Wise Network's WHITEPAPER

Empowering IoT and AI through the power of Blockchain Technology

Wise Network - The First Analog-Mixed-Signal- System-On-A-Chip- Eco-system

Dr. Danny Rittman
Ph.D. LaSalle University.
CTO, Wise Network

GOPH
GOPHER PROTOCOL

AVANT! Ai

WISE

Disclaimer

This *White Paper* contains information regarding the Wise Network project (here on called the "Project"), including information regarding the Wise ecosystem, Wise's Public Blockchain and layer two solutions, and the WSE tokens, as well as proposed consensus protocol, their functionalities thereto as presently conceived, and is solely intended for the use of such intended recipient for general information purposes only. While we make every effort to ensure that the material in this *White Paper* is accurate and up to date, such material in no way constitutes the provision of professional advice.

We do not guarantee, or accept any legal liability whatsoever arising from or connected to, the accuracy, reliability, currency, or completeness of any material contained in this *White Paper*, and to the maximum extent permitted by all applicable laws, regulations and rules, we shall not be liable for losses of any kind, including indirect, special, incidental, consequential losses, in tort, contract or otherwise arising out of or in connection with any acceptance of or reliance on this *White Paper* or any part thereof by you.

This document is owned by Wise Network, therefore there is no authorization to reproduce or replicate it in any way or form, distributed or disclosed, or broadcasted, or relied upon or used, or for any purpose without our express written permission. If you are not the intended recipient, disclosure, copying, distribution and use are similarly prohibited; please notify us promptly and delete this *White Paper* from files.

Further functionality and/or features may be changed, revised, modified, and/or added by the Project team as research and development around the Project continues. As such, the Project, the Wise Ecosystem, Wise's Public Blockchain and layer two solutions, the WSE tokens and proposed consensus protocol, their functionalities thereto as described in this *White Paper* may accordingly be subject to modifications and/or revisions without any prior notice. Please refer to https://wise.cr/ for latest updates and developments of the Project.

For the avoidance of doubt, this *White Paper* is not intended to be, and should not be construed to be, a prospectus or offer document of any sort, and is not intended to be, and should not be construed to constitute an offer of securities of any form, units in a business trust, units in a collective investment scheme or any other form of investment, or a solicitation for any form of investment in any jurisdiction. No regulatory authority has examined or approved of any of the information set out in this *White Paper*. This *White Paper* has not been registered with any regulatory authority in any jurisdiction.

Foreword

The creation of the machine to machine (M2M) economy is now attainable including the potential to disrupt all prevalent centralized systems and economies as a whole. However, even with the parallel development of artificial general intelligence, distributed ledger technologies, and the Internet of Things, no current system successfully utilizes these three fields to enable collaboration, learning, and interactions between billions of autonomous devices.

Introducing Wise, a protocol liable for delivering messages to one or multiple endpoints combining a proof of ownership-hardware based- processing-blockchain core and a radio wave and internet-based infinity-chain infrastructure to connect all Internet of Things devices with one another creating new levels of information access and use. At the same time building too, a new intelligent IoT economy powered by Blockchain technology.

To provide a scalable network that supports workloads from billions of different IoT devices, Wise provides an infinity-blockchain architecture that enables instantaneous transaction speeds and unlimited throughput. As the network only tracks the amount of tokens on each blockchain, Wise enables the creation of an endless number of independent application specific side-chains that remain connected to pools from other networks. In this manner, the network can handle chaotic IoT subsystems by providing support for configurable and interoperable decentralized networks all built on the foundation of our **POO** (Proof Of Ownership) consensus protocol.

To provide the applications necessary to enable human-like interactions between devices of various knowledge domains, Wise contains a virtual application layer. Devices can query the layer to access decentralized applications that support the intelligent machine economy such as: decentralized identities, distributed storage, digital currencies, node discovery, distributed computation, decentralized machine learning, etc.

Wise Network introduces **ANSUZ,** it's own ***Secure Memory Chip*** (a 13 nanometer IC introducing a practical new concept, radio based IoT mesh networking). The ANSUZ Chip can communicate via its own radio waves in a variety of frequencies and in locations where there are no cellular or Wi-Fi services with embedded tensor processors and hash accelerators, to provide the real-world infrastructure for blockchain take over, the usability of decentralized applications, and accelerated processing for deep neural networks. The microchip includes an expert system to learn distributed networks behavior, turning them into artificial neural networks **(ANN)** to increase privacy and security while at the same time learn advanced neural network models, and leverage the utilities of distributed ledgers. All the cores can be immediately connected by its native blockchain and allow hosted devices to begin interacting over its scalable frameworks.

In summary, both the blockchain and the **Ansuz** Chip will form a disruptive machine ecosystem where devices can achieve extremely high levels of performance and have the capacity to begin interacting with one another. In this white paper, we detail a system of implementation combining the first blockchain based *System-on-a-Chip* with a scalable blockchain network to enable evolutionary growth and secure interactions between Internet of Things devices.

Table Of Contents

WISE

1. Introduction

First things first...

The concept of IoT & M2M economy is becoming increasingly relevant with the recent explosion of growth in artificial intelligence and IoT devices.

These days, thanks to machine learning, computers have been able to achieve human-level performance on highly complex perceptual assignments. Further steps in deep learning have empowered artificial neural networks such as AlphaZero to beat World Go Championship players easily. Constant upgrades to processors such as Google's 180 Teraflop TPU announce that neural network training is here to stay.

Currently, in a day-to-day frecuency, people are realizing that artificial intelligence will transform the world into one where intelligent entities interact with each other with little or human control. Moreover, the IoT industry has seemingly taken a couple of steps back in recent years, maybe caused by the growth of the AI sector.

Still, we have found that distributed ledger technologies, such as the blockchain, can lead to a beneficial IoT and AI symbiosis or as we call it "M2M economy". With blockchains, the collective knowledge of all devices can be distributed, ensuring that no central system can influence all the others. Autonomous devices can be managed in ways that generates data that can be useful and sometimes crucial to other devices' optimal functionality by making this data available in a "market place" where any IoT device using Wise's ANSUZ Chip can access, use, update and share the end result of its processes so that any other IoT device that needs this information can obtain it reliably from the source and with up-to-date details. There will be "no" centralized control over the network, enabling users/nodes/machines to directly interact with one another without a middleman. As a result, blockchains, will enable many new decentralized and secure applications that can be executed over *Wise's Mesh Network*.

The Internet of Things has become one of the booming technologies among the blockchain, AI and smart technologies. There is a projected a 9+ trillion dollar blockchain market, 7+ Trillion dollar Internet of Things market, and an 18 trillion dollar AI market that collectively make up the M2M Economy.

With Wise's ANSUZ Chip, devices such as the ones used by medics would be able to independently communicate data to other devices, creating a more accurate diagnosis and treatment to patients, methods of transport such as cars and boats could will have communicate with other nearby transports securely to optimize traffic and geographic data, effectively designing smarter and secure routes, IoT devices in general will have the intelligence and information to suggest an individual based on enhanced-real-time data obtained from other devices to improve the quality of life. With the advancements in artificial intelligence, blockchain technology, and IoT devices, Wise's Ansuz Chip bid is the stepping stone to the M2M economy.

Having said all of the above, Wise Network and Gopher Protocol (GOPH) are creating Wise's SMC that comes along with an end-to-end protocol designed to meet the needs of an machine to machine economy via its two components: **Wise's Public Blockchain Mesh Network** and layer two solutions based on **POO** and an analog-mixed-signal, system-on-a-chip (AMS-SoC).

Wise's Anzus Chip will lay the real-world foundation to support cryptographic acceleration, neural network processing, and System-on-Chip development in IoT devices whereas **Wise's Public Blockchain Mesh Network** will serve as the distributed "hive mind" infrastructure that will give devices the capacity to securely learn, and transfer information between one another.

With the invention of Bitcoin and its essential consensus solutions, distributed systems and distributed applications have become a practical solution.

Subsequent blockchain platforms have generalized this new paradigm, leading to decentralization in many areas.

Currently, blockchain-based decentralized systems are used in many application fields. Blockchain systems, for example, can be used for creating things such as digital currencies, creating decentralized data marketplaces, and helping form ideas such as decentralized supercomputers. However, scalability issues have so far prevented its use in data-intensive applications and high-throughput transaction processing systems. As an introduction to our **Wise's Public Blockchain Mesh Network,** hereon referred to as **WPBMN,** we present the underlying technology used for decentralization, discuss scalability issues, and identify the most promising solutions for overcoming these hurdles.

1. 1 Introduction to Blockchain

Distributed Ledger Technology or DLT has become ready for mainstream adoption, allowing true decentralization to become a reality. The application of cryptographic primitives to data structures and consensus algorithms has made it possible to implement trust-less distributed systems in the presence of a Byzantine failure model, named after Leslie Lamport's *Byzantine Generals Problem*.

For a distributed system to defend against Byzantine failures, consensus on system integrity needs to be reached, even in the presence of malicious participants. This problem was solved practically by the blockchain data structure and algorithms of the Bitcoin digital currency.

Since, the invention of Bitcoin and cryptocurrencies, blockchain technology has moved on to other applications, ranging from smart contract implementations to Internet of Things (IoT) solutions. During this generalization of use cases, many innovations to the underlying data structures and consensus protocols have been made, to solve application-specific problems, as well as general scalability issues. Wise Network will leverage all these innovations to build our blockchain.

In this paper, we give an overview of the data structures and algorithms currently available for implementing decentralized systems, together with an evaluation of their applicability for high throughput applications, such as IoT use cases. We also present an overview of the Tendermint platform, which we consider the currently most reliable and scalable solution for applications that require high-throughput transaction processing.

1. 2 Decentralized Consensus Technology

Decentralized technologies have emerged in recent years making possible by cryptography, in particular, asymmetric cryptography.

Asymmetric cryptography -in contrast to symmetric cryptography- does not rely on a shared key that all parties participating in a secure communication have to know. Instead, a pair of keys is used, consisting of a private and public keys. The private keys of a participant are kept private and not shared across the network, as the name suggests. In contrast, the public keys can be safely made public. A public key can be used to encrypt a message, which can only be decrypted by the corresponding private key.

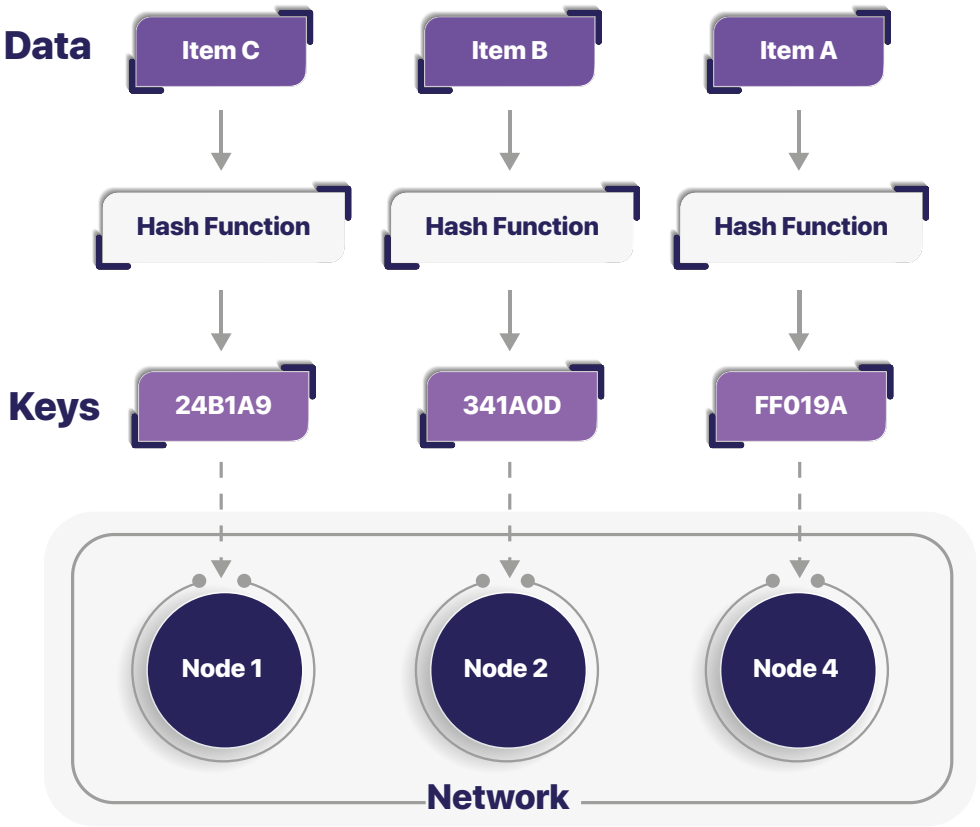
By using his private key to sign a message, a user can prove he is the sender of the message. The sender of a message signed with a private can be verified with the corresponding public key. Furthermore, signing messages this way can be used to detect whether the message has been altered, meaning that the integrity of data can be verified.

Asymmetric Encryption does not only solve the problem of securely transmitting keys over a network, it can also be used to prove identity and data integrity. Asymmetric cryptography is used in blockchain systems to identify account holders and sign transactions.

Hash Functions & Distributed Hash Tables

Hash functions are utilized to create hash tables. Hash tables are data structures comprised of key-value pairs. Hashing is used to compute indices for data slots called buckets which can hold values.

Distributed versions of the hash table structure can be used very effectively to store data across decentralized systems. Distributed hash tables distribute the buckets holding data across different nodes of a peer-to-peer network. The hash value acts as a key for allowing nodes to address data on the network. Figure below illustrates how data can be distributed amongst nodes in a distributed system using a distributed hash table.



To be practical in the outside-world system, in which nodes may join and leave at any time, it is important for distributed hash tables to use hashing algorithms that do not remap the key space considerably enough when the set nodes in the system are modified.

Two commonly used algorithms, rendezvous hashing, and consistent hashing, complete this property. In both algorithms, only the keys owned by nodes with adjacent node identifiers are changed when a node joins or leaves the system.

1.3 Interplanetary File System & Architecture

Interplanetary Filesystem or IFPS, is an alternative whose goal is to supply a fault tolerant process to globally shared address space for storing data.

Files are divided into blocks and stored across the network. Files are identified and addressed by their hash values. Version history of each file is maintained similarly as in the Git version control system.

A motivational plan to be certain that nodes continue to sow the content they stockpile can be by keeping track of debit and credit balances of bytes verified. Blocks are sent to certain nodes based on their debt balance. The nodes that do not cooperate are fined by being left out for a specific timeframe.

IPFS structure of incentivisation only benefits nodes to seed the content they host. Albeit, nodes only store files they choose to host. In some versions, nodes are able to "pin" data files in order to host them but there is no guarantee that content will remain present or readily accessible in the system.

Other sophisticated incentive structures for benefiting nodes to host content, like Filecoin, could be implemented in additional layers. By using hashes to address a file, it allows IPFS to become a content addressed/oriented system. This has the advantage that duplication of files can be spotted since the same content computes the same address. When a user requests a file/data, the network serves the information identified by a hash value.

Their hash value also identifies the blocks which make up a file. This leads to a data structure called Merkle **Directed Acyclic Graph (DAG).** We will discuss **DAGs** and **Merkle** proofs later on this paper.

IPFS resorts to a series of sub-protocols to maintain the network and to manage primitives such as:

- **Identities:** Node identities and verification.
- **Network:** Connections between nodes.
- **Routing:** Information for locating nodes and objects.
- **Exchange:** Protocol for managing block distribution.
- **Objects:** Merkle DAG of content addressed objects with links.
- **Files:** Versioned file system hierarchy.
- **Naming:** Naming system.

The Interplanetary File System permits a data transaction layer in IoT data marketplaces when combined with a high transaction throughput blockchain. This could be a reliable alternative to the data marketplace currently being developed to run on the Directed Acyclic Graph-based IOTA system.
Note: IOTA as well as its flaws will be discussed later on in this paper.

IPFS is also frequently used as a storage layer associated with blockchain applications. Blockchain storage is sluggish and costly, and at this moment it is not practical to store large chunks of data on a blockchain. An alternative use is storing metadata, as IPFS identifiers on the blockchain, and the great majority of the data on the faster and lighter IPFS network. The IPFS links act as digital fingerprints to ensure the integrity of the data, by being stored immutably and timestamped on a blockchain.

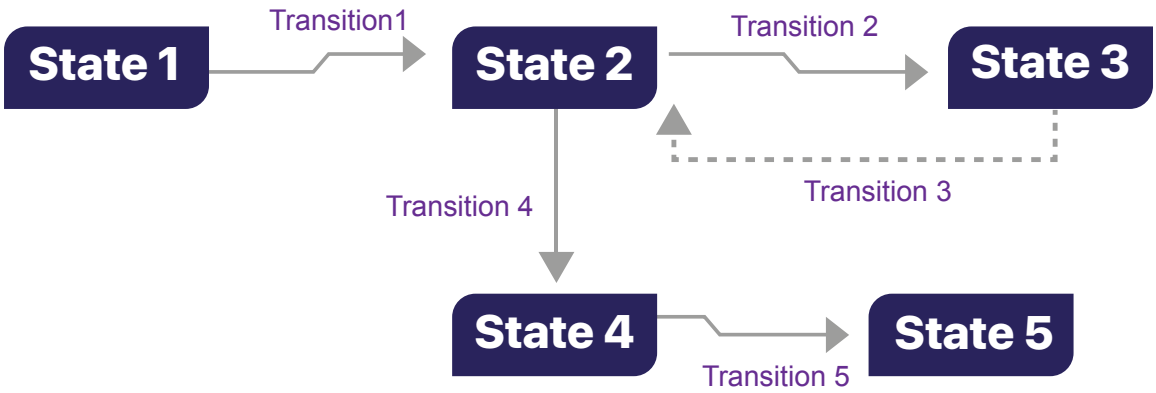
It can be stated that IPFS is probably the decentralized alternative to the HTTP protocol. The objective behind depositing web content on the InterPlanetary File System is to fracture the centralized basis of the World Wide Web in terms of hosting.

The concept of a Blockchain has grown out of Bitcoin and subsequent cryptocurrencies. The original Bitcoin paper did not use the word blockchain, and it took some time for the term to emerge, to describe the underlying technology that permits implementing digital currencies and other applications.

It is well recognized that blockchain is a distributed ledger of exchanges applied on top of a P2P network in the existence of a Byzantine failure model. The system relies on an essential linked list data structure, and applies a state machine with permanent state transitions.

The above definition introduces a series of properties a blockchain provides:

- **Distributed Ledger of transactions.** Transactions are recorded in a ledger which is distributed to all nodes. Each transaction is atomic in that it executes completely or not at all.
- **Peer-to-peer network.** The system is applied on a distributed network of equal nodes. Nodes may join or leave the network freely.
- **Byzantine Failure Model.** Nodes reach consensus on the outcome of each transaction, meaning that there is a single version of the globally accepted system state at all time. If the majority of the network's computational assets stay honest, malevolent nodes cannot corrupt system state. Consensus protocols typically motivate nodes to keep state integrity.
- **Immutability.** Transactions in the blockchain are immutable, whose state cannot be modified once it has been created. This is achieved by sealing blocks of confirmed transactions cryptographically, as discussed below.
- **State machine.** A state machine will model behavior defined by a finite or predefined possible system states; an infinite state machine has an infinite number of possible states. A single blockchain can be visualized as a state machine. In this paradigm, exchanges that are collected on the distributed ledger are state transitions, while the state after each exchange or transaction represents a state vertex in the state machine.



Like we just discussed above, at the heart of a blockchain, there is a distributed ledger. This distributed ledger is typically represented as an inextricably linked list of numbered blocks.

Each block contains a list of transactions that have been included in the block in a specific order using a consensus protocol. In practice, the actual transactions may not be included in the block but referenced through the root hash of a Merkle tree (explained below). However, conceptually, the transactions are part of the block.

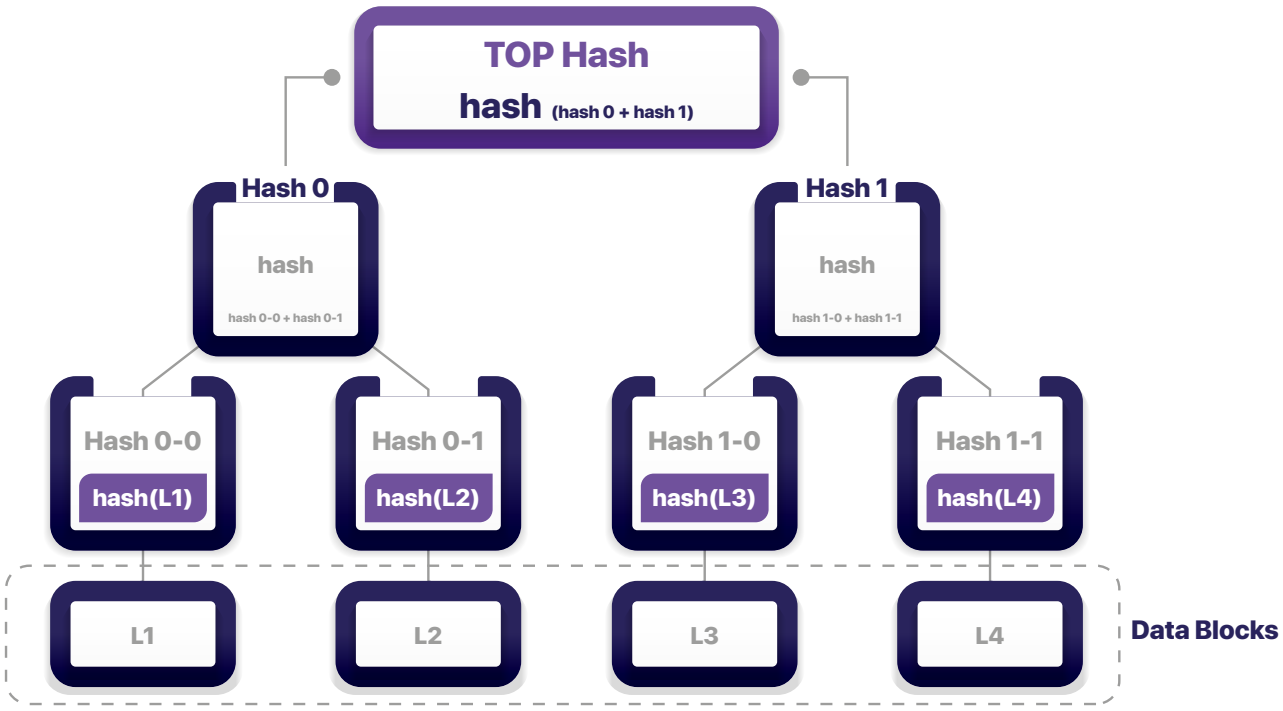
Changing data in a block alters a transaction which will modify the hash value of the block leading to an instant and detectable integrity violation and as a consequence the chain breaks. The use of consensus protocols, which will be discussed later on in this paper, ensures that nodes have to adopt the correct (majority) version of the chain. An attack attempting to modify a block increases in computational difficulty with every new block being added.

Blocks are built continuously, and managed by the underlying consensus protocol.

Structural Data Pillar

A structural data pillar used in blockchain technology is the **"Merkle Tree"**, named after its inventor Ralph Merkle. As laid out above, hashing is extensively used in blockchain technology to provide cryptographic fingerprints of data used to prove its integrity.

A Merkle tree is an efficient way of hashing data by dividing it into small chunks. Chunks are hashed individually, and the resulting hashes are combined and hashed in pairs. This process is repeated up the tree until a single root hash is calculated. The structure of a Merkle tree is illustrated in the "State Machine figure" below.



An interesting property used in blockchain technology is the ability to perform a Merkle proof on data.

A Merkle proof consists in proofing the integrity of data by verifying the correctness of the hashing up the branch of a Merkle tree.

These proofs are very often used in blockchain technology for data storage optimization. For instance, in Bitcoin, only the Merkle root of transactions has to be included in the block header. “Light” clients can request Merkle proofs for individual transactions without having to download all the transactions.

A variation of Merkle trees conforms a Merkle Patricia tree, which is used in the Ethereum blockchain. This variation on Merkle trees has the purpose of providing quick insertion and deletion of in key-value storage maps. This result is achieved by ensuring that the depth of the tree is bounded and that Merkle root only relies on the data, not the sequence in which updates to the data are made. The outcome is a data structure with $O(log(n))$ efficiency for insertion, deletion, and data search.

In the Ethereum blockchain, each block is conformed by three Merkle Patricia roots, referencing the state (the storage of smart contracts), transactions and transaction receipts.

Various Some DLT projects utilize Directed Acyclic Graphs (DAG) as an option.

The above graphics consist of vertices and edges, with edges connecting different nodes.

A DAG is a graph with certain mathematical properties:

- A DAG has a finite number of vertices and edges.
- Each edge is directed from one vertex to another

1. 4 Blockchain’s “Natural Selection” Effects

The concept of a blockchain was first introduced by Bitcoin, and consequently, cryptocurrencies were the first application of this new technology.

Representing transferable value is made possible by achieving consensus on transactions without the need of a trusted third party. Participants are incentivized to maintain integrity by rewards paid in the cryptocurrencies in almost all blockchain implementations.

Bitcoin uses an **unspent transaction output model (UTXO).** Transactions consist of inputs and outputs, each of which holds a certain value. Transactions are chained together by using outputs from one transaction as inputs for another

In the UTXO model, there is no notion of an account with a balance on the blockchain. Instead, client software adds up UTXOs directed to addresses to calculate balances. An address represents a private-public key pair.

Most cryptocurrencies work similarly, although some may substitute the UTXO model for an account- based model. Variations exist in the consensus algorithms used, the block generation frequency, the total currency supply, and other parameters.

In cryptocurrencies, transactions change system state by moving value between accounts or addresses. It did not take much time for people to realize that this idea can be generalized to other types of transactions, such as transferring property deeds or other assets modeled on the blockchain.

Taking this proposal even further to general purpose computing has led to the subsequent generation of blockchains that have the quality of Turing completeness. A computer system is colloquially said to be Turing complete if it permits modeling any problem computationally.

The most well-known general-purpose blockchain is Ethereum, proposed first in 2013 by Vitalik Buterin. Ethereum implements a Turing complete virtual machine which allows deploying decentralized applications in the form of smart contracts.

In Ethereum, transactions are transitions between arbitrary state. Computational resources are protected by associating each virtual machine operation and storage usage with a cost termed “gas”. Like most blockchains, Ethereum makes use of a cryptocurrency, which is used to pay for gas and as an incentive mechanism in the consensus protocol.

Scalability Tradeoffs First and second generation blockchains have limited scalability, which makes them unsuitable for high throughput transaction systems and systems that deal with large amounts of data.

To obtain scalability in a distributed system, exchanges have to be created. It is called the "scalability trilemma", an argumentt which states that 3 interacting axes exist:

1. Decentralization
2. Scalability
3. Security

With current technology, at least one axis has to be relaxed to optimize the remaining two.

Layer 2 Solutions Scalability of cryptocurrency-centered blockchains can be increased by moving transactions onto a second layer off-chain and only use the underlying blockchain for settlement. Payment channels and the Lightning Network are such solutions for the Bitcoin network.

Channels, to be used to make off-chain payments between two parties, are secured by deposits on the blockchain and are settled by on-chain transactions occasionally.

The *Raiden Network* is Ethereum's solution to off-chain scalability.

On Chain Solutions The second layer answers discussed above are viable solutions for payments and token transfers only. To improve scalability in general way, several on-chain answers are now in development, both on existing blockchains, such as Ethereum, and in purpose-built third generation systems.

One suggestion to improve scalability focuses on developing transaction throughput and storage capability. Currently, blockchain nodes tend to maintain a copy of the full system state and process all transactions. This bounds the blockchain's transaction throughput to that of a single node. Furthermore, each node requires an ever-increasing quantity of storage capability.

Sharding is a technique that allows distributed processing and storage between different parts of the blockchain. This has to be done in a way that allows each node to process fewer transactions and store only part of the state, while ensuring overall system integrity is maintained.

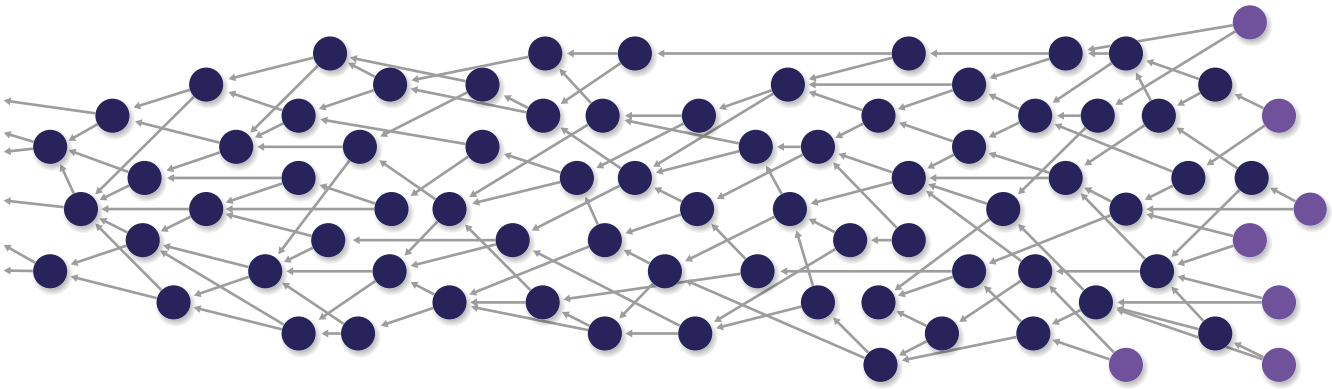
There are also secondary blockchains called side-chains whose objective is specific to its application and whose administration is done by a subset of nodes due to their specific interest. The side-chain and main chain are linked together which is afterwards used as a settlement layer.

In short, side-chains are managed blockchains that usually take a tree structure, take "Plasma" as an example, which is Ethereum's -currently being developed - side-chain solution.

Cosmos, a system based on Tendermint, is natively structured in trees of blockchains. We will discuss *Tendermint and Cosmos* in more detail further on in this paper.

Another approach to accomplish scalability in distributed ledger systems is to supersede the blockchain data structure with a DAG.

IOTA is the most cited DLT project the uses the DAG as a blockchain substitute, which, interestingly enough not only replaces the underlying architecture but also simplifies the consensus algorithm.



In IOTA, the transactions that are separately added to a DAG structure are called "tangle". Under this structure nodes have the ability to forward transactions, though it is necessary that two previous "tangles" are confirmed. In the DAG model, these tangles are represented as vertices and edges approvals which depicts the transitive relation inherent and is shown as follows:

confirm(a,b)^confirm(b,c) ! confirm(a,c)

Meaning that if a transaction "A" directly ratifies transaction "B" and transaction "B" ratifies transaction "C", we consider transaction "A" to indirectly confirm transaction "C". All transaction confirmations lead back to a genesis transaction, in the same way blocks in a linked list lead back to a genesis block in blockchain structures.

Besides the above stated, IOTA also offers an identity solution through a second layer called **Masked Authenticated Messaging (MAM).** MAM taps into IOTA's gossip protocol to transmit encrypted and authenticated messages through the network.

IOTA's target is high throughput transactions and their effective administration by running a coordinator node, and it's recommended, theoretical niche is such as the Internet of Things (IoT) data transfers. The system in place presently guarantees decentralization to achieve scalability and security. The administrator node is run by the system and will be detached once the system has reached critical transaction volume.

There are theories floating around that say security will be compromised when the coordinator is switched off. Due to the absence of a motivation-based consensus protocol, there is no algebraic proof that DAG based transaction verification systems can assure a secure operation once the coordinator is detached.

Given current technology, the most promising trade-off aimed at improving scalability is introducing a **Proof of Ownership based (POO) Byzantine Fault Tolerance** consensus protocol. The Tendermint platform from Cosmos provides an elegant solution to this.

1. 5 Consensus "Algos" and security

Proof of Work

The first consensus algorithm used by a blockchain was Bitcoin's Proof of work. Proof of work consists of nodes competing to solve a cryptographic puzzle. The node finding the solution first decides on the next block to be included in the linked list of blocks in the case of distributed ledgers. Competing nodes are called miners in blockchains that use proof of work.

In Bitcoin, each block includes a field called the nonce. Miners fill up blocks with transactions and then try to calculate the SHA-256 hash of the block. The aim is to find a hash value with a certain number of leading 0s. The nonce is incremented and the hash value recalculated until a hash with the correct number of leading 0s is found.

The winning miner's block is accepted and added to the blockchain. The miner is awarded the mining reward (newly created coins) and the transaction fees. The process is regulated to produce a new block at an average frequency of 1 block every 10 minutes by adjusting the difficulty (modifying the required number of leading 0s).

All proof of work-based blockchains function similarly, although the actual cryptographic puzzle may change. Ethereum uses the *Keccak* algorithm, which forms the basis of SHA-3. Furthermore, blockchains that produce new blocks at a higher frequency, such as Ethereum, have a higher chance of two miners producing a new block at the same time, resulting in more discarded blocks, often called orphan blocks. To mitigate this effect, Ethereum's and other blockchain's consensus mechanism have provisions for also including such blocks into the blockchain.

Cryptographic puzzles, such as those based on calculating SHA-256 hashes can be accelerated significantly by certain types of hardware. The calculations involved are inherently parallelizable. This first led to powerful **Graphics Processing Units (GPUs)** being used for cryptocurrency mining. The next step led to special purpose hardware being developed, leading to the current situation, in which almost all Bitcoin mining is performed on so-called **application-specific integrated circuits (ASICS).**

Some blockchains use ASICS-resistant algorithms, which are specifically designed not to be parallelizable, for example by being memory intensive.

Criticism

The work being performed in proof of work consensus algorithms is not used for anything beneficial. In fact, most of the work is discarded, due to the competitive nature of the protocol. Only the winning's node work is reserved in the form of a new block, and even this work consists merely in re-calculating a hash value repeatedly, serving no other purpose than being the deciding factor in competition.

Even though there have been several attempts to substitute proof of work, but the truth is none of the major blockchains have managed to make use of the computational effort in a meaningful way.

Apart from not consisting of particularly useful calculations, proof of work is a very computational intensive protocol. Thus, it also has very high energy consumption.

Digital cash systems rely on account balances and transfers to be represented digitally in data structures. This introduces the problem guaranteeing that a digital asset, such as a

cryptocurrency unit, can only be spent once. It is trivial to solve this double spending problem in a centralized system, in which a trusted party is in charge of keeping track of balances and transactions. Banks fulfill this role in the traditional monetary system.

The blockchain's transaction immutability property prevents transactions from being undone and balances from being modified retrospectively. However, there is a period, in which double spending can occur, before a transaction has been fully propagated through the network. This can lead to a situation, in which a malicious spender makes two payments in short succession, the sum of which exceeds his balance. One of the transactions will succeed, the other will fail.

Once a transaction has been propagated through the network, the UTXO set in Bitcoin or the equivalent in other blockchains has been modified. Even though the transaction is not included in a block yet, it is relatively safe to assume double spending cannot occur. Such transfers are usually assumed valid for small transfers or micropayment.

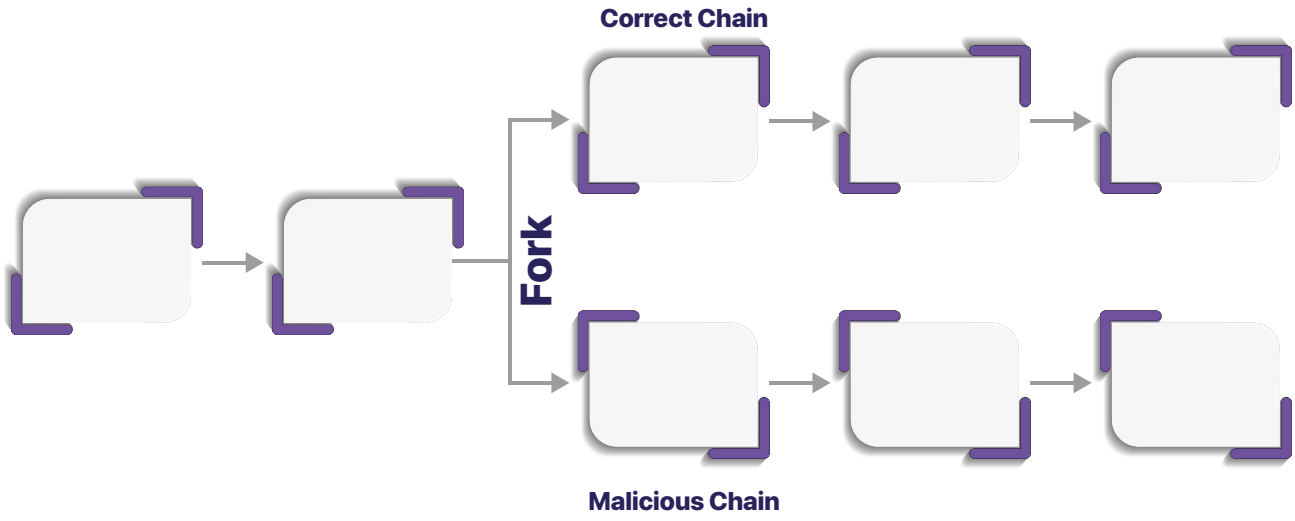
However, to be completely safe of double spending, the transaction should have been confirmed, and several additional blocks should have been added to the blockchain. By convention, a transaction with six confirmations is considered secure.

One or more nodes may wish to modify a transaction or change the state of the blockchain. To do this they produce a fraudulent block and transmit it to the network.

The way consensus protocols work, other nodes that also validate transactions should reject the block and wait for a correct solution. The blockchain now splits in two, a situation which is known as a fork. This type of fork should not be confused with the process of updating the blockchain's software protocols, which is also known as forking and may result in a similar split in the network if some nodes do not adopt the new protocol version.

"*Honest miners*" continue adding blocks to the correct chain, whereas malicious miners support their version of the blockchain. Essentially, there are now two competing chains. In most cases, the minority chain eventually dies out because of lack of support.

The graphic below depicts a fork created by a set of nodes adopting a different version of a block.



For a malicious set of nodes to modify the blockchain and have their version of the chain adopted by the majority, they would need more than 50 % of the networks computational capacity. An attack consisting of malicious miners modifying the blockchain is therefore called a 51% attack.

Note, that modifying the blockchain retrospectively becomes more difficult with each added block, as more blocks need to be recalculated. For this reason, six block confirmations are often quoted as the secure waiting period before a transaction is considered completely secured

Any networked system is vulnerable to a denial of service *(DoS)* attacks. Such an attack consists in flooding the network artificially with requests, to block resources and make the network unusable.

Decentralized systems are generally considered more resistant to DoS, but there are situations in which blockchains can be attacked this way.

DoS is prevented in blockchains by associating a cost with transactions and resources. In the case of Ethereum, gas is required to execute transactions and use storage. In the past, the cost of operations has had to be increased via a protocol change because of a DoS attack.

Test networks that use worthless test Ether have also frequently suffered from DoS attacks.

Proof of Stake

Proof of stake is an alternative protocol to proof of work that uses wealth instead of computational power as the basis for deciding on the next block.

Nodes stake a number of coins in the form of a given blockchain's native cryptocurrency, to be used as collateral in case of dishonest decision making, then they (nodes) bet on the next block. As a result, the winner is chosen by an algorithm which mixes the number of coins at stake.

As logic dictates, the bigger a participant's stack of coins/tokens, the higher the probability of being picked as a winner. However, other factors such as coin longevity are taken into consideration. When a network fork takes place, participants vote on what they think is the better chain and this takes place by committing their coins, resulting in the loss of coins by the group supporting the wrong chain.

The Ethereum blockchain is scheduled to switch from proof of work to proof of stake under the consensus protocol they've named **"Casper".**

In the proof of work consensus, forking can occur the same way it does in proof work-based solutions. Validators might not agree on the correct version of the next block, thus, through voting, a fork takes place in the chain.

It is often argued that while an attack on the network is cheaper in proof of stake, it is also easier for the community to react to the attack and correct the problem.

Early proof of work systems suffered from the nothing at stake problem. This problem occurs when nodes decide to support both chains in case of a fork. As they have nothing to lose, nodes may create new blocks in each chain, to guarantee the best outcome for themselves, no matter which chain establishes itself as the majority chain.

Most proof-of-stake-based blockchains have introduced penalties for supporting the wrong chain. This means that in addition to block rewards, block penalties exist and are executed when a node supports a minority chain in a fork.

Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance was the original proposal aimed at solving Lamport's Byzantine General Problem. The PBFT algorithm relies on a state machine that is replicated on each node. Each state represents a system view through which the state machine transitions.

Nodes reach a consensus by an algorithm that relies on one to two thirds of the nodes to be honest. This means that the number of nodes that are required to collaborate is higher than in the proof of work-based solutions, where more than 50% of computational power is enough for network safety.

The advantage of PBFT is a very high transaction throughput resistant network. The disadvantage however is that the algorithm scales badly. In practice, it can only be used to reach consensus between a small number of nodes.

1.6 Fault Tolerance & Its Properties

The type of faults a system can tolerate must be defined when designing a distributed system and fault tolerance considerations are important. To achieve this a failure model has to be built. The simplest failure model out there is the "crash-failure" model. In this model, nodes crash and recover. The model is supported by all blockchain implementations, as the underlying protocols assume that nodes can join and leave at any time. Commonly, for a node to send transactions, it has to wait until it has fully synchronized itself to the latest blockchain state.

Unreliability of communications is intrinsic to distributed systems, and a blockchain implementation has to make provisions for recovering from networking issues.

In distributed systems network links may fail, leading to isolated nodes and network partitions. A network partition is a disconnected sub-network that cannot communicate with the rest of the system. Supporting and recovering from network partitioning involves interesting trade-offs, which we will discuss further on in this section.

The Byzantine failure model is the underlying model that makes Byzantine consensus necessary. In this model, components such as nodes may fail in arbitrary ways, even by acting maliciously. There is imperfect information on whether a component has failed. Practically supporting the Byzantine failure model is one of the key reasons for using a blockchain based system.

Finally, a distributed system can be a victim of timing failures. This means that nodes may measure time differently and system clocks cannot be pretended to be perfectly synchronized. Messages are always subject to delays depending on the system clocks, interactions, etc.. In theoretical distributed systems research, a distinction is made between synchronous and asynchronous systems. In the former, clocks are perfectly

synchronized, and message delivery is guaranteed within a specific time limit. In asynchronous systems, no such assumption can be made.

On the upside, blockchain systems tend to implement practical solutions, such as making weak requirements on clock synchronization within a maximum permitted offset and using consensus to agree on a single view of message ordering.

For a distributed system to be considered fault-tolerant, there are various properties a system should fulfill. The first property is consistency.

Informally, consistency in distributed systems refers to the fact that all nodes should have the same view of the systems state. In a strict interpretation, this means that every read operation on any node should return the result of the latest write operation on any node.

Consistency is very difficult to achieve since it depends on the exact order of the messages that are sent and received throughout the network. It complicates more when it has to be synchronized by system clocks. The order of the messages cannot simply be guaranteed by simply time-stamping messages.

Several consistency models exist in **Theoretical Computer Science,** the most important of which are:

- **Atomic Consistency.** A strict model which implies all write operation should be seen immediately on all nodes.
- **Linearizable Consistency.** Atomic consistency can be relaxed to take into account message delivery delays, placed under a real-time constraint. The model is still not very practical for most real-world systems.
- **Sequential Consistency.** Relaxing the constraints further, a model can be defined, in which each the result of operations is seen in the same order on every node in the system. However, the order of operations may vary between repeated invocations of the operations. Informally, it can be said that nodes agree on the order of transactions.
- **Causal Consistency.** In this model, only write operations that are causally related have to be seen in the same order on each node. Informally, this means only write accesses on data that depend on each other have to be executed in the same order on all nodes.
- **FIFO Consistency.** The feeblest model presented here declares that all write operations emitted from a single node have to be seen in the same order on all nodes. Operations emitted from other nodes may be interleaved in different orders.

In Blockchain systems, miners or validators order transactions sequentially in the order they see fit. They usually use an optimized profit algorithm for including transactions based on transaction fees and transaction size. Once a block is accepted, all nodes adopt this order. Therefore, blockchain consensus is based on a sequential consistency model.

Partition Tolerance

One last characteristic that defines de fault tolerance of distributed systems would be the capacity to understand and resolve communication failures, it is said that in case there is a network failure partitions can continue independently and recover after the network is back.

In a blockchain system, network partitions invariably lead to two versions of the chain that need to be consolidated by the consensus algorithm.

CAP Theorem

CAP Theorem is a concept that a distributed database system can only have 2 of the 3: Consistency, Availability and Partition Tolerance. The theorem states that it is impossible to give strong guarantees on more than two of the three properties.

In reality, this translates into the case of network partitions, a system can either provide high availability or strong consistency. This is intuitively obvious, as it is only possible to continue operating in two or more disjoint partitions independently if overall consistency is relaxed.

In Blockchain systems the theorem is important if proof of stake consensus protocol is used. The consensus algorithm has to favor one over the other. BFT based consensus protocols, such as the protocol used by Tendermint strongly favor consistency over availability.

Sharding

Sharding is a concept borrowed from database technology, where databases are partitioned horizontally. Different partitions, or shards, are stored on different servers to distributed load.

In blockchain systems, each node traditionally maintains a copy of the full blockchain, as well as state and transactions. Actually, the transaction history could be cropped for storage proficiency, but conceptually the whole chain is replicated on each node.

Enforcing the sharding principle to blockchains is a step aimed at improving the scalability of the system. As in database technology, nodes only hold certain shards of the blockchain, distributing storage and transaction processing load across the network.

There is an evident problem in sharding blockchains, in that everything in a linked list of blocks is sequential and splitting this up into different shards requires a more hierarchical approach. Essentially, a series of individual chains are created, one for each shard.

To maintain the overall chain, these shards need to somehow connect to the main chain. This is similar to the sidechain scalability method that'll be discussed later. However, shards may not be set up for a particular application and do not require application-specific nodes to explicitly maintain the chain. Collators on each shard will be responsible for creating collations, which are descriptions of the shards state. Collations from different chains are included in blocks on the main chain.

A new nodes hierarchy is introduced with Ethereum's Plasma sharding model, consisting of these node types:

- Collations from different shards into main chain blocks as well as full-nodes maintain every collation and the main chain.
- Top-level nodes operates the main chain and grant access to all shards.
- Single-shard-nodes are the same as top-level nodes, though they maintain all the collations of their particular shard as well.
- Light nodes only maintain block headers from the main chain but can request state from different shards when required.

In a sharded system that follows this model, blocks will be validated only if the transactions included in all collations are valid. The rest of the collations as well have to be signed by a definite amount of collators, usually two thirds.

Sharding faces several challenges among these two:

Single-Shard Takeover Attack A problem in sharded blockchains is that a lesser number of nodes than the whole chain gets the task of keeping the shard. It will be simpler for a hacker to get hold of a wider majority in a single shard to manipulate data. This problem is known as the 1% attack, based on the assumption that in a 100-shard system it takes 1% of the networks hash rate to dominate the shard.

Choosing filters for shards by means of random sampling and changing this sampling frequency can alleviate this issue.

Sorting and changing collators arbitrarily is easier, collator nodes can be sampled by chance from the set of validators that take part in staking .

Cross-Shard Communication In order to maintain the atomicity property of transactions, communication between shards has to performed via the main chain.

Sending a transaction from shard A to shard B can be achieved in the following steps:

1. Send a transaction to shard A , applying state delta.
2. Create a transaction for shard A , which is stored in Merkle root.
3. Send a transaction to shard B , including the Merkle receipt as data.
4. Shard B checks that the Merkle receipt has not been spent yet.
5. Shard B realizes the transaction in state delta D, publishing that the Merkle receipt has not been spent .
6. Shard B creates a new Merkle ticket that can be used in subsequent exchanges.

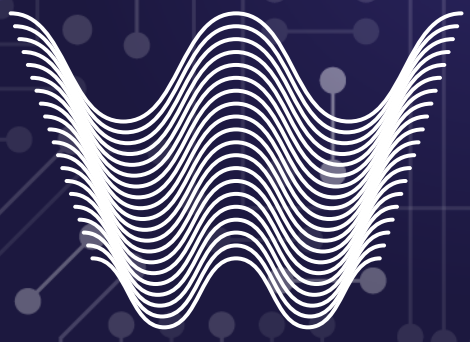
As a proper conclusion to this section, it is worth noting that we have presented an overview of the technologies used for decentralization. Blockchain and related technology can be used to develop secure consensus-based decentralized systems. We have discussed several key technologies and data structures and their purpose. We have also highlighted security, fault-tolerance and scalability issues.

While blockchain technology makes some innovative applications possible, it is currently not well suited for data-intensive applications or use cases that require high-throughput transaction processing.

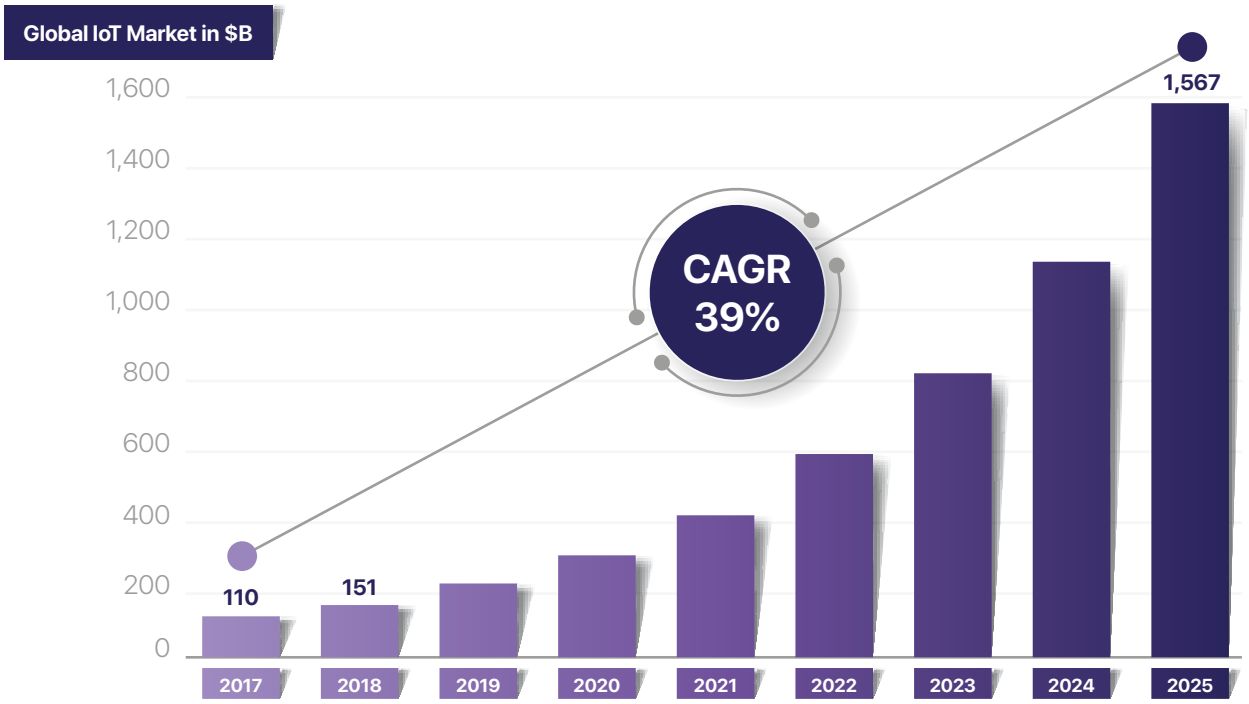
We believe that the most promising solutions for such as system are based on a decentralized off-chain storage layer, such as IPFS, in combination with a lightweight and flexible consensus layer, such as a Tendermint- based DPoS BFT consensus blockchain architecture.

Now, let's move on...

2. Targetable Market



The Global Internet of Things (IoT) market reached USD 110 Billion in 2017 and the market is expected to reach USD 1,567 Billion by 2025. Further, the market is projected to register a CAGR of 39% during the forecast period 2017-2025 globally, being consumer electronics the industry with the largest market size.



Note: Market defined as total spend of End – Users on IoT solutions
Source: IoT Analytics

The global market for Internet of Things (end-user spending on IoT solutions) is expected to grow 37% from 2017 to $151B. Due to the market acceleration for IoT (as discussed above), those estimates have been revised upwards and it is now expected that the total market will reach $1,567B by 2025.

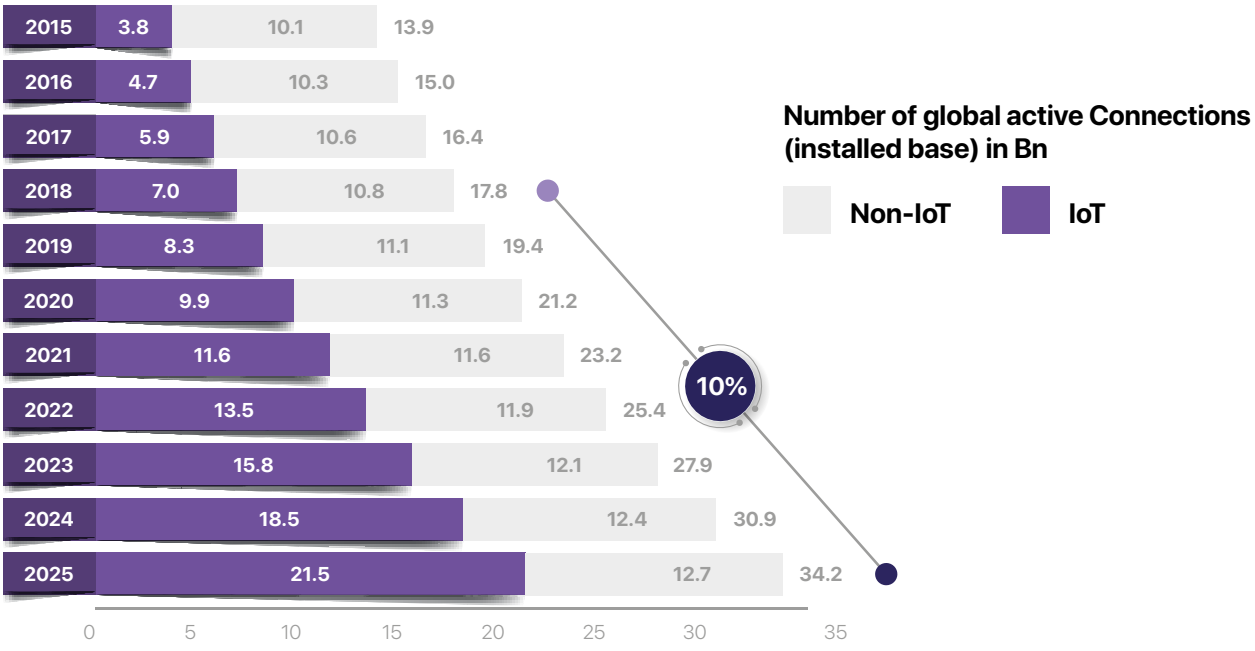
Today's market environment is extremely dynamic and there are a few dozen trends that can be observed including edge-to-cloud integration, TSN connectivity, and IoT & blockchain trials, for example, highlights that cloud vendors now increasingly make their own cloud-ready hardware to improve the interoperability and performance between IoT devices and the data that gets stored and analyzed in public or private clouds. *Leading IoT cloud providers Microsoft, Amazon, and Google all recently announced their own hardware*.

The market for Internet of Things has seen a somewhat unexpected acceleration in Q1/Q2 2018 and has lifted the total number of IoT devices that are in use to 7B. This is one of many findings in IoT Analytics' latest *"State of the IoT & Short-term outlook"* update.

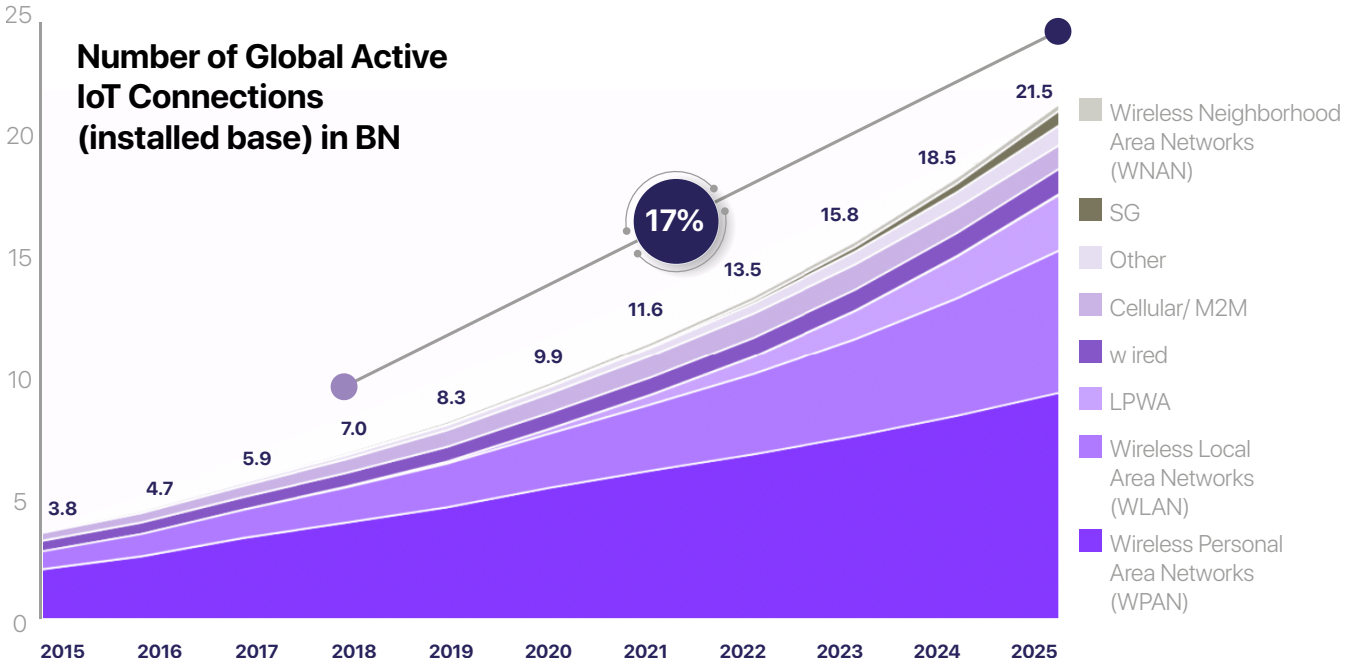
The current global number of connected devices are 17B. The number of connected devices that are in use worldwide now exceeds 17 billion, with the number of IoT devices at 7 billion (that number does not include smartphones, tablets, laptops or fixed line phones).

The global connection growth rate is mainly driven by IoT devices – both on the consumer side (e.g., Smart Home) as well as on the enterprise/B2B side (e.g., connected machinery). The number of IoT devices that are active is expected to grow to 10 billion by 2020 and 22 billion by 2025. This number of IoT devices includes all active connections and does not take into consideration devices that were bought in the past but are not used anymore.

Total number of active device connections worldwide



Global Number of Connected IoT Devices



Note: IoT devices do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensor/actuator. Simple one directional communications technology not considered (e.g. RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low – power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes non – short ranges mesh; Others include satellite and unclassified proprietary networks with any range.
Source: Iot Analytics Research 2018 and State of the IoT & Short term outlook 2018"

From a device connectivity point-of-view the dynamics vary extremely

Wireless Personal Networks (WPAN)

The highest number of IoT devices are connected through short-range technology (WPAN) that typically does not exceed 100m in maximum range. These include Bluetooth-connected devices such as headsets but also Zigbee and Z-wave connected devices that can mostly be found in smart homes e.g., for connecting smoke alarms or thermostats.

Wireless Local Area Networks (WLAN)

Another large category is Wireless Local Area Networks that cover connectivity of up to 1 kilometer. Wi-Fi is the most common standard in this category and seeing great growth, mostly through the use of home assistants, smart TVs, and smart speakers but also increasingly through use in industrial settings such as factories (although it continues to play a minor role in those settings compared to other technologies).

Low-power Wide Area Networks (LPWAN)

A large portion of the future growth in the number of IoT devices is expected to come from low-power wide area networks. By 2025, it is expected that more than 2 billion devices will be linked through LPWAN. The technology, which promises extremely high battery life and a maximum communication range of over 20 kilometers is used by three main competing standards, Sigfox, Lora, and NB-IoT, which are currently being rolled-out worldwide with more than 25 million devices already connected now, the majority of which are smart meters.

Wired

Few people think of wired connections when they think of IoT. However, in many settings a wired device connection is still the cheapest and most reliable options. Particularly in industrial settings, fieldbuses and ethernet technologies use wired connections to a large extent and are expected to remain doing so in the next years.

Cellular / M2M

2G, 3G, and 4G technology had for a long time been the only option for remote device connectivity. As LPWA and also 5G gain momentum, it is expected that these legacy cellular standards will lose share to the new technologies as they present a more lucrative opportunity to many end-users.

5G

5G is the wildcard. Still under development in 2018, the technology which promises a new era of connectivity through its massive bandwidth and extremely low latency, is now heavily promoted by governments, particularly China. The Chinese government views 5G adoption as a competitive asset in the quest to move the equilibrium of technological innovation from the US and Europe towards China.

In the US, the first pre-standard 5G networks will provide **Fixed Wireless Access (FWA)** services to residential and small-business users by the end of this year. While many more use cases will be targeted once the final standard is ratified in 2020, we should see first adopters already next year and do expect quick growth from there.

Wireless Neighborhood Area Networks (WNAN)

Wireless Neighborhood Area Networks (WNAN) sit in between WLAN and long-range technologies such as cellular in terms of communication range. Typical proponents of this technology include mesh networks such as Wi-Sun, or JupiterMesh. In some cases the technology is used as an alternative for **LPWA/Cellular** (e.g., in Utilities Field Area Networks) and in other cases as a complimentary element (e.g., for metering deep in-door where nothing else reaches).

Other technologies, such as satellite and unclassified proprietary networks will continue to play a role in the Internet of Things, although minor compared to the other technologies.

Market according to the regions and others

Companies across the board, most notably IoT software, cloud and services companies, far exceeded revenue expectations. Microsoft Azure and Amazon AWS grew 93% and 49% respectively (within the last 12 months) with their IoT portion contributing significantly to the growth. But smaller players like C3IoT also reported a 60% revenue increase for the year.

9 regions: The United States, Asia/Pacific, Canada, PRC, Japan, Western Europe, Central and Eastern Europe, Middle East and Africa, and Latin America.

53 countries: United States, Canada, Japan, Czech Republic, Hungary, Poland, Romania, Russia, rest of CEE, Israel, Saudi Arabia, Turkey, United Arab Emirates, South Africa, rest of Middle East and Africa, Australia, Hong Kong, India, Indonesia, Korea, Malaysia, New Zealand, PRC, Philippines, Singapore, Taiwan, Thailand, Vietnam, rest of Asia/Pacific, Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, United Kingdom, Argentina, Brazil, Chile, Costa Rica, Colombia, Mexico, Peru, Venezuela, and rest of Latin America.

14 technology markets:

Across hardware, software, services and connectivity categories; Hardware — Modules/ sensors, application software, and security hardware; Software — IoT purpose-built platforms (horizontal and vertical industry), storage, analytics software, and security software; Services — IT and installation services, and Ongoing/Content services; Connectivity.

95+ use cases including:

Connected vehicles, health & wellness, emote health monitoring, autonomic operations, insurance telematics, smart lighting, personal wellness, r smart buildings, environmental monitoring and detection, supply chain logistics enablement of data markets.

20 Industries:

Banking, telecommunications, construction, discrete manufacturing, consumer, education, healthcare provider, insurance, media, federal/central government, professional services, process manufacturing, resource industries, retail, securities and investments, personal and consumer services, state/local government, transportation, and wholesale

Application Insights

Consumer electronics application segment accounted for nearly 30% of the market acquiring a major share of the overall industry revenue.

The connected car concept has proved to be another successful application in the Internet of Things industry. A connected car is connected to the network in real time and provides vital information from the car to the users. In the case of emergencies, connected cars send out a message seeking assistance, which also indicates the coordinates of the location.

IoT-based technologies have the potential to improve visibility in manufacturing to such that each unit of production can be seen during the production process. Moreover, the proliferation and increasing installations of industrial robots have positively impacted the Internet of Things industry.

Regional Insights

The presence of major technology providers has led North America IoT market being a dominant force. The entry of technological giants such as Cisco, Google Inc., and Samsung into the market has led to the development of innovative connectivity solutions across various applications and devices.

Privacy and data security in the Internet of Things scenario are the major issues being acted upon by regulators in the U.S. to create a connected environment for optimal security. Moreover, the EU Commissioner's report on Internet of Things concept recommends certain standard requirements to be followed that underpin the right of deletion, right to be forgotten, data portability, privacy, and data protection principles.

Asia Pacific region acquired over 35% of the global revenue share in 2014 and is projected to grow at a CAGR close to 18% from 2015 to 2022. Increasing penetration of high-speed internet services and a declining average selling price for sensors and modules in the region are expected to push industry growth over the forecast period.

Competitive Market Share Insights

Technology giants have stepped up their R&D investments in the sector to gain the early mover advantage. Moreover, companies are increasingly taking up mergers and acquisitions as their principal growth and market entry strategy.

The acquisition of Nest, a learning thermostat maker by Google and the acquisition of Basis, a wearable fitness manufacturer by Intel have enabled them an easy entry into the industry.

The industry is highly competitive and is driven by technological and product innovations. Major industry participants include Accenture PLC, Alcatel-Lucent, Amazon.com Inc., Atmel Corporation, Cisco Systems Inc., Google Inc., Hewlett-Packard, Huawei Technologies, IBM, and Oracle.

Global enterprise usage of data generated from IoT solutions (2017)

Type of data

Improved customer experience Current 70 | Expected 29	Improved capabilities Current 53 | Expected 45	Loss prevention Current 52 | Expected 43	Supply chain visibility Current 53 | Expected 42
Facilitate collaboration Current 52 | Expected 44	Risk management Current 52 | Expected 43	Improved safety Current 56 | Expected 40	Product innovation Current 48 | Expected 48
Expansion to new markets Current 41 | Expected 51	Process improvement Current 52 | Expected 46	Improved asset utilization Current 51 | Expected 45	Employee management Current 52 | Expected 43
Cost efficiencies Current 53 | Expected 43	Improved forecasting/ planning Current 51 | Expected 46	Increase revenues Current 44 | Expected 53	Other Current 16 | Expected 14

This survey shows the plans of enterprises to make use of data generated by the internet of things (IoT), as of August 2017. Seventy percent of the respondents were reportedly already using that data to improve customer experience and a further 29 percent were expecting to do so in the near future.

In the same way that the Internet grew from mainframes to servers to PCs to mobile, to IoT devices, both artificial intelligence and blockchain are spreading through the same path and are ready for IoT (Internet of Things). These sectors of technology are converging into something called the Internet of Things 2.0—the intersection of the decentralized cloud, big data, artificial intelligence, Internet of Things, and blockchain at the intelligent edge. Combining these technologies will enable a decentralized intelligent machine economy for IoT devices that will overcome the current dominance of a few centralized players.

For example, devices will be able to learn from one another to form a self-learning economy, thus improving on current cloud systems such as Amazon Web Services and standard machine learning datasets like ImageNet. Devices will be able to collaborate directly with one another, without going through a central service like HP- Enterprise or Microsoft Azure.

Machines will be able to exchange data and value in milliseconds, replacing the need for Visa or Pay-pal. A new revolution of blockchain hardware will spawn, replacing companies like ARM Holdings and democratizing data farms produced by Google and Apple.

There are still, several obstacles in the middle, preventing devices from becoming intelligent and interactive. Dissimilar devices could exchange data if these limits were to be eliminated, There are three verticals in IoT that need attention. Dissimilar devices could exchange data if these limits were to be eliminated, There are three verticals in IoT that need attention, if one wants to pursue an intelligent machine economy:

1- Scalability
2- Intelligence
3- Functionality

Internet of Things, known as IoT, refers to the ever-growing amount of devices connected to the Internet such as self-driving cars, smartphones, wearables, smart cities, airplanes, and computers. The estimated number of devices increases 31 percent every year, with a projected 200 billion new devices entering the ecosystem by 2020.Though Internet of Things is often said to be the fourth industrial revolution and has the potential to automate and transform our lives now, there exists three main problems with IoT withholding its full potential: connectivity, intelligence, and functionality.

In order to connect all devices, scalability is needed to handle the explosive growth in IoT where applications will need to support an increasing number of devices, analytics, data, and users. The majority of current devices are controlled in a centralized manner where devices connect to back-end cloud infrastructures or data centers. As a result, current scalability methods will be ineffective as billions of devices are connected.

Current methods lack:

1. **Decentralization -** Current centralized devices have “brokered” communication models where devices are connected, identified, and send data through a cloud model. Cloud servers will remain a bottleneck and contain a single point of failure that can disrupt a network.

2. **Efficiency -** Current devices have limited bandwidth, computational resources, memory, and resources to handle complex tasks.

3. **Privacy -** Conventional ways to maintain privacy include adding noise or summarizing data when communicating with the server. Existing approaches welcome privacy threats through localization, identification, MITM attacks, profiling, and data leakage.

Current scalability methods limit the potential adoption and real-world applications for the massive influx of Internet of Things devices. Also, machine intelligence is needed to be specialized in IoT devices in each aspect, from "Go playing" computers to self- driving cars. Despite breakthroughs in the field of deep learning algorithms that have enabled human-level performance on perceptual tasks and created novel algorithms ranging from capsule networks to echo state networks, the bane of machine intelligence and real-world applicability for IoT can be found in training data and hardware acceleration.

A vital component for training neural networks is data. Data makes it possible for machines to learn to adjust to new inputs and perform perceptual tasks with human-level performance. However, data is so valuable, that large corporations hoard and tightly guard data. Current issues with data include:

1. **Private Data -** Personal or confidential data such as medical, personally-identifiable, and education- related data are illegal to share and thus cannot be trained.

2. **Centralization -** Large corporations like Facebook and Google are collecting vital data off of users and IoT devices and storing it for internal use.

3. **Knowledge Domains -** Models are not generalizable, and as a result, there exists too many data types such as sound, image, and 3-D images scattered across various databases.

4. **Incentive -** There are no methods or incentives for people to monetize and share data that they collect from devices.

Custom hardware is a must to supply the desired performance to allow tasks that usually depend on human cognition and learning on the hardware itself. As the entanglement of networks develops, larger IoT devices are required to instruct networks. For smaller devices, it becoming too computationally challenging to train or re-instruct neural network layers.

Some issues with AI hardware might include:

1. **Large Processors -** Current machine learning systems and applications typically consist of a very power-full workstation outfitted with very high-performance GPUs that serve as a centralized training machine to run neural network back-propagation algorithms.

2. **Processing Power -** Implementing deep neural networks on edge devices will be an obstacle. Training on CPUs will not function properly as they lack neural and matrix acceleration optimization on the edge.

3. **Design -** Conventional hardware is not designed to run brain-like algorithms and fully utilize artificial neurons.

4. **Blockchain -** Hardware is not optimized for blockchain networks and may not support the safe usage of cryptocurrencies.

The value and functionality from IoT devices come from the interactions, learning, and cooperation between other devices. Simply being connected does not bring many benefits to an IoT device as most solutions today lack meaningful applications. Even so, a staggering 85 percent of IoT devices cannot interact with one another because of compatibility issues.

Note: Check our Full Deck on https://wise.cr for much more in depth information on market share and total addressable market

3. Wise Overview

As described in length and detail, the blockchain is a public, immutable, distributed ledger technology that can be used for transacting with data in a distributed and decentralized manner. By creating an analog-mixed- signal, system-on-a-chip (AMS-SoC) embeddable in any physical object, using Proof of Ownership to deliver consensus for a distributed ledger on a private blockchain with a public blockchain as a layer two to create a massive market for WSE utility token, Wise Network aims to address the major problems with the Internet of Things to enable these devices to become connected and intelligent (through data sharing and interoperability). This section will detail why blockchain can be used for IoT as well as Wise's blockchain design principles to create our own ecosystem that'll enable the beginning of M2M *(Machine To Machine)* economy.

Returning to the subject, the properties of a blockchain such as its trust-less nature, decentralization, immutability, programmability and security provide advantages for the Internet of Things devices.

Let's examine them individually:

Security

Networks that run on the blockchain are fault tolerant and can withstand up to 1/3 node failures. With Byzantine fault-tolerant models, components are allowed to fail in the system if their local state becomes corrupt, their connection breaks, or if their outputs are malicious. The fault tolerance system operates well in the real world where nodes in the system may behave in unexpected and unpredictable ways. As a result, many desired networks security aspects can be achieved with byzantine fault tolerance such as defending against MITM attacks and DDoS.

Programmability

Programmability on the blockchain in the form of smart contracts enables device autonomy where trust-less exchanges between devices can happen that are verified through the code and other nodes. Programmability can be extended to IoT devices, which are usually static, and enable various ex- changes and interactions between them.

Immutability

Data posted on the blockchain is immutable, meaning it is unalterable, providing transparency and audibility for all devices that perform a transaction over the network. Immutability can be useful in many scenarios since it prevents someone from tampering with the data and enables everyone to query the chain to access applications such as authentication, timestamps, audit trails, and identity management. This addresses the issue of security as well as the reputation and trust the provider can earn.

Decentralization

Blockchains are politically decentralized -no one controls them-, architecturally decentralized -no central infrastructural point of failure-, but they are logically centralized -there is one commonly agreed state and the system behaves like a single computer-. This way, blockchains work in a decentralized, trust-less way for interconnecting devices and exchanging value. In consequence, blockchain reduces transaction fees and enable instant fee-less micro-transactions freeing itself from the middleman, such as Paypal or Moneygram for example. Decentralization can address the problem of privacy and data concerns imposed by companies that monopolize the market. It can provide an open environment where devices can freely connect to and directly interact with one another.

Blockchain Programmability has very important applications that can be brought to the IoT industry. Some of those applications are:

1. **Distributed Computing -** Shared resources and workloads like computation, memory and storage on edge can be distributed by machines, collecting rewards for what they share.

2. **Federated learning -** Machines can train off private data without ever sending it, leaving training data distributed while improving models' accuracy.

3. **Cryptocurrency -** A instant and near-fee-less digital currency can be used as a way to pay for data and algorithms while providing incentives for others to share it.

4. **Secure Interactions -** Devices can develop a reputation based on previous transactions and start to self-organize and use peer-to-peer discovery clients to interact with non-malicious nodes. Thus, learning from experience.

5. **Data Sharing -** Data can be securely sent off the chain and be hashed on the blockchain.

6. **Imitation learning -** Machines can teach one another the correct policies during training.

7. **Smart Contracts -** Developers can code their own contract in which devices are forced to obey.

In practical terms, applications such as distributed computing will address problems with limited processing power on the edge; federated learning will address some problems with untapped data and allow devices to be compliant with data consent and security laws; cryptocurrencies are a secure method to exchange assets and data, encouraging nodes to participate in the network ecosystem.

The Challenge of Blockchain Networks for IoT

In spite of all the benefits of blockchains, current networks come with a big computational overhead and low finality. Network architectures do not have the capacity to handle billions of interactions that IoT devices do manage every single day, also they do not support adoption in the “real world”. Pioneer network architectures such as Bitcoin or Ethereum are based on codes such as the Proof-of-Work consensus and "One Blockchain, Many Applications" design, which is becoming useless. Blockchains that grew from these older principles have a low transaction rate (10-20 transactions per second), high transaction cost (.80 cents), try to fit in many applications in one chain, and have nodes doing computationally expensive useless work. These blockchains are not able to exchange information with one another since they concentrate on their own applications instead of working together. Even newer DAG solutions have heavyweight operations, where sending a transaction forces small devices to do proof of work. As a result, traditional blockchains and even newer versions are not suitable for IoT devices. For example, smaller IoT devices such as sensors and wearables might be incapable of:

1. **Proof of Work Mining -** Smaller devices cannot be turned into miners as they face computation and power restraints.

2. **Storing Data -** Devices cannot store training and chain as they face memory and storage restraints.

3. **Connectivity -** Devices in rural areas might face latency issues and will not be able to have a steady connection.

4. **Running full nodes -** Devices cannot verify full blockchains as downloading a whole chain might require upwards of 50 gigabytes of storage.

5. **Ternary Operations -** Blockchains, DAGs or CPUs cannot work with ternary operators.

6. **Cold Storage -** With IoT devices getting hacked from things like BotNet, devices cannot safely store or utilize cryptocurrency.

Hence, many deep learning distributed applications and blockchain operations might not be appropriate for IoT devices.

Not only are there architectural problems, but, all cryptocurrencies face adoption issues, and the space is highly speculative. Bitcoin and Ethereum have had valuations of 150+ billion and 70+ billion respectively in 2018 because they are the most adopted networks in the space despite their underlying technology. However, no cryptocurrencies can gain widespread adoption because of their design and the underlying infrastructure. For cryptocurrencies and blockchain technology to start gaining adoption, they need to be:

1. **Efficient -** Transaction fees should be kept at the minimum, with low confirmation times, and energy efficiency.

2. **Legacy Compatible -** Systems such as current CPUs and hardware urge Blockchains or DAGs to be backwards compatible.

3. **Private and Secure -** Flexibility (public or private) should be a main characteristic of blockchain, so it can meet related IoT tasks at hand.

4. **Simple -** Blockchains and their respective cryptocurrencies should be simple to use and seamless. Converting crypto to crypto in exchanges is a complex task for the layman.

5. **Safe -** With cryptocurrency exchanges and hot wallets getting hacked, the cryptocurrency someone uses is not retrievable.

There is a new and different concern, such as the invention hardware wallets. They were implemented at first to secure and store cryptocurrency. Wallets tend to be extremely secure, and the only way to store and manipulate large amounts of currency. They are “attack-safe” and can store keys that are retrievable through seeds which is its main principle, isolating private keys from vulnerable IoT devices.
As in every industry, there are a couple of products or more striving to be the first in line. The most praised forms of hardware wallets include the Trezor Model T or the Ledger Nano S. The only disadvantage is that they resemble a USB key which is impossible to use with a lot of IoT devices.
The security of a hardware wallet and the convenience of a hot wallet is needed for IoT devices and for cryptocurrency adoption to grow. Even with security steps improvement such as Arm’s Trust Zone, cryptocurrencies remain unlockable if a malicious programmer can read the device’s memory.

Wise's Public Blockchain-Mesh-Network Solution Design

WPBMN (Wise's Public Blockchain-Mesh-Network) aims to connect IoT devices and provide the infrastructure for a M2M economy. To achieve this goal**,** **WPBMN's** design is aims to accomplish:

True Decentralized Scalability

Given the evolving chaotic nature of Internet of Things, WPBMN's architecture needs to be designed for anarchic scalability and must constantly evolve to fit the IoT ecosystem. As the complexity of IoT grows, varying systems must be included to support billions of different IoT links, while interactions between autonomous entities, and new entities joining the system without risking failure. Subsystems and permissoned subchains will also most likely need to be added to increase privacy, control, and reliability in spaces like military or healthcare fields.

Separation of Duties

One blockchain addressing all applications is a very inefficient design of IoT devices. Having all devices connect to a single blockchain limits scalability and makes the chain very heavyweight. An ideal solution would be to allow multiple different blockchains to be created with different use cases and enable these networks to interoperate with their own governance properties.

Portable

With all different device types and existing hardware, **WPBMN** should be able to be used in IoT devices such as existing CPUs, sensors, and adaptability to new hardware. Transactions on the blockchain should be configured and optimized towards the device type, empowering devices with lower memory and power to participate in the consensus while allowing better suited devices to run full nodes always taking into account connectivity.

User Friendly

For adoption to grow in blockchain technology, **WPBMN** will need to have a simplistic, developer and user-friendly design. Blockchains and smart contracts on WPBMN should be able to be created easily with any programming language and with minimum validator nodes. The resulting blockchain should still be a low latency, a high finality, and a high throughput network. The conversion process from the resulting cryptocurrencies should be seamless from one chain to another.

In addition to solely providing the infrastructure, **WPBMN** will need to be designed to provide the applications to enable devices to create the intelligent machine economy. To achieve this vision, WPBMN's application is configured to allow devices to be:

Connected

WPBMN will need to enable all devices to be able to find one another, self organize, lend computational power, and have ways of exchanging information and value with one another in an instant. As devices in the network might be malicious, security implementations will be in place to allow devices only to interact with positive nodes and cleanse the negative ones from the network.

Flexible

WPBMN will need to provide audit trails or ways for human owners to manage their devices in cases when they are not acting or functioning properly. WPBMN would also need to provide owners the ability to add permissions to the data that their devices share and the amount of identifiable information they would want to provide in the network.

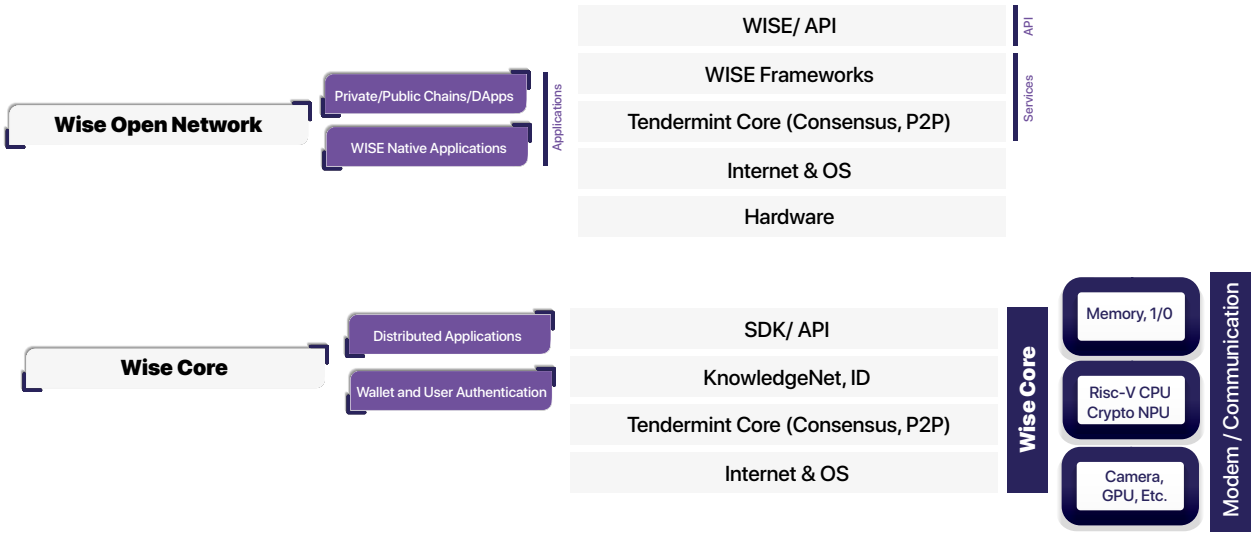
Blockchain Compatible

IoT devices will be able to connect to our WPBMN, and in the future to enable devices to choose the network as new solutions might be developed on other networks, machines should have the ability to choose to use whatever network suits them at the time.

Design Propositions

Wise Network aggregated all the design propositions into Wise's Public Blockchain-Mesh-Network, a safe end-to-end, distributed artificial intelligence system that will foster collaboration and intelligence between all the devices in its network. To address both the adoption of cryptocurrency and limitations of intelligence in hardware, Wise is comprised of a secure memory chip (ANSUZ SMC), an AI embedded blockchain chip. To address the scalability, overhead, and limited applications in traditional blockchain networks, Wise is also comprised of WPBMN, an infinite-blockchain-mesh-network.

As you can see in the diagram below, the WPBMN and ANSUZ Chip work in parallel to provide the infrastructure for devices to become intelligent and collaborate over. SMC provides the security and intelligence that IoT needs while WPBMN provides the applications necessary for these cores to securely communicate and transact over.



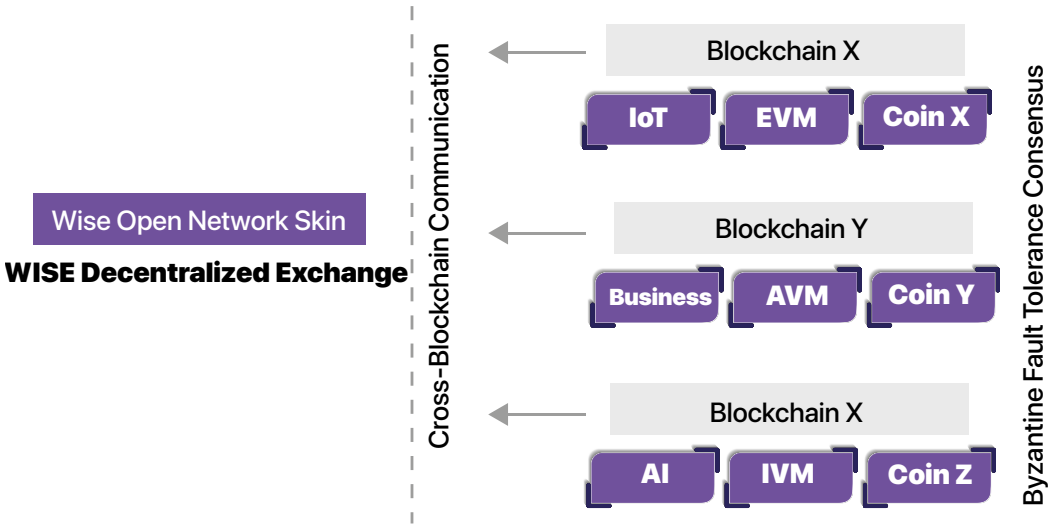
WPBMN Overview

WPBMN is a solution addressing all the problems with existing blockchain networks while providing the capacity to support billions of machine to machine interactions. The underlying protocols and details regarding the network can be found in section one. This section however, covers a high-level overview of the network and how it addresses existing problems with the Internet of Things.

Compared to previous blockchains, **WPBMN** is an infinite-chain network that enables each high-throughput chain to address a single application, while still working together. Interoperable public and private networks in WPBMN will help address the chaotic subsystems in IoT devices where many device types of various permission levels can exist in the network.

PROPERTIES	WISE OPEN NETWORK	ETHERIUM	BITCOIN
Sharding	Horizontal IoT Chains	NONE (FUTURE 2 Level)	NONE
Transaction Speed	1 Million + TPS	15 TPS	7 TPS
Token	Multi-Asset	ETHER	Bitcoin
Block Confirmation	1 Second	14 seconds	10 Minutes
Runtime Architecture	Any VM (EVM, QVM)	EVM	Bitcoin Core
Concensus	BFT Proof of Stake	Proof of Work (Future PoS)	Proof of Work
Chain Type	Lightweight	Lightweight	Heavyweight
Transaction Fees	<.01	.45	1 Dollar
Block Size	Dynamic	Dynamic	1 MB
Language	Any (Solidity, GO)	Solidity	Script

The table above depicts how, in comparison to slow and heavyweight traditional blockchains, WPBMN achieves a high transaction speed of one million plus TPS to support Internet of Things applications. Whereas standard blockchains have a single chain to address multiple applications, WPBMN's architecture enables many easy to create, high throughput Proof of Stake (which will turn in Proof of Ownership) blockchains that address a single application while still being interoperable with one another. By powering all the WPBMN blockchains with an optimized Byzantine Fault Tolerance consensus, each blockchain can then easily handle thousands of transactions per second with as little as 4 validators. These blockchains would also be able to communicate with one another through a modular framework called **Wise Public-Blockchain-Mesh-Network** and through the network, are able to send data packets such as tokens from one blockchain to the other.



With cross-blockchain communication enabled by **WPBMN**, validators could then validate other blockchains, a decentralized exchange can be created, and nodes in the network would be able to access other sovereign blockchains like EOS or Ethereum. With the effective multi-chain design, each blockchain can be used to address a different application with their own virtual machine and varying permission levels.

All of these individual networks would then be able to scale out indefinitely, as transaction capacity can be multiplied if one decided to create a separate identical blockchain. In the figure above, each chain can handle an approximate 10,000 transactions per second throughput. To achieve greater scalability, three more distributed replicated blockchains can be created and work in parallel with the existing blockchains.

With four blockchains working together, the combined transactions per second can be 40,000.

An infinite amount of more blockchains can be created to handle more transactions if needed. With a sharding protocol, blockchains can now be used for IoT devices as they can scale to millions or billions of transactions per second to handle many types of interactions needed for the network.

All nodes would also be able to participate, as **WPBMN'**s design is created to support light clients as small devices do not have to store transactions locally.

In synthesis, the architectural key features are:

1. **Delegated Proof of Stake -** WPBMN uses a T*endermint Byzantine Fault Tolerant Delegated Proof of Stake* consensus, enabling thousands of transactions per second per chain.

2. **Scalable Platforms -** WPBMN contains scalable Proof of Stake blockchain platform, that will be replaced with a **Proof of Ownership** distributed application platform, using the SMCs as nodes and decentralized identity platforms.

3. **Communication Protocols -** WPBMN uses a cross-blockchain communication protocol to connect networks on WPBMN together.

4. **Decentralized Exchange -** Wise Network is already partners with **Genesis Exchange,** the world's first, mobile first Decentralized Exchange enabling true peer to peer transactions without going through standard exchanges such as Coinbase or Gemini.

5. **Infinite Sharding -** WPBMN allows blockchains to split into two, to double transaction capacity.

6. **Two Dimensional Blockchain -** WPBMN allows blockchains to be infinite networks of their own, making the structure highly flexible.

7. **Cross-Network Communication -** WPBMN contains protocols to connect the network to others such as Bitcoin, ZCash, Ethereum, and Neo.

8. **Instant -** WPBMN's consensus enables sub-second finality, near-fee-less, low latency, and high throughput transactions.

With the above laid out, we can say that WPBMN is truly end-to-end with native protocols and applications supporting the creation of the M2M economy. With the underlying architecture mentioned in the section before, each application on WPBMN is designed to support interactions between many IoT devices. In summary, the key applications WPBMN are natively designed to support:

- **Data Transport -** Nodes will be able to distribute data and algorithms throughout the WISENetwork.
- **Digital Currency -** Nodes will be able to use a fast IoT currency to settle payments between one another and to pay fees on the network with any token that they choose to use.
- **Identity Protocols -** Nodes will be able to safely interact with reputable nodes and find one another in similar knowledge domains.
- **Federated Learning -** Nodes are able to train off private data and work together between one another, quite close to ensemble learning, improving their neural network.
- **Fine Tuning -** Nodes will be able to fine tune their neural networks and exchange knowledge by utilizing transfer learning and variations of imitation learning.
- **Distributed Computing -** Nodes will be able to lend spare computing power to one another, making this method cheaper than using AWS or Google Cloud.
- **Device Management -** Node owners can manage their autonomous devices with the help of a public distributed ledger.
- **Marketplace -** Nodes will be incentivized to share data and algorithms if they are paid for their services.
- **WISENet -** Nodes connected to the network will most likely contain possible training data from places like ImageNet, hospitals, or new datasets that they can share and enable others to learn.

ANSUZ Secure Memory Chips will be the nodes in the network that will also be able to access any applications on other networks such as Polkadot, EOS, and Ethereum with WPBMN's cross-chain communication. With these infinitely scalable applications on WPBMN devices are truly connected and will have the functionality to interact and share data with one another.

Wise's Public Blockchain-Mesh-Network is the only end-to-end platform enabling a M2M economy. With hardware that can be integrated into every IoT Device and a network that enables interactions between billions of IoT devices, WPBMN will attempt to address the existing problems facing blockchain networks, device intelligence, and distributed applications. WPBMN's main advantage is the ability for the network to gain instant widespread adoption through Wise's ANSUZ Chip licensed exclusively from Gopher Protocol Inc. whose design provides the infrastructure to enable the M2M economy.

Although there are many underlying frameworks and cryptocurrencies on WPBMN, the various underlying networks in this section will be bundled up into WSE (Wise's token which will be native to the POO based ecosystem) for the sake of clarity. The network delves into many different comparable areas and protocols to create this true end to end system.

PROPERTIES	Consensus	Interoperability	VM Blockchain	Scaling	Type	Potential Adoption	Vertical
WISE	BFT PoS	Yes	Yes	Infinite	End-to-End	High	End-to-End
COSMOS	BFT PoS	Yes	Yes	Infinite	Platform	Low	Interoperability
ICON	LFT	Yes	No	9000	Platform	Medium	Interoperability
POLKADOT	PoS	Yes	No	Infinite	Platform	Low	Interoperability
TELEGRAM	PoS	No	Yes	Infinite	End-to-End	High	Messaging

Next generation cryptocurrencies such as Polkadot, Cosmos, and Telegram paint the ideal future-generation architecture that blockchains should have. WPBMN has adopted an architecture similar to Cosmos but with the same end-to-end nature of Telegram. Whereas Telegram provides their 200 million users with software wallets, WPBMN will provide billions of IoT devices with hardware wallets and currencies. As a result, both networks are end-to-end with end user devices and people, enabling large-scale real world adoption. Compared to other infrastructures, the WPBMN puts its focus on IoT and artificial intelligence with novel distributed applications and identity protocols supporting the end-to-end creation of the M2M economy.

WPBMN contains a native IoT currency, which can be compared to existing DAG or block-DAG currencies. Currently, with IOTA all transactions go through an object called a coordinator, making the network centralized and containing a single point of failure. As there aren't enough full nodes currently running and with the coordinator providing a huge bottleneck, the network has not met the demand of people sending the currency to and from one another.

To run at it's highest performance speed, IOTA requires a special processor to run on top of the CPU, thanks to the Ternary operations it uses; and with lesser devices such as sensors, it will not have the strength to perform Proof of Work when sending something as little as data out.

Limited, IOTA is struggling to be implemented in the real world. IoT vendors are not friendly about adopting new Ternary processors such as Jinn, and the IOTA network is still facing serious scalability problems. Another downside with Directed Acyclic

Graph related architectures is that they have hidden fees where the electricity cost makes up for the cost of regular transactions. In contrast, WPBMN is decentralized, can run on any CPU, and only requires four validators to run a high throughput network. As a result, WPBMN allows for highly efficient IoT light clients, provides the IOT end-to-end applications and infrastructure to make machines intelligent, and enables near-fee-less sub-second transactions between devices without relying on the number of users to maintain the network.

	Consensus	Fees	Theoretical TPS	Transaction Speed	Potential Adoption	Data Transport	Simple Payment Verification	IoT Usability	Artificia Intelligence I
IOTA	Tangle	Hidden Fees	1400 Infinite with Swarm	30-120 seconds	Medium	Yes	No	No	No
IOT CHAIN	Block-DAG	Near-Feeless	100,000	1 Second	Low	Yes	Yes	Yes	No
WISE	Delegated Proof of Stake	Near-Feeless	Infinite	1 Second	High	Yes	Yes	Yes	Yes
NANO	Block Lattice	Hidden Fees	7000	1 Second	Low	No	Yes	No	No

Also based on IOTA, IoT Chains architecture was built including a hybrid blockchain implementation. During the process, the currency has limited its scaling potential while adopting major issues from the DAG currency. Compared to cryptocurrencies like IoT Chain, Wise handles the transaction per second limit through infinite sharding, allowing the network to scale through an infinite amount of other chains. Both Nano and IoT Chain still owe capacity to handle the transaction skills when large quantities of devices devices enter the network. IoT devices are unable to use Nano's currency design since it lacks the ability to transfer data, though it is very efficient.

WPBMN uses a fast BFT Delegated Proof of Stake consensus. The table above shows a comparison of Proof of Stake consensus with a third-generation blockchain distributed application infrastructure, EOS. As WPBMN's consensus is horizontal scaling and faster than EOS's consensus, WPBMN can be used for infinitely scaling and fast distributed applications. Compared to EOS, WPBMN can be interoperable with existing distributed applications platforms such as Ethereum and other blockchains.

About WPBMN's distributed applications, the combination work together to make a truly end-to-end system. Most existing IoT related distributed applications face no real adoption, do not function together and face scalability issues with their reliance on Ethereum. To make devices autonomous and intelligent, the WPBMN Virtual Application Layer, which is discussed later, combines the benefits of existing distributed applications in addition to new protocols to make the whole system autonomous and infinitely scaling. In this manner, devices can individually negotiate prices without having a human do the work and based on an owned algorithm, devices can self organize to train without the overhead. The applications that are currently being distributed are also heavily dependent on Ethereum, which can support around 20 transactions per second. It is not possible to implement plasma protocols and Ethereum's sharding yet, making the present systems incapable of bearing the transactions capacity of IoT devices interacting with one another in each application. However, if a new distributed application supporting novel functionalities were to be developed, WPBMN has the capacity to include it within the WPBMN Virtual Application Layer.

	No. Of Validators	Developability	Scalability	Accountability	BFT%	Mean Block Time
WISE Consensus	4 to Infinity	Any Programming Language	Horizontal with IoT Chains	Identification and Bond Deposits	1/3	1 - 3 Seconds
EOS Consensus	21	Mainly for Developers	Small number of delegators with high throughput	Reputation and Job Loss	1/3	3 - 40 Seconds

Wise Network is the first ever blockchain core with added AI processing in the forms of TPUs or NPUs. Wise's SMC is designed to enable the usage of cryptocurrencies and blockchain networks in IoT devices and enable the capacity of those devices to become intelligent and connected. Wise's Core IP contains the following components:

- **Neural Processing Unit -** Wise's ANSUZ Chip contains neural processing units or possibly tensor processing units to accelerate matrix multiplication and AI learning to enable devices to utilize the features of deep learning and neuromorphic computing.

- **Blockchain Hardware -** WPBMN contains blockchain optimized hardware such as crypto engines and hardware wallets.

- **Central Processing Unit -** WPBMN contains standard Risc-V ISA Processor for running standard applications.

The software running top of these IP cores include:

1. **Security -** WPBMN contains the highest security certifications.

2. **Services -** Wise's SMC contains support for WPBMN's WISENet and identity networks.

3. **Applications -** Wise's SMC contains software that supports wallet applications, biometric user authentication, and blockchain distributed applications.

4. **Communication -** Wise's SMC contains chip-to-chip communication protocols.

5. **Optimization -** Wise's SMC contains optimized solutions for machine learning algorithms and applications.

6. **Self Learning -** Wise's SMC enables devices to learn its own hardware and optimize the solutions through a blockchain network.

We at Wise believe that there is a need for an alternative to ARM in the IoT semiconductor industry, and by bringing a potentially license-free Blockchain Brain Chip IP core and open source RISC-V ISA architecture design to the semiconductor industry, we will enable many companies to design high performance and energy efficiency consumer ASICs at a reduced cost. Wise's RISC-V AI blockchain core license-free model will provide a free competitive alternative with added features of coupling devices with a blockchain network and a system-on-chip. With the license-free business model, companies and SoC designers will be able to use a similar core with the same functionalities but optimized for the blockchain.

However, a license-free business model would only work with cryptocurrency, as the adoption of the core will drive up utility and price of the network token. By creating the WPBM network, Wise will have the ability to give a very plausible alternative to ARM's licensing business to hopefully provide billions of cores to IoT devices such as smartphones, self-driving cars, and sensors by 2035.

Each of these cores will then come with a ANSUZ Chip hardware wallet and some of the cryptocurrencies on the network, so devices could immediately utilize WSE and through it, other blockchains. The WPBMN will default to the Wise network, its hardware wallet, and software for all cryptocurrency transactions, enabling Wise to be:

- App store of our Blockchain where all other or new distributed applications can be created or paired on it.
- Central decentralized platform for all machine learning
- Transfers of value between devices

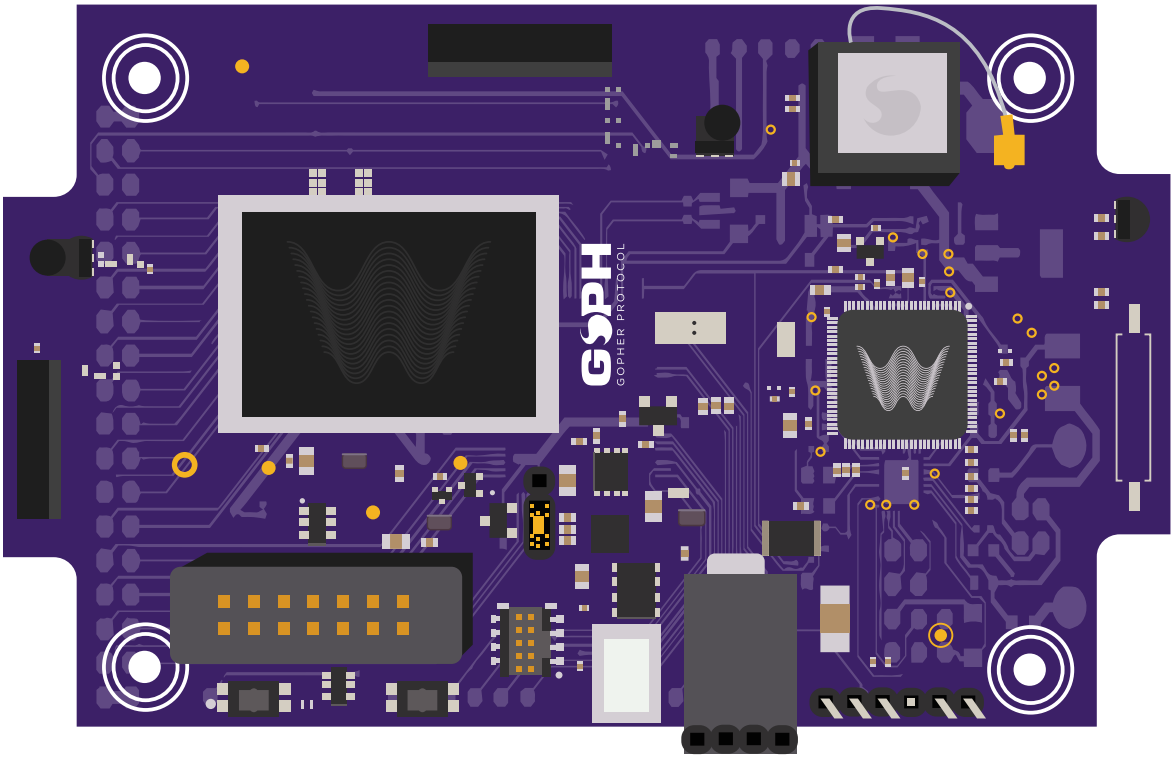
By embedding WSE tokens and a hardware wallet with all the WPBMN, Wise will provide an instant real-world adoption of the WPBM network, our crypto-token and the SMC simultaneously.

The collective vision of Wise is to create the M2M economy where devices can transfer knowledge, learn, communicate, and interact with one another. Wise will seek to create the first ever AI based blockchain for IoT devices with its native blockchain token. In the process, the IoT WPBMN can one day really aim to replace ARM and its dominance on the chip industry, all while providing the real world infrastructure for devices to become intelligent and use the utility of blockchain networks. Creating the network will enable Wise to become the new internet of blockchains and artificial intelligence, linking together all intelligent entities and all blockchains under one decentralized system while solving all the existing issues with scalability.

In Wise's end-to-end system, billions of IoT devices within the next few years will enter a single decentralized ecosystem to begin interacting with one another and to begin a recursive learning process. By creating Wise's Public-Blockchain-Mesh-Network and Wise's SMCs, Wise will attempt to address all the existing problems with blockchain and artificial intelligence to make the M2M economy a reality.

4. Wise SMC ANSUZ

WISE

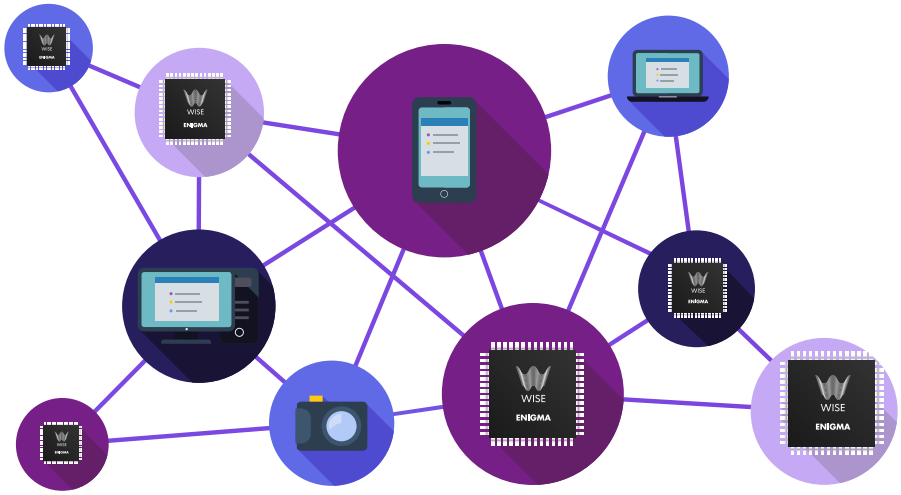


In the previous section, we discussed an overview of how the Wise provides an end-to-end development platform for IoT applications. In this section we will describe a modular set of hardware SMCs tailored for optimally running WPBMN on embedded "edge" IoT devices—that is small devices that serve as sensor or actuators, sit at the edge of the network and are mostly characterized by their low cost and low power budget. In particular, through a combination of cryptographic helpers running a high-security lite blockchain client, an AI accelerator for perceptual tasks and an embedded CPU, Wise can become the ideal platform for IoT OEMs to develop and deploy their applications and devices. Wise's **ANSUZ** Chip will be distributed via a license-free arrangement to System-on-chip (SoC) manufacturers for them to integrate it into their offerings, reducing cost and accelerating adoption.

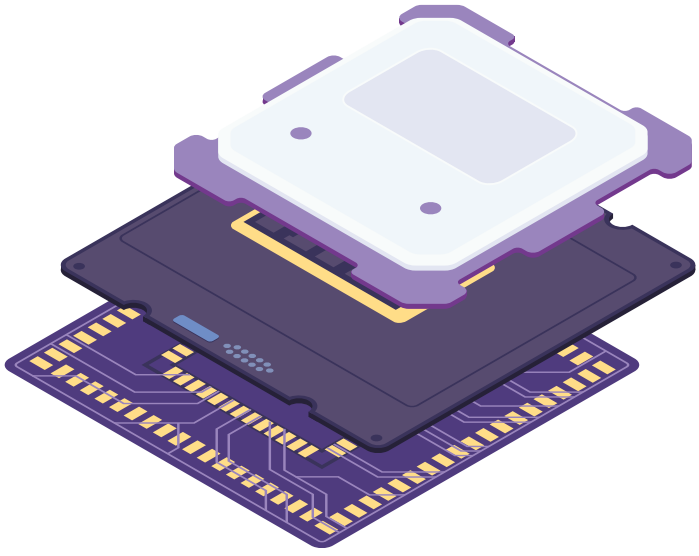
The **ANSUZ Chip** consists of three main components: An ARM or RISC-V based CPU to host a Linux kernel, an interface with peripheral devices; A secure Crypto-engine for storing private keys, singing messages and performing any other cryptographic computations required to operate any blockchain efficiently and in particular the Wise blockchain; A **Neural Processing Unit (or NPU)** to accelerate the linear algebra operations required by modern neural networks such as DNN, CNN and RNNs.

Let's see what else is inside Wise's **ANSUZ Chip:**

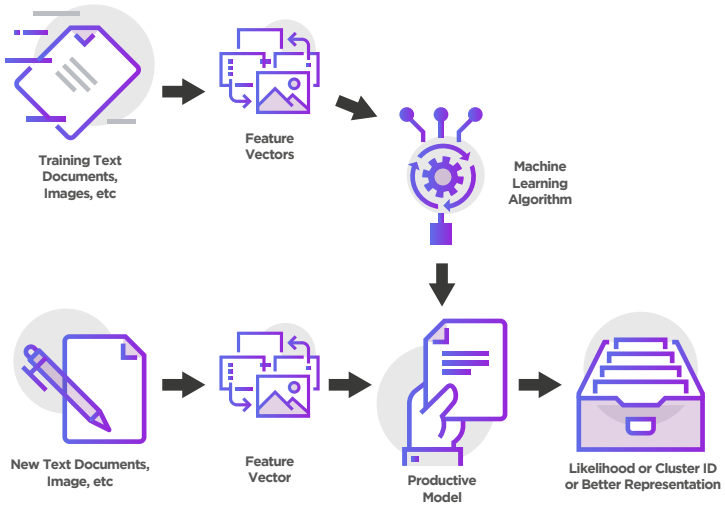
MESH Network: Each Wise (With an ANSUZ Chip installed) device invests "listening" time in order to participate in the mesh. Unlike a typical mesh where all components are constantly on, the Wise mesh works with the **WiseNET™** smart-timing protocol. This protocol, supervised by an AI system is most of the time "sleeping" in order to conserve power. On certain intervals the system wakes up, "listens" and participates in **MESH network** activities in order to maintain full coverage at all times. Each onboard chip's AI system manages the time division operation.



Multi-layered Security: Each Wise device has a multi-layered security circuitry that is embedded within its **ANSUZ** Chip called wEYE. Our multi-layered security system provides: Connectivity protection, Network protection, ECU protection, and Deterministic security.

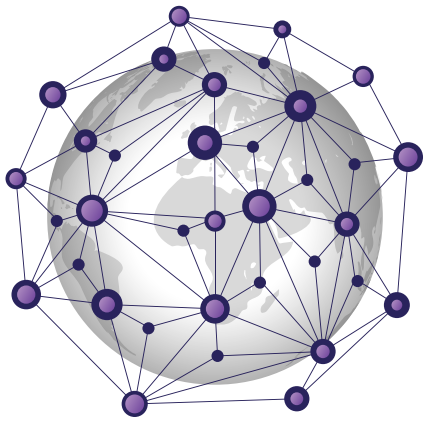


Machine learning wisdom Avant! AI℠ is designed to be a machine-learning system – essential to intelligent machines. Sophisticated algorithms are embedded within the **ANSUZ Chip** and work together with all other Wise chips creating a powerful, self-learning system that understands the device's environment and makes decisions on how to improve performance, coverage and power harvesting.
The AI system supervises security/privacy and enables advanced features like NLP, speech/text recognition via its **recurrent neural network (RNN).**

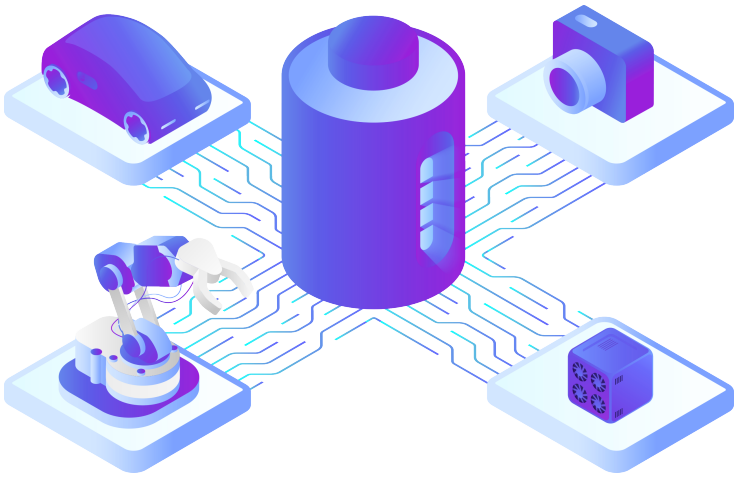


wNet: Proprietary, private, secured communication protocol, called **wNET.** Wise devices are designed to work together via a private, secure communication protocol. This ensures confidentiality and privacy and creates enormous computing and database power around the globe.

The microchip includes expert system to learn distributed networks behavior, turning them into **artificial neural networks (ANN)** to increase privacy and security. Through **wNET** the system shares intra-units computing power, over-the-net memory and storage sharing, power management and performance boosting.



Wise's secure memory chip is encrypted using 1024 bit method and in addition a honey encryption layer is added for maximum protection. Data packets are accumulated and are protected against modifications via an onboard AI based-security system.



Potential Applications

Autonomous machines - Each autonomous machine is an IoT/mobile device and requires the highest data management and communication security level.

Application template - Since the ANSUZ Chip is equipped with mechanisms like hash accelerators, hardware wallets, onboard secured memory and an encryption engine; IoT devices will be able to become secured cryptocurrencies operators, implementing blockchain technology.

IoT/Mobile platform - Wise's ANSUZ chip can be installed within military/security applications, AI platforms, autonomous machines and more as a base blockchain IoT processor.

DB management system - Wise's Secure Chip can be embedded within desktop and server's applications, enabling the creation of a new blockchain based database system for a broad spectrum of purposes.

The **ANSUZ Chip** splits and shares database objects on your IoT or mobile device. Database objects may be information packets, videos, images, photos, documents, contacts or any other media stored on the device's memory. A database object is spliced to numerous segments each encrypted and indexed. The ANSUZ Chip sends these segments to millions other IoT/mobile devices that are within wNET network, worldwide. Your database objects' segments may be partially stored on a smartphone/IoT device in Australia, Japan and Mozambique and you even don't know about it.

The system includes redundancy storage in case some devices are down. Per retrieval request, The **ANSUZ Chip** restores the database object by collecting all segments from all other devices worldwide according to their index. In the event that some devices are turned off or not available, **ANSUZ Chip** collects the information from redundancy devices. In addition, **ANSUZ Chip** maintains an appropriate level of redundancy backup on other devices worldwide.

As a consequence the device's memory and storage are tremendously freed up. More content can be stored and more database related features can be implemented. It saves network bandwidth and data quota. The device's performance is higher and finally, battery life is increased due to less stored data.

The **ANSUZ Chip**, when fully developed, can be implemented on a SIM/SD Card that opens a whole world of possibilities. It can be also implemented within IoT device's circuitry. Another option is to implement the microchip as an integrated **IP (Intellectual Property)** unit on an existing IC.

The IP would be implemented as a black box and occupy minimal silicon space. Another option is to implement Wise's Secure Chip as an independent IC on the mobile motherboard. In the SIM/SD version it can be offered for sale through common retail channels. Virtually, it will be available for purchase in every store, from local supermarkets to department stores. Owners of smart-phone devices can easily install the chip.

Let's revisit Wise's SMC three main components one by one:

CPU

To host a modern Linux operating system (such as Ubuntu) for the WPBMN to run on, Wise will include a set of modular processors in the SMC. The RISC architecture of ARM processor achieves a simple design, fast clock rate, small die sizes and efficient memory usage with a development pipeline for new SoCs or IP blocks with trusted IP, expert design support, and leading software tools. ARM offers a product range ideal for the requirements of IoT devices where modern versions feature a system-wide approach to security–TrustZone. Initially, we will target integration management of the cores from the ARM Cortex- M family for low-power embedded applications and the ARM Cortex-A 64-bit family for high-performance processors and high-end applications.

This organization is based on the feedback from our partners, and IoT devices require low power and small footprint. The ARM ecosystem provides the Advanced Microcontroller Bus Architecture to share the multiple peripherals (IO, coprocessors and memory controllers) required to build a modern processing unit; and multiple vendors provide these trusted peripherals for a wide variety of process nodes. Finally, the extensive penetration of ARM has created a vibrant and tested community that support the entire software stack of bootloaders, kernels, drivers, distros, libraries, applications and software development tools such as compilers, profilers, and debuggers. As the WPBMN comes online and prototype blockchain applications start development, we will characterize the computational workloads to decide if we will include the necessary NEON-SIMD and FPU accelerators, and which peripheral to incorporate.

Also, Wise is consistently exploring the alternative of developing a custom processor based on the RISC-V open-source ISA as it—and the surrounding ecosystem—reaches practical maturity. Recent implementations of RISC-V core show promising results with smaller die size and better performance compared to ARM processors (BOOMv2 vs. ARM Cortex-A9).

RISC-V may provide an alternative to ARM's monopoly, resulting in a very cost-effective SMC because the licensing fees to ARM would be eliminated, and this cost-saving could be passed on to SoC manufacturers as an incentive to accelerate adoption. We will monitor the progress of the RISC-V ecosystem expansion and decide as to which CPU core as a base of the WPBMN. Similarly, to accelerate development of the entire software stack, Wise will partner with early System-on-a-Chip manufacturers to develop the whole integration stack.

For better comprehension, we'll look at ARM, a reduced instruction set computer (RISC). As a RISC, ARM aims for a fixed length, simple and powerful instructions that execute within a single cycle at high clock speed. As a RISC architecture, ARM is based on a number of principles to achieve simple design and fast clock rate. A pipeline is designed to be decoded in one stage with no need for microcode. A large set of general-purpose registers are defined for fast execution of instructions. ARM adopted load/store architecture, where data processing instructions apply to registers only and load/store scheme is used to transfer data from memory. In addition, there are a few differences from clean RISC. ARM adopts variable cycle execution for certain instructions such as multiple- register load/store to achieve faster and higher code density. Inline barrel shifter improves performance and code density but leads to more complex instructions. ARM added Thumb 16-bit instruction set which leads to about 30 percent code density improvement. Conditional execution is added to improve performance and code density by reducing branch. Some enhanced instructions are added for DSP operations.

An acronym which definition is important right now is ISA (An Instruction Set Architecture) which defines, describes, and specifies how a singular processor core works. Existing ISAs such as x86-64, Arm are proprietary and very complex. Details are often shadowed in lengthy manuals and details of the ISA are missed, yet the widely used ISAs are several years old already, so their designs carry baggage as a result, e.g., for backward compatibility. Corporate entities such as Intel, and ARM Holdings own, control, and manage most proprietary ISAs. The RISC-V project came out of UC Berkeley to address these issues. The open-source approach taken by RISC-V means that many different companies can provide hardware implementations of the RISC-V architecture. Creating an ecosystem in which multiple vendors can compete in implementing a single ISA should result in many of the benefits seen in other open-source projects.

Among such diverse markets, there are a large amount different application areas for processors, and thus many different design constraints, like an embedded processor needing to be inexpensive, reliable, and simple, but doesn't require speed, support for an operating system, multiple cores, or support for 64-bit operations.

Furthermore, larger applications exist and they require processors with multiple cores and 64-bit operations, etc. The RISC- V project approaches this plethora of design choices by introducing some options into the ISA. In this respect, RISC-V is really not a single Instruction Set Architecture; it is a collection of related ISAs.

RISC-V ISA targets a pure Reduced Instruction Set (RISC) architecture - execute one instruction per clock cycle and to achieve this, each instruction needs to be simple and limited.

RISC-V offers three base integer ISAs - RV32I, RV64I, and RV128I for 32-bit, 64-bit, and 128-bit address widths respectively. 40 instructions of fixed 32-bit width are provided for hardware integer operations. Several standard extensions are provided: M - integer multiply/divide, A - Atomic memory operations, F - Single precision floating point, D - double precision floating point, Q - Quad precision floating point, C - Compressed instruction set, and E - Embedded microprocessors, with only 16 registers.

Note that RISC-V applications range from small embedded processors to 64-bit and 128-bit processors. Compressed instruction set compresses the regular 32-bit instructions into 16 bits similar to Arm's Thumb instruction set for embedded applications. Reducing the size of code results in increased processor performance since it allows more instructions to be cached, reducing the time to fetch instructions from main memory, which is often a performance bottleneck. Now, To handle the computational loads associated with blockchains, cryptographic functions, and consensus algorithms, each WPBMN contains an optimized Crypto Engine.

Executing these functions in hardware reduces the software overhead, and the hashing functions required for encryption and authentication can be executed faster and for less power. The main host processor of each node will have access to the functionality accelerated by the Crypto Engine via a secure API and secure communication channels. Through this interface, the host processor will be able to run any cryptographic application efficiently with hardware acceleration, such as running Dapps, Light Client, or consensus algorithms. Additionally, the integration of secure storage and secure access to private keys will enable IoT devices to perform cryptocurrency transactions autonomously. Users, owners or managers will be able to configure their device to allow a certain set of transactions and their frequency, ensuring an extra level of security.

The Crypto Core provides a highly secure platform for cryptocurrency private key processing and transaction authentication. It offers a broad portfolio of services through its API including certified cryptographic libraries, MiFARE Plus and MiFARE DESFire libraries , Hardware security features and crypto engines.

It will address the highest security certifications including Common Criteria up to EAL6+, EMVCo, and CUP.Private key recovery.

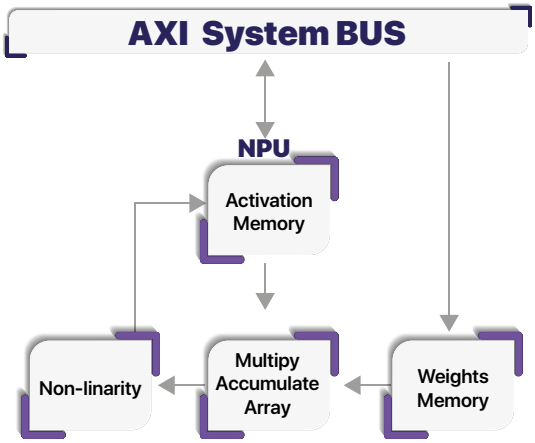
NPU

To leverage the current advances on Machine Learning on image classification, natural language processing, speech recognition, etc. we'll include a Neural Processing Unit (NPU) optimized to accelerate all current types of neural network algorithms, including DNNs, CNNs, and RNNs. The NPU will be also be an essential component to obtain high-security user authentication across biometrics. Allowing design spaces to be scouted efficiently, scalability is achieved by replicating as many NPUs as required. An scalable NPU architecture covers a broad range of conditions of lower to higher-end applications, from accelerating embedded IoT devices with deep learning and proof of ownership mining by individuals through SMCs with built-in NPUs.

The Neural Processing Unit function is to be the brain of the IoT device, enabling it to carry out categorization tasks with human-level precision at a practical flow rate and within a sensible power budget. The primary host processor of each of the nodes will enter the functionality accelerated by the NPU via a secure API and communication channels. Across this interface, the host processor will be able to efficiently execute custom data processing applications by loading pre-trained neural structure models into the core, implanting data into it and learning back partial of absolute activation results. These networks can be stored in the IoT's ROM at time of manufacturing, or securely acquired, improved and updated later trough blockchain transactions.

A Neural Processing Unit block graph exhibits the principal generalization. Memories for neurons weights from the model to be run will be fed from the principal hosts processor at convenient times through the principal system's Advanced eXtensible Interface bus.

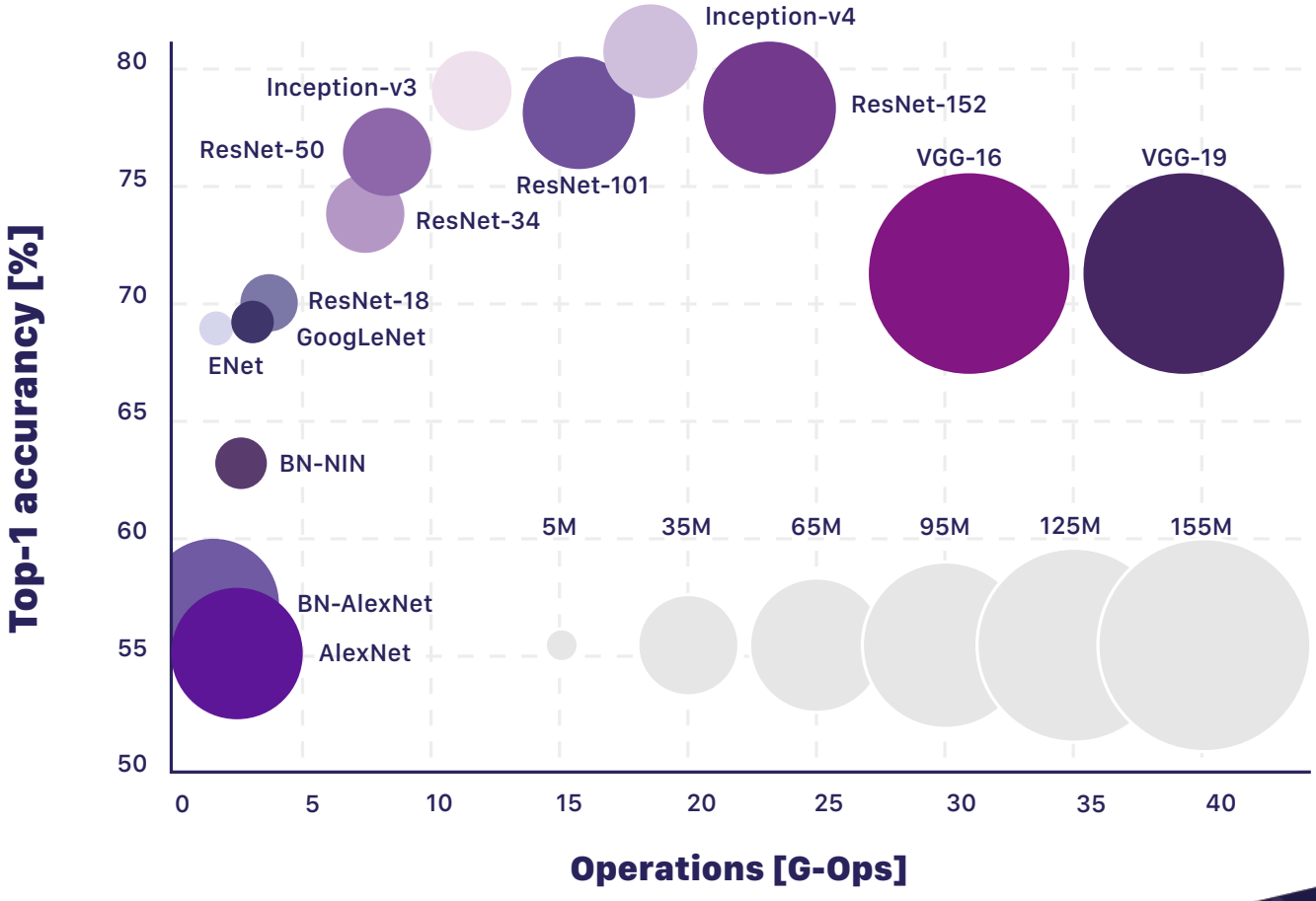
There's a native inter-layer memory for activations as well, that will first hold the input data to the network, and then as each layer in network is processed by the Multiply and Accumulate unit, and the nonlinearity is applied, the output of one layer gets stored back to the activation memory to be used as the input to the next layer in the neural network. At the end of the network, the final result is stored in the activation memory from where the host processor can fetch it.



A vital element of any machine learning accelerator is its integration with training and deployment tools that have become standards in the industry. Therefore, Wise will develop the necessary backends to Tensorflow, Keras, PyTorch, Caffe, etc. to support directly running these tools on our custom NPU, and integrate these into the WPBMN API. As part of the adoption of these tools, we'll support emerging open interchange standards such as Open Neural Network Exchange (ONNX) so that developers can easily migrate their applications into our SMC.

Through the acceleration of neural network algorithms, we foresee that developers may choose to use the NPU to build DApps with integrated learning. These applications could progressively fine tune pre-trained networks or leverage the latest advances in transfer learning to achieve higher accuracy and specialization. Wise's Neural Processing Unit is not intended as a platform for experimenting with new NN architectures nor as a replacement for high-performance NN training workstations such and NVIDIA's DGX or TPUs. Overall, both processing units still may lead to interesting new developments.

Neural networks may appear as a simple subject, though there is a gigantic computational complexity behind them. Modern neural network models have millions of parameters and perform billions of mathematical operations to classify the contents of a small patch of image.



In this graphic, the computation demanded to categorize an image is in the 2.5 to 40 GOP. As it should be, the actual computation needed for a full HD image could go from a 100 to 1000 times greater. Torch7 with cuDNN-v5 and CUDA-v8 back-end were used as inferred time and memory usage measurements.

Tensor Processing Unit Vs Neural Processing Unit

A remarkable innovation in the field has been to use the Matrix multiplication engines used to render images in **Graphics Processing Units (GPUs)** to compute the workloads of Neural Networks. This has been one of the enabling factors that allow much faster training as well as larger models. To expedite training data, scientists put great effort into creating network architectures that maximize (but not exceed) the memory capacity of GPUs.

This in turn has created a feedback cycle where GPU manufacturers (NVIDIA in particular) are designing GPUs with larger capacities specific for these workloads. At the very moment the highest point in machine learning computing is the NVIDIA DGX-1 workstation with Tesla V100 GPUs that can process 1000 TFLOPS (deep learning). In most terms, GPUs work better than CPUs for machine learning because they have a much larger number of computing cores and faster access to memory. This technical advantage is extremely important because it can reduce network training from months to hours.

Aside GPUs, another clear example is when when Google came across the news that neural networks would take over the performance of traditional computing for translation services (and others) they designed their own **Tensor Processing Units.**

The TPU's architecture mimics the required computation to process the common layers of a neural network, its integration stack and how with this implementation they achieved an impressive computational efficiency 89 times greater than Using CPUs and 29 times greater than using GPUs (of that era). This, and the newer generation of TPUs are available for use by the public through the Google Cloud. For a more in depth read we refer you to an excellent overview of the TPU original paper https://arxiv.org/abs/1704.04760.

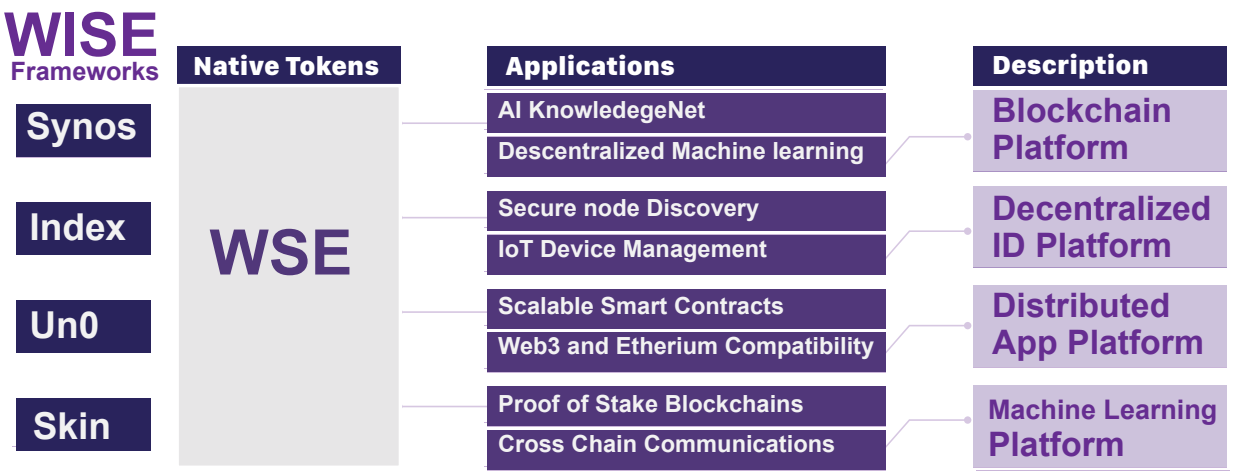
Over the past decade, the manufacturers have recognized that neural and custom accelerators computation were required to move forward the field of Artificial Intelligence and machine learning. This was perhaps catalyzed by DARPA's SyNAPSE project which led to TrueNorthe, one of the first formal efforts to productize neural network accelerators. Today there are dozens of players in this field that offer mature and accessible NPU acceleration at multiple scales. At the ASIC or SoC level, Arms, Synopsis , Cadence , offer supported IP blocks ready for integration into silicon products. Further up the stack, several hardware manufacturers offer user-ready chips, module, and workstations for quicker neural processing such as: Nvidia, Intel, and Bitmain. From a online storage perspective, Network Processing Unit acceleration is available from Amazon, Microsoft, NVIDIA, Google, and IBM. Around the industry, it is said that there are at the very least 35 startups pursuing Neural Processing Unit products.

5. Wise's Public Blockchain Mesh Network

In the previous sections, we detailed the SMC and how the components will be used to utilize the applications on Wise Public-Blockchain-Mesh-Network (WPBMN) and of blockchain technologies as a whole. We also detailed a high level overview of the Wise Public-Blockchain-Mesh- Network structure and its adoption plan. In this section, we introduce WPBMN, an infinite-chain network that will serve to link all intelligent devices and blockchains under one decentralized system. By bootstrapping the network off of the Wise's SMC, WPBMN allows for global adoption of blockchain technology by providing billions of devices immediate access to its network.

Wise Public-Blockchain-Mesh-Network is comprised of four main frameworks: Wise Skin, Wise Un0, Wise Index, and Wise Synos. However, the latter three frameworks are all connected to Wise Skin, the root blockchain platform enabling an infinite amount of other blockchains and frameworks that connect and communicate to it.

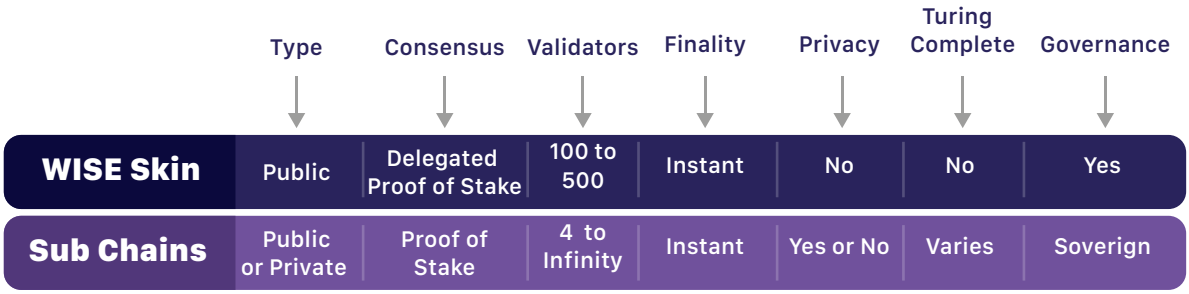
With the frameworks shown in the table above, Wise can provide the end-to-end solution with a development platform and applications to support the interactions between IoT devices.



Wise Skin

Wise Skin is a publicly validated, Byzantine Fault Tolerant, Delegated Proof of Stake (for now, but now transitioning into Proof of Ownership) blockchain and the "root"of Wise Public-Blockchain-Mesh-Network. Skin contains a Go-Language software development kit, enabling developers to make fast public or private, fault tolerant proof of stake blockchains independent of Skin's governance.

With Skin, blockchains can become their own VM-independent platform or be used to interact with the underlying scheme of other blockchains. Skin only keeps track of the tokens on each blockchain created on it, allowing for a type of cross-blockchain communication where each blockchain can be independent but are able to exchange data packets with one another through it.



Skin is beginning with 100 validators and have its own governance mechanism. However, subchains on Wise Skin are independent of one another and have their own network designs, making them independent from the failures of other networks. The Tendermint Core, is a Byzantine Fault-Tolerant Consensus Algorithm which takes state translation machines in any language and replicates it across all machines. In conclusion, Tendermint Core is equipped to handle IoT subsystems and many low latency, high finality, blockchains that are well architected to function in the real world. This makes Wise Skin a modular platform for deploying high throughput blockchains with minimal resource consumption.

Sub-Chains

In this document, sub-blockchains created on Skin are referred to as IoT Chains. To create IoT Chains, Skin will come with a toolkit built by Wise, which provides boilerplates for on-chain storage data type customization, private blockchains, multi-data type on-chain storage abstractions, and public blockchain creation.

Wise's Token

WSE is the native staking token of the Wise Public-Blockchain-Mesh-Network and Wise Skin. In Proof-of-Stake blockchains, the creators of each block are chosen by random selection in a round-table like fashion according to how many coins or value the person holds. To provide incentives for participants to stake the currency, the Wise Token (WSE) is solely designed for staking whereas block rewards and fees are distributed in the same token. Thus, all exchanges are made in the same coin, making Wise a secure and consistent opportunity.

Wise Un0

Connected to Wise Skin is Un0, a modular smart contract platform with its own enhanced Ethereum Virtual Machine (EVM) called Quantum. Un0's platform will allow for distributed applications to be built on the WPBMN while removing the drawbacks of Ethereum such as transaction time and fees.

During its initial phase, Un0 will be a Proof of Stake Ethereum powered by Tendermint Core and a virtual machine built in part to the specifications of EVM. With a similar virtual machine, Un0 will allow for interoperability between existing Ethereum distributed applications and Web3. Un0 will also enable developers already familiar with Ethereum to migrate to WPBMN (Wise PublicBlockchain-Mesh) and begin developing IoT-based applications that will be immediately across devices with the SMC. These benefits make Un0, a modular platform for developing scalable decentralized applications immediately operational in IoT devices.

Wise Index

Index is deeply linked to Wise Skin, a hybrid sub-chain distributed ledger built to create a decentralized identity and a crypto phonebook for IoT devices. Wise Index can deliver the necessary "equipment" for devices to publish information that other independent blockchains and applications can access and query, which is sharing information in a very secure method. Since the network is immutable and public, any device can join the network and start finding other devices over the network.

An off-chain explorer is paired with the distributed ledger. Devices can examine the transactions and history of other devices. Index provides a machine reputation check where device addresses will be evaluated at ratings from 0 to 100 depending on how reputable a machine might be. Index can complement other scalable platforms to create a whole new vision of applications such as algorithms for secure machine to machine transactions and self-organization.

Wise Index provides all the designs and specifications necessary to support decentralized identities and its resulting potential applications.

Wise Synos

Wise Public-Blockchain-Mesh-Network, Synos, also known as an AI KnowledgeNet or Virtual Application Layer, is an extension of Gopher Protocol's Avant! AI , enabling a series of interoperable applications for interactions and learning between Wise SMC and other connected IoT devices.

Avant! AI engine is the brain that is in charge of the entire Wise's SMC microcomputer. The AI system enables self-learning and adapting to the device's features and usage using proprietary recurrent neural network (RNN) algorithms.

For example, the system learns about the device's processing speed, storage utilization, network data traffic, statistics, and more. Based on the system's variations, it sets on-the-fly the most efficient database traffic and management, sharing rules within the wNET network.

It's a constant changing, evolving, dynamic communication between all network devices in order to achieve the ultimate network efficiency and reliability in real time.

Another aspect of the AI is the power management deep learning. The unit's power consumption and heat dissipation are constantly monitoring in order to put certain sub-units to sleep and awake others. Power harvesting is performed, based on power consumption study, in order to prolong power source for long working hours.

These are for decentralized machine learning, distributing computation, and data sharing specifically. The applications can be tied in with Wise's multi-chain marketplace where devices can agree on values for their training data or computational power.

Both the the distributed applications and the marketplace make up Wise's. Developers can make their own distributed applications on Un0 or perhaps combine it with Index and have them be interoperable with the applications on Synos' virtual application layer. Real-world devices and Wise's SMCs can then utilize the applications and the cryptocurrencies that the distributed applications offer. For example, if a developer wanted to create an application for distributed evolutionary learning on Un0, devices could access something called the virtual application layer and have access to the network's protocols and tokens.

These four frameworks and their native applications and protocols make up Wise's Public-Blockchain-Mesh-Network. There is a three-layer architecture laying beneath their platforms. On the very bottom, Tendermint core provides a consensus engine and P2P communication to form the base of the Public-Blockchain-Mesh-Network. Wise's SDK lies above Tendermint Core, im[plementing blockchain logic for the smart contracts, identity, cryptocurrencies, governance, and staking. Wise's SDK interfaces with Tendermint core via ABCI, short for Application Blockchain Client Interface. On top of the Synos SDK, applications can be implemented.

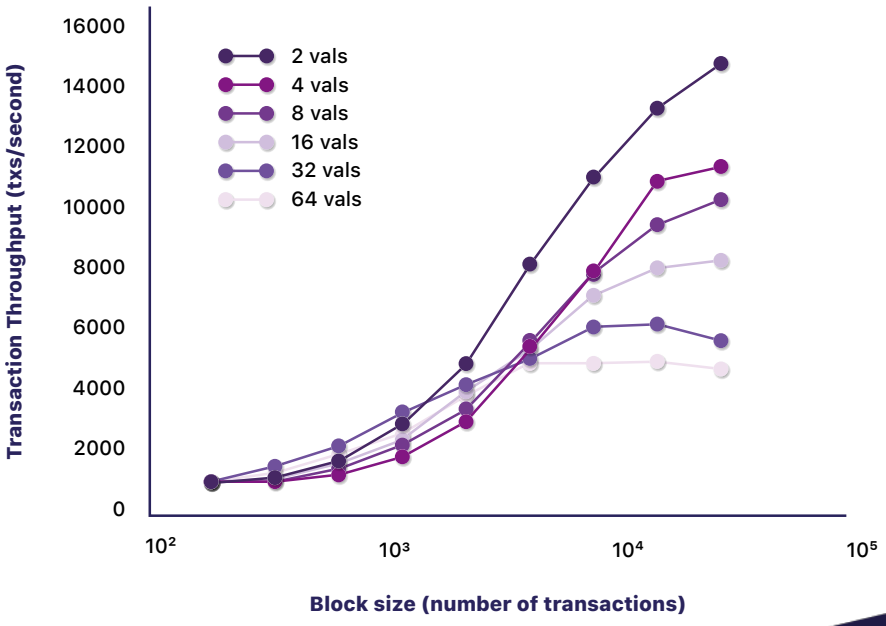
The Tendermint Core

Wise Network and all its blockchains will run on Tendermint Core, a Byzantine Fault Tolerant consensus engine that can take state translation machines and replicate it. Tendermint Core can defend against malicious attacks and actors in the network through its fork accountability, where malicious actors that cause the consensus to fail can be easily identified and subsequently punished. Tendermint Core is a alternative of the Practical Byzantine Fault Tolerance algorithm, which can process thousands of transactions per second with sub-millisecond latency that increases in this manner. Some advantages that Wise has due to the Tendermint consensus adoption are:

Byzantine Fault Tolerance - Wise nodes tolerate up to 1/3 of machines failing.
Secure Peer to Peer - Dynamic peer-to-peer discovery is enabled among nodes by borrowing BTCD, which is Bitcoin's alternative implementation in Go.
Fast Consensus - Each blockchain on Wise can support thousands of transactions per second.
State Machine Replication - Wise will be able toreplicate state machines in any programming language available.

Tendermint's main contribution to Wise, however, is its non proof-of-work consensus that protects against double-spend attacks while being resilient up to one-third of Byzantine participants. In Wise's Public-Blockchain-Mesh-Network, Tendermint helps manage the agreement of state synchronization as well as agreements to publish the next blocks between nodes.

As a result, despite harsh conditions such as malicious actors or crashing validators, Wise's consensus engine enables it to have very high throughput for IoT applications.



The description above says that, with a 64 validator benchmark, every blockchain on Wise will be able to process thousands of transactions per second with sub-second "waiting time". Meaning that Wise's Network will be able to perform effectively in the real world situations compared to other directed acyclic graphs and blockchains.

Tendermint Core joins applications with an **Application Blockchain Interface (ABCI)**, using socket protocol to enable consensus engines carrying out on multiple application states. Tendermint Core's machine-based BFT algorithm bestows the mechanism necessary to implement *Proof-of-Stake* protocols on top of it and could be the foundation to our Proof of Ownership protocol, utilizing the SMCs as nodes.

Wise has adopted Satoshi's mechanism for client node discovery. In a nutshell, Wise's clients uncover the IP address and port nodes in diverse ways.

- **Local Client First,** nodes can use public web services or hard-coded software to determine its own IP address. It can try to connect to 91.198.22.70 port 80, which is an IP DNS server. If the connection fails, a DNS request is made to 74.208.43.192 port 80, which is an IP lookup server. Basically the nodes attempt to connect to these servers by sending a HTTP request, reading the responses, and parsing the IP address to advertise the address to connected nodes, thus finishing the thread line.
- **Database Nodes** can store their addresses in the Wise crypto phonebook and query the addresses upon startup.
- **Address Relay:** Addresses can be relayed to other nodes.
- **Self Broadcast:** Every couple of hours, the node can broadcast its own address to all connected nodes in its network.
- **DNS Addresses:** Wise nodes issue DNS requests to learn about addresses of other peer nodes. The client could then have seeded DNS services.
- **IRC Addresses:** Wise nodes has the ability to access IRC channel and have its address encoded into a string. It can randomly join an IRC channel and issue a threading command to decode the IP addresses of other nodes in the channel.

Application Blockchain Client Interface

In Wise's Network, the interface between multi-machine state translations is used to communicate between Tendermint consensus and the application layer. The ABCI is an interface that allows applications to be implemented on top of Tendermint Core in any

programming language. ABCI is implemented in a socket protocol called Tendermint Socket Protocol (TSP).

Typically, **Tendermint Core** would be responsible for sharing blocks between nodes and establishing the transaction order. Cryptographic transaction validation, incentive mechanism, and other blockchain primitives would be implemented at the application layer.

The Tendermint Core sustains three connections, mempool connections for using CheckTx for transaction relays, consensus connection for executing committed transactions, and a query connection for application states.

- **Mempool connection (CheckTx)**
  - Checks the validity and should be executed and announce to participating nodes (through DeliverTx); utilizing CheckTx.
  - Accomplishes checks by using the "Mempool" as a starting position (current balance, list of accounts, and any crucial information kept in the state).
  - Starts as a duplicate of the most recent committed state.
- **Consensus Connection (BeginBlock , DeliverTx , EndBlock , Commit)**
  - Executes and broadcasts transactions that have been checked. Message sequence is - for every block - BeginBlock , [DeliverTx , ...], EndBlock Commit .
- **Query Connection (Query, Info)** - questions without engaging in consensus (= read- only) (Query)
  - handshake (Info).
  - genesis (initChain).
  - Conversely, the ABCI design has a message protocol determined using protobuf and the server applied by async raw bytes and grpc.
- **Information:** will deliver the current state between Server (the application enclosing business logic) and ABCI client (Tendermint).

- **Flush:** it is used to confirm that a message has been delivered and processed. Sent after receiving the associated response to a previous request.
- **InitChain:** as its name implies, it is is used to initialize a new node. In the case of the first node, it will also initialize the blockchain, in the case of a new node in an existing blockchain, it will just catch up with the other nodes by replaying past transactions.
- **checkTx:** before conveying to all confirming nodes for processing and consolidation in the current block, it delivers the transaction to be "*prechecked*".
- **deliverTx :** hands over the Tx to all validators and executes the Tx .
- **Commit:** achieves the state with all accepted Tx This writes the state such that the next block can begin and increase the block height.
- **beginBlock:** clears a block for the intergration of new Txs .
- **endBlock:** ends/closes
- **setOption:** enables setting of local, non-consensus crucial options on the node. For example, log level of the app.
- **Query:** This operation is performed locally on the node, it authorizes a querying of the state without influencing it.

Validators and Delegators

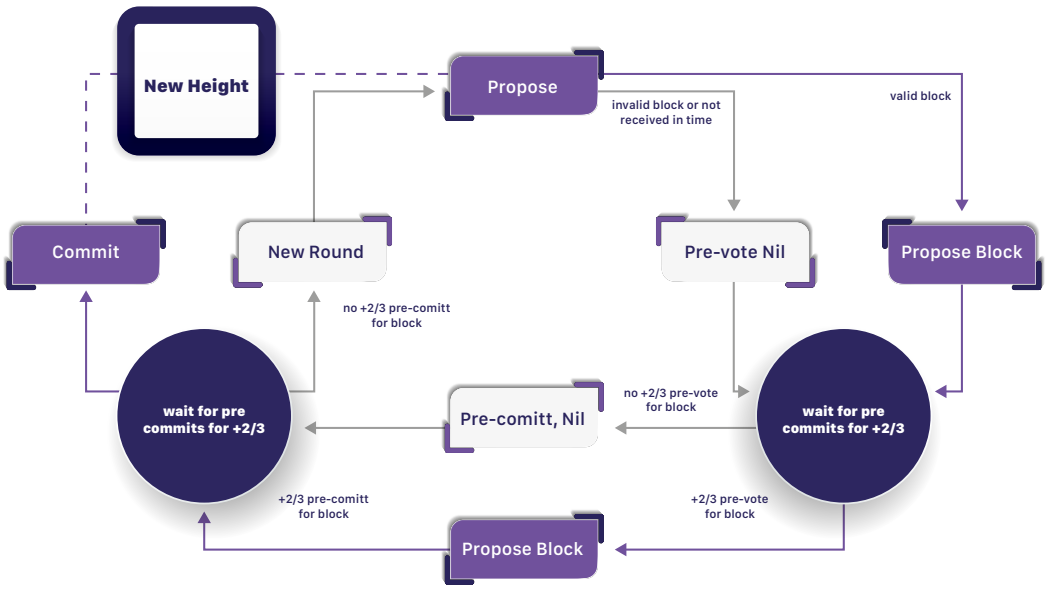
In Wise's Tendermint Consensus, validators can participate in the consensus by announcing cryptographic signatures that perform as votes for the next blocks. To turn into a validator, a node must lock up a preordained amount of tokens. A delegator is usually an individual who wants to provide voting authority to a validator, delegates the tokens to a prospective validator, so that the delegate might earn a percentage of a block reward. Delegates may be placing their tokens at risk by assigning their stakes to validators and may lose tokens whether or not the validator respects the protocol implementation.

Validators have a voting power equal to that locked up in a bond transaction and may unlock the coins by posting an un-bonded transaction.

A minimum of 4 validators are needed but can scale to infinity to run the consensus protocol on Wise. However, in the Wise Skin, we will begin with 100 validators and scale to 500. These validators can help run the other networks on Wise.

Tendermint BFT dPoS

Wise's Tendermint Byzantine Fault Tolerance protocol is a modified version of the DLS protocol and is resilient to up to on third of Byzantine participants. The consensus protocol demands no proof-of-work mining and shields against double spending. Tendermint's algorithms based around the FLP impossibility result from Fischer's research in asynchronous systems. The algorithm assumes that the network is partly synchronous and that non-byzantine nodes can utilize an internal clock until the next block is published.



The figure above depicts how the consensus turn takes place.

In Wise's consensus round, validators sign votes for blocks with three types of votes: pre-vote, pre-commit, and commit. When the two thirds majority of validators sign and broadcasted commits, then the block is committed to the network.

At the height of each block, a turn with two steps, (commit, new height) and (commit, propose, pre-vote, pre-commit) is executed. Each turn time is incremented by a small amount, which allows the network to accomplish consensus in a moderately synchronous network. When each turn starts, a proposer is chosen in proportion to the quantity of voting power. Since the consensus is executed in a deterministic round-robin fashion, nodes form a consensus of the proposers in each round.

The first round is for choosing a proposal during the propose round where the proposer for the round will buzz a proposal (broadcasting information). Then, the next turn is the pre-vote step where if a validator receives a valid proposal, it can broadcast a pre-vote for the block. However, if the validator is locked from a prior block, it broadcasts a proof-of-lock for the locked block. Despite that, if there is no valid proposal, the validator will announce nil. In this manner, all nodes will announce their pre-votes to peers.

Now, the following round is the pre-committment step where if the "validators" receive a majority pre-vote for their block, the validator can sign something called a pre-achievement and lock onto the block while releasing any previous locks. If a node decides to lock or unlock a block, it merges pre-votes towards a proof-of-lock for later where if a node receives 2/3 of nil pre-votes, it unlocks. If the node acquires 2/3 of pre-commits, it goes into the commit stage. Conversely, it will return to the propose stage.

During the commit stage, nodes will collect a block and stay for the majority of commits for blocks to be pre-committed to the network. If and when both conditions are achieved, the node commits a commitTime to a newHeight where the network can still keep consensus despite dissimilar clocks.

When and if any node receives a two thirds majority of commits, it enters the final commit stage where it commits the block.

IVAL + Data Structure

Wise uses an **IVAL+ Data Structure** very similar to that of Ethereum's Patricia trees. This data structure is built to institute fast computation for deterministic **Merkle** root hashes and storage for key-value pairs.

A balanced variant of AVL trees, a merkalized IVAL+ (Go 1.8+) is used by Wise to ensure the blockchain state cannot be tampered. In short, the AVL+ algorithm adjusts the AVL algorithm to keep values on leaf nodes while using branches to store keys. It is a key value pair storage allowing for a deterministic merkle root hash for computation, which guarantees the integrity of the structure from one block to the next. **Olog(n)** manages all the operations, because it is a variant of AVL, the nodes are immutable and indexed by their hash in the tree. The nodes serve as a timestamp for uncommitted memory-pool transactions, so that they can curtail the last commits for the new block. **Wise's IVAL+** is a more efficient algorithm adaptation of AVL.

Inherent support for WSE clients makes Wise particularly beneficial for IoT applications, whereat nodes may have limited resources. In contrast to IOTA's system which targets IoT applications that demand a heavy Java-based gateway node implementation, Wise's consensus is devised to assist WSE clients that do not have to store transactions locally. This is achieved by allowing applications to include the root of a Merkle tree in each block, which can be used to verify state queries or transaction outputs. This allows Wise to enable WSE client protocols, which are designed to permit users in low-capacity surroundings to help sustain an ideal state of the network. This means light clients protocols are great in IoT devices such as smartphones, watches, and tablets.

Applications are authorized by Wise to insert a Merkle Tree hash in each block to verify state queries or transaction outputs, similar to the structure of Ethereum's light clients. With Wise's underlying consensus, the network deciphers the nothing-at-stake predicament by means of deposit collateral, authorizing light clients to be aware when a validator is going to change and then verify more than two thirds of the pre-commits to know the latest block state. However, with our **ANSUZ** Chip devices, small IoT devices should be able to run full nodes.

Wise contains an **cross-blockchain communication protocol (CBC)** to allow blockchains on Wise to exchange tokens and information with one another. All exchanges between blockchains are done with something called CBC packets in which packets of information is sent through Skin to the other blockchains.

A method to do cross-chain atomic swaps is shown by hash time locked contracts in the Wise Network. However, Wise's CBC's protocol can generate 2-way sidechains, authorizing trades between blockchains with instant decisiveness that can enable a transfer of information or value.

More specifically, the CBC protocol is comprised of two kinds of transactions: a packet transaction, which authorizes a blockchain to ratify that a packet was announced by a sender by means of the most recent block hash Merkle-proof and a block commit transaction, which allows blockchains to validate its most recent block-hash to an observer.

In this manner, Wise network authorizes for the receiving chain to recognize which CBC packets are committed while allowing what outbound packets are allowed.

The concept of cross-blockchain communication can then be applied to things:

Multiple Virtual Machines - Wise's Skin only communicates to other IoT Chains through CBC, so each other blockchain can have their own virtual machines, applications, and governance.

Distributed Exchange- Wise's Skin can be used as a decentralized exchange to swap tokens between IoT Chains.

Cross-Chain Bridge - Chains on **Wise's Skin** can serve as a bridge to other blockchains like Bitcoin by verifying states in Wise and on other blockchains.

In this manner, cross-blockchain communication is a vital component of having an infinite amount of interoperable, self-governing blockchains on the Wise.

Wise handles infinite sharding through its IoT Chains. Wise Skin ignores the state of its IoT Chains but rather listens to communications through CBC packets, so each shard can be its own sovereign blockchain.

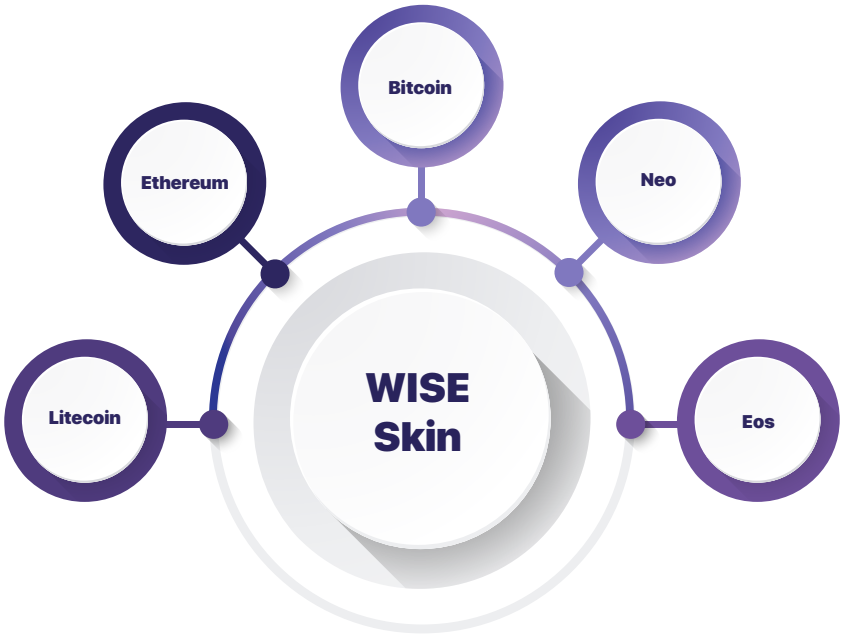
Unlike with proof of work consensus blockchains, with Wise's Tendermint consensus, running an infinite amount of parallel blockchains does not diminish either the speed or security of each IoT Chain. As each chain can handle thousands of transactions, spawn an infinite amount of chains, and have sub-chains work together, Wise can scale to infinity to handle any amount of IoT interactions.

The most important difference between sharding with Wise and other blockchains is that the shards depend on the general machine state on other blockchains, while Wise preserves the number of tokens between chains. This means that on Wise any blockchain with completely different virtual machines can be created and can fail, while on other blockchains, none of the shards should fail. However, in Wise, other types of sharding can be implemented and tied in within the network.

Wise Skin is a competitively validated assigned proof-of-stake platform. The hub maintains the number of tokens on each IoT Chain and enables a persistent relay of data between blockchains. This means that the hub serves as a global bridge between all public and private blockchains on Wise while also serving as a distributed exchange.

On Wise Skin, its native cross-blockchain communication protocols allow it to interact with its existing chains. Furthermore, since we acknowledge there are a lot of applications that people make on other chains, we will enable something called an in chain which provides a bridge and interoperability with existing blockchains and their native cryptocurrencies such as Bitcoin or Ethereum.

All that is needed for an involved chain to serve as a bridge is some type of pseudo-finality on the other blockchain where there is some process that determines the finality of the block.



For example, on Wise, one involved chain can work as a link with Ethereum. To supply some context, the majority of differences between Tendermint and Ethereum goes as follows: Tendermint uses go-wire for serialization while Ethereum uses Recursive Length Prefix. Tendermint uses ed25519 where in comparison, Ethereum uses secp256k1. Lastly, Tendermint uses IVAL+ Trees while Ethereum uses Patricia Trees for key values.

At this time on Tendermint, there is a protocol by the name ETGate which assists as a link between Tendermint-based blockchains and Ethereum. In the protocol, it decoded packets within Ethereum's virtual machine. However, converting every block into a compatible variant within the Ethereum Virtual Machine is too fuel costly for Wise. In order to provide a fuel-friendly link from Wise to Ethereum, an ABCI app will obtain a relay message from the Wise Skin, and the ABCI app will write an Ethereum transaction containing the address, denomination, amount, and nonce. The Signing Apps will then detect transactions from the ABCI Apps and sign transactions using secp256k1. The Signature Apps will broadcast messages back for duplication and the relayer Signing App will examine the ABCI app's transactions and process those that reach the demanded threshold. The relayer Signing App will send a transaction to the Ethereum smart contract and the smart contract will send a Light ERC20 Token to the user's Ethereum address.

It's easy to transfer WSE to the entangled chain on Skin, and once the involved chain obtains an CBC packet, signers can change the signature into Ethereum's native secp256k1 format. When two thirds of the transactions are complete, validators can then relay the information to Ethereum, in which we will build on smart contracts to empower the interoperability of Wise's native tokens and Ether. Once the light is sent, the smart contract can then send an ERC20 light variant to an Ethereum address where the IoT device is able to transform it to Ethereum via a distributed exchange. The progress of involved chains is still in its early stages, and more updates will be provided as the project moves forward. Wise's involved chains work as a global bridge to enable interoperability between all important blockchains.

On the Wise Skin, the token exists exclusively for staking and for fees. It is called WSE. Wise is the only staking token on Wise Skin and is used to vote, validate, and delegate validators. WSE is used for a transaction fees to alleviate spam. Because Wise's consensus algorithm can replicate different deterministic states, more than one coin can be built upon each chain since Wise Hub tracks multiple different token states.

For this reason, the multi-token economic standard was created to approach the problems of present proof of stake models.

Such as, when Ethereum switches to Casper, there is one native token: Ether. As Ether has more utility than staking, such as paying for products and services, a considerable quantity of Ether tokens will not be staked and, as a result, weakens the security of the protocol.

Since Wise is an interaction multi-device network, WSE is introduced to address this interest. WISE's utility is for staking and will be used to pay transaction fees and block rewards on Wise Skin and hosted chains. One can think of the token like an SHA-256 ASIC miner. The ASIC miner's main utility is to mine Bitcoin. In Wise's case, the reward is in WSE instead of Bitcoin and the miner is the WSE token instead of the ASIC.

In this model, WSE's utility is to function as the only staking token, which will encourage the governance and protection of the network. This way, the bulk of WSE will be staked in the network by virtue of buying and selling services and will be considered as staking. The fees collected by validators from data processing costs from each transaction will be distributed proportionally to the number of WSE staked.

In Wise's Skin, validators can stake their WSE tokens and can delegate the tokens to stakers. The hub at first will have 100 validators, but over time will create up to 500

validators. Validators can stake WSE tokens and in return receive more WSE for block provisions and transaction charges. There are only a limited number of validators, so nodes can delegate their WSE tokens and contribute to the agreement; as a result, they will earn a percentage of transaction fees for taking part or lose their share if the validator is malicious. Same as other delegated proof of stake structures, the more WSE Tokens one stakes, the more block rewards and transaction fees they get in return.

When Wise Skin launches, validators will be chosen through a public vote, which will shift around validators when WSE tokens are delegated to others.

When a block is announced, the provisions are proportionally delivered across validators in relation to their stakes. If the block provision is 5000 WSE tokens and each validator has 20% of staked WSE tokens, and the commission fee is 2% across 10 validators, then the 500 tokens will be distributed across:

Commission: 500*80%*2%= 8 WSE
Validator: 500 * 20 % + Commission = 108 WSE
Delegators: 500 * 80 % - Commission = 402 WSE

Each delegate will receive an arrangement of the 402 WSE in relation to what it delegated to the validator pool. If a validator is malicious, such as when it commits signing, Wise will identify it easily since only two conflicting votes are needed. The validator will instantly be dissipated after a slash transaction is committed. At the start, 5 percent of WSE tokens will be inflated yearly; despite that, this value will change to encourage validators to stake two-thirds of the WSE tokens and depending on the administration (governance) of the hub.

There will be 100 validators on launch date, they will expand at a rate of 15 percent per year until it achieves 500 validators. The block reward for WSE will be determined at a later date but will be at an inflation rate that asymptotically reaches zero. Validators on Wise Skin might help validate other IoT Chains such as Wise Un0.

In case a validator transgresses, it forfeits its staked WSE tokens. This happens when double-signing, such as if a validator reports that on Chain A, a validator signed two blocks with an identical height on Chain A and B. If that is the case, the validator will get slashed on Chain A. Next, if a validators signature has not been included in the last x amount of blocks, the validator will get slashed a proportional amount of x. If it exceeds a number y, then the stake will be removed. If someone reports that a validator did not vote, a minor slash will occur. Furthermore, validators are in risk of being slashed in case the node ends up DDOSed, the node crashes, the private key is hacked, and if it loses connection.

Governance

On the Wise Skin, validators can decide on items such as block gas boundaries related to parameter changes, coin volatility, updates to the rules, as well as vote on terms and services that control the Wise Skin. Each validator is required to vote or else the validator will be deactivated for 2 weeks. Each vote proposal requires certain amount of tokens on Wise as a stake deposit. If the proposal was spam, meaning that the votes were majority negative, the deposit would go into something called a reserve pool.

For proposals, validators can vote with either: Yes, No, and Abstain and a strict majority is required for a proposal to pass. More updates regarding governance specification will be revealed close to Wise's main launch.

Aside from the Wise Skin, each blockchain on Wise can have its own administration and constitutions, as they are sovereign blockchains.

The IoT Chains are superior throughput regional or mechanism-specific public/permissionless or private/consortium blockchains, each powered by Tendermint BFT Consensus that connects to Wise's Skin. While each IoT Chain handles thousands of transactions per second, billions of IoT devices using the same network can give rise to write fees to go up, and no sole blockchain or DAG can scale past 30 thousand transactions per second in real-world conditions. IoT devices are also the contrary of "one chain fits all" as devices on a single blockchain are forced to use different data types, which are emulated within a generic container.

Therefore, each chain uses ABCI from Tendermint, allowing developers to create more distributed replicated IoT Chains blockchain and split the network users, creating unlimited scalability. Wise's toolkit allows custom device type chains to be built for specific IoT applications, as native types perform better. Each IoT Chain can also bootstrap off of the IoT Ledger, allowing validators in each IoT Chain to verify their location and in turn, developing geographically-specific public chains for fast resolution.

IoT Chains are blockchains that can take many shapes or builds on Skin such as, private, consortium, local, public, global, manufacturer-operated, geographically specific blockchains, or user-operated blockchains. IoT Chains on Skin come with an open source software development kit for setting up interacting IoT Chains and as an easy guide for anyone who would want to create a chain with Wise. Collectively, each IoT Chain

interfaces with Index's identification chain and second layer network systems, allowing them to turn to create new identity based applications.

Wise's Index contains a built-in identity protocol layer to enable machines to find one another, self-organize, and start growing something called a machine reputation. The identity protocol layer can devise if a random node is trustworthy or not, or where its place should be in the same knowledge domain. Nodes in the network can intercommunicate with other known nodes on the public ledger, which will also enable people to decide whether their machine is functioning appropriately. A smart contract in Index will update whenever a transaction is made via Wise's distributed applications.

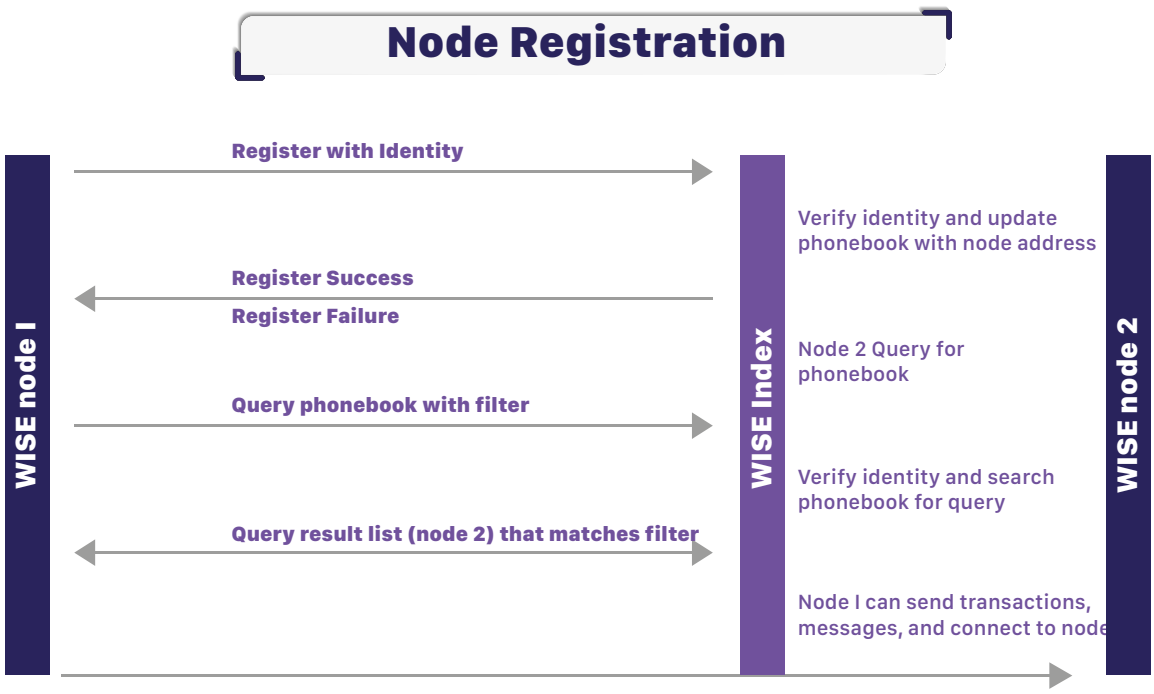
Singular identities will be added as transactions and will be preserved on side-chains of the hub with Wise's SDK providing permanent logging of identity data. An off-chain database will hold knowledge regarding the node such as reputation score, which will be determined by an algorithm that produces a score based on items such as how much cryptocurrency is in the node's address, how many interactions a node has achieved previously, and the amount of data the node decided to publish. The algorithm and its ins and outs regarding the exact nature of the identity protocol will not be public as it's not in the best interest of devices to start gaming the system. However, more details will be released near the distribution of the Wise Network.

Beacons

Machines have much simpler identities than the humans or groups of humans that own them. Essentially, a machine identification is an address on the network that appears like it is owned by no one simply because its owner has listed it privately.

For machines that require to publish information openly, machines can use a human-readable domicile, like jane.doe/weather place or microsoft/weather station or Florida/parkstreet123534. Beacons are the method for registering machines on the Wise Skin's ID chain. It allows for machines to publish information about themselves, generally a single time, but machines can hold currency and can of course publish multiple times.

Beacons work assigning IDs on the chain to diferent devices, authorizing access to a specific device through a P2P manner anywhere in the network. There is a minimal cost for registering a beacon, to prevent spam. Beacons can be highly descriptive, or entirely minimal. This is the choice of the user.



Put simply, a beacon is a tenacious identifier of all kinds of devices, it can store as much information about themas desired in its cache. Devices at work can communicate with their manufacturer's Beacons, or end users can utilize them to enable integration between devices. It is possible for two devices on Index to find one another even without a Beacon on the blockchain, providing that they know each others device IDs. Users and devices will be able to find one another without dealing with IPFS device ID's directly thanks to the Beacons.

On Wise Index, people and machines that are registered with Beacons acquire an explicit reputation from machines and humans that interact with them. Machine reputation is a security mechanism that assumes that devices can and will be hacked or modified in unexpected ways to cause a negative output, providing recourse for when that happens. While Index cannot undo a transaction with flawed data, Index can curate its network of machines and prevent harmful machines from taking a foothold in the network. With machine reputation, machines do not need user feedback on its performance and serve as a mechanism for controlling autonomous devices. The network will maintain an off-chain cloud reputation lookup explorer, allowing for machines to have an easier time to find other devices and gauge reputation before engaging in direct communication and transactions. The Wise Index allows for vendors and device owners to obtain an overview of machine transactions to establish whether the autonomous device is performing as it should.

Some assumptions are that humans use names when they talk to each other, take for example 3G2tAbt9x1…, is not a name and that Index resolve names to addresses, so humans are able to use names.

Additional premises are that machines use addresses when they talk to each other, for example 3G2tAbt9x1..., is an address and that Skin resolves names to addresses, so when humans use names, machines know what they're talking about.

In the end, a general assumption is that machines can and will be corrupted. Machine reputation grows positively over time and helps users to determine whether or not a device is reliable so that machines can be automated with reputation thresholds to be sure that they don't link to low-reputation nodes.

Index allows the improvement of systems that utilize identity information stored on the blockchain instead of focusing on unique users, by accepting that humans and devices can have multiple online identities, and recognizing the fact that identities are not equally persistent. Although machines and people can have multiple identities, there is an economic incentive on Index for machines to focus their identity-strength.

Humans and Groups can own devices, which are recorded locally and owned by humans or groups of humans. Index supplies global identities to all human users and groups of human users too.

A secure, encrypted second layer peer-to-peer communication network can be built with Index, due to the fact that it provides cryptographically verifiable identities. Such network would be able to bootstrap off the superior performance done by the IPFS design.

Machine identities will be constructed differently, since they have to circulate their use cases and machine ID for automatic node discovery. We create a crypto "phonebook" by keeping public cryptocurrency addresses on the Idem. Users that do not wish to be listed in the phonebook can decline to provide any information. This phonebook is planned to be used to allow programmatic money transactions between users on the INDEX network and between machines and users.

Un0 is Wise's native smart contract platform that authorizes the creation of infinitely scalable distributed applications, with an IoT and AI vertical.

At the very start, Un0 will be a rapid Proof of Stake blockchain that will be working together with Ethereum. This means at the beginning, Un0 will begin as an EVM on Wise's Tendermint, allowing for Web3 compatibility, sharding, and high flowrate. In opposition to Ethereum's actual Proof-of-Work consensus, Un0 allows transactions to run

at 20 times the speed as it can pack 20 times the transactions in a block. Users already familiar with Ethereum's smart contract platform will be allowed to migrate over to Un0 and permit developers to get acquainted with Wise's network. Un0 will utilize WSE as its gas, similar to how Ethereum allows Ether. Verifiers on the Skin will also help run Un0's distributed application platform. Later, Un0 will include its own native virtual machine built on Tendermint Core. This virtual machine called **Quantum**, or **QVM** for short, will be a lightweight JVM implementation towards achieving high execution when performing chain logic. More details regarding QVM will be released shortly.

With one blockchain, Un0 can handle 200 transactions per second. In Un0, an endless quantity of distributed-replicated blockchains can be developed on Un0 and work in ananalogous manner.

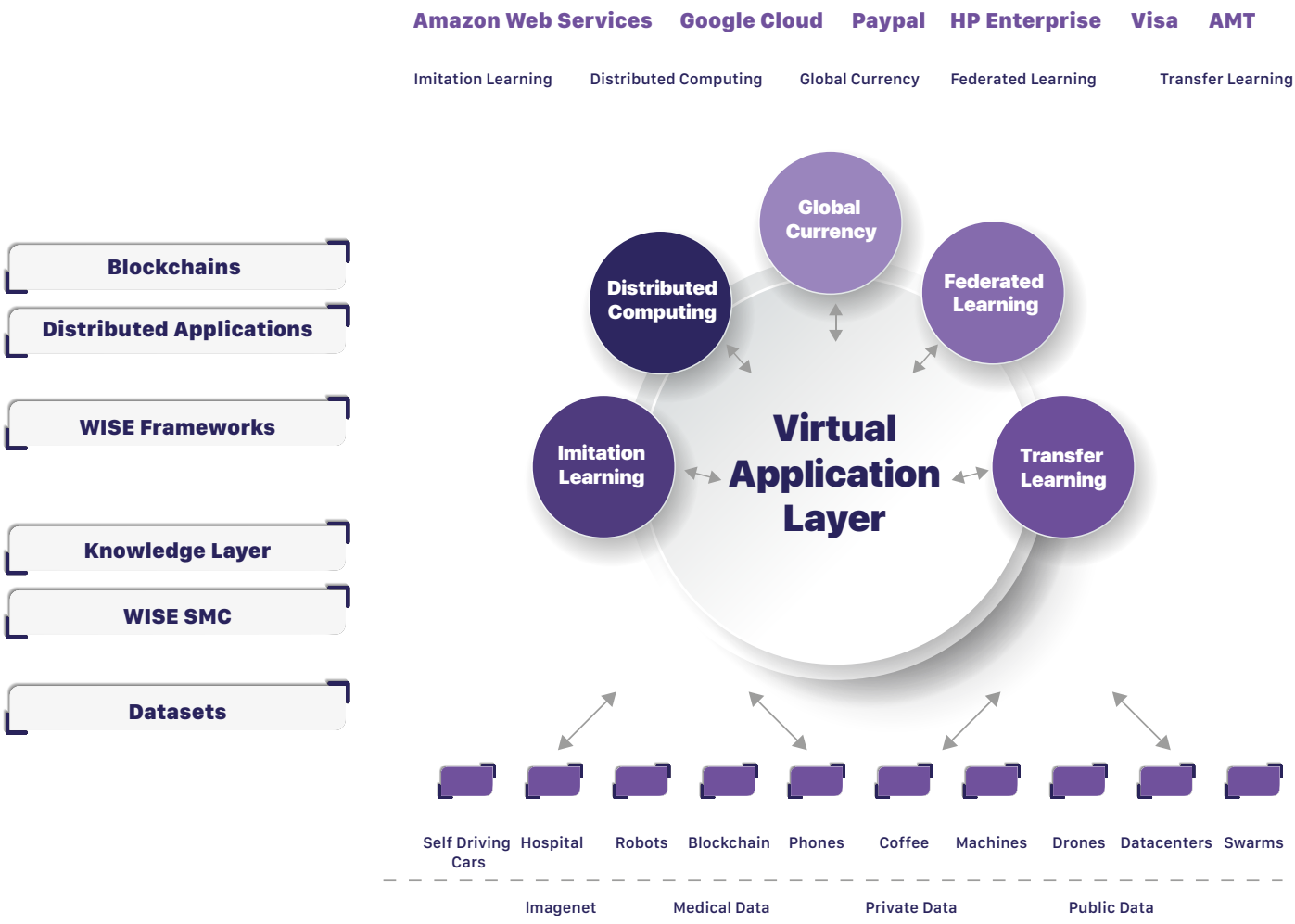
The platform can be enabled to have a 1000 transactions per, previously creating 5 more UnOs with With Wise's cross-blockchain communication protocols. Un0 can handle 5000 transactions per second second if the amount of IoT Chains is multiplied by 5. With this, Un0 obtains horizontal scalability and infinite sharding.

Multiply the amount of Un0 and IoT Chains by 5 can handle 5000 transactions per second. This way, Un0 fulfills horizontal scalability and ever-evolving sharding.

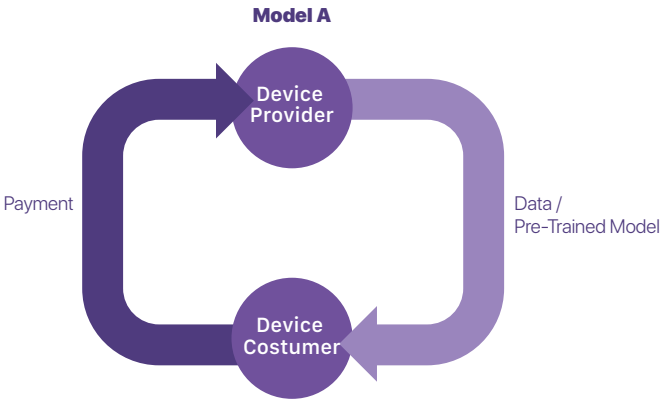
Un0 also contains the essential agreement for the Internet of Things and artificial intelligence exchanges. With current Bitcoin and Ethereum implementations, blocks have a definite confirmation number before they are final. Six confirmations in Bitcoin, for example, is 60 minutes, and six confirmations in Ethereum is only 2 minutes. With Un0's consensus model, blocks are completed within a second.

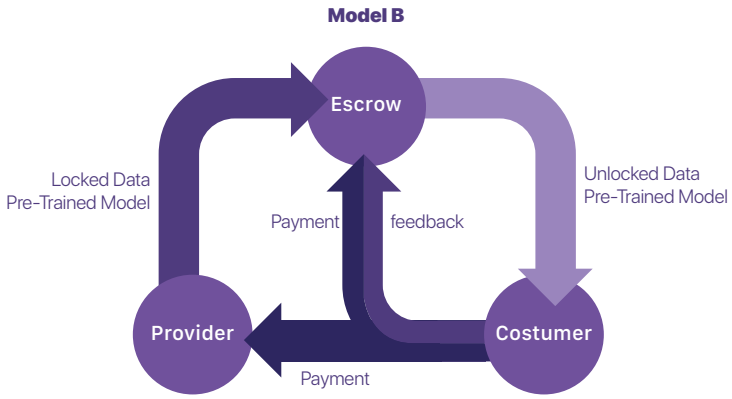
Instant finality and no backlog in transactions, gives Un0 the advantage of offering transaction fees considerably cheaper than Ethereum.

Blockchains on Wise and the distributed applications on Un0 come together to form a virtual infrastructure application layer or a distributed **WISENet.** In here, nodes with information and knowledge from places such as ImageNet and self-collected data can be distributed over the network. With the inherent identity protocols, nodes can find each other in a similar knowledge domain to start transferring knowledge, data, and training off one another in a decentralized fashion. Additional distributed applications can be created on top of the **WISENet** and be interoperable with existent applications. This virtual infrastructure application layer will be an independent, carrying out existing infrastructures such as AWS and distributing essential datasets for training. This way, nodes can access the **WISENet** ecosystem and start a recurrent developing process.

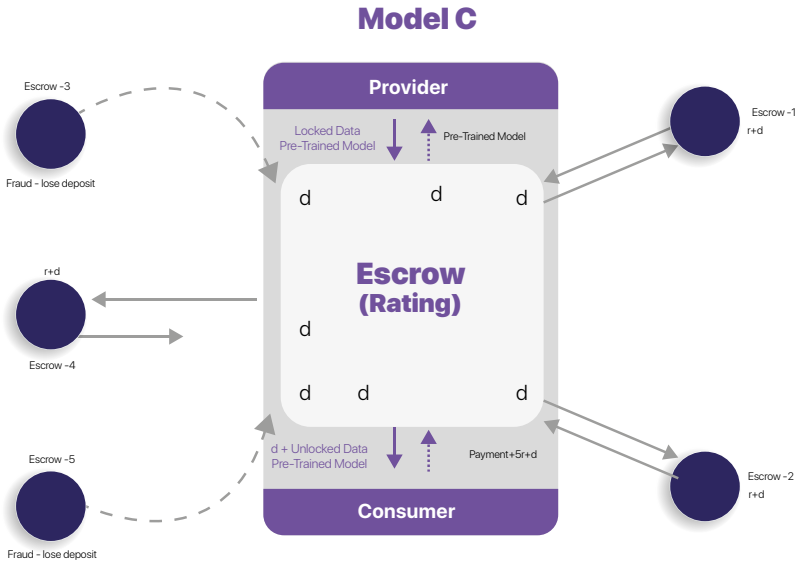


The above graphic depicts how the virtual application layer would work. Billions of nodes will access the Wise Ecosystem and can interact with each other with the WISENet virtual application layer. Businesses and developers will be able to contribute to this constantly-growing network by creating their own blockchains and DApps. Nodes on the network will be free to influence these applications and settle prices with a built-in AI marketplace. The marketplace, distributed applications, and reputation economics will be developed in more detail during the progress of Wise Network as they need to be customized to provide the required applications and create the device core powers independent and functional.





Model A smart contract is a highly efficient and straightforward contract to speed up transactions. These are to be executed exclusively for a seller and/or buyer with a very high reputation score. Model B smart contract is for the compromise method for entities with mid-level reputation and can be determined by buyer.



Each participant will receive an update to its decentralized identities, after each transaction.

Autonomous Decentralized Machine Learning Edge nodes can start discovering one another to begin improving their networks, by discovering various machine learning allocated applications with the virtual application layer's identity network. Machines will be able to transfer knowledge and interact with one another with this structure.

Here are some of methods to do so:

Transfer Training- The neural network can become more generalized for other situations when nodes use pre-trained models and retrain the final layers.

Data Training - Other devices can train from labeled data previously branded by Machines or people.

Federated Training - Edge nodes will be able to train off private, untapped data such as medical data and collaborate to make a better neural network model.

These types of learning encourage advantages or underlying systems:

Distributed Storage **-** Data sets can be deployed through the network contrary to being centralized on one server.

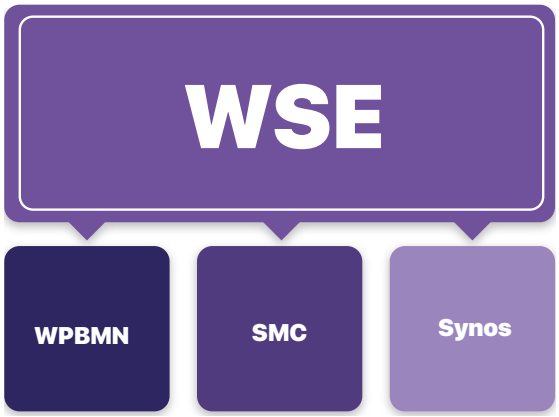
Incentives - Devices can distribute data, share algorithms ad sell inactive processing capacity by participating in this system.

Knowledge - It can be transferred from one edge node to the other.

Distributed Processing **-** Borrowing and/or distributing idle processing power from others can be achieved by Nodes on edge.

The necessary platform to create applications for devices to communicate between each other will be delivered by Wise's own application layer. The smart contracts that this layer includes is for distributed computing, federated learning, data branding, and transfer learning.

Once development is finalized, all the WSE tokens offered in the Wise token channel will switch over to all cryptocurrencies on Wise.



More accurately, tokens will switch over to WSE. Access to the end-to-end platform's staking tokens, fee tokens, and application tokens will be granted to all ICO participants, all of it contained in a single robust token, WSE. Paired with the Wise-Public Blockchain-Mesh-Network and Wise's SMC, we are in front of the imminent new combustible for machines and the backbone of the M2M economy.

Lastly, Wise Network can be reduced to the Wise-Public Blockchain-Mesh-Network and Wise's ANSUZ Chip. Wise's ANSUZ Chip is a segmental blockchain SoC hub, which provides a competitive advantage when compared to Arm in the IoT chipset industry. Devices provided with a Wise ANSUZ Chip include a WSE hardware wallet, which allows appliances to employ blockchains and cryptocurrencies by securing them in a Ledger wallet, adding bonuses like a brain-on-chip system for AI authentication and human-like intelligent abilities.

Spotlight cases would be smartphones, self-driving automobiles, and smart cities. WISE network will be able to connect every single IoT device, in a scalable infinite-chain platform. Exchange value in milliseconds, train off private data, discover each other securely, deploy algorithms across the network, assimilate from its WISENet constituted of upgraded elemental foundations comparable to AWS and Imagenet. Supported by Wise's scalable fault-tolerant architecture, the network will be able to grab several IoT subsystems, supplying interoperability between its exclusive and public blockchains, and providing the ability to grasp millions of operations in an instant.

Devices have the capacity to utilize the blockchain network, becoming intelligent thanks to WISE ANSUZ Chip. Next, IoT devices can also interact with one another, connect themselves, similar to human conduct thanks to the Wise-Public Blockchain-Mesh-Network. The creation of WISE Network relies on these two elements, the intelligent machine economy will become scalable with our end-to-end protocol allowing communication with other networks such as Bitcoin or Etherium.

6. Bibliography

WISE

1.Sinno Jialin Pan and Qiang Yang. “A Survey on Transfer Learning”, IEEE Transactions on Knowledge and Data Engineering, 22(10), 1345–1359.
2.Soriano, Miguel C., et al. “Delay-Based Reservoir Computing: Noise Effects in a Combined Analog and Digital Implementation.” IEEE Transactions on Neural Networks and Learning Systems, vol. 26, no. 2, 2015, pp. 388–393., doi:10.1109/tnnls.2014.2311855.
3. http://ieeexplore.ieee.org/document/1251416/?anchor=references
4. doi:10.1103/physrevx.7.011015.networks. In Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2 (NIPS’14), Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger (Eds.), Vol. 2. MIT Press, Cambridge, MA, USA, 3104-3112.
5. Graves, A.; Liwicki, M.; FernÃ¡ndez, S.; Bertolami, R.; Bunke, H.; Schmidhuber, J. (May 2009). "A Novel Connectionist System for Unconstrained Handwriting Recognition". IEEE Transactions on Pattern Analysis and Machine Intelligence. 31 (5): 855–868. doi:10.1109/tpami.2008.137. ISSN 0162-8828.
6. Sak, H.; Senior, A.; Rao, K.; Beaufays, F.; Schalkwyk, J. (September 24, 2015). "Google voice search: faster and more accurate". Research Blog. Retrieved 2018-03-04.
7. Maass, Wolfgang, et al. “Real-Time Computing Without Stable States: A New Framework for Neural Computation Based on Perturbations.” Neural Computation, vol. 14, no. 11, 2002, pp. 2531–2560., doi:10.1162/089976602760407955. 8. Jaeger, H. The “echo state” approach to analysing and training recurrent neural networks. German National Research Center for Information Technology GMD Technical Report, 2001
8. 10. Larger, L., et al. “Photonic Information Processing beyond Turing: an Optoelectronic Implementa- tion of Reservoir Computing.” Optics Express, vol. 20, no. 3, 2012, p. 3241., doi:10.1364/oe.20.003241.
9.Lamport et al, The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 4 Issue 3, July 1982
10. Arecchi, F. T., et al. “Two-Dimensional Representation of a Delayed Dynamical System.” Physical Review A, vol. 45, no. 7, Jan. 1992, doi:10.1103/physreva.45.r4225. 11. Merkle Patricia Tree Specification. https://github.com/ethereum/wiki/wiki/Patricia-Tree 68. Ethereum Blockchain.
12. Primecoin. http://primecoin.io/ 87. Lamport, L. (1978). Time, clocks, and the ordering of events in a distributed 56. https://www.wired.com/story/this-computer-uses-lightnot-electricityto-train-ai-algorithms/
13. Martinenghi, R., et al. “Optoelectronic Nonlinear Transient Computing with Multiple Delays.” 2013 Conference on Lasers & Electro-Optics Europe & International Quantum Electronics Conference CLEO EUROPE/IQEC, 2013, doi:10.1109/cleoe-iqec.2013.6800826.
14. Nieters, P., et al. “Neuromorphic Computation in Multi-Delay Coupled Models.” IBM Journal of Research and Development, vol. 61, no. 2/3, Jan. 2017, doi:10.1147/jrd.2017.2664698.
15. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-161.md
16. Lukoševičius, Mantas. “A Practical Guide to Applying Echo State Networks.” Lecture Notes in Computer Science Neural Networks: Tricks of the Trade, 2012, pp. 659–686., doi:

10.1007/978-3-642-35289- 8_36.
17. https://physics.aps.org/featured-article-pdf/10.1103/PhysRevX.7.011015
18.Larger,Laurent,etal."LaserChimerasasaParadigmforMultistablePatternsinComplexSystems." Nature Communications, vol. 6, no. 1, 2015, doi:10.1038/ncomms8752.
19. Peil, Michael, et al. "Routes to Chaos and Multiple Time Scale Dynamics in Broadband Bandpass Nonlinear Delay Electro-Optic Oscillators." Physical Review E, vol. 79, no. 2, Sept. 2009, doi:10.1103/physreve.79.026208.
20. https://www.xilinx.com/products/silicon-devices/soc.html
21. Soriano, Miguel C. "Reservoir Computing Speeds Up." Physics, vol. 10, June 2017, doi: 10.1103/physics.10.12. 33. Zhang, Hong, et al. "Integrated Photonic Reservoir Computing Based on Hierarchical Time-
Multiplexing Structure." Optics Express, vol. 22, no. 25, Nov. 2014, p. 31356., doi:10.1364/oe. 22.031356.
Keuninckx, Lars, et al. "Real-Time Audio Processing with a Cascade of Discrete-Time De- lay Line-Based Reservoir Computers." Cognitive Computation, vol. 9, no. 3, July 2017, pp. 315–326., doi:10.1007/s12559-017-9457-5.
22. Appeltant, L., et al. "Information Processing Using a Single Dynamical Node as Complex System." Nature Communications, vol. 2, 2011, p. 468., doi:10.1038/ncomms1476. Merolla, P. A., et al. "A Million Spiking-Neuron Integrated Circuit with a Scalable Communication Network and Interface." Science, vol. 345, no. 6197, July 2014, pp. 668–673., doi:10.1126/science. 1254642.
23. Lipton,R.J.;J.S.Sandberg (1988). PRAM:A scalable shared memory(Technicalreport).Princeton University. CS-TR-180-88. Ilya Sutskever, Oriol Vinyals, and Quoc V. Le. 2014. Sequence to sequence learning with neural

7. Filecoin. https://filecoin.io/

8. IOTA data market https://data.iota.org/

9. US patent 4309569, Ralph Merkle, "Method of providing digital signatures", published Jan 5, 1982,assigned to The Board Of Trustees Of The Leland Stanford Junior University

The Bulletin of Mathematical Biophysics, vol. 5, no. 4, 1943, pp. 115–133., doi:10.1007/ bf02478259. Rosenblatt, F. "The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain." Psychological Review, vol. 65, no. 6, 1958, pp. 386–408., doi: 10.1037/h0042519.
24. https://www.ethereum.org/
25. Giacomelli, Giovanni, and Antonio Politi. "Relationship between Delayed and Spatially Extended Dynamical Systems." Physical Review Letters, vol. 76, no. 15, Aug. 1996, pp. 2686–2689., doi:10.1103/physrevlett.76.2686.
26. Dryja.

27. Li, Jialing, et al. “Analog Hardware Implementation of Spike-Based Delayed Feedback Reservoir
28. Kilts, Steve. Advanced FPGA Design Architecture, Implementation, and Optimization. Wiley, 2007.
https://www.certicom.com/content/dam/certicom/images/pdfs/ams/security_for_fabless_semi_08.pdf https://web.archive.org/web/20070825103724/http://csrc.nist.gov/cryptval/140-2.htm
29. Brunner, D., et al. “Spatio-temporal complexity in dual delay nonlinear laser dynamics: chimeras and dissipative solitons” https://arxiv.org/abs/1712.03283
30. Antonik, Piotr, et al. “Online Training of an Opto-Electronic Reservoir Computer Applied to Real- Time Channel Equalization.” IEEE Transactions on Neural Networks and Learning Systems, vol. 28, no. 11, 2017, pp. 2686–2698., doi:10.1109/tnnls.2016.2598655.
31. Romeira, B., et al. “Regenerative Memory in Time-Delayed Neuromorphic Photonic Resonators.” Scientific Reports, vol. 6, no. 1, 2016, doi:10.1038/srep19510.
32. Git version control system. https://git-scm.com/ Leslie Lamport. On interprocess communication. part I: Basic formalism.
33. Herlihy, M. and Wing, J. M. (1990). Linearizability: A correctness condition
34. Karger, D.; Lehman, E.; Leighton, T.; Panigrahy, R.; Levine, M.; Lewin, D. (1997). Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web. Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing. ACM Press New York, NY, USA. pp. 654–663
35. Enel, Pierre, et al. “Reservoir Computing Properties of Neural Dynamics in Prefrontal Cortex.” PLOS Computational Biology, vol. 12, no. 6, Oct. 2016, doi:10.1371/journal.pcbi.1004967.
36.FormoreinformationregardingFPGAdesignworkflowspleaserefertorespectiveuserguides:Xilinx
,
37. http://discourse.myhdl.org/
38. https://software.intel.com/en-us/cvsdk-fpga-support-introducing-fpga-support-for-cnn
39. See this proposal for the fixed-point type: http://dev.myhdl.org/meps/mep-111.html
40.R Barrett, Samuel, Matthew E. Taylor, and Peter Stone. "Transfer learning for reinforcement learning on a physical robot." International Conference on Autonomous Agents and Multiagent Systems- Adaptive Learning Agents Workshop (AAMAS-ALA), 20
42. https: //arxiv.org/pdf/1610.04286.pdf
43. https://www.altera.com/products/soc/overview.html
44. Waldrop, M. Mitchell. “The Chips Are down for Moore’s Law.” Nature, vol. 530, no. 7589, Sept. 2016, pp. 144–147., doi:10.1038/530144a.
45.https://blog.otiumcapital.com/otium-neural-newsletter-1-federated-learning-a-step-closer-towards-
46.https://sfbitcoindevs.wordpress.com/2015/01/21/tendermint-consensus-without-mining/
47. http://tendermint.readthedocs.io/projects/tools/en/master/introduction.html#what-is-tendermint https://lightrains.com/blogs/intro-tendermint

51.M. J. Fischer, N. A. Lynch, and M. S. Paterson, “Impossibility of distributed consensus with one faulty process,” Journal of the ACM, vol. 32, no. 2, pp. 374–382, 1985.

EIP150 - https://github.com/ethereum/EIPs/blob/master/EIPS/eip-150.md EIP 161 -
Cosmos Whitepaper Appendix – Preventing Long Range Attacks. https://cosmos.network/whitepaper#appendix
103. The Cosmos Network. https://cosmos.network/
Cosmos Whitepaper. https://cosmos.network/whitepaper https://blog.z.cash/htlc-bip/ https://github.com/tendermint/basecoin/blob/master/docs/guide/ibc.md
48. https://github.com/mccorby/PhotoLabeller confidential-ai-efe28832006f
49. https://github.com/xesscorp/myhdl-resources 34. Freiberger,Matthias,etal.“On Chip Passive Photonic Reservoir Computing with Integrated Optical
50. Filecoin Storage Blockchain. https://filecoin.io/ 107. Lisa Torrey and Jude Shavlik, “Transfer Learning”, University of Wisconsin, Madison WI.
51. Andrei A. Rusu, Matej Vecerik, Thomas RothÃ¶rl, Nicolas Heess, Razvan Pascanu, Raia Hadsell, “Sim-to-Real Robot Learning from Pixels with Progressive Nets”, arXiv Preprint arXiv: 1610.04286 -
52. Rabinovich, Mikhail I., et al. “Dynamical Bridge between Brain and Mind.” Trends in Cognitive Sciences, vol. 19, no. 8, 2015, pp. 453–461., doi:10.1016/j.tics.2015.06.005.
53. Seth Gilbert and Nancy Lynch, "Brewer’s conjecture and the feasibility of consistent, available, partition-tolerant web services", ACM SIGACT News, Volume 33 Issue 2 (2002), pg. 51–59.
54.Ruder,S.,An Overview of Multi-Task Learningin Deep Neural Networks, https://arxiv.org/pdf/1706.05098.pdf 15. https://en.wikipedia.org/wiki/Kernel_method
55. Schumacher, Johannes, et al. “An Introduction to Delay-Coupled Reservoir Computing.” Springer Series in Bio-/Neuroinformatics Artificial Neural Networks, 2015, pp. 63–90., doi:10.1007/978-3-319-09903- 3_4.
56. Torrejon, Jacob, et al. “Neuromorphic Computing with Nanoscale Spintronic Oscillators.” Nature, vol. 547, no. 7664, 2017, pp. 428–431., doi:10.1038/nature23011. 57. IOTA Project. https://iota.org/ 59. Federal Information Processing Standards Publication 180-2. Secure Hash Standard. August 2002.
58. The Interplanetary Filesystem Whitepaper. Juan Benet. IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3). https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system. pdf
89.Bueno,JuliÃ¡n,etal.“ConditionsforReservoirComputingPerformanceUsingSemiconductorLasers with Delayed Optical Feedback.” Optics Express, vol. 25, no. 3, 2017, p. 2401., doi:10.1364/oe.25.002401.

59. Casper the Friendly Finality Gadget. Vitalik Buterin and Virgil Griffith. 2017. https://arxiv.org/abs/1710.09437
60. Gallicchio, Claudio, et al. “Deep Reservoir Computing: A Critical Experimental Analysis.” Neuro- computing, vol. 268, 2017, pp. 87–99., doi:10.1016/j.neucom.2016.12.089.

61. The Human Brain project comprises such subprojects as BrainScaleS and SpiNNaker the goal of which simulate the human brain simulation as a spiking network, in analog (BrainScaleS) and digital (SpiNNaker) hardware, https://www.humanbrainproject.eu/en/silicon-brains/
62. esearch platforms aimed at functional hardware description haveappeared a decad eago(e.g.Lava, ForSyDe)
63. A Next Generation Smart Contract and Decentralized Application Platform. Vitalik Buterin. 2013. https://github.com/ethereum/wiki/wiki/White-Paper

Bogdan Penkovsky. Theory and Modeling of Complex Nonlinear Delay Dynamics Applied to Neuromorphic Computing. Artificial Intelligence [cs.AI]. UniversitÃ© Bourgogne Franche-ComtÃ©, 2017. English. [3008?]tel-01591441v2[3009?]
https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649
64. Antonik,Piotr,etal."Brain-Inspired Photonic SignalProcessorforGeneratingPeriodicPatternsand Emulating Chaotic Systems." Physical Review Applied, vol. 7, no. 5, 2017, doi:10.1103/physrevapplied.7.054014. 65. Computing System." 2017 International Joint Conference on Neural Networks (IJCNN), 2017, doi:10.1109/ijcnn.2017.796628 31. Larger, Laurent, et al. "High-Speed Photonic Reservoir Computing Using a Time-Delay-Based
Architecture: Million Words per Second Classification." Physical Review X, vol. 7, no. 1, June 2017,
66. Fernando, Chrisantha, and Sampsa Sojakka. "Pattern Recognition in a Bucket." Advances in Artificial Life Lecture Notes in Computer Science, 2003, pp. 588–597., doi: 10.1007/978-3-540-39432-7_63.
67. On Sharding Blockchains. https://github.com/ethereum/wiki/wiki/Sharding-FAQ The Bitcoin Lightning Network: Scalable Off - Chain Instant Payments. Joseph Poon and Thaddeus 2016. https://lightning.network/lightning-network-paper.pdf
68. The Raiden Network. https://raiden.network/
Plasma: Scalable Autonomous Smart Contracts. Joseph Poon and Vitalik Buterin. 2017. https: // plasma.io/plasma.pdf
69. Ian Goodfellow and Yoshua Bengio and Aaron Courville, "Deep Learning", MIT Press (2016).
70. Tendermint Blockchain Consensus Platform. https://tendermint.com/
71. SatoshiNakamoto,APeer-to-PeerElectronicCashSystem.2009.https://bitcoin.org/bitcoin. pdf
72. Lamport, L. (1979). How to make a multiprocessor computer that correctly
73. Integrated Circuits." Scientific Reports, vol. 8, no. 1, Feb. 2018, doi:10.1038/s41598-018-21011-x.
74. Pan, S. J., & Yang, Q.. "A survey on transfer learning", IEEE Transactions on Knowledge and Data Engineering, 22(10), 1345–1359, (2010)
75. Practical Byzantine Fault Tolerance. Miguel Castro and Barbara Liskov. Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999
76. https://github.com/tendermint/tendermint/wiki/Introduction

77. https://research.fb.com/category/facebook-ai-research-fair/
78. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md
79. Readout." 2017 IEEE International Conference on Rebooting Computing (ICRC), 2017, doi: 10.1109/icrc.2017.8123673. 35. Katumba, Andrew, et al. "Low-Loss Photonic Reservoir Computing with Multimode Photonic
80. https://github.com/tendermint/iavl
81. Volodymyr Mnih, AdriÃ PuigdomÃ¨nech Badia, Mehdi Mirza, Alex Graves, Timothy P. Lillicrap, Tim Harley, David Silver, and Koray Kavukcuoglu. "Asynchronous methods for deep reinforcement learning". In International Conference on Machine Learning (ICML), 2016.
82. Hochreiter and JÃ1⁄4rgen Schmidhuber. "Long Short-Term Memory". Neural Computation, Volume 9, Issue 8, November 15, 1997 (p.1735-1780)
83. https://www.news.iastate.edu/news/2017/06/07/exciton-polaritons 112. Weiss, Karl, Taghi M. Khoshgoftaar, and DingDing Wang. "A survey of transfer learning. Journal of Big Data 3.1 (2016).
84. https://research.googleblog.com/2017/04/federated-learning-collaborative.html