen A.Thompson Ma.Nijdam R.Garg. Helium: A Decentralized Wireless Network 2018 0.4.2, http://whitepaper.helium.com/

Trent McConaghy. Ocean Protocol: Tools for the Web3 Data Economy, Version 2022-FEB-24, https://oceanprotocol.com/tech-whitepaper.pdf

Jae Kwon. Tendermint: Consensus without Mining. 2014, Draft v.0.6 (outdated). https://tendermint.com/static/docs/tendermint.pdf

Jonas Nick Andrew Poelstra Gregory Sanders. Liquid: A Bitcoin Sidechain. May 22, 2020. https://blockstream.com/assets/downloads/pdf/liquid-whitepaper.pdf

Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013. https://ethereum.org/en/whitepaper/

"Celestia: A Scalable General-Purpose Data Availability Layer for Decentralized Apps and Trust-minimized Sidechains", Mustafa Al-Bassam. Nov 6, 2019. https://blog.celestia.org/celestia-a-scalable-general-purpose-data-availability-layer-for-decentralized-apps-and-trust-minimized-sidechains/

Mustafa Al-Bassam, Alberto Sonnino, Vitalik Buterin, "Fraud and Data Availability Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities". 2019. https://arxiv.org/pdf/1809.09044

Mustafa Al-Bassam, "LazyLedger: A Distributed Data Availability Ledger With Client-Side Smart Contracts". May 2019. https://arxiv.org/pdf/1905.09274

Al Bassam, Mustafa. "Securely Scaling Blockchain Base Layers". Doctoral thesis (Ph.D). 2020. https://discovery.ucl.ac.uk/id/eprint/10117245/1/thesis.pdf

"Bitcoin Monetary Inflation", diagram. Lasgt accessed April 01, 2022. http://bashco.github.io/Bitcoin_Monetary_Inflation/

"The Emergence of Cryptoeconomic Primitives". Jakob, Cofounder of Zora. Coinbase.com, last accessed Apr. 01, 2022. https://blog.coinbase.com/the-emergence-of-cryptoeconomic-primitives-14ef3300cc10

Ryan Zurrer. Keepers — Workers that Maintain Blockchain Networks. Aug 5, 2017. https://rzurrer.medium.com/keepers-workers-that-maintain-blockchain-networks-a40182615b66

Josh Stark. "Bounty" ICOs. Jun 6, 2017. https://jjmstark.medium.com/bounty-icos-61232e73370b

Kyle Samani. New Models For Utility Tokens. Feb 13, 2018. https://medium.com/multicoin-capital/new-models-for-utility-tokens-d26c12ec00c5

Mike Goldin, Sep 14, 2017. Token-Curated Registries 1.0. https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7

Dimitri De Jonghe, Dec 4, 2017. Curated Governance with Stake Machines. https://medium.com/@DimitriDeJonghe/curated-governance-with-stake-machines-8ae290a709b4

Billy Rennekamp, Feb 26, 2018. What happens when a Bonded Token owns an NFT? https://billyrennekamp.medium.com/re-fungible-token-rft-297003592769

Decentralized Identifiers (DIDs) v1.0. W3C Proposed Recommendation. August 2021. https://w3c.github.io/did-core/

Filecoin: A Decentralized Storage Network. July 19, 2017. https://filecoin.io/filecoin.pdf

Jae Kwon, Ethan Buchman, Cosmos: A Network of Distributed Ledgers. https://v1.cosmos.network/resources/whitepaper

Figure index

Table index