Humanode—A distributed consensus mechanism based on private biometrically encrypted equal human nodes

Whitepaper v 0.9.5 'Ayanami'

David Kavazi, Maxim Kupriianov, Victor Smirnov and Sasha Shilina, PhD

20th November 2020

A Public Permissionless Financial System based on consensus between equal human nodes with rule-based monetary policy targeting real value growth and proportional emission

1 Abstract

The pursuit of new decentralized financial systems has engulfed the world. In the last few decades, dozens of different protocol prototypes have been deployed to achieve a decentralized state of finance, but most were unable to deliver the immutability and consistency required for large adoption. The advent of blockchain technology has led to a massive wave of different decentralized ledger technology (DLT) solutions. Such projects as Bitcoin and Ethereum have shifted the paradigm of how to transact value in a decentralized manner, but most have different core technologies with their own advantages and disadvantages. This paper aims to describe an alternative to modern decentralized financial systems by introducing the Humanode network. Humanode is a network safeguarded by biometrically encrypted private replicas (or human nodes). Using solutions that provide fully homomorphically encrypted feature vectors for biometric processing and the Merkle-CRDT mechanism, users will be able to deploy replicas through staking their encrypted biometric data. This approach can potentially lead to the creation of a public permissionless financial system based on consensus between equal human nodes with algorithm-based emission mechanisms targeting real value growth and proportional emission.
Humanode combines different technological stacks to achieve a decentralized, secure, scalable, efficient, consistent, immutable, and sustainable financial system:

- Private biometrics with homomorphically encrypted feature vector floating points that ensure mathematical irreversibility of the embedded template.
- Fully homomorphically encrypted (FHEd) search and matching operations on embedded templates that safeguard the integrity of biometric data in transcendence.
- A Merkle-CRDT mechanism between equal human nodes in a public IPFS cluster.
- Inter-Planetary File System (IPFS) as an environment for working with Merkle-DAGs (Directed Acyclic Graphs).
- IPFS's bitswap, DHT, and pubsub as networking transport, discovery, and data transfer layers.
- Vortex as a DAO governing system.
- Fath as a monetary policy and algorithm targeting real value growth and proportional emission.

All the implemented technologies have nuances that are crucial for the integrity of the network. In this paper we address these details, describing problems that might occur and their possible solutions. The Humanode core acknowledges the power of internal multi-modal biometric processing methods that if implemented properly might tremendously increase resistance against Sybil attacks and overcome the challenges and limitations of modern biometric authentication and identification systems. The main goal of Humanode is to create a stable and just financial system that relies on the existence of human life.

Contents

1 Abstract **1**

2 Introduction **3**

3 Humanode network **4**

4 Humanode's strategic approach **5**
4.1 Humanode's long-term goals and objectives . . . 5
4.2 Solutions for Governments . . . 5
4.3 Shout-out to white hats . . . 5

5 Merkle-CRDT mechanism between equal human nodes, leveraging IPFS **6**
5.1 Merkle-DAGs . . . 6
5.2 Conflict-Free Replicated Data Types (CRDTs) . . . 7
5.3 IPFS Cluster . . . 8
5.4 Merkle Clocks . . . 8
5.5 Merkle-CRDTs . . . 9
5.6 Delta-state CRDTs . . . 11
5.7 Transaction latency . . . 11
5.8 Residual increase in number of replica human nodes . . . 11
5.9 Slashing system . . . 11

6 Fath **13**
6.1 Transaction-based emission algorithm example . . . 15
6.2 Implications of the transaction-based Fath system for a distributed network economy . . . 15

7 Biometric approach to user identification **16**
7.1 Merits and demerits of biometric identification . . . 16
7.2 Humanode's biometric identification methods . . . 16
7.2.1 Emerging biometric modalities . . . 19
7.3 'Biometric Identification Matrix' . . . 20
7.4 'Humanode Biometric Modalities Score' . . . 22
7.5 Types of attacks on biometric systems and their solutions . . . 25

8 Private biometrics **28**
8.1 Private biometrics . . . 28
8.2 Neurosignature . . . 28

9 Humanode's approach to identity attack prevention **31**
9.1 Self-sovereignty . . . 31
9.2 Privacy-preserving . . . 31
9.3 Sybil-resistance . . . 31

10 Human node registration and private authentication scheme **35**
10.1 Private smart contracts . . . 35
10.2 Humanode IPFS cluster . . . 35
10.3 Human node enrollment process . . . 35
10.4 Enrollment, authentication of users, and private biometric key management . . . 37

11 Current inefficiencies of public permissionless networks **39**
11.1 Blockchain technology . . . 39
11.2 Gas prices . . . 39
11.3 Capital-based consensus mechanisms . . . 39

12 Transaction fee economics of the Humanode network **40**
12.1 Transaction acceptance . . . 40
12.2 Flexible guaranteed transaction persistence . . . 40
12.3 Fee-setting and distribution mechanisms in the Humanode protocol . . . 40
12.4 External protocol fees in the Humanode network . . . 41

13 Vortex **42**
13.1 Vortex default characteristics . . . 44
13.2 Veto rights . . . 45
13.3 Proposal system . . . 45
13.4 Formation . . . 45
13.4.1 Assembling a team . . . 48
13.4.2 Slashing . . . 48

14 Strategic roadmap **49**
14.1 2020 . . . 50
14.2 2021 . . . 50
14.3 2022 . . . 50
14.4 2023 . . . 50

15 18 month "Road to Mainnet" **51**
15.1 2020 . . . 51
15.2 2021 . . . 51
15.3 2022 . . . 52

16 Discussion **53**
16.1 Gradual decentralization . . . 53
16.2 The iron law of oligarchy . . . 53
16.3 Vote delegation . . . 54
16.4 Populist tide and professional backslide . . . 55

17 Conclusion **56**

18 References **57**

2 Introduction

From truth = authority to truth=money, how much has changed? In the Humanode protocol, truth=human existence

Increasing attention to decentralized ledger solutions over the recent decade gave rise to a whole class of projects oriented toward the constant technological research in encryption methods and consensus mechanisms. These scientific pursuits have never been exposed to capital in such a direct manner. An abundance of capital has created a massive research wave on a variety of decentralized transaction verification systems. Simultaneously, biometric processing has evolved to a stage where search and matching operations can be carried out in a fully homomorphic way.

Humanode is a network based on private biometrically encrypted nodes (or replicas). Using solutions that provide fully homomorphically encrypted feature vectors for biometric processing and a Merkle-CRDT mechanism, people will be able to deploy replicas to create a public permissionless financial system based on consensus between equal human nodes with a rule-based monetary policy targeting real value growth and proportional emission.

Modern decentralized verification systems rely on a concept of material obligations in case of malicious activity. Proof-of-Work (PoW) blockchain systems blacklist mining equipment, Proof-of-Stake (PoS) slashes tokens. The main focus of these protection mechanisms is to create a system where attacks are unimaginably costly for any hypothetical predator. This reliance rises from problems of distrust on many levels, but most importantly because any trust system requires an instrument for preventing malicious activity. As human nodes are not created through mining farms or monetary obligations in the form of staking, they are not exposed to the same angle of attacks. The Humanode network will prevent malicious activity by blacklisting biometric data, meaning that your biometric identity becomes the stake.

Human nodes are created through encryption of the user's biometric data. Thus, the user's biometric identity becomes the stake that gives access to the creation of a replica that verifies transactions. This approach mitigates the problem of the disproportion of power in decentralized systems such as mining cartels or validator oligopolies. In the Humanode network, only one node derives from one biometric identity. This also means that every node is equal in terms of voting and computation power, while rewards for verification and storage are equally distributed among the human nodes.

As human nodes are not entangled with the token, it allows the implementation of any monetary system without the necessity of conforming with the monetary requirements of a standard consensus mechanism. With human nodes replacing staked assets, it is now possible to avoid a disproportion of newly issued token distributions between those who stake, validate, or simply hold the asset. Humanode will implement the Fath hypothesis as the mechanism for monetary supply adjustment and proportional distribution of emission. The main idea behind the Fath hypothesis is the full-reserve system that calculates the amount of goods and services sold in equal periods of time. If the value created in the new period is greater than the value in the previous one by 1%, the Fath protocol issues 1% of the supply and delivers it to every single wallet in the network, depending on the account balance (savings). If the wallet holds 1% of the supply during the emission, it gets 1% of the minted tokens directly from the protocol.

Any person in the world, no matter where they are from or where they are, can become a human node, as long as that person has access to devices that can conduct biometric processing (such as, for example, a smart phone with biometric processing applications for fingerprints or face recognition) or other verified hardware. The system ensures the privacy and integrity of biometric data through implementation of one-way fully homomorphic Euclidean-measurable feature vectors. It safeguards the private keys that are created based on a biometric feature vector in the private layer that hides the key from any participant of the network. It delivers the equality of every single human node by deriving only one replica from one biometric identity and mitigates any disproportion of power due to reward inequality of individuals. Humanode gives access to decentralized storage and verification of transactions through the implementation of the Merkle-CRDT mechanism, which means that the assets solely belong to the individual who holds them and cannot be frozen or revoked by any third party. Storage of data is carried out on IPFS and distributed among participants so that there is no single point of failure. As the system implements the Fath hypothesis, which negates the effect of devaluation on agents of the system, this narrows the gap between participants of the network as the emitted value is distributed proportionally across every participant.

The main goal of Humanode is to create a stable and just financial system that relies on the existence of human life itself. We aim to alleviate all the intermediaries that stand between a person and his ability to become a validator of transactions. Humanode strives to make node creation easy and natural for any human being, as a key derives from one's biometric data and it is extremely hard to lose. We acknowledge the power of a strong and idea-driven community, and that is why Humanode will be an open-source project. We believe that by joining forces together with passionate minds and hearts throughout the world we will be able to achieve a balanced state of the system that will ensure our economic freedom and stability, and safeguard the future of our children, grandchildren, and many generations to come. The symbiosis of humans and technology is inevitable, and Humanode is just a small but important step in the large transcendence period that we are all going through.

3 Humanode network

The Humanode network is a protocol that can prove one's unique identity through novel authentication schemes and grant permission to launch a node and verify transactions running through a public permissionless network based on human existence.
The core stack of technologies enabling human-node technology include:

- Private biometrics with fully homomorphic encrypted feature vectors, which ensure that the embedded template cannot be mathematically reversed to its original state. They satisfy the requirements of data safety, as they exist in plaintext only for a few seconds at the inception and are deleted immediately afterward. Having multiple biometric types coupled with liveness detection makes it less likely for an adversary to simulate biometric data, as it becomes almost impossible to recreate or steal.
- An IPFS public cluster, which becomes a permissionless public protocol for trusted asset and data transfer maintained by human nodes. It has a cost-based fee model and flexible guaranteed persistence of data.
- A private smart contract on Secret Network for private biometric decentralized key management. The user's root private key is issued in the private smart contract so that nobody can get access to it.
- The Merkle-CRDT mechanism between equal human nodes in a public IPFS cluster to achieve consensus on the current state of the ledger. It provides strong eventual consistency. Using Merkle Clocks, we ensure causality of events and global convergence of data among replicas.
- IPFS as the environment for working with Merkle-DAG;
- IPFS's bitswap, DHT, and pubsub features as networking transport, discovery, and data transfer layers.
- Vortex as the DAO governing system.
- Fath as the monetary policy and algorithm targeting real value growth and proportional emission.

4 Humanode's strategic approach

4.1 Humanode's long-term goals and objectives

- Creation, proliferation, and development of a strong and dedicated community of backers;
- Secure, scalable, efficient, consistent, immutable, and sustainable Merkle-CRDT mechanism;
- Secure biometric processing protocols;
- Multi-modal biometric processing in replica creation;
- Solutions that provide fully homomorphic Euclidean-measurable feature vectors through multi-modal biometric processing;
- Private smart-contract layer solutions;
- Deployment of the Humanode network with working biometrically encrypted nodes;
- Inter-Planetary File System (IPFS) as a storage, networking transport, discovery, and data transfer layer;
- Humanode token (HMND) with Fath monetary system, equal fee distribution, and proportional emission distribution on the Humanode network;
- Vortex, a DAO (Decentralized Autonomous Organization) that regulates the existence of Humanode network through voting;
- A proposal system that pulls trending proposals to vote in Vortex;
- Formation, a system that distributes grants across approved proposers and helps them to assemble a team to develop Humanode solutions;
- A BCI (brain-computer interface) protocol for biometric processing;
- Internal biometric processing protocols in replica creation;
- Biometric avatars;
- Ability to deploy your own tokens on Humanode with different monetary policies and systems;
- Ability to deploy Fath-based monetary systems;
- A judicial system that complies with international, regional, and governmental law systems;
- Free, easy-to-use applications that deliver proper flows in UX/UI;
- Real-time proof of human existence;
- A public Humanode knowledge base that stores all the information, research and analytics carried out by teams assembled in Formation. It will also act as a base in educational sessions and programs carried out in Humanode;
- Humanode development framework with modular solutions.

4.2 Solutions for Governments

The reliance of human beings on governments is undisputed. Governments play a very important role in the lives of most people in the world. We believe that many countries are willing to try and make their financial systems more secure, decentralized, and just. So we are willing to help out any administration or any other form of government that is willing to deploy human-node–based national currencies, backed by citizen human nodes or even a Fath monetary system for fair, direct and proportional distribution of emission and extraction of excessive monetary supply. Fees generated through verification of a user's existence can also become a solution in terms of a universal basic income. Governments that decide to make the experiment and pursue a transcendent solution will get the full support of the international human-node community and the Humanode core will assist those courageous people with research, analytics, and development, if Vortex, the Humanode network decision-making body, approves.

4.3 Shout-out to white hats

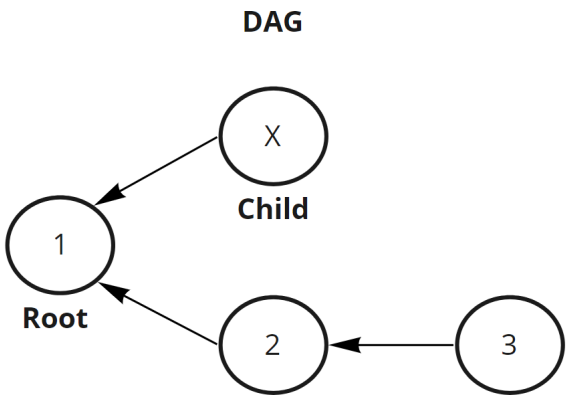
As we are building a system that is based on highly experimental data, we want to ask all the white hats to try and pwn our network hard. The future security of a network is very dependent on the amount of pwnage it has to go through in the early days of its testing and creation. Someone finds an angle of attack, tests it, shares the results with the Humanode community, and makes a proposal to research and develop a solution that mitigates this attack. Then, if this proposal is approved by Vortex the team behind the solution gets a grant with rewards for pwnage included. So please come and test our system's resolve, we will get stronger with each attack!

5 Merkle-CRDT mechanism between equal human nodes, leveraging IPFS

As the Humanode network consists of equal human beings who become equal network peers, we are able to choose a different approach to achieve consensus among peers compared to those dominant now in permissionless blockchains, i.e., Nakamoto, used by PoW networks, and Byzantine Fault Tolerance (BFT), widely adopted by PoS networks. Our choice of consensus is to replace it with a new type of mechanism between equal human nodes inspired by the unique characteristics of Conflict-Free Replicated Data Types (CRDTs), which when merged with Merkle Clocks (H. Sanjuan, S. Poyhtari, P. Teixeira & I. Psaras, 2020) provide the necessary properties for a permissionless distributed network: strong eventual consistency, causality of events, and maintaining availability without choosing a leader and without the necessity for all peers to stay online to maintain the same state of the ledger. Merkle-CRDTs are agnostic to peer discovery data systems. IPFS serves both as an environment for working with Merkle-DAGs and as a networking transport, broadcasting, discovery, and data transfer layer. Merkle-CRDTs work only in environments where the peers are equal, which hinders the adoption of this technology by current blockchain protocols with unequal power distribution. In our protocol, human nodes are equal in their voting and computing power, as they are all human. Terminology in Merkle-CRDTs utilizes the word "node" to describe events that are happening in DAGs and is a separate entity from human nodes, which we address as "replicas" throughout the rest of this paper.

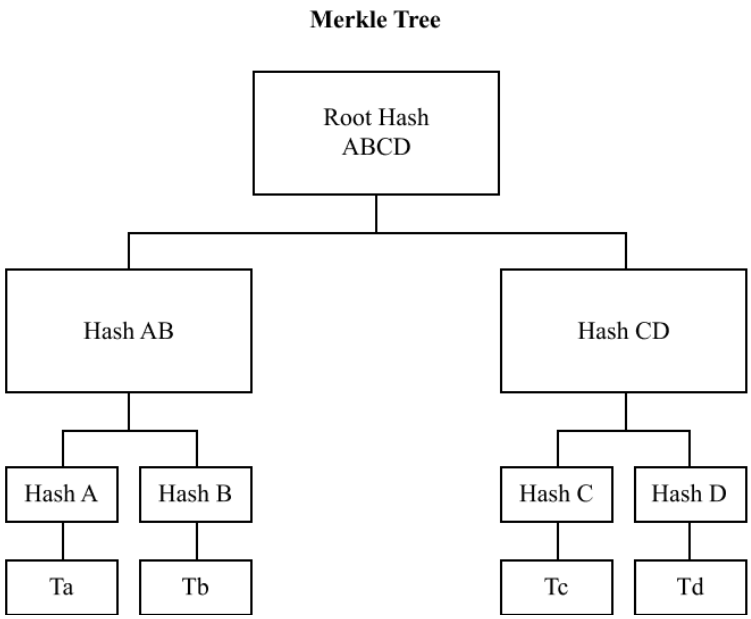
5.1 Merkle-DAGs

Figure 1: Root and child nodes in a Merkle-DAG



Merkle DAGs are distributed authenticated hash-linked data structures.
A *Directed Acyclic Graph (DAG)* is a type of graph where edges have direction and cycles are not allowed. A linked list $1 \rightarrow 2 \rightarrow 3$ may serve as an example of the DAG: list member 1 references 2 while 2 references 3. As 1 has a link to 2, 2 is *a child* of 1. Therefore, we call 1 *a parent to* node 2[1]. Nodes that are not children to any other node in the DAG are called the root nodes. List member 1 cannot reference 3, as this will be considered a cycle.

Figure 2: A Merkle Tree example



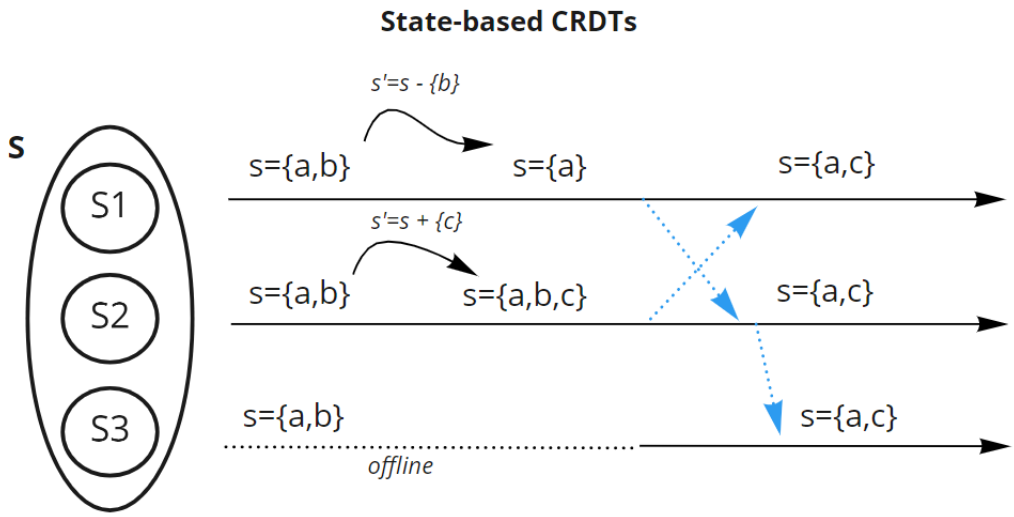
The best example of a *Merkle data structure* is a *Merkle Tree* (R. C. Merkle, 1998). It is used by all existing blockchains, in

[1] In graph theory, nodes are interlinked fundamental units that can represent linked data, unlike in blockchain where physical machines of the network are called nodes

which all the data inputs represent transactions (Ta, Tb, Tc, Td). Then the data is turned into hashes using a cryptographic hash function like SHA256. After this, we combine Hash A and Hash B and hash the result, which gives us Hash AB. Then we do the same with Hashes AB and CD to get the root of the tree—Hash ABCD.
Merkle trees offer huge benefits over hash lists, as they require fewer actions to check the integrity of the data.
A *Merkle-DAG* is a bit different. In a Merkle-DAG, there is a parent Merkle-DAG and local or sub-Merkle DAGs. Parent Merkle-DAG always consists of roots of sub-Merkle-DAGs (child-free nodes). But instead of storing all the nodes, Merkle-DAG interacts and syncs only child-free nodes, e.g., parents. This data structure is similar to a Merkle tree but allows more freedom: Merkle-DAG does not need to be balanced, and its non-leaf nodes are allowed to contain data. The human nodes work as replicas: storing the hashing result of root nodes and comparing them amongst each other. If the hashing result of the root node differs from root nodes of other replicas, then one of the children in this Merkle tree was altered. Humanode protocol will detect such intrusions and slash malicious actors accordingly.
The main idea is that although we might not know the order in which all events happened globally, at least a replica knows the order of events issued by itself. Any other replica that receives this information would be able to know the order of events based on preconditions. Commonly, logical clocks are representations of causal history and provide partial ordering between events. They help to understand whether A happened before B, B before A, or concurrently. The practical implementation of logical clocks usually involves metadata that travels attached to every event in the system.
Information-centric networks (ICN) do direct content-naming, routing, and forwarding based on content names. 'Transport-agnostic' state synchronization via Merkle-CRDT handles state synchronization directly through named network objects and brings standard ICN advantages to Merkle-CRDTs.

5.2 Conflict-Free Replicated Data Types (CRDTs)

Figure 3: Convergence of states in state-based CRDTs



The main challenge for any decentralized ledger technology is to maintain the consistency and integrity of causal information. Causal history is defined as the history of states an object went through, which consists of queries, updates, merges, etc.
Introduced by M. Shapiro, Conflict-Free Replicated Data Types (CRDTs) are data types that guarantee the convergence of data among replicas in spite of any failures, leading to partitioning of replicas in distributed systems (M. Shapiro et al., 2011).
CRDTs are widely deployed in practice among tech giants as a perfect fit for collaborative applications. CRDTs are used by Apple in Notes to sync offline edits and by League of Legends for in-game chat, handling 7.5 million concurrent users and 11,000 messages per second.
CRDTs achieve *strong eventual consistency* (SEC), which means that if two replicas receive the same updates, their state will be the same. This is quite a useful property for a decentralized ledger technology.
Among the advantages of CRDTs are:

- Updates do not require synchronization;
- CRDTs avoid the complexity of conflict resolution and roll-back;
- Conflict-freedom ensures safety and liveness despite any number of network failures;
- Monotonicity—mathematically ensured absence of conflict;
- Replicas provably converge to a correct common state;
- Replicas remain responsive, available, and scalable despite high network latency, faults, or disconnection.

The diagram shows how different replicas S1, S2, S3 change their local state, represented by a simple set, and then disseminate the state (blue lines) to other replicas, eventually converging to the common state among all 3 replicas including one that was offline.

5.3 IPFS Cluster

Merkle-CRDT has been implemented as a pluggable datastore component and integrated as a consensus engine into the IPFS Cluster. The IPFS Cluster provides data orchestration across a swarm of IPFS daemons by allocating, replicating, and tracking a global pinset distributed among multiple peers. Cluster peers form a distributed network and maintain a global, replicated, and conflict-free list of pins.
IPFS utilizes a distributed hash table (DHT) to announce and discover which replicas provide certain Merkle-DAG nodes. It also implements a node-exchange protocol bitswap to retrieve DAG nodes from any provider. At the same time, IPFS is built on top of libp2p, which provides a broadcasting mechanism. With Inter-Planetary Linked Data maintaining content identifier (CID) support for nodes and all the properties mentioned above, IPFS seems to be very suitable for Merkle-DAG. IPFS acts as an asynchronous messaging layer that provides communication between separate replicas run by two main operators: the DAG-syncer and the broadcaster.
As the Humanode protocol is a public cluster, 2/3 of human nodes have to be non-malicious and maintain server availability. While a Sybil attack is still possible, it requires the coordination of 51% of malicious human nodes, unlike the requirement of rented equipment in PoW or token purchase in PoS to attack the network, where a small group of ultra-high-net-worth individuals are able to halt the network or verify a fraudulent transaction. Hence, the security of the network grows with the number of active human nodes and cannot be easily breached by capital attacks.

5.4 Merkle Clocks

A Merkle Clock is a Merkle-DAG where each node represents some kind of event. By merging DAGs between replicas, we build a new DAG. New nodes are added as root nodes, while previous root nodes become their children. It is worth mentioning that a Merkle Clock may have several roots at a given time. A Merkle Clock ensures consistency of causal history by resolving any issues connected to the order of events.
For example, if we have two Merkle Clocks then they will carry out the convergence of data based on the pre-conditions for the particular case. For example, if the roots of two different Merkle Clocks are the same, it means that no action is required as the DAGs are already the same. If there are some differences in nodes, then the system through DAG-syncing will understand the order of events and update all of the replicas accordingly. But if the Merkle Clock would not understand the order of events even after DAG-syncing then it means that neither of the replicas has any data that are linked to one another and Merkle Clock would have to merge both nodes by keeping both DAGs until resolution is eventually reached. Both Merkle Clocks can be fully disjoint or not, depending on whether they share some of their deeper nodes. This makes Merkle-Clocks a convergent, replicated data type.
Merkle Clock DAGs are presented as a growing set of CRDTs and therefore they can converge in multiple replicas.
There are four main steps in replica synchronization through Merkle Clocks:

1. Broadcasting of the content identifier (CID) of the new root to other replicas. The whole Merkle Clock is identified by the CID of its root, and its full DAG can be analyzed from it if there is a need.

2. Replicas make a quick comparison by querying and pulling only those nodes that it does not already have. That is possible due to the immutable nature of Merkle-DAGs.

3. Merkle-DAG nodes can be pulled from any source that wants to provide them, as they are self-verified through their CIDs and immutable to corruption and tempering.

4. The design of the system does not allow duplication. This is why identical nodes are de-duplicated at the end of the process, as there can only be one unique representation for every event.

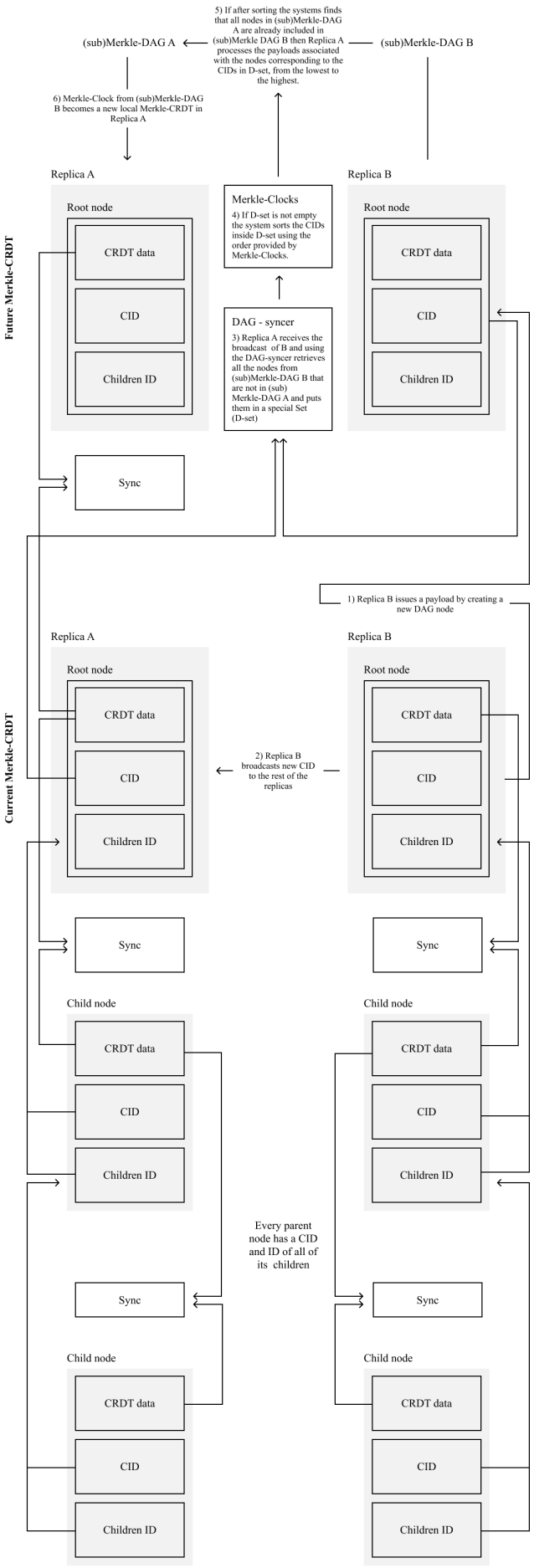
In a Merkle Clock, every replica pulls causal histories from other replicas. A newly born replica with no previous history will fetch the full causal history automatically. A Merkle Clock replaces timestamps and the logical clocks that are usually used as part of CRDTs. By implementing Merkle Clocks, we are able to disconnect the causality of information from the number of replicas, which stands as a limitation in many solutions using logical clocks. By doing so, we can reduce the size of the messages in CRDT implementation and try to solve the problem of keeping up the operation of the clock when replicas randomly join and leave the system.
Merkle Clocks solve many problems of distributed causal history ordering by design. In many systems *dropped messages* might prevent replicas from learning about the existence of new roots, but Merkle Clock DAGs are superseded by new DAGs that download and synchronize all information and missing parts in the *eventual consistency* mechanisms that heal eventually on their own. *Out of order delivery* cannot harm the system for the same reason. *Duplicated nodes* are simply ignored by replicas as they are already incorporated into their Merkle Clocks.
The main problem with Merkle Clocks is that they cannot define which of the events happened first if they have multiple roots, so they would stay in a diverged state until the order is resolved through the logic of causal history in other replicas. To solve this problem we need to address approaches to sorting out concurrent events that would qualify as data-layer conflict resolution. This is where Merkle-CRDTs come in handy.

5.5 Merkle-CRDTs

The *Merkle-CRDT* approach facilitates the use of CRDTs in a P2P environment with a large number of replicas (human nodes) without the need for message delivery guarantees (H. Sanjuan, S. Poyhtari, P. Teixeira, I. Psaras 2020). A Merkle-CRDT is a Merkle Clock whose nodes carry an arbitrary CRDT payload, which qualifies as data-layer conflict resolution. This approach mostly addresses the ambiguity of concurrent events because for the payload to converge properly it must be of the convergent data type.
Replica B issues a payload by creating a new DAG node and broadcasts the new CID to the rest of the replicas in the network. Replica A receives the broadcast of replica B and uses the DAG-syncer to retrieve all the nodes from (sub)Merkle-DAG B that are not in (sub)Merkle-DAG A and stores them in a special D-set. If the D-set is empty then no further actions are required, as it means that both Merkle-DAGs are already the same. If the D-set is not empty then the system sorts the CIDs inside the set provided by Merkle Clocks from both sub-DAGs. After the sorting is done, if the system finds that all nodes in (sub)Merkle-DAG A are included in (sub)Merkle-DAG B and that nodes in D-set come from (sub)Merkle-DAG B then Replica A will process the payloads associated with the nodes corresponding to the CIDs in the D-set from the lowest to the highest and the Merkle Clock from (sub)Merkle-DAG B becomes a new local Merkle-CRDT in Replica A.
CRDTs and Merkle-DAGs complement one another: the former ensures eventual global state convergence without complicated and costly consensus mechanisms; the latter allows the Humanode network to take advantage of the IPFS content-addressing layer for discovery and self-verification of data. By embedding CRDT objects inside Merkle-DAG nodes, we get a convergent system.
A Merkle-CRDT node carries:

- A CID - content identifier;
- An opaque data object with CRDT properties
- A set of children identifiers

Figure 4: Merkle-CRDT mechanism



5.6 Delta-state CRDTs

Delta-state CRDTs solve the problem of propagation and merger of the full state each time the change is made by a replica (human-node). This is done via delta-mutations (P. S. Almeida, A. Shoker, and C. Baquero 2015).
In state-based CRDTs, the entire state is periodically propagated and merged with other replicas. As the local state grows, this approach becomes impractical. Delta state–based CRDTs disseminate only recent changes to the state instead of the whole state incurred in its local state. Using Delta-CRDTs increases memory and computation efficiency, maintaining mathematically verified strong eventual consistency (T.Blau, 2020).

5.7 Transaction latency

Latency is measured between a point in time when a transaction has been gossiped into the network and the point when it is processed and accepted by consensus. The standard transaction confirmation means that a quorum of 2/3 nodes among validators has reached a consensus. Due to the 1-confirmation finality rule, the transaction is considered final immediately.

5.8 Residual increase in number of replica human nodes

As Merkle-CRDT is an emerging technology that has never been implemented as an algorithm for data convergence in a public permissionless cluster on IPFS, the number of nodes will be first restricted to thousands, potentially scaling to millions depending on the public Merkle-CRDT cluster research and development.
The limitation will be set following Vortex voting. When the limitation of human nodes is still low, it remains possible to attack the system by coordination among more than 51% of active human nodes. In order to lower the number of malicious human nodes that verify transactions in the early days of the protocol, we impose additional selection criteria on candidate human nodes based on Proof-of-Time and Proof-of-Devotion. Those with a higher tier or longer governing history are going to be the first candidates to enter the Humanode public cluster on the mainnet as replicas.

5.9 Slashing system

Any verification system requires executive tools that safeguard consistency, immutability, and governing mechanisms of the network. The fiat credit-cycle utilizes law-enforcement and jails, PoW blacklists mining equipment, PoS slashes staked cryptoassets, and Humanode slashes your biometric identity by blacklisting your hashes for a period of time. As you might already know, biometric hash derives from multi-modal biometric processing. That hash cannot be reverted mathematically. If a malicious actor tries to harm the network in any way, the system will blacklist his hash, thus indirectly blacklisting his biometrics. After being slashed the perpetrator will remain blacklisted for a determined time period and will not be able to sign any transactions in the Humanode network. That period is defined by the severity of the malicious act itself. Any changes to severity levels of perpetrations and blacklisting periods are defined through Vortex. Proposal rights to change any slashing conditions are given to governors upon reaching the legate tier.
Some preparations have blacklist-period scaling mechanisms. Blacklist periods start with the base parameters stated in the table below and then can only scale upwards. Scaling has steps pre-determined by Vortex: 0.5 months (the basic one), 1 month, 2 months, 3 months, 6 months, 1 year, 2 years, 3 years, 10 years, 20 years, forever.

Table 1: Slashing severity levels and types.

Perpetration	Severity level	Blacklisting period, months	Additional consequence	Blacklist period scaling
Did not verify existence once in a quarter	0	0.5	Human node is excluded from public IPFS cluster and stops receiving fees from the protocol	No
Made a proposal where the meaning of propositions does not match the proposal type	1	1	None	No
Failed to deliver upon an agreed formation proposal in time	2	1	None	Yes
Replica remained offline for more than 48 hours	2	0.5	Human node is deactivated and stops receiving fees from the protocol	Yes

Made a proposal where the meaning of propositions did not match the proposal type and the governor himself did not have the right to propose that type because of the tier level	3	1	Human node is deactivated and stops receiving fees from the protocol	Yes
Replica overall uptime less than 91%	3	1	None	Yes
Tried to push in a false transaction	5	120	Human node is deactivated and stops receiving fees. Governing time and proof of dedication nullified.	Yes

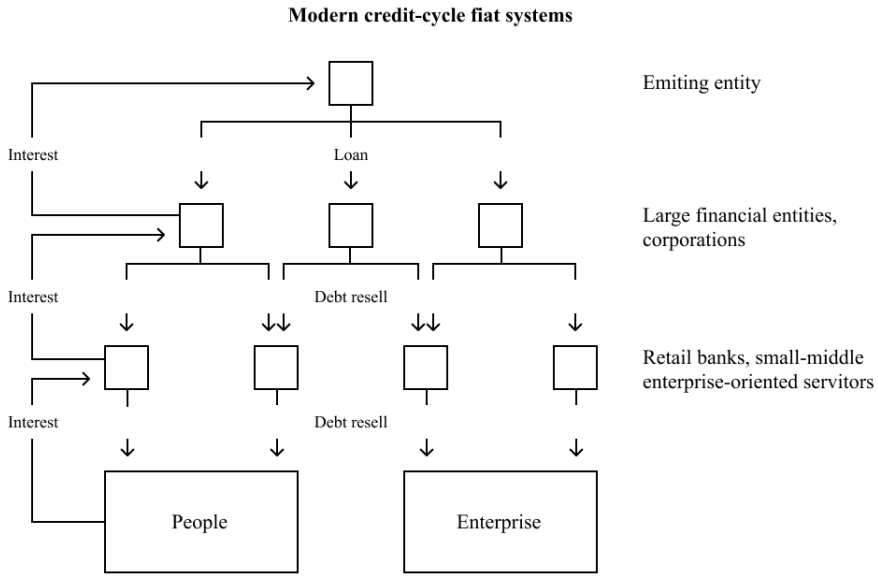
Trying to push false transactions in the Merkle-CRDT system might come in two ways:

1. If the message broadcasting a new root is corrupted, then it will be a hash corresponding to a non-existent DAG that cannot be fetched by the DAG-syncer and will eventually be ignored, and its source slashed.
2. If a DAG node is corrupted on download, the DAG-syncer component (or the application) can discard it if its CID does not match the downloaded content.

6 Fath

Humanode dismantles the involvement of token in the consensus mechanism, meaning that different monetary systems can be implemented on top of the Humanode network without the necessity to conform with the requirements of token-entangled protocols. Humanode will implement the Fath hypothesis as the basis for the circulation of HMND (Humanode Token).

Figure 5: Issuance in modern credit-cycle fiat systems

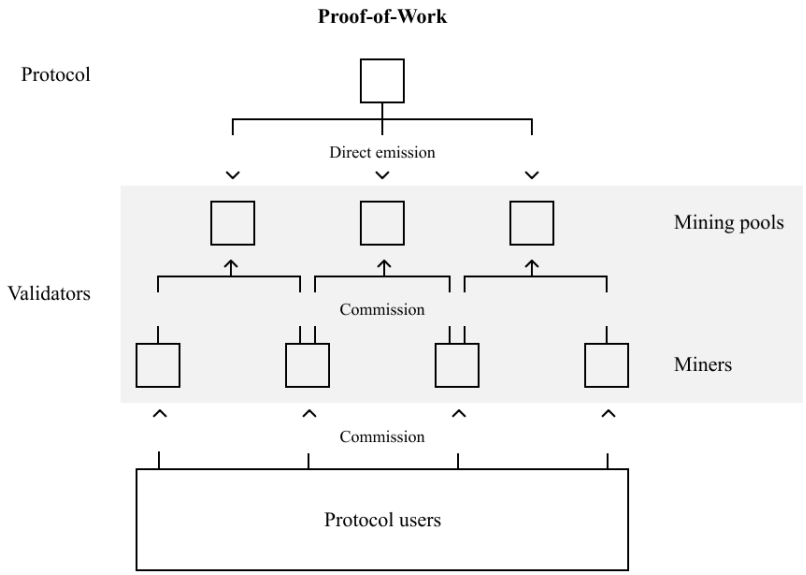


Fath is a monetary system with a proportional distribution of money issued. The amount of issuance is determined by the amount of additional value created in the monetary system—the economic output of goods and services sold. The distribution of money issued happens proportionally based on the currency savings of each holder. When the output of the economic system around Fath currency rises by 1%, 1% of the monetary base is issued. As a result, every wallet gets 1% of the currency on top of their holdings.

The idea behind Fath is to create a monetary system where emission is distributed proportionally, in contrast to how modern fiat credit-cycle financial systems and capital-based public blockchain networks operate.

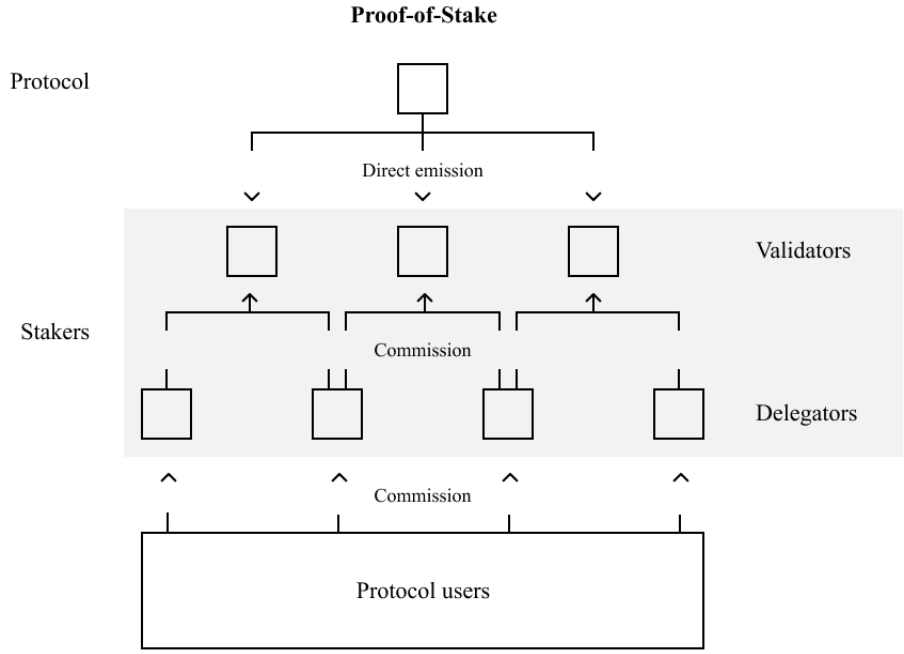
With the global conversion to fiat and decimalization that overwhelmed most countries in the early 1970s, world leaders decided to transcend us all to a system into which emission is injected as a form of debt. Afterward, it is passed down the system in the form of loans. Even if we leave out the fact that some of that issuance forever resides on one of the upper levels because of corruption and fraud, people, enterprise and retail banks are the ones who are constantly cornered because they are the ones paying for that emission and the only ones they can resell their debt to is each other. If for some reason one of the large financial organizations fails to accumulate enough money to cover its expenses and interest then in most cases the emitting entity prints a relief package to save it. If ordinary people or enterprises fail likewise, in most cases they are fined, thrown onto the street by law enforcement, go bankrupt, or go to jail. Consider the fact that every time the emitting entity prints money it increases the money supply and devalues the currency, meaning that agents at the bottom of the emission pyramid not only get devalued with each coin printed, they also pay for it to happen.

Figure 6: Issuance and commission in Proof-of-Work blockchains



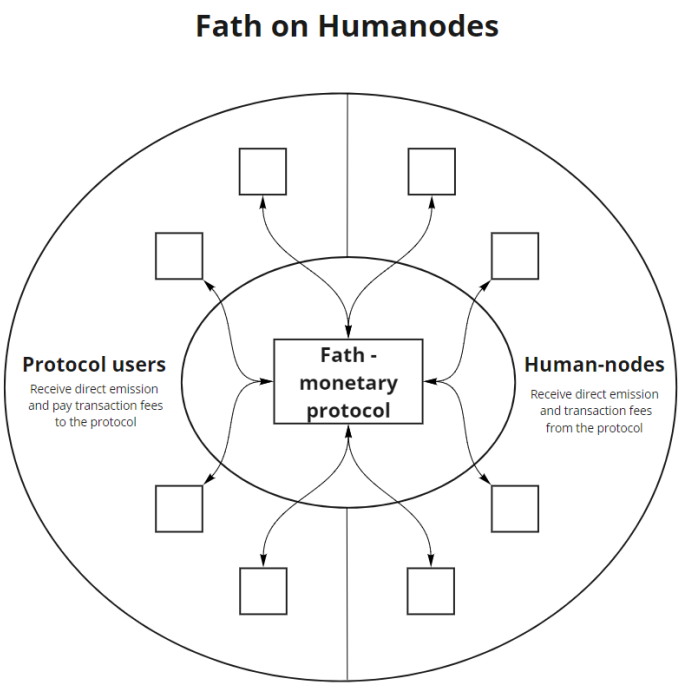
In Proof-of-Work blockchains, the protocol acts as the emitting entity. Most PoW coins have set the emission and max supply, for example, Bitcoin has a max supply of 21 million coins. At the time of the creation of this paper its circulating supply is 18.5 million. With emission set in every block and halving that happens every four years, it will take approximately 120 years to mint everything. Emission is received by miners not in a form of a loan, but directly. However, only miners receive it. Ordinary users and even financial entities that hold large chunks of bitcoin get nothing. Miners either decide to hold onto the emitted money or sell it on the market. This system does not sell debt to the agents at its bottom, but devaluation of non-miner agents' assets, even if very small, still happens, as the emission is received only by miners. Another thing is that supply is not balanced with value creation, meaning that the limited supply is not lining up to the growth of value in the system. That makes it deflationary, which on a nation-sized scale makes economies unhealthy and can even lead to a crisis.

Figure 7: Issuance and commission in Proof-of-Stake blockchains



As in Proof-of-Work, in Proof-of-Stake the protocol acts as the issuance entity. In most cases, PoS have some kind of governing entity that decides upon emission; it can be either pre-set as in Bitcoin or it can be flexible with many different methods of realization. Commonly there is a DAO that sets the emission. As in Proof-of-Work, validators receive issuance directly from the protocol, but in delegated PoS, they also redistribute it across their delegators. Protocol users get nothing from emission and DAO can set emission at any level. Sometimes devaluation is very strong because validators accumulate minted tokens and sell them on the market to cover expenses and for profit—at the same time their networks are not as big as Bitcoin to counterweight the devaluation effect.

Figure 8: Issuance and commission in Fath



The emission of tokens in Fath happens differently from the systems mentioned above. One of the hypotheses that lies as the basis of Fath is that it is possible to mitigate the long-term effects of devaluation by the proportional distribution of emission. Emission is delivered to every single member of the network directly from the protocol, regardless of whether a person is a validator or not.
The amount of emission is defined by the Fath protocol algorithm, which calculates the difference between real value creation (rVC) in two different time periods. If rVC in the second period is different from rVC in the first then the algorithm calculates the percentage difference and changes the monetary supply by the same percentage.
We consider the HMND token first of all to be a transaction-processing network, which is why rVC in the first implementation of Fath will be calculated based on the transaction fees spent by participants of the network. If the amount of commission received by human nodes in the second period is different from the first then the algorithm applies the same difference in percentage to supply and rebalances every single wallet that exists.
There are two types of rebalances that occur: inFath and outFath. If the amount of commission paid out in the second period of time exceeds the commission paid out in the first period, then inFath occurs and emission is distributed across every wallet proportionally. If the amount of commission paid out in the second period is smaller than in the first then outFath occurs and protocol proportionally burns excessive supply throughout every single wallet as well.

6.1 Transaction-based emission algorithm example

End of Year 0
Supply: 10,000,000 HMND
Commission paid out: 1,000,000 HMND
Your wallet: 1000 HMND
End of Year 1
Supply: 10,000,000 HMND
Commission paid out: 2,000,000 HMND
As commission paid out in Year 1 exceeds the same quantity in Year 0 by 100%, inFath occurs. A total of 100% of the supply is minted and given out to everyone proportionally to ledger balances.
New supply: 20,000,000 HMND
Your wallet: 2000 HMND
End of Year 2
Supply: 20,000,000 HMND
Commission paid out: 1,500,000 HMND
As commission paid out in Year 2 is smaller than in Year 1 by 25%, outFath occurs. A total of 25% of the monetary supply is minted and rebased proportionally to balances.
New supply: 15,000,000 HMND
Your wallet: 1500 HMND
Such a rebalance mechanism tries to:

- mitigate the long-term effect of devaluation due to disproportional emission and
- negate macroeconomic shocks and structural inefficiencies that occur due to the monetary supply not satisfying the needs of the growing or shrinking rVC[2]. If you are interested in Fath hypotheses that are based on data from monetary systems from the 3rd century BC, you can read more about it here.

6.2 Implications of the transaction-based Fath system for a distributed network economy

If the total fees (TF) in the Humanode network in the terms of the dominant currency stay the same, the price change of the HMND token will be followed by changing the price of the transaction in HMND according to the formula stated in *Fee-setting and distribution mechanism in the Humanode network*.
As we found out, the fee paid in HMND changes proportionally in the direction opposite to the price change. The token issuance is tied to the change in total fees in HMND. If the change of size and complexity of the transactions in the Humanode protocol is greater than the asset price change, the protocol will launch inFath. The change in the amount and complexity of transactions should reflect the price change for the protocol to initiate inFath at the end of the period.
However, over time, the network and its token obtain new use-cases other than trust in processing valuable data. That is when we need to account for value creation in the network and derive a value that was created in the system, other than transaction processing. When the system obtains new properties, new Fath modules, except for the transactional module, should be launched to account for new values created and to change the algorithm accordingly. In the end, Fath is supposed to have modules that combined are capable of self-accounting for as many transaction types as the calculation of GDP involves.

[2] Due to monetary supply divergence from rVC changes

7 Biometric approach to user identification

Rapid development in IT, DLT, and AI are prompting biometrics to constantly innovate and make the most of market demand. According to a report from Global Industry Analysts, the global biometrics market is forecast to reach $82.8 billion by 2027, growing at a 19.3% CAGR from an estimated $24.1 billion in 2020. In terms of authentication type, voice recognition is supposed to witness significant growth due to consumer desires for a safer identity mechanism. Facial recognition is also poised for growth, as it is witnessing a boost from the launch of Apple's Face ID system.
In 2020, the global market for mobile biometrics was estimated at $18 billion, and it is projected to reach a revised size of $79.8 billion by 2027, growing at a CAGR of 23.7% over the analysis period 2020–2027. Growth in the scanner segment is readjusted to a revised 20.1% CAGR for the next seven-year period. Fingerprint reader technology is projected to record a 25.5% CAGR and reach $48.6 billion by the end of the period.

7.1 Merits and demerits of biometric identification

The use of biometrics, the science of analyzing physical or behavioral characteristics unique to each individual to recognize their identity, has many benefits. However, there are some risks associated with biometric authentication, which are as follows.

Table 2: Merits and demerits of biometric identification

Merits	Demerits
• *High levelof security and accuracy* in contrast to passwords, as biometric data cannot beforgotten or exchanged. • *Simplicityand convenience for the user* is a significant factor in the growing popularity of biometric authentication. • *Higher levelof authenticity* for users prone to weak passwords that may be commonto multiple users or easily shared. • *Affordability*, asbiometric authentication is now possible in a wide range of common devices. • *Flexibility*, as usershave their own security credentials with them so they do not need to bothermemorizing a complex password. • *Biometricsis trustable*, as reports from 2020 claim that the youngergenerations trust biometric solutions more than others. Biometric solutions are *time conserving*.	• *Requiresintegration and/or additional hardware.* • *Higher errorrate,* asenvironment and usage can affect measurements. • *Bias andinaccuracy,* as even the best of recognition systems are not 100% accurate. • *Physicaltraits are not changeable,* as most of the biometric modalities work withphysical traits (fingerprint, iris, palm veins, etc.), which cannot be reset once compromised. • *The cost* of biometricdevices is comparatively higher than traditional ones. • *Delay,* as somebiometric recognition methods may take more than the accepted time. *Physicaldisability,* as some people are not fortunate enough to be able to participate in the enrollment process.

7.2 Humanode's biometric identification methods

The 'Biometric Identification Matrix' was created by the Humanode core to understand which of the existing biometric types are the most suitable and superior and, therefore, to choose the proper ones for Humanode biometric processing methods. According to recent studies, *there are three types of biometric measurements* (G. Kaur et al., 2014):

- Physiological measurement includes face recognition, finger or palm prints, hand geometry, vein pattern, eye (iris and retina), ear shape, DNA, etc.
- Behavioral measurement relating to human behavior that can vary over time and includes keystroke pattern, signature, and gait (S. Jaiswal et al., 2011).
- There are also some biometric traits that act as both physiological and behavioral characteristics (e.g., brain waves or electroencephalography (EEG)). EEG depends on the head or skull shape and size, but it changes from time to time depending on circumstances and varies according to age.

In light of the latest developments, we propose a fourth measurement—*neurological*—as a part of both physiological (internal) and behavioral measurements. We believe that neurosignature, the technology of reading a human's state of mind, i.e., signals that trigger a unique and distinct pattern of nerve cell firing and chemical release that can be activated by appropriate stimuli, should be developed and implemented in the Humanode as the most reliable and secure way of biometric processing. Until then, Humanode implements a multimodal biometric system of several biometric modalities. Each biometric modality has its own merits and demerits. It is laborious to make a direct comparison. Since the end of the 1990s, when A. K. Jain, R. M. Bolle, and S. Pankanti conducted their comprehensive research on all existing biometrics (Jain et al., 1999), seven significant factors were identified to study and compare the biometric types: acceptability, universality, uniqueness (distinctiveness), permanence, collectability, performance, and resistance to circumvention—which are also known as *'the seven pillars of biometrics'* (K. A. Jain, A. Ross & S. Prabhakar 2004).
Based on Jain et al.'s classification and recent all-encompassing surveys on various biometric systems (A. C. Weaver 2006; T. Sabhanayagam, V. Prasanna Venkatesan & K. Senthamaraikannan, 2018), cancelable systems (B. Choudhury, P. Then, B. Issac & V. Raman, 2018), and unimodal, multimodal biometrics and fusion techniques (A.S. Raju & V. Udayashankara, 2018), we provide a comparison study of different biometric modalities, and propose a 'Biometric Identification Matrix', by studying and combining characteristics revealed in the aforementioned works and by adding factors we found necessary to examine. Thus, we divided the 'Performance' category proposed by Jain et al., which relates to the accuracy, speed, and robustness of technology used, into two sub-categories ('Accuracy' and 'Processing Speed') to study the space in more detail. Thereby, as the performance of any biometric authentication techniques are measured by the various parameters, we chose to add the 'Crossover Error Rate (CER)' subcategory, also known as the Equal Error Rate (EER), used to summarize the operating characteristics of a biometric system (L. Taylor & M. Shepherd, 2007). The category 'Hardware' which relates to the type of hardware, its prevalence, and cost, was added to understand which devices are required to be used nowadays and which are best to use in the network.

- **Acceptability**
  'Acceptability' relates to the relevant population's willingness to use a certain modality of biometric, their acceptance of the technology, and their readiness to have their biometrics trait captured and assessed.
  Fingerprints are the oldest and still the most advanced and popular way of biometric authentication. The majority of smartphones feature an in-display fingerprint ID. Facial recognition technology is not far behind, as it is one of the easiest and favored ways of recognizing individuals. It gets dynamic and constant improvement, and it is totally non-intrusive, i.e., involves no physical contact. However, most people are still uncomfortable using it because of privacy abuse. Behavioral modalities such as signature, lip motion, and voice recognition are traditionally highly accepted without any substantial objection as well.
  Complex and intrusive technologies have low levels of public acceptance. Retina recognition is not socially acceptable, as it is not a very user-friendly method because of the highly intrusive property authentication process using retina scanning (J. Mazumdar, 2018). Electrophysiological methods (EEG, ECG) and neurosignatures are not highly accepted nowadays, as they are intricate and not yet well-known or fully developed.

- **Collectability**
  'Collectability' refers to the ease of data capturing, measuring, and processing, reflecting how easy this biometric modality is for both the user and the personnel involved.
  Fingerprint and hand geometry recognition techniques are very easy to use. Their template sizes are small and so matching is fast (S. Jaiswal et al., 2011). Similarly, the advantage of face biometrics is that it is contactless and the acquisition process is simple. With the achievements and spread of modern technology, ear shape and iris scanners can be deceived by high-quality images.
  The advantage of all behavioral recognition methods is the ease of acquisition as well.

- **Permanence**
  'Permanence' relates to long-term stability—how a modality varies over time. More specifically, a modality with 'high' permanence will be invariant over time with respect to the specific matching algorithm.
  Physiological measurements tend to be permanent, while behavioral measurements are usually not long-term stable. Such modalities have a low or medium level of permanence.
  The same person can sign in different ways, as it is affected by physical conditions and feelings. Voice is not constant, as it may change based on an individual's emotion, sickness, or age (L. Rabiner & B.-H. Juang, 1993).
  Facial traits are persistent, but may change and vary over time, although heat generated by the facial tissues has a measurable repeatable pattern. It can be more stable than the facial structure (Hanmandlu et al. 2012). Finger and palm prints and vein patterns tend to remain constant. Hand geometry is more likely to be affected by diseases, weight loss/gain, injury. However, the results of hand geometry recognition are not as much affected by skin moisture or texture changes depending on age. Ear size changes over time (S. Jaiswal et al., 2011; Abaza et al. 2013). DNA is highly permanent. Iris remains the same throughout life (G. Kaur et al., 2014; Bowyer et al. 2008). However, diabetes and some other serious diseases cause alterations in it. Likewise, the stable retina pattern changes during medical conditions like pregnancy, blood pressure, other ailments, etc.(G. Kaur et al., 2014).

- **Universality**
  'Universality' means that every person using a system may have the modality.
  Different biometric systems have their own limitations, likewise the modalities. For example, some people have damaged or eliminated fingerprints, hand geometry is efficient only for adults, etc. Biological/chemical, electrophysiological, and neurological (in theory) biometrics measurement categories should have the highest level of universality.

- **Uniqueness**
  'Uniqueness' relates to characteristics that should be sufficiently different for individuals such that they can be distinguished from one another.
  Every person has a unique walking style as well as writing style and hence a person has his own gate and signature. Voice recognition technology identifies the distinct vocal characteristic of the individual. Even so, human behavior is not as unique as physiological patterns.
  Finger and palm prints are extremely distinctive. The blood vessels underneath the skin are also unique from person to person. The iris is highly unique and rich in texture. Moreover, the texture of both eyes are different from each other. Each person has a unique body odor and such chemical agents of human body odor can be extracted from the pores to recognize a person (M. Shu et al. 2014). People display a distinct 'brain signature' when they are processing information, similar to fingerprints. At one time, neuroscientists thought brain activity was pretty much the same from one person to another (E. Finn et al., 2015,https://doi.org/10.1038/s41593-019-0487-z; A. Demertzi et al., 2019).
  Nevertheless, even physical modalities have limitations. Thus, faces seem to be unique, however, in the case of twins, distinctiveness is not guaranteed. DNA itself is unique for each individual, except identical twins, therefore, it achieves high accuracy. However, retina recognition is highly reliable, since no two people have the same retinal pattern and even identical twins have distinct patterns We assume that neurosignature is to be one of the premier biometric technologies on grounds of the unique nature of human thoughts, memories, and other mental conditions.

- **Accuracy**
  'Accuracy' is a part of the 'Performance' category. It describes how well a biometric can tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results.
  Facial recognition may give inaccurate results, as facial features tend to change over time due to age, expression, recording devices, and other external factors. It is highly dependent on lighting for correct input. Thermograms, which are easy to obtain and process, are invariant to illumination and work more accurately even in dim light, are far better.
  Palm prints show a higher level of accuracy than fingerprints. Considering the number of minutiae points of all five fingers, the palm print has more minutiae points to help make comparisons during the matching process compared to fingerprints alone (A. Kong et al. 2009).
  The iris provides a high degree of accuracy (iris patterns match for 1 in 10 billion people; (J. Daugman, 2004), but still can be affected by wearing glasses or contact lenses. Similarly, retina recognition is a highly accurate technology, however, diseases such as cataracts, glaucoma, diabetes, etc. may affect the results.

- **Processing Speed**
  'Processing Speed' is a part of the 'Performance' category. It is related to the time it takes a biometric technology to identify an individual.
  As different modalities have different computation requirements, the processing power of the systems used varies. Fingerprints and face recognition are still the fastest in the identification process. The time used by vein recognition systems is also very impressive and reliable, in terms of the comparison of the recorded database to that of the current data. Currently, the time which is taken to verify each individual is shorter than other methods (average is 1/2 second; P. O'Neill, 2011). Iris recognition has a small template size so promising processing speed (2 to 5 seconds), as well as retina recognition with a little verification time. Ear shape recognition techniques demonstrate faster identification results, thanks to reduced processing time. The more complicated the procedure, the longer it takes. Behavioral modality identification is fast in processing. Signature, voice, lip motion recognition takes a few seconds. The EEG and ECG processes differ. Acquisition of a DNA sample also requires a long procedure to return results (S. Bhable et al., 2015).

- **Circumvention**
  'Circumvention' relates to an act of cheating; thus, the identifying characteristic used must be hard to deceive and imitate using an artifact or substitute.
  Nearly every modality may become an easy subject for forgers. Signatures can be effortlessly forged by professional forgers; voices can be simply spoofed. Fingerprints are easily deceived through artificial fingers made of wax, gelatin, or clay. Iris-based systems can be attacked with fake irises printed on paper or wearable plastic lenses, while face-based systems can be fooled with sophisticated 3D masks (A. Babu & V. Paul, 2016). Even vein patterns can be imitated by developing a hand substitute.
  DNA is believed to be the most difficult characteristic to dupe, as the DNA of each person is unique and it is impossible to replicate (Maestre, 2009). Brain activity and heartbeat patterns are also hard to emulate.

- **Hardware**
  'Hardware' category refers to the type and cost of hardware required to use the type of biometric.
  Nowadays, there is no need for extra new devices if you have a smartphone for the biometric recognition. Fingerprint

ID is a common feature of smartphones. For facial and lip motion recognition existing image capturing devices, i.e., cameras, can be used. Thermograms need specialized sensor cameras. Voice recognition is also easy to implement on smartphones or any audio device. Hand vein recognition has a low cost in terms of installation and equipment. Nowadays, mobile apps for vascular biometric recognition are integrated using the palm vein modality (R. Garcia-Martin & R. Sanchez-Reillo, 2020). For eye vein ID, smartphones are currently in development, while retina recognition is still an expensive technology, i.e., a high equipment cost. Keystrokes need no special hardware or new sensors, and low-cost identification is fast and secure. Image-based smartphone application prototypes for ear biometrics are in development (S. Bargal & A. Welles, 2015; A. F. Abate, M. Nappi & S. Ricciardi, 2016), as well as mobile apps with digital signatures(E. Rahmawati, M. Listyasari, A. S. Aziz & S. Sukaridhoto, 2017).
In the meantime, electroencephalograms are needed for EEG, and electrocardiograms for ECG. Brain-computer interfaces (BCI) are needed for neurosignature. Special expensive equipment and hardware are needed for DNA matching procedures.

- **Crossover Error Rate (CER)**
  'Crossover Error Rate (CER)' describes the overall accuracy of a biometric system.
  Biometric systems have parameters that can be tuned to adjust the False Acceptance Rate (FAR) - the proportion of times a system grants access to an unauthorized person, and False Rejection Rate (FRR) - the proportion of times a biometric system fails to grant access to an authorized person. Adjust these to the point where the FAR and FRR are equal. When the two are equal, their common value is the CER or EER (Equal Error Rate). The CER gives a way to compare systems. The smaller the CER the better. Still, different approaches to measure have their pros and cons, and each technique differs in error rates (A.S. Raju & V. Udayashankara, 2018; I. Traore, M. Alshahrani & M. S. Obaidat, 2018;R.S. Choras, 2019).

7.2.1 Emerging biometric modalities

- **Neurosignature**

We assume that a combination of the aforementioned biometrics methods (and even multimodal biometrics) is not one hundred percent safe/secure. In the future, we plan to expand the system with this multimodal scheme, making neurosignature one of the main methods of Humanode user identification/verification.
Other emerging modalities to research and to possibly implement in Humanode's verification system are as follows (Goudelis et al. 2009):

- Smile recognition
- Thermal palm recognition
- Hand/finger knuckle
- Magnetic fingerprints/smart magnet
- Nail ID
- Eye movement
- Skin spectroscopy
- Body salinity
- Otoacoustic emission recognition (OAE)
- Mouse dynamics
- Palate
- Dental biometrics
- Cognitive biometrics

7.3 'Biometric Identification Matrix'

Table 3: 'Biometric Identification Matrix': Biometrics Techniques Comparison

		Characteristics/Factors (L- Low, M- Medium, H-High)									
Measurement	**Biometric Modality**	Acceptability	Collectability	Permanence	Universality	Uniqueness	Accuracy	Processing Speed	Circumvention	Hardware	CER
External Physiological	Facial Recognition	H	H	M	H	M	M	H	H	H	1.8%
	Facial Thermography Recognition	H	H	M	H	H	M	H	L	L	no data
	Fingerprint	H	M	H	M	H	H	H	M	H	2%
	Palm Print / Footprint Recognition	M	M	H	M	H	H	H	M	M	0–0.5 %
	Finger/Hand Geometry Recognition	M	H	L	H	M	M	H	M	L	1%
	Finger/ Hand Vein Recognition	M	M	M	M	M	H	H	L	L	0.15 –1.74%
	Iris Recognition	M	H	H	H	H	H	M	L	M	0.01%
	Retina Recognition	L	M	H	H	H	H	M	L	L	0.8%
	Eye Vein Recognition	L	L	H	H	H	H	M	L	M	no data
	Ear - Shape	H	M	H	M	M	M	M	M	M	4%
	Body Odor	M	L	H	H	H	L	M	L	L	no data
	DNA Matching	L	L	H	H	H	H	L	L	L	–
Physiological + Behavioral	Brain Activity (EEG)	L	L	M	H	H	H	L	L	L	3%
	Electrocardiography (ECG)	L	L	M	H	M	H	L	L	L	0.92 –9.01%
Internal Physiological + Behavioral	Neurosig -nature	L	L	H	H	H	H	H	L	L	–
Behaviometrics	Gait	M	H	M	M	M	L	M	M	L	no data
	Keystroke Dynamics	H	H	L	L	L	L	M	M	M	1.8%
	Lip Motion Recognition	H	H	M	H	L	L	H	H	H	1.65–16.5%
	Signature Recognition	H	H	L	L	L	M	H	H	M	4.2 –4.8%
	Voice Recognition	H	H	L	M	L	L	H	H	H	0, 96–6%

In the above table 3, we presented CER (Crossover Error Rate) data on the most advanced biometrics techniques. However, for Humanode, the CER coefficient is not as much important, as nowadays different techniques exist, the newest of which have not yet been fully investigated. The error rate for the modern and more advanced techniques may be lower than that previously measured for older ones.
The different biometrics techniques are discussed. The advantages and disadvantages associated with each of them are listed in Table 4.

Table 4: 'Biometric Identification Matrix': Biometrics Techniques Pros and Cons.

Measurement	**Biometric Modality**	**Pros**	**Cons**
External Physiological	Facial Recognition	non-intrusive, fast, easy to set up, no additional hardware needed	face recognition systems are vulnerable to manipulation and imposter attacks, errors: lighting, age, glasses, hair
	Facial Thermography Recognition	non-intrusive, non-invasive, more stable than the facial structure, does not depend on external illumination	illnesses, high cost of implementation, more expensive
	Fingerprint	inexpensive, socially acceptable, easy to set up and easy to collect, ability to enroll multiple fingers	easily deceived through artificial finger made of wax, cuts, scars, or absence of finger can produce obstacle for the recognition process
	Palm Print / Footprint Recognition	has more minutiae points to make comparisons during the matching process compared to fingerprint, does not pose high-security threats	injuries, dryness, dirt, age, not suitable for high-security apps
	Finger/Hand Geometry Recognition	easy to use, simple and fast, can withstand harsh environmental conditions, not affected by surface condition of the skin	requires training for the users, needs a large space or sensor to acquire the hand geometry, and not distinctive enough to distinguish over a large database, errors: diseases, weight loss/gain, injury, age
	Finger/ Hand Vein Recognition	the vein patterns tend to remain constant over a long period of time	visibility depends on the factors like age, mole, physical activity, thickness of the skin, etc.
	Iris Recognition	iris remains stable for years, well protected from damage, possible from a distance	can be affected by age and eye diseases that deteriorate transparency of cornea, errors: reflection, poor lighting, eyelids, eyelashes, contact lenses, glasses, etc.
	Retina Recognition	one of the most secure and extremely accurate methods	expensive, special equipment is required, highly invasive, not socially acceptable, the pattern changes during medical conditions like pregnancy, blood pressure, other ailments, etc.
	Eye Vein Recognition	long-term stability, the technology works even with glasses or contact lenses	quality of image is affected by numerous factors such as body temperature and heat
	Ear - Shape	can use with existing cameras and image capture devices, does not require close proximity	errors in recognition as the images are not ideal, unclear recognition due to the effect of hair, hats, and earrings, not believed to be very distinctive
	Body Odor	identification is possible by a mixture of characteristic odors and recognizing the mixture's components	artificial noses are not comfortable, distinctiveness is reduced by deodorants and perfume

Table 4: 'Biometric Identification Matrix': Biometrics Techniques Pros and Cons.

	DNA Matching	provides high accuracy, does not suffer from system performance issues	complex method, requiring a physical sample which has to be stored with appropriate environmental conditions
Physiological + Behavioral	Brain Activity (EEG)	high security and accuracy	time-consuming and expensive process, brain signals for the specific task might change during different circumstances and a person can change his/her own brainwave pattern
	Electrocardiography (ECG)	high security and accuracy	time-consuming and complex process
Internal Physiological + Behavioral	Neurosignature	the most secure type, easy to use one's mental state, conscious state, or simply motor signals from the cortex	highly intrusive, no technology yet
Behaviometrics	Gait	unobtrusive method, easy to set up, video footage from existing surveillance cameras can be used	injuries, low reliability of results, computationally expensive since it requires more computations
	Keystroke Dynamics	works in the background, needs no special hardware, low cost	hand injury, tiredness, gap in days, change of keyboard etc. can change the typing rhythm
	Lip Motion Recognition	fixes shortcomings associated with classic biometric methods, easy to set up, interaction of a user is not necessary and can be used without the knowledge of user	still in its infancy, the relevant information may not be acquired from the specific facial attributes
	Signature Recognition	wide acceptance in public, non-invasive in nature, easy to restore the template if it is stolen	changing or evolving signatures, excludes people who are illiterate and people who are not able to write their signature
	Voice Recognition	reliable and easy to use	prone to spoofing attacks, a massive amount of storage is needed, technology is highly affected by the background noise

7.4 'Humanode Biometric Modalities Score'

We assigned each factor its own value point depending on its effectiveness for the enrollment of new human nodes to the network:

- Acceptability (6)
- Collectability (6)
- Permanence (5)
- Universality (5)
- Uniqueness (10)
- Accuracy (8)
- Processing Speed (3)
- Circumvention (10)
- Hardware (8)

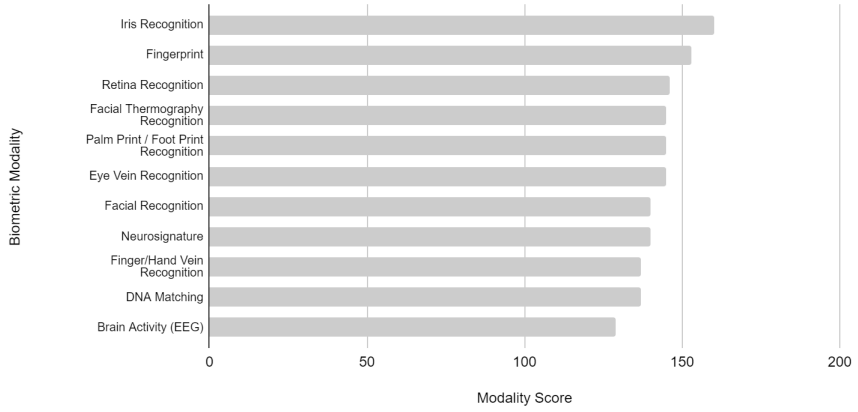
Thus, we assume that the most significant for the network are 'Uniqueness' of the biometric modality, 'Accuracy' of the biometric method, low level of 'Circumvention,' and 'Hardware' type used.

Table 5: 'Biometric Identification Matrix': Modalities Scores

	Characteristics/Factors (1- Low, 2- Medium, 3-High)									
Biometric Modality	Acceptability (6)	Collectability (6)	Permanence (5)	Universality (5)	Uniqueness (10)	Accuracy (8)	Processing Speed (3)	Circumvention (10)	Hardware (8)	**Modalities Score**
Facial Recognition	3	3	2	3	2	2	3	1	3	140
Facial Thermography Recognition	3	3	2	3	3	2	3	3	1	145
Fingerprint	3	2	3	2	3	3	3	2	3	153
Palm Print / Footprint Recognition	2	2	3	2	3	3	3	2	2	145
Finger/Hand Geometry Recognition	2	3	1	3	2	2	3	2	1	117
Finger/ Hand Vein Recognition	2	2	2	2	2	3	3	3	2	137
Iris Recognition	2	3	3	3	3	3	2	3	2	160
Retina Recognition	1	2	3	3	3	3	2	3	1	146
Eye Vein Recognition	1	1	3	3	3	3	2	3	2	145
Ear - Shape	3	2	3	2	2	2	2	2	2	118
Body Odor	2	1	3	3	3	1	2	3	1	127
DNA Matching	1	1	3	3	3	3	1	3	1	137
Brain Activity (EEG)	1	1	2	3	3	3	1	3	1	129
Electrocardiography (ECG)	1	1	2	3	2	3	1	3	1	119
Neurosignature	1	1	3	3	3	3	3	3	1	140
Gait	2	3	2	2	2	1	2	2	1	103
Keystroke Dynamics	3	3	1	1	1	1	2	2	2	94
Lip Motion Recognition	3	3	2	3	1	1	3	1	3	113
Signature Recognition	3	3	1	1	1	2	3	1	2	98%
Voice Recognition	3	3	1	2	1	1	3	1	3	103

To evaluate every aforementioned biometrics modality technique, we proposed the 'Humanode Biometric Modalities Score,' based on the 'Biometric Identification Matrix' analyzed. The study revealed that iris recognition techniques have the highest (160), with fingerprints are not far behind (153). Retina recognition (146), facial thermography recognition (145), palm print/footprint recognition (145), and eye vein recognition (145) also got quite high scores.
To create a human node, only those modalities are used that have score points above the median value (>133), i.e., facial recognition, facial thermography recognition, fingerprint, palm print/footprint recognition, finger/hand geometry recognition, finger/hand vein recognition, iris, retina, vein recognition, EEG, DNA, and neurosignature (in future).

Figure 9: 'Biometric Identification Matrix': Modalities Scores



We divided selected biometric modalities into 6 groups depending on the body part and techniques used, which belong to 3 main tiers:

Table 6: Humanode biometric modality tiers

Tier	Group	Biometrics Modality
Basic	Face	Facial Recognition
		Facial Thermography Recognition
	Hand	Fingerprint
		Palm Print / Footprint Recognition
		Finger/Hand Vein Recognition
	Eye	Iris Recognition
		Retina Recognition
		Eye Vein Recognition
Intermediary	Electrophysiological	Brain Activity (EEG)
Advanced	Chemical	DNA Matching
	Neuro	Neurosignature

Basic:

1. Face (facial recognition, facial thermography recognition)
2. Hand (fingerprint, palm print/footprint recognition, finger/hand vein recognition)
3. Eye (iris, retina, vein recognition)
   Intermediary:

4. Electrophysiological (EEG)

   Advanced:

5. Chemical (DNA)
6. Neuro (Neurosignature)

To become a human node you have three options:

- Pick up at least 1 biometric modality from 'Advanced' tier;
- Pick up 2 modalities from 'Basic' and 'Intermediary' tiers combined;
- Pick up 3 modalities from 'Basic' tier combined.

Due to the possible development of cheap methods of attacks on the current biometric security set-up in the future, the Humanode network will require human nodes to provide additional biometric data during network upgrades. For instance, once iris verification is proven to be secure on smartphone devices, it will be added as an additional minimum requirement to deploy a node. While Samsung already has made attempts to deploy consumer-scale iris recognition into its smartphones,

its quality and security levels are quite low compared to specialized hardware.
On top of this, in order to increase the cost of possible attacks on biometrics, the Humanode network requires high standards for the multimodal biometric system used for granting a new user permission to launch a human node, including but not restricted to:

- Multiple fingerprints for fingerprint biometrics;
- 16–20 pictures of the face with 8 KB quality of image;
- Passive and active software-based liveness detection to mitigate spoofing and alteration attacks.
- Authorized hardware to prevent the attacker from simulating new person enrollment with generated biometric traits.

Testnet: Until the mainnet, Humanode implements homomorphically encrypted face recognition with a voice liveness detection technique for user registration.
Mainnet: Once implemented, Humanode user verification and human-node setup are to be a result of homomorphically encrypted multimodal biometric processing through authorized hardware for the following modalities:

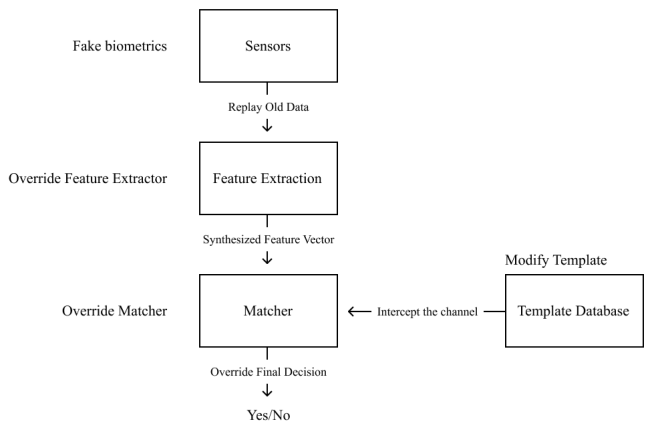
- Facial recognition
- Touchless fingerprint identification using optical scan (camera) or capacitive sensor
- Voice (speaker) identification
- Lip sync timing
- Vein matching, heart rate, EEG (Apple watch)
- Liveness detection—voice, heart rate, step counts, and health conditions, head movements detection (monitored by Airpods)

Also, the ability to create several wallets and to choose their types in the system will be correlated with the biometric modalities selected. For example, to create a high-value wallet, a more secure and complex verification technique should be chosen, and vice versa.

7.5 Types of attacks on biometric systems and their solutions

Currently, there are eight possible attacks against biometric systems.

Figure 10: Possible attacks on biometric verification systems



- **Attack on the sensor** Attackers can present fake biometrics in front of sensors (Jain et al., 1999). For example, someone can make a fake hand with fake vein patterns, or finger with fake wax fingerprint; someone can wear special-made lenses to bypass the iris scanner; other intruders can create images of a legitimate user to bypass the face recognition system, etc. The possible solutions for this type of attack are multimodal biometrics, liveness detection, as well as soft biometrics (Kamaldeep, 2011).
  Multimodal biometrics is the main way to prevent attacks and make the biometric system more secure. Multimodal biometrics refers to methods in which several biometric features are considered for enrollment and authentication. When multiple biometric characteristics are used, it becomes difficult for an attacker to gain access to all of them.
  Humanode utilizes multimodal biometrics. The network has three tiers with combined biometric modalities that are required to set a human-node (read more in the 'Humanode Biometric Modalities Score' section).
  Liveness detection uses different physiological properties to differentiate between real and fake characters. The methods are classified into:

- *Software*, where the fake trait is detected with a normal sensor, while real is differentiated from a fake with features from the biometric sample.
- *Hardware*, where an additional device is installed on the sensor to detect the properties of a living person: fingerprint sweat, blood pressure, or specific reflection properties of the eye.

With liveness detection, the chances of successful spoofing become low enough to make the cost of an attack higher by an order of magnitude in comparison to the potential transaction fees collected by an artificially created human node. The Humanode network implements liveness detection from the testnet. Voice recognition is a part of liveness detection from its genesis.
Soft biometrics is an additional solution, as some characteristics are not specific enough to distinguish users. If soft biometric parameters are also considered (gender, skin color and eye color, height, weight, etc.), the security level of the system increases. To help measure the correct threshold for conformity assessment in both unimodal and multimodal biometrics, Humanode is implementing soft biometric techniques as well.

- **Replay attack** A replay attack is an attack on the communication channel between the sensors and the feature extractor module. In this attack, an impostor can steal biometric data and later can submit old recorded data to bypass the feature extraction module (Jain et al., 1999).
Traditional solutions to prevent this kind of attack are as follows.

  - *Steganography* is the way by which biometric characteristics can be securely communicated without giving any clue to the intruders. It is mainly used for covert communication and therefore biometric data can be transmitted to different modules of the biometric system within an unsuspected host image.
  - *Watermarking* is a similar technique where an identifying pattern is embedded in a signal to avoid forging.
  - A *challenge-response system*, in which a task or a question as a challenge is given to the person and the person responds to the challenge voluntarily or involuntarily (Kamaldeep, 2011).

- **Attack on the channel between the database and the matcher** The attacker intrudes the channel to modify the existing data or to replay the old one. Traditionally, this attack can be prevented by such solutions as challenge-response systems, watermarking, and steganographic techniques as a Replay attack (Bolle et al. 2002).
The Humanode system is initially built in such a way that this attack cannot be performed. Depending on the use case, either private smart contract or public IPFS cluster with FHEd templates of human nodes, are the matchers and the database. The permissionless nature of databases and the matching process make attacks on them both problematic and costly.

- **Attack on the database:** The attacker can intervene in the database where the templates are stored to compromise the biometric characteristics of a user, replace, modify, or delete the existing templates.
There are two common template protection schemes to counter this attack:

  - *Cancelable biometrics*, in which the intruder cannot get access to the original biometric pattern from the database because instead of the original data, a distorted version is stored.
  - *Biometric cryptosystem*, where all data is encrypted before sending in the database while the original template is deleted, therefore, it is quite difficult for the attacker to steal the original template, as it exists only for a few seconds on the user's device.

  The Humanode network uses the second type. Biometric data is fully-homomorphically encrypted before sending it to a permissionless cluster.

- **Override the final decision** As the software application may have bugs, an intruder can override the actual decision made by the matcher.
The actual decision is taken by the smart contract that decrypts the result of the matching operation received as FHEd data. After that, the private smart contract authorizes the user. This attack can be prevented using soft biometrics as well (Kamaldeep, 2011).

- **Override feature extractor** This attack relates to overriding the feature extractor to produce predetermined feature sets, as the feature extractor is substituted and controlled remotely to intercept the biometric system.
In the Humanode system, feature extraction takes place on the client's device, controlled by authorized hardware. The human node encrypts the embedded feature vector using the public key and gets the FHEd feature vector as a result, hence the attacker is unable to override it.

Table 7: Attacks on biometric systems and their possible solutions

Attacks	Solutions	Humanode's approach
Attack on the sensor	Liveness detection, multimodal biometric systems, soft biometrics	Liveness detection, multimodal biometric systems, soft biometrics
Replay attack	Steganography, watermarking techniques, challenge-response systems	Steganography, watermarking techniques, challenge-response systems
Attack on the channel between the matcher and database	Steganography, watermarking techniques, challenge-response systems	Private smart contract or public IPFS cluster of human nodes is the matcher and database at the same time
Attack on the database	Cancelable biometrics, biometric Cryptosystem	Biometric data is FHEd before sending it to a permissionless cluster
Override final decision	Soft biometrics	The actual decision is taken by the smart contract that decrypts the result of the matching operation received as FHEd data. After that, the private smart contract authorizes the user.
Override feature extractor	-	Feature extraction takes place on the client's device, controlled by authorized hardware
Override matcher	-	User authentication is secured by private smart contracts, user enrollment is FHEd, and all scores are stored in the encrypted domain, therefore an attacker cannot take control over or modify matching scores
Synthesized feature vector	-	There is a private channel between the feature extractor and the matcher, thereby these kinds of attacks are impossible

- **Override matcher** Overriding the matcher to output high scores compromises system security. In this way, the intruder can control the matching score and generate a high matching score to confirm authentication to the imposter. User authentication is secured by private smart contracts, user enrollment is FHEd, and all scores are stored in the encrypted domain, therefore an attacker cannot take control over or modify matching scores.

- **Synthesized feature vector** The route from the feature extractor to the matcher is intercepted to steal the feature vector of the authorized user. The legitimate feature sets are replayed later with synthetic feature sets to bypass the matcher (Bolle et al. 2002); (Jain et al., 1999); (Kamaldeep, 2011).
  In the Humanode system, there is a private channel between the feature extractor and the matcher, thereby these kinds of attacks are not possible.

8 Private biometrics

8.1 Private biometrics

The ability to privately secure user authentication through biometrics has been the goal of many cryptographic researchers. For the last two decades, cryptographers have concentrated their efforts on solving the problem of biometric protection against malicious activities of the verifier. Solutions like two-way partial homomorphic encryption, BioHashing, Biometric Cryptosystems, and cancelable biometrics were all researched and proven to be inefficient or insecure for a hypothetical user (G. Davida et al., 1998; N. Ratha, J. Connell & R.M. Bolle, 2001, 2002; A.T.B Jin, D.N.C Ling & A. Goh, 2004; A. Kong, 2006; A.B.J. Teoh, Y.W. Kuan & S. Lee, 2008; C. Rathgeb & A. Uhl, 2011; M.A Syarif, et al., 2014; B.J. Jisha Nair & S. Ranjitha Kumari, 2015).

Until not so long ago, biometric identification methods carried a heavy risk to personal privacy. Biometric data is considered to be very sensitive, as it can uniquely be associated with a human being. Passwords are not considered PII (Personally Identifiable Information), as they can be changed and not associated with any person directly. The main risks of biometric matching in the past were based on the fact that they required the biometric data to be visible at some point during the process. That led to two problems. First, as ciphertext converted back and forth to plaintext because of the decryption methodology, it created the necessity of powerful computation, complex key-management systems, and a large amount of data storage. In other words, it was inefficient. Second, the very conversion to plaintext meant vulnerability to loss.

Modern private biometrics are able to solve the above-mentioned problems by implementing *one-way, fully homomorphic encryption (FHE)*. This type of encryption makes computations on ciphertext possible, moreover, they hide original biometric data and return an encrypted value. As verification procedures are conducted on a ciphertext, they allow search and matching through an encrypted dataset without revealing the original biometrics to any party. We get a very accurate, fast, and private system that eliminates any risk of a user's biometrics falling into the wrong hands.

A malicious actor is unable to bypass a private biometric system because the plaintext communication path is segregated from every other, even at a low-level interaction. The biometric data in this case is transient at inception meaning that biometrics exist only for a fraction of a second or a few seconds, depending on the device, and are never stored.

The biometric feature vector is created through a one-way cryptographic hash algorithm. It maps plaintext biometric data to a feature vector of a small size, around 4 kB. This algorithm is invoked using a convolutional neural network that takes a vector from an image or any other source (for example, FaceNet by Google and Apple Face ID use an 8 MB facial biometric) and turns it onto a 4 kB vector of variables between zero and one that sum to one. It is mathematically impossible to reconstruct the original plaintext image from a private biometric feature vector of 128 floating-point numbers.

8.2 Neurosignature

With the evolution of neural implants, it became possible to convert the neuroactivity of the brain into electronic signals that can be comprehended by modern computers. Since the 1960s, the neurotech field has moved from simple electroencephalography (EEG) recordings to real brain-computer communication and the creation of sophisticated BCI-controlled applications. Since the late 2010s, large companies have begun to actively pursue brain-computer interface (BCI) development, rapidly approaching its adoption. In 2014, Brainlab developed a prototype that allows a Google Glass user to interface with and give commands to the device using evoked brain responses rather than swipes or voice commands. In 2015, Afergan et al. developed an fNIRS-based BCI using OST-HMD called Phylter, a control system connected to Google Glass that helped prevent the user from getting flooded by notifications. In 2017, Facebook announced the BCI program, outlining its goal to build a non-invasive, wearable device that lets people type by simply imagining themselves talking. In March 2020, the company published the results of a study that set a new benchmark for decoding speech directly from brain activity. Companies, like BrainGate and Neuralink[3], have manufactured working prototypes of invasive and noninvasive brain-computer interfaces that build a digital link between brains and computers. Even with the immeasurable complexity of neurons and ridiculous entanglement of somas, axons, and dendrites, the above-mentioned projects were able to create devices that not only stimulate and capture the output but also distinguish patterns of signals from one another.

This means that neurosignals can be converted into an embedded template. Humanode protocol will implement homomorphic encryption on this template to conduct search and matching operations only on ciphertext, meaning that a person will be able to use his own mental state, conscious state, or simply signals from the motor cortex to initiate node deployment and verify transactions without compromising the data itself.

Compared to any other biometric solution besides direct DNA screening and other biochemical solutions neurosignature biometrics can be considered to be the most secure way of biometric processing, as it is impossible to forge a copycat or to emulate the prover and try to bypass the system.

[3] In August 2020, Elon Musk unveiled a working brain implant in pigs.

Figure 11: Block diagram of a BCI system

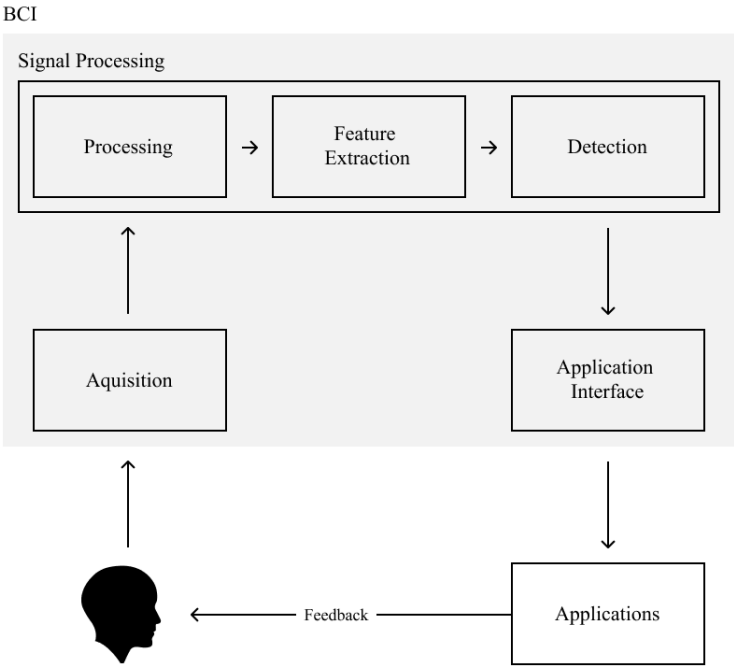


Table 8: Summary of signal acquisition method (Mudgal et al., 2020)

Types	Example	Signal Type	Portability	Spatial Resolution	Temporal Resolution
Invasive	Intra-cortical	Electrical	Portable	Very high	High
Semi-invasive	ECoG	Electrical	Portable	High	High
Non-invasive	EEG MEG fMRI fNIRS	Electrical Magnetic Metabolic Metabolic	Portable Non-portable Non-portable Portable	Low Mediate High Mediate	Mediate Mediate Low Low

While BCI hardware enables the retrieval of brain signals, BCI software is required to analyze these signals, produce output, and provide feedback.
Moreover, neurotech continues to evolve—hybrid BCIs (hBCIs), which are the combinations of BCIs with a wide range of assistive devices (ADs), prove it (G. Pfurtscheller, 2010; G.R. Müller-Putz et al. 2015; I. Choi et al., 2017;Yang et al., 2020). These hBCI systems are categorized according to the type of signals combined and the combination technique (simultaneous/sequential). Electroencephalography (EEG), due to its easy use and fast temporal resolution, is most widely utilized in combination with other brain/non-brain signal acquisition modalities, such as functional near-infrared spectroscopy (fNIRS), electromyography (EMG), electrooculography (EOG), and eye-tracking technology (K.-S. Hong & M. Jawad Khan, 2017). In general, the essential goal of combining signals is to increase the detection accuracy, enhance system speed, improve user experience, and overcome the disadvantages of BCI systems (S. Sadeghi & A. Maleki, 2018). With hBCIs, Humanode can achieve unprecedented multi-modality based on internal biometric processing protocols.
There are many different ways to collect data on brain activity, but more importantly, there have been many software layers already created by different organizations and communities such as OpenBCI, BCI2000, NFBLab, PsychoPy, rtsBCI, OpenVibe, OpenEEG, BF++, etc.
These types of software can be divided into three different groups:

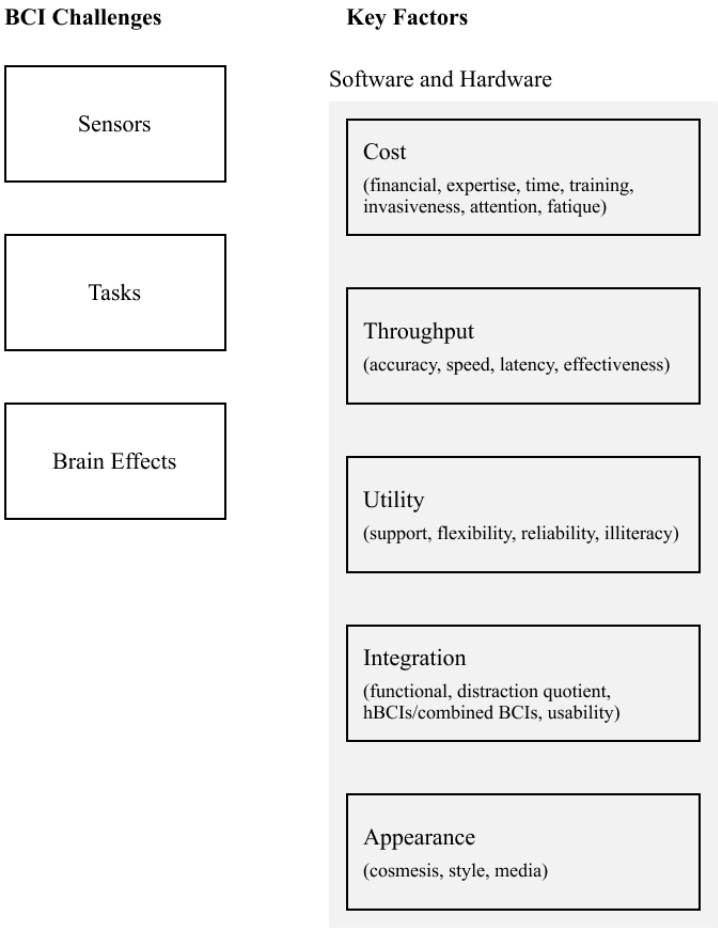
1. Software that provides a stack of protocols that try to precisely read, analyze, and store brain activity data through different types of signals (EEGs, fMRIs, invasive implants, etc.);

2. Software that converts brain activity data into commands for different computer languages and systems; and

3. Supplementary software that converts received brain activity data into different types of variables for research and development purposes.

Researchers are making great strides towards resolving all of the above-mentioned challenges. The majority of investigators believe in BCI mass adoption in the following years. Recent research examines the possibility of using BCI in everyday-life settings in different contexts (Blum et al., 2012; Hu et al., 2019; Park et al., 2019; D. Friedman, 2020; Benitez-Andonegui, et al., 2020). There is a relevant body of work addressing not only technology improvements (Liberati et al., 2015) but also the fact that BCI design and development should become more user-friendly to achieve successful mainstream applications (Kübler et al., 2014; Nijboer, 2015).

Figure 12: Factors that influence adoption

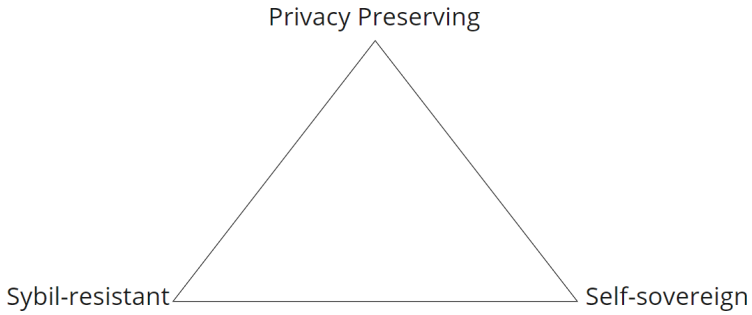


Humanode core wants to dedicate a team of researchers and developers to create a layer that converts precise brain activity data utilizing multimodal biometric processing into fully homomorphic Euclidean-measurable floating points to generate a private key that can safeguard a Merkle-CRDT mechanism based on human nodes.

9 Humanode's approach to identity attack prevention

The amount of research exploring the use of distributed ledger technology to launch new types of identity management systems has lately increased (Baars, 2016; Jacobovitz, 2016; Tobin & Reed, 2016; Dunphy & Petitcolas, 2018) along with studies combining these systems with biometrics (Hammudoglu et al., 2017; Garcia, 2018; Othman & Callahan, 2018).

Figure 13: Decentralized Identity Trilemma (Maciek, 2019).



Alongside maintaining *self-sovereignty* (anybody can create and control an identity without the involvement of a centralized third party) and being *privacy-preserving* (anybody can acquire and utilize an ID without revealing personally-identifying information (PII)) the system also needs to achieve *Sybil-resistance*, as the majority of large-scale peer-to-peer networks are still vulnerable to Sybil attacks. These occur where a reputation system is subverted by a considerable number of forging IDs in the network (J. R. Douceur, 2002; R. John, J. P. Cherian & J. J. Kizhakkethottam, 2015; A. M. Bhisea & S. D. Kamble, 2016k; D. Siddarth, S. Ivliev, S. Siri, & P. Berman, 2020).
None of the existing solutions are privacy-preserving, self-sovereign, and Sybil-resistant at the same time(Maciek, 2019). We at Humanode propose potential the following solutions to break the trilemma.

9.1 Self-sovereignty

The Humanode protocol applies principles of self-sovereign identity (SSI), requiring that users be the rulers of their own ID (C. Allen, 2016). In Humanode, there is no centralized third party to control one's ID, thus ID holders can create and fully control their identities.

9.2 Privacy-preserving

The Humanode system has two layers of privacy-preserving solutions. First, there are private computations on homomorphically encrypted data. It means that the biometric data does not exist in plaintext after it is sent from the client to the secret contract through the private channel. The second solution is fully homomorphic encryption, thus there is no personally identifying information (PII) in the system. To tackle the scalability issue of 1-n verification needed to launch a new human node, we will utilize fully homomorphically encrypted biometric embedded vectors and send them to IPFS. Human nodes will perform 1-n computation.

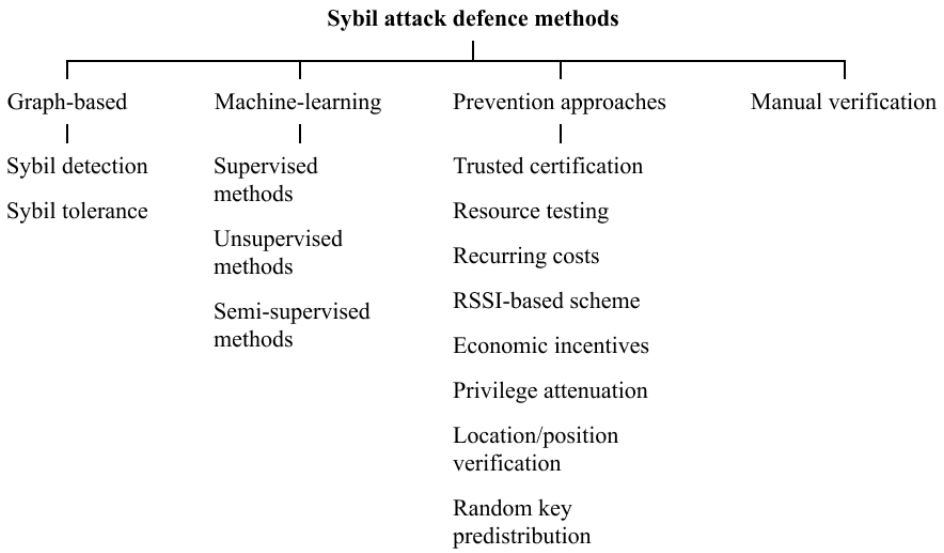
9.3 Sybil-resistance

A Sybil-proof system was best conceptualized by Vitalik Buterin as a *"unique identity system"* for generating tokens that prove that an identity is not part of a Sybil attack (V. Buterin, 2014; 2019). In recent years, attempts in the field were made by blockchain-based initiatives like HumanityDAO, POAP, BrightID, Idena Network,Kleros, Duniter, etc. Nevertheless, there are still no relevant Sybil-resistant identity mechanisms. In other words, in today's digital space a possibility remains for users to create multiple accounts in one system using distinct pseudonyms to vote several times or receive multiple rewards, etc.

Table 9: Comparison of Sybil attack types

Type of Attack	Description	Defense Method
Routing	These attacks include distortion of routing protocols: single multiple paths through Sybil nodes, or geographic routing, in which sensor nodes send data to a base station.	Graph-based detection methods
Distributed Storage	An attacker stores data about false IDs and manipulates users to store data in multiple Sybil IDs of a network node.	Machine learning techniques
Data Aggregation	An attacker uses multiple IDs and modifies aggregation readings in the sensor network as a strategy to save energy.	Machine learning techniques
Voting/ Reputation Systems	An attacker manipulates systems that use voting to accept false solutions and affects the ranking mechanism in reputation systems.	Graph-based detection methods
Resource Allocation	These attacks are common in networks where resources are assigned depending on the number of nodes. Malicious nodes can deny legitimate ones from accessing network resources.	Prevention schemes and graph-based detection methods
Misbehavior Detection	An attacker creates multiple Sybil nodes to spread false alarms to impact system performance and compromise detection accuracy.	Graph-based detection and manual verification

Figure 14: Main Sybil attack defense methods



- *Graph-based methods*
  Graph-based methods rely on a social network's information to represent dependencies between objects. These schemes fall into two categories:

  1. Sybil detection techniques based on the concept of graph random walk and mix time
  2. Sybil tolerance techniques, which limit the effects of Sybil attack edges (M. Al-Qurishi et al., 2017; A. Alharbi et al., 2019).

- *Machine-learning methods*
  These methods fall into the following categories:

  1. Supervised, which use regression models, support vector machine (SVM) (P. Gu et al.,2017), and decision tree models
  2. Un-supervised, which use fuzzy logic, Markov models (K. Zhang et al., 2015), and clustering methods
  3. Semi-supervised, which use sets of data to improve the quality of learning.

- *Manual verification methods*
  This scheme relies on users to increase security through user verification, e.g., this may include asking users to report malicious content in the network.

- *Prevention methods*
  Prevention schemes refer to such traditional approaches as using trusted authorities or resource testing. They may also include the use of crypto puzzles (CAPTCHA) for users to access systems and verifying their ID by sending a verification SMS message to the user's phone.

Humanode uses various techniques for preventing Sybil attacks:

Table 10: Main techniques for preventing Sybil attacks

Technique	Application Domain	Description
Trusted Certification	General	Certification solution involves the presence of a trusted certifying authority that validates identities. Douceur has proven that trusted certification is the only method that may potentially eliminate Sybil attacks completely (J. R. Douceur, 2002). However, the approach is not cost efficient and has larger overheads when applied to a large-scale system (A. M. Bhisea & S. D. Kamble, 2016).
Resource Testing	General	This verification method aims to determine if the identity has as many resources as the single physical device it is associated with.
Recurring Costs	General	This technique is a form of resource testing where resource tests are performed at regular time intervals to impose a certain "cost" on the attacker that is charged for every identity that she controls or introduces into the system (Y. Muliadi et al., 2003; B. Awerbuch & C. Scheideler, 2004, P. Maniatis et al, 2005.) However, these researchers have used a computational power in their resource test that may not be sufficient to control the attack, since the attacker only incurs a one-time cost that can be recovered via the execution of the attack itself (B. Levine et al., 2005).
Economic Incentives	General	This technique is based on a scheme where economic incentives are used to reward the adversaries if the identities that are controlled by it are revealed (N. Margolin & B. Levine, 2007;M. B. Shareh, et al., 2019 ,2020). The main disadvantage is that it may encourage attackers economically.

From the very start, Humanode uses the aforementioned prevention methods to successfully counter Sybil attacks. Also, imposing economic costs as barriers to becoming a human node are used in the system to make attacks more expensive and less feasible. Moreover, human nodes perform 1-n computation over FHEd templates, which means there were no nodes registered with the same biometrics before.
In order to create a Sybil-resistant system for human identification, Humanode ensures that every identity is:

- *Unique* (two individuals should not have the same ID)
- *Singular* (one individual should not be able to obtain more than one ID; F. Wang & P. De Filippi, 2020)

To validate users' identities and to create a Sybil-proof system, Humanode introduces a verification mechanism when the identity is derived from one or more unique features of the human body—with the implementation of premiere biometric solutions such as:

- Multimodal biometric processing with liveness detection and periodical verification of identity *(Humanode testnet)*
- Biochemical biometrics—direct DNA screening, and neurosignature biometrics through BCI *(Humanode mainnet)*
- Furthermore, in order to reduce the possibility of the attack, particular authorized biometric hardware will be added as a part of the network *(Humanode mainnet)*

DNA screening and neurosignature biometrics can be considered the most secure way of user verification, as it is totally impossible to forge to bypass the system:

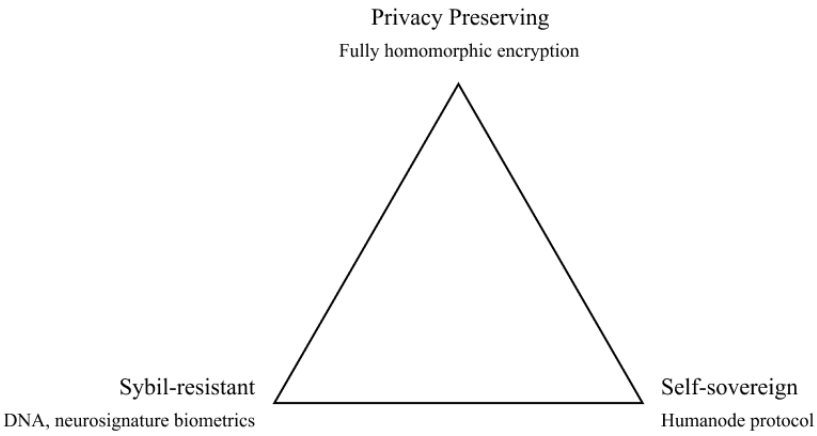
- Each individual can generate a unique brain signal (mental state, mental-emotional state) / Each individual has a unique DNA profile
- Each person can generate the same brain signal (mental state, mental-emotional state) / Each person's DNA is the same in every cell
- An individual's DNA profile remains the same throughout life (P. Balaji, 2010;M. Hashiyada, 2011).

In addition, the IFPS structure implemented in Humanode may minimize the possibility of a Sybil attack. To give users their own namespace in the system and to let them gain credibility or favor IPFS, nodes have Content Identifiers (CIDs) that help the system prevent Sybil attacks, and the security grows with the number of active human nodes. Thereby, due to the unusual accumulation of overlay connections and the fact that requests are sent randomly to all direct peers, content retrieval in IPFS is achievable even if an attacker could place Sybil nodes at key locations in the overlay (Benet J., 2014; S. Henningsen et al. 2020). Nonetheless, IPFS currently implements no restriction on node identity creation, and IP address-based Sybil protection measures, such as limiting the number of connections to nodes from the same/24 subnet, are not in use as well. Humanode system and its replicas can serve as a Sybil resistance mechanism for IPFS applications and users.

***

Thus, in a nutshell, Humanode's identity attack prevention scheme solves Maciek's 'Decentralized Identity Trilemma' as the system applies self-sovereignty, privacy-preservation, and Sybil-resistance principles as illustrated below:

Figure 15: Humanode's approach to identity attack prevention



10 Human node registration and private authentication scheme

In this section, we will dive into details of the technologies and procedures that lead to the creation of a human node. The same architecture lets network users register their biometric modalities to create an account (User Enrollment) and later go through authentication to control previously created private keys (User Authentication).
There are three actors: the client device, private smart contract, and the Humanode public cluster.

10.1 Private smart contracts

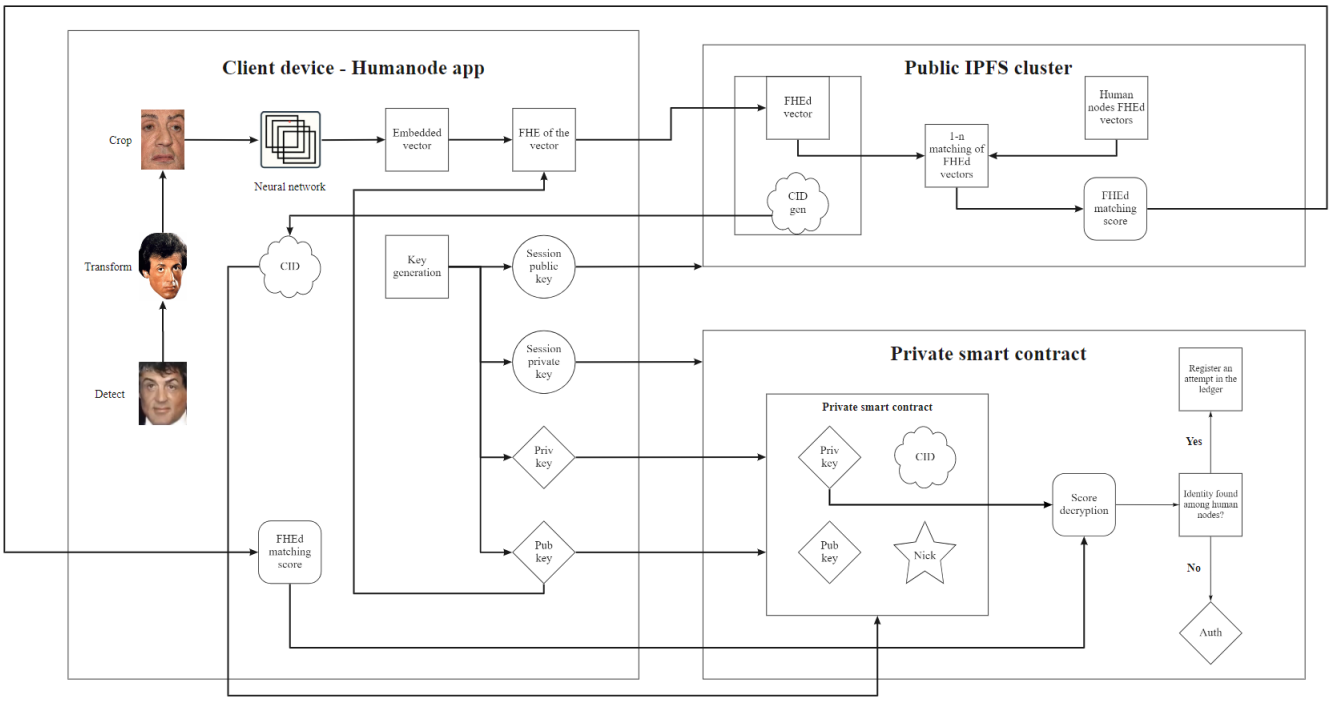
Dominant crypto-assets and smart-contract platforms do not provide necessary user privacy, as all transactions, wallet holdings, and smart contract data are publicly available despite being pseudo-anonymous. While major implementations of permissionless blockchains with privacy features are mostly focused on hiding the data of the sender, receiver, or the transaction itself (Z-cash), MimbleWimble only a few projects have zoned in on bringing privacy to smart contract data and execution (Secret Network, previously Enigma).
Secret Network is a peer-to-peer network, enabling different parties to jointly store and run computations on data while keeping them completely private. Its computational model is based on a highly optimized version of secure multi-party computation, guaranteed by a verifiable secret-sharing scheme. The secrecy of shares is ensured by mandating that nodes running the network use Intel's trusted execution environments (TEE), known as enclaves, for computations and data storage. This feature encrypts sensitive data, hiding it from everyone including the node operator (G. Zyskind, et al., 2015).
In order to build Humanode, we use private smart contracts technology for decentralized private key generation and storage.

10.2 Humanode IPFS cluster

Humanode network leverages IPFS to store Fully Homomorphically Encrypted (FHEd) feature vectors from biometric data. Humanode IPFS clusters provide allocation, replication, and tracking of data among human nodes, including biometric data. In our case, nodes are empowered with even greater abilities: they perform 1-n computation over FHEd templates that is necessary to make sure there were no human nodes registered with the same biometrics before.

10.3 Human node enrollment process

Figure 16: Human node enrollment process



Client device
The process starts with the user choosing a nickname and scanning the biometric modalities required by the network. To facilitate explanation, in our example the modality is facial recognition. The application detects, transforms, and crops the image. The residual neural network transforms the biometric image into embedded vectors.
In the meantime, the client device generates two sets of keys:

1. Session public and private key;

2. A key pair for Fully Homomorphic Encryption: public and private key.

Still using the client device, a would-be human node encrypts the embedded feature vector using the public key and outputs the FHEd feature vector as a result.

Client–public cluster communication
The user submits the FHEd feature vector, signing it with the session private key along with the FHE public keys to the IPFS public cluster. Now, having the public keys, the cluster is able to perform computations over the FHEd vectors the user submits without being able to decrypt them. Once the vectors and keys are pinned to IPFS, the cluster returns Content Identifier-CID (content hash and session public key) to the client device.

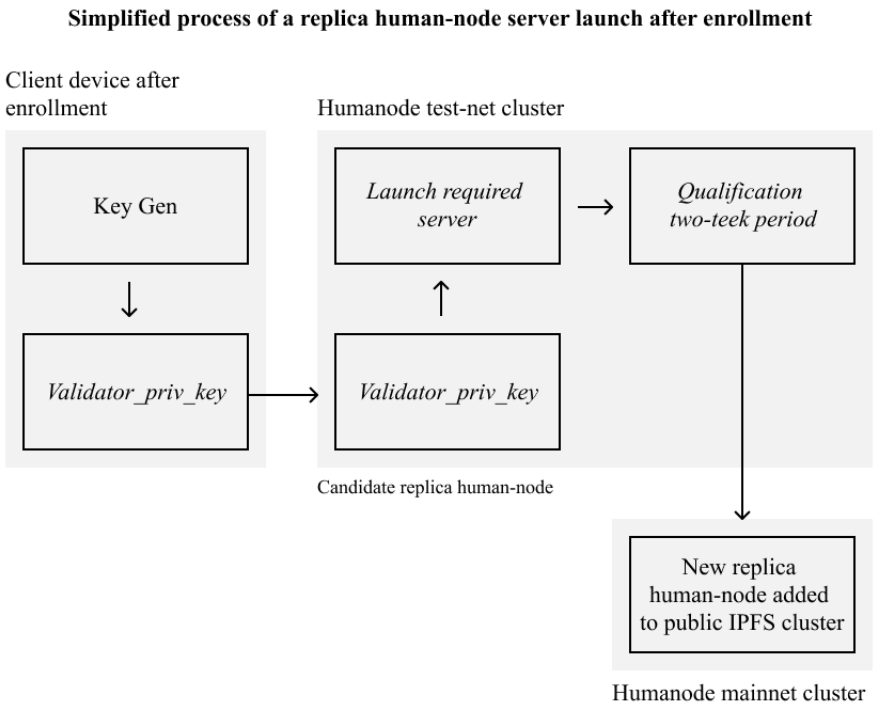
Client–private smart contract communication
The user submits the hash of the nickname (moniker), embedded vector, FHEd public and private keys through a private channel using the session public key. The private smart contract fetches CID to the hash of the nickname, encrypts the data, and stores it in the encrypted domain. Fetched CID and nickname are used later for authentication.

1-n matching of FHEd templates on the public cluster
As the Humanode cluster maintains the pins of FHEd biometric feature vectors, we can now compare them to the FHEd vector of the enrolling human-node. The result of 1-n matching is an encrypted score. The score is sent to the client device.

Authorization of a new human-node by a private smart contract
The client device sends the FHEd matching score to the private smart contract. With the FHE private key, it decrypts the score. If the score is above the threshold, this means the same FHE vector already exists among the human nodes, and the attempt of a new human node authorization is denied. If the score is below the threshold, the private smart contract authorizes the public key of the user to launch a human node.

Launch of a replica human node
Here we provide a simple process of launching a replica human node.
After the user is authorized to launch a replica human-node server, the client generates a validator private key that he puts

Figure 17: Simplified process of a replica human-node server launch after enrollment



into the server together with a public key. As the public key is already authorized in the private smart contract, the user joins the Humanode testnet cluster. After two weeks of the testing period, if the candidate node passes the requirements the new human-node server moves to the Humanode mainnet cluster.

10.4 Enrollment, authentication of users, and private biometric key management

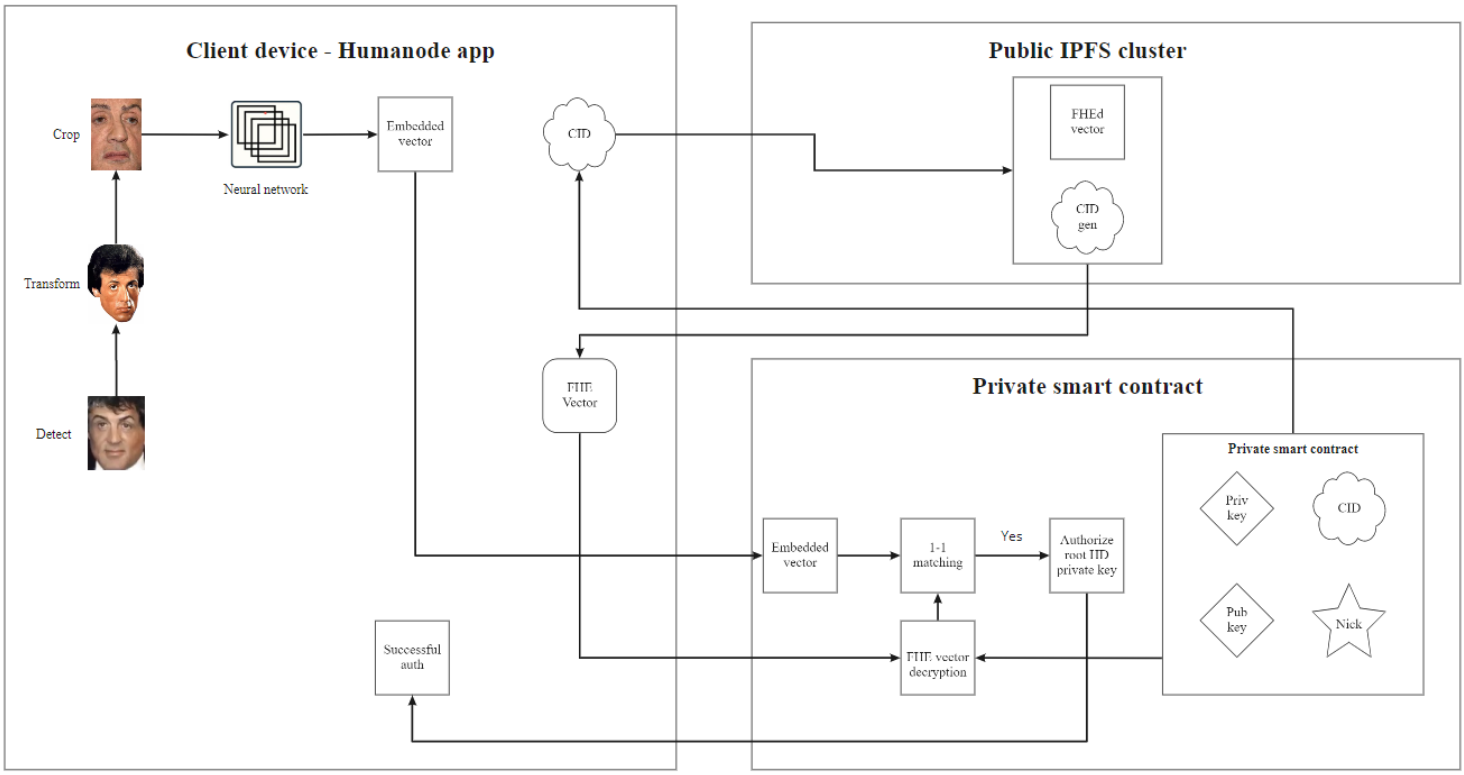
By using the same approach of combining the FHEd vector database on IPFS and the private smart contract, we introduce a secure approach to private biometrics for user authentication and a biometric key management solution.

User Enrollment
The User Enrollment scheme mimics that of human-node enrollment. However, it utilizes a biometric database of all FHEd vectors stored on the IPFS public cluster submitted by all users, not only human nodes authorized by protocol, and performs 1-n matching over them.
After the private smart contract receives a matching score below the threshold, it generates a new root HD (hierarchical deterministic) key and stores it in the encrypted domain hiding even from the user. Otherwise, the user is pointed to his previously registered account.

Private biometric key management
Now, as the private contract generated HD key is tied to a person's identity, the user can generate as many wallet addresses as he wishes to, using a biometric modality of his choice, cold wallet device, or password. Maximum security is achieved by combining multiple methods through threshold key signatures. For instance, biometric modalities can be set to be insufficient for authentication without a token.

User authentication

Figure 18: User authentication scheme in the Humanode network



Client device
In order to repeatedly authorize in the Humanode network or in applications using Humanode private identity protection, the user, again, starts with biometric verification. He detects, transforms, crops, and processes the required biometric trait, depending on the chosen account settings. After putting the biometric floating points into a residual neural network, the user device sends the output, embedded vector to the private smart contract, where it is later used for 1-1 matching.

Pulling enrollment FHEd vectors
By sending the hash of the user's nickname to the private smart contract, the client device gets a fetched CID. Now it can send the CID to the Humanode public cluster to receive the FHEd vector submitted by the authorizing user during enrollment.

1-1 matching in a private smart contract
The user submits the FHEd vector to the private smart contract. As the contract already stores a keypair for the FHEd vector, it decrypts and compares it to the embedded vector taken at the start of the authentication process. This results in a score. If the matching score is above the threshold, that means the biometric data matches the one previously submitted. The user is successfully authorized. Otherwise, the protocol saves an unsuccessful attempt of authentication using the personal

moniker of the individual.

An alternative user authentication scheme
In the alternative option, a public cluster of human nodes performs 1-1 matching operations, sending the encrypted score through the client to the private smart contract. The private smart contract decrypts the score and authorizes the user if the score is above the threshold.

11 Current inefficiencies of public permissionless networks

11.1 Blockchain technology

Blockchain as a technology concept has been developed and evolved around a Proof-of-Work (PoW) consensus. It achieves the most benefits under the PoW model, like vanilla Bitcoin or its forks.
These principles add a great deal of overhead and complexity to the nodes, because of the block's meta-data, processing, and verification. While classic Bitcoin has lower complexity, modern chains such as Ethereum, whose goal is to provide distributed computation and not just a value transfer, lack simplicity. It is more challenging to verify the state on the Ethereum network, and even harder for Ethereum 2.0.
While this overhead represents advancement in Computer Science in general and adds more agility to the chain while retaining the same level of security, it becomes clear that for many domains and use cases this overhead can cause unintended problems.
The overhead of such a fundamental piece of technology unfortunately spreads across the whole tech stack of a project. It leads to increased infrastructure costs for node-runners, which are reflected in gas prices, thus reflected in the end-user experience. Pure blockchain almost always results in bad UX, either due to high gas cost or timing of transaction processing. Nowadays, many advanced blockchain companies try to fix these UX flaws while retaining the blockchain at the core of their product. However, for most tech companies the blockchain brings more downsides than advantages.
Even when the block-time is decreased to 1 second, which is still a lot of latency, it is very stressful for consensus. However, from an external point of view, the chain is still just a slow database (DB). And the transaction pricing model cannot be accepted by all users as well, so this DB is not only slow but also costlier.
Thus, the cases when a company replaces an enterprise DB layer with strong ACID guarantees, such as DynamoDB from AWS, and installs a private blockchain instead are hardly imaginable.

11.2 Gas prices

Gas prices are paid once during transaction (TX) creation, however, any TX places a liability on the node-runners to keep its data and metadata forever. That means gas should include the future costs of node-running, otherwise, eventually it creates tension between application users and node runners. For example, when Ethereum prices skyrocket, any low-value transfer app becomes unusable.
Blockchains that are innovative in blocktime optimizations, for example,Klaytn, with a rich governance council and the ability to produce blocks exactly each second, have struggled to retain all metadata for a year already. It took more than 1 TB of disk space to keep the metadata of the blockchain running, which quickly becomes a problem for any node that wants to provide read-only access to the state.
Thus, some gray pruning schemes were applied. We call them "gray" because they weren't part of the original spec or whitepaper, they did not go through enough testing, and there have been multiple attempts to implement them, for example in the Cosmos Network. Klaytn did this gracefully, reducing the trail of metadata to just only 200 GB, but that is not compaction, so full archival nodes still are required to keep the whole data set.
While the requirements to achieve historical data lookup are astronomical, there was no business-case precedent to keep the data retrievable for 10 years or more. Most of the stakeholders of the crypto industry are forward-focused and the protocols themselves change very rapidly. Old transactional data becomes useless, yet still takes up room in every user's node disk space.
This requirement to keep all the historical data for the retrievability of the recent data has a symmetrical case on the user side: most blockchains have a pay-gas-or-die scenario for any kind of transaction. The gas price can affect the transaction acceptance time, but it will not be acceptable to pay less gas to have less archival guarantees. One must always pay full gas with no exceptions, but the network guarantees full data are available until the heat death of the universe.

11.3 Capital-based consensus mechanisms

Proof-of-Work (PoW) and Proof-of-Stake (Pos) networks, despite being public and permissionless, build trust through capital requirements—running devices or acquired and locked tokens. Hence, they are always susceptible to a *direct attack* that needs only capital or to an *attack of the external network* (B.Ford & R.Bohme, 2019) of a greater hashing power or capitalization. For this reason, the main principle behind the Humanode network is equal control of the shared truth among each person joining the system where one cannot achieve additional voting power toward the consensus of global truth through money or authority. One living person can launch only one replica.

12 Transaction fee economics of the Humanode network

This part of the paper explains important considerations when selecting the optimal fee strategy. It is proposed that the Humanode network will have a cost-based fee policy and flexible data persistence settings, which differentiates it from the existing public permissionless systems based on blockchain.

12.1 Transaction acceptance

In many popular blockchains, the transactions are included in blocks, which in turn are being "mined" and sealed in the PoW scenario or validated with a Delegated Proof-of-Stake (DPoS) algorithm. Users normally have different expectations from each system. In particular, transaction confirmation may take from 1 second to days; also a gas fee might range from 0.00001 to hundreds of dollars.
The transaction is considered accepted unless it conflicts with the account's nonce, is not underpriced, and does not 'revert' during Virtual Machine (VM) execution (in smart contract–enabled networks).
Once included in a block, the transaction still can be reverted as a consequence of chain reorganization—a process when a longer chain of correct blocks has been discovered by a network. This is natural, especially to PoW chains such as Bitcoin and Ethereum; this is why transaction finality is a subjective concept based on trust and one's risk factors. There are different confirmation amounts suggested per chain. The minimal necessary confirmation requirements are suggested differently depending on the chain.
The difference is obvious when PoS with BFT (Byzantine Fault Tolerance) is being used for consensus (i.e.,Cosmos-based), which usually results in near-instant transaction finality. Chain reorganizations are not a phenomenon in PoS networks, thus greatly affecting usability properties.
In the Humanode network, we have an optimistic approach with eventual consistency that converges based on logical clocks and guarantees the correct order of events. The state is merged from updates on state CRDTs that can only grow, meaning that the transaction eventually appears, but once accepted it cannot be "dropped"; in other words, there are no chain reorganizations.

12.2 Flexible guaranteed transaction persistence

Transactions in Humanode networks have flexible pricing. Due to the nature of the mechanism, we can allow more flexible terms of transaction processing and persistence.
Transactions have a pre-defined cost-basis estimation depending on the computational complexity and the storage used. If a transaction stores lots of data, it will cost more for the user to submit it.
We propose different price tiers for transaction persistence after the transaction has been processed by human nodes. In many classic blockchains, the transaction fee is charged once; however, transaction persistence is an ongoing burden on the node operators. This results in high infrastructure costs or the need for pruning schemes that reduce decentralization.
Instead of guaranteeing perpetual persistence of any data for free, we make the pricing more transparent.

$$Price_{tx} = C_{Computation} + C_{GBperperiod} * TX_{size} * Persistence\,Time \tag{1}$$

For applications where persistent transactions are not critical, users can select a lower tier and pay fewer transaction fees. If the transaction persistence is required for reasons such as compliance, the system explicitly provides such guarantees.
Guaranteed persistence or 'pinning' is the opposite of pruning. This protects the transaction's data from being collected by a garbage collector on the nodes. The full set of 'pinned' transactions is called a pin-set, which is a dynamic set with expiration times. When a transaction leaves the pin-set due to expiration or a governance action, the nodes may remove the data from storage. The transaction will be known to the network while at least one machine keeps its data, but since the active pin-set is not keeping it anymore, any persistence would be a voluntary effort (or self-persistence of one's own transactions).

12.3 Fee-setting and distribution mechanisms in the Humanode protocol

To overcome the problems that current public permissionless networks face, we apply a cost-based approach to set transaction fees. This enormously decreases the influence of the market on the base transaction cost.
Storage and computing are commodities. Web-service providers with data centers across the globe quote their prices openly. The amount of Humanode tokens (HMND) that is spent on renting computation from the largest web service provider in a certain period determines the amount of HMND tokens that have to be distributed for the computation to each human node. At the same time, the total computational costs the network incurred for processing a user's transaction is the computational transaction fee of the user.
Now after agreeing on the transaction, human nodes have to pin it to the public cluster global pin-set and change the ledger balances. It requires *storage* on the rented or self-launched server. Storage costs are time-based. Knowing the market price per GB per month quoted by the leading web-service provider in HMND tokens, we set the base cost for a given time period. The Humanode network offers different transaction tiers depending on the guaranteed data persistence set by applications or users. In other words, the transaction tier depends on how long the transaction has to be stored by human nodes.
We know or have quotes for the hourly storage costs for a given month. However, the price is not the same if stored for a longer time period. Hence, we have to provide a formula that determines the cost of long-term and permanent storage

required for high-value data and asset transfers.
Over the past 50 years, the cost of commercially available storage (C_{GBH}) has been decreasing at an annual rate of 30.57% (S. Williams, 2018). Extrapolating the data, the costs of perpetual data storage can be presented as:

$$C_{perpitualdatastorage} = \sum_{0}^{\infty}(Transection\ size * C_{GBM(i)}) \tag{2}$$

where $C_{GBM(i)}$ is the cost of space rent of a gigabyte of data per month at a given month (i). Based on these costs, we derive a transaction fee the user will have to provide to the Humanode protocol for perpetual storage of the transaction.

$$TX_{feeforpermanentstorage} = C_{perpitualdatastorage} * N_{human-nodes} \tag{3}$$

Submitting the transaction, the user pays the cost of perpetual storage to the Humanode protocol, which distributes the fees equally among human nodes. This mechanism ensures that the human nodes costs are covered and creates an incentive to continue operating a Humanode server, ensuring the network's long-term stability.
We note that the guarantee of perpetual storage of data is satisfied even if there is only one replica node online maintaining the pin-set. At the same time, we have to ensure that the network maintains enough available pins on IPFS to keep the full and updated state. Every governor who becomes a Legate has to both maintain a human node and keep the common global state available.
Not all of the transactions are equal. *The size of the transaction changes with the amount of data and computation complexity.* The core functions of the Humanode protocol are to

- register a biometric identity and saving its fully homomorphic encrypted vector permanently pinning it to IPFS;
- perform 1-n matching of FHEd vectors for user and human-node enrollment;
- return an FHEd vector to the client for user authentication:
- process computations to support the operation of Merkle-CRDT algorithm;
- and execute smart contracts.

A particular transaction cost depends on the transaction properties, that is:

- The size of the data in the transaction. For example, interaction with a smart contract requires more data than send-receive operations, hence, the greater size of the transaction.
- The permanence of the transaction. Not all of the data has to be permanent, in many use cases network users are not motivated to incur costs for the future existence of the data among human nodes. They can choose the permanence time of the transaction beforehand.

12.4 External protocol fees in the Humanode network

As the Humanode network uses many components to facilitate the network operations, it requires a protocol to streamline payments to its supporting networks. At the moment it uses Secret Network, enabling a general-purpose secure Multi-Party Computation protocol.
As a human node, launching a replica server requires a number of operations, described in the human node Enrollment process, including communication with the private smart contract on Secret Network.
A user, who wants to process a transaction through the network might require the protocol to

- issue new keys derived from Hierarchical Deterministic (HD) root in the secret smart contract on Secret Network to create easy-to-use ways of signing transactions through privately encrypted biometrics or other authentication methods;
- call Secret network smart contracts to sign a transaction by a previously set biometric modality and perform 1-1 matching or score decryption for authentication (user authentication).

These fees are determined by the external network. Knowing the cost of the fees in HMND, we include them into the user's transaction fee. After receiving external fees, the protocol exchanges HMND into the external network's tokens and sends it as a fee for that transaction.
The total fee for a given transaction is the sum of Humanode protocol computing and storage fees and external protocol fees.

13 Vortex

The concept of a "Decentralized Organized Company" (DAO) was proposed by Daniel Larimer (2013) and implemented in Bitshares in 2014. In 2014, Vitalik Buterin, the founder of Ethereum, an open-source, public, blockchain-based distributed computing platform, proposed that after a DAO was launched, it might be organized to run without human managerial interactivity, provided the smart contracts were supported by a Turing-complete platform (V. Buterin, 2014). Ethereum, launched in 2015 shortly after this publication enables such DAOs. Thereby, DAO clearly designates something broader than the typical definition of "organization"—a social group that brings people together and works toward a common purpose. Vitalik thus defines a DAO as "a decentralized autonomous community" in which all members have a share in the decision making (V. Buterin, 2013), "an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do" (V. Buterin, 2014).
Governance in the Humanode Network will be decentralized from genesis and is to be known as Vortex—the Humanode DAO, a Decentralized Autonomous Organization to rule over the changes. Vortex consists of human nodes, delegators, and governors.

1. *Human node*—a user who has gone through proper biometric processing and receives network transaction fees but does not participate in governance.
2. *Delegator*—a human node who decides to delegate his voting power to a governor.
3. *Governor*—a human node who participates in voting procedures according to governing requirements. If governing requirements are not met, the protocol converts him back to a non-governing human node automatically.

The governors will have different rights according to their ranks. Ranks are based on Proof-of-Time (POT) and Proof-of-Devotion (PoD), meaning that devotion in the system is valued more than the riches one has. Ranks do not give any additional voting powers to their holders, instead they are given an ability to make and promote others' proposals on crucial matters.

Table 11: Governor requirements and tiers

Req \ Tier	Citizen	Senator	Legate	Consul
Need to govern, years	0	1	2	4
Participate in formation	Not required	Not required	Required	Required
Maintain the pin of the full state of the network	Not required	Not required	Required	Required
Have one of your proposals approved by Vortex	Not required	Not required	Not required	Required

The combination of PoT and PoD in Humanode governance means that a governor progresses through ranks based on the time his node was considered governing. On top of that, to progress to a Legate or higher a Governor must participate in Formation, a proposal-based grant mechanism, and maintain available data on the updated state of the ledger of the Humanode network. Even if a governor participates in Formation during the first days of his node's existence, they will still be required to govern for another three years to become a Legate.

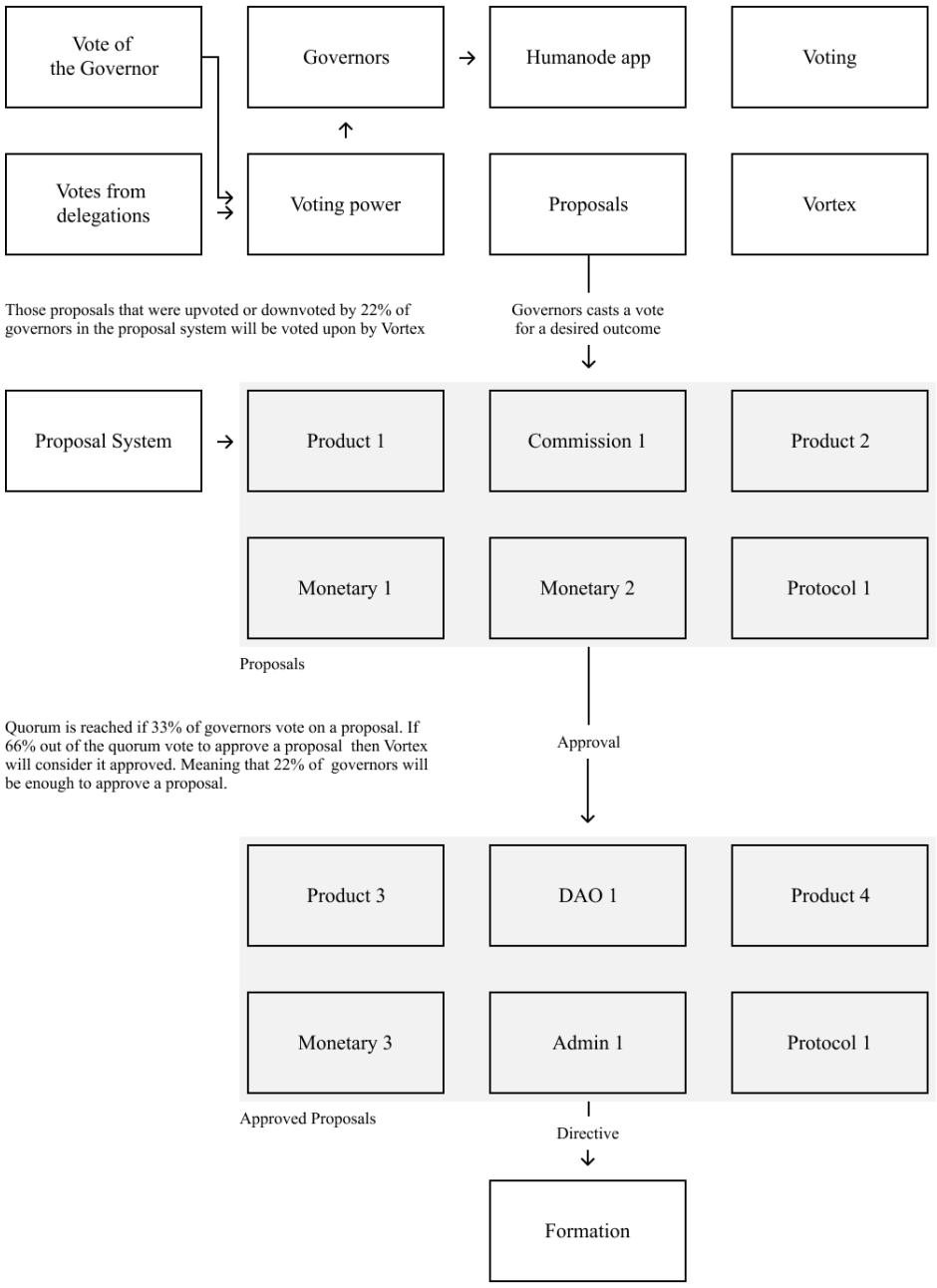
Table 12: Governor rights

Right \ Tier	Citizen	Senator	Legate	Consul
Vote on proposals	Yes	Yes	Yes	Yes
Participate in Formation	Yes	Yes	Yes	Yes
Nominate proposals of non-human nodes	Yes	Yes	Yes	Yes
Receive voting delegation	Yes	Yes	Yes	Yes
Make product proposals	Yes	Yes	Yes	Yes
Fee distribution proposals	No	Yes	Yes	Yes
Monetary policy proposals	No	No	Yes	Yes
Protocol level proposal	No	No	Yes	Yes
Administrative proposal	No	No	Yes	Yes
Vortex core proposal	No	No	No	Yes
Veto	No	No	No	Yes

A quorum is reached if at least 33% of the Governors vote on a proposal. If 66% Governors out of the quorum vote to approve a proposal, then Vortex will consider it approved. This means that 22% of the overall number of Governors will be

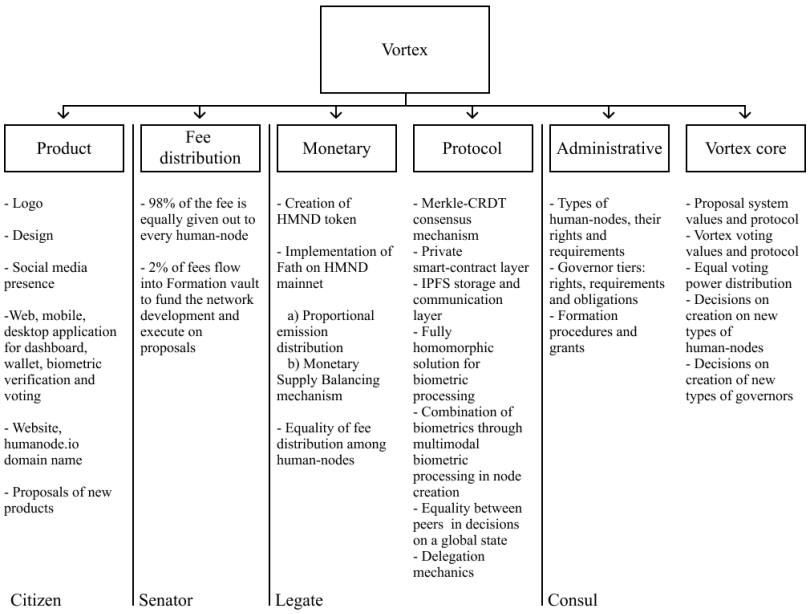
enough to approve a proposal. Human nodes that do not participate in governance are not counted to reach a quorum.
The voting power of each Governor is equal to 1 + the votes of his Delegators.
Any proposal that is pulled out of the proposal pool gets a week to be voted upon in Vortex.
Becoming a part of Vortex gives access to different governing tools based on governor rank. Hypothetically, separation of voting power from proposal rights that are solely determined by time and participation should make the whole system reasonably decentralized, preventing malicious actors from a quick attack on the Humanode network.

Figure 19: Vortex voting procedures



13.1 Vortex default characteristics

Figure 20: Vortex default characteristics



The above-mentioned characteristics will be implemented on top of the Humanode network at the deployment stage.

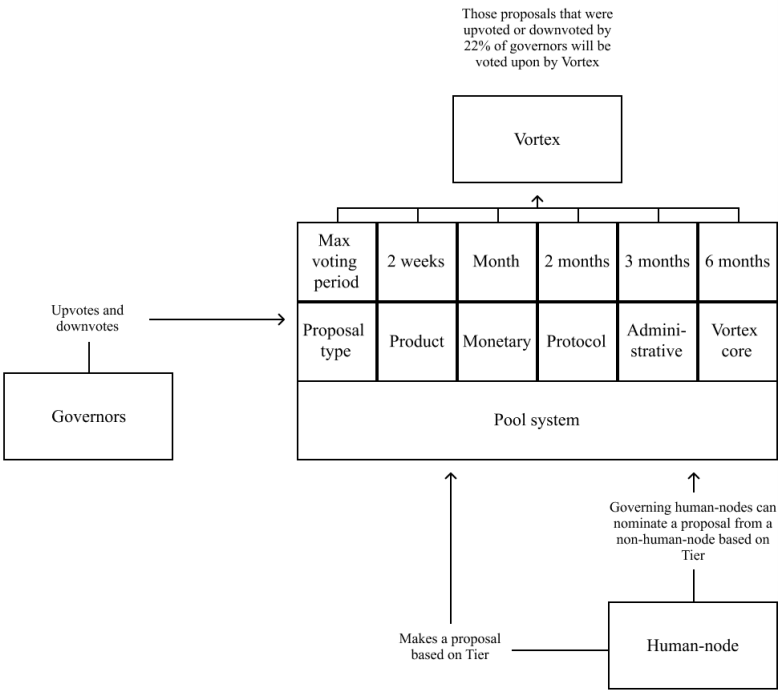
13.2 Veto rights

If for some reason 66% percent of Consuls decide that it is necessary to veto a decision then it will be possible to do so, and the decision will be considered declined by the Vortex. But they cannot veto *the same decision* more than two times *in a row*, meaning that if a proposal is approved thrice then the veto cannot be implemented. Vetoes are important to safeguard the system from panic-based attacks and the dilemma where a minority of professionals might be able to see things clearer than the whole mass of voters. But liberty, public opinion, and democracy should prevail in the end as the Consuls' veto cannot be implemented more than 2 times for a particular decision.

13.3 Proposal system

The two main principles behind creating the Humanode proposal system are to mitigate chokepoints and to keep up the quality of proposals. Governors can participate in every part of the system whilst other human nodes can only make proposals. Non-human nodes cannot propose directly but can be nominated by any Governor to do so. A human node cannot create more than 5 proposals at the same time.

Figure 21: Proposal pool system and voting periods



How it works:

1. A human node casts the proposal into the pool system, defining a header, the voting period, writing a description, adding docs, etc., but more importantly, choosing one of the types of proposals that are available depending on the governing tier.
2. Inside the pool, Governors upvote or downvote different proposals. Each Governor can give each proposal an upvote or a downvote. Each pool consists of different boards: fresh, trending, popular, new, etc.
3. Proposals that receive upvotes or downvotes from 22% of existing Governors are immediately conveyed to Vortex for voting. Proposals that do not receive enough upvotes or downvotes in the max voting period get deleted from the pool and can be proposed again in two weeks' time.
4. The voting procedure in Vortex takes up strictly a week for each proposal to be voted upon.
5. If approved the proposal is conveyed to Formation to receive funding and assemble a team.
6. If declined by Vortex, the proposers must wait out a period of two weeks to propose again.

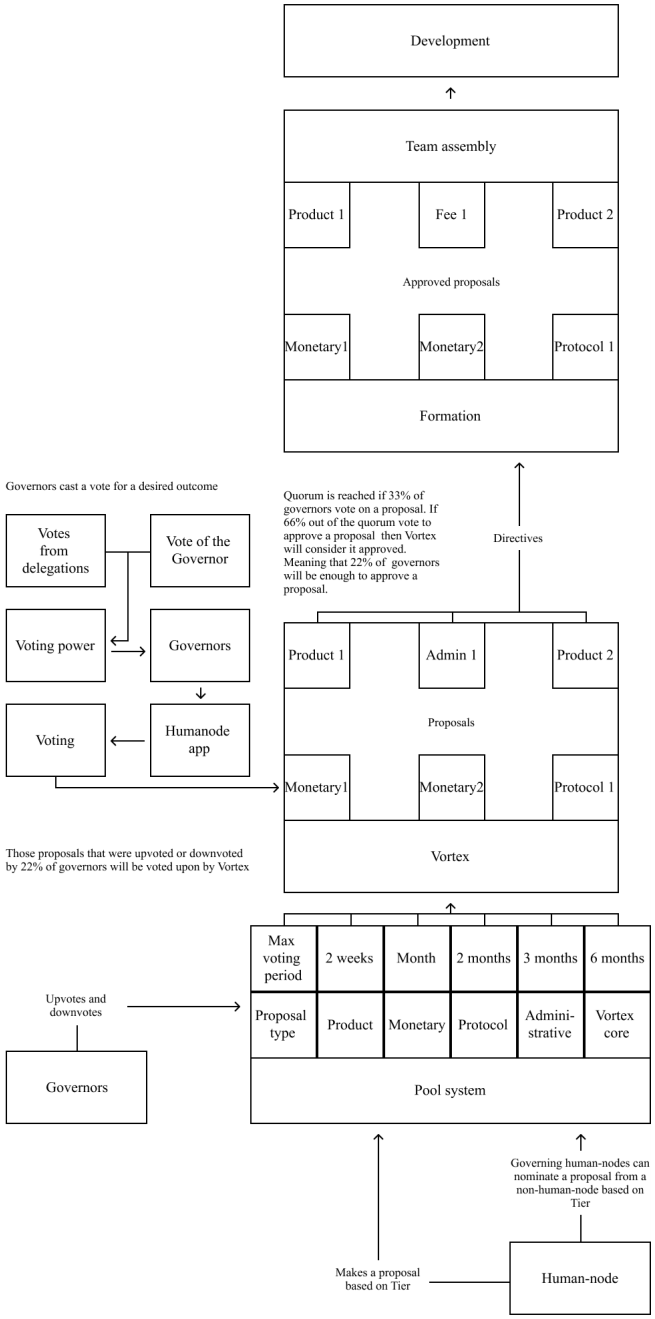
13.4 Formation

Vortex governs the Humanode by deciding on key parameters through the voting power of human nodes.
Formation is a part of the Humanode community. It is a special grant-based development program. It provides grants,

investments, service agreements, and employment. It is dedicated to supporting the Humanode network and all related technologies.
Any human node can join Formation to make a grant proposal or apply to become a part of a team that already develops an approved proposal. Proposals by non-human nodes can only reach Formation if one of the governing human nodes decides to nominate them. Such limitations allow us to protect devoted followers and contributors to the Humanode network.

The process is as follows:

Figure 22: Proposal pool, Vortex and Formation processes



Human nodes create proposals, which is DAO's basic method of making decisions, allocating funding for their implementation, and taking collective action. Governors upvote and downvote them. We assume that 2% of fees go to Formation as the network begins to function. Then, the proposers, i.e., Vortex, will regularly determine the percentage of the fees going to Formation.
The Humanode network's DAO supports a number of different proposal directions.

Generally, Formation funds:

- *Research*: Advancing basic and applied research in cryptography, distributed systems, IPFS, formal verification, economics, and biometrics.

- *Development & Product*: Development turns research into software, while Product turns it into user-experiences. The formation is primarily interested in technologies that expand the Humanode network, its potential, capabilities, and security, as well as the ecosystem.
- *Social Good & Community*: Formation supports community members to bring awareness to open-source, decentralized, and bio-technologies, and scale community outreach for the Humanode network.

In more detail, Humanode Improvement Proposals (HIPs) types are divided into the following categories that are based on the inception characteristics of Vortex:

Product

Changes in the product itself. Max voting period: 2 weeks.

- Logo
- Design
- Social media presence
- Web, mobile, and desktop application for dashboard, wallet, biometric verification, and voting
- Website, humanode.io domain name
- Proposals for new products

Fee distribution

Vortex can change fee distribution. Max voting period: 1 month.

- 98% of the fee is equally given out to every human node
- 2% of fees flow into Formation vault to fund the network development and execute on proposals

Monetary

Modifying Humanode's monetary system and its principles via DAO. Max voting period: 1 month.

- Creation of HMND tokens
- Implementation of Fath on Humanode mainnet

1. Proportional emission distribution
2. Monetary Supply Balancing mechanisms

- Equality of fee distribution among human nodes

Protocol

HIPs are the way to create enforceable change to the Humanode protocol. Max voting period: 2 months.

- Merkle-CRDT consensus mechanisms
- FHEd biometric vector search and matching procedures
- IPFS storage and communication layers
- Combination of biometrics through multimodal biometric processing in node creation
- Equality between peers in decisions on a global state
- Delegation mechanics

Administrative

Max voting period: 3 months.

- Types of human nodes, their rights, and requirements
- Governor tiers: rights, requirements, and obligations
- Formation procedures and grants

Vortex Core
A DAO begins with a defined scope of proposal types to prevent detrimental actions. But it is not supposed to stay narrow. The system will eventually allow the submission of HIPs to do anything possible on the DAO. Simply by submitting proposals, Vortex can go wherever the imagination takes proposers. Max voting period: 6 months.

- Proposal system values and protocol
- Vortex voting values and protocol
- Equal voting power distribution
- Decisions on the creation of new types of human nodes
- Decisions on the creation of new types of governors

The Formation funds are mainly used to maintain the network.
Once a proposal is submitted, it will enter the voting process, where it will either pass or fail.

13.4.1 Assembling a team

We at Humanode core understand how crucial it is to find and coordinate people that are willing to support the proliferation of the Humanode network. That is why we are developing a special team-assembly procedure in the Humanode app that will allow those whose proposals were approved by Vortex to find passionate professionals to assemble their team from among the members of the international Humanode community. All the proposer has to do is send a digital offer to any other human nodes that he thinks are a good fit for his projects. Their proposal must have the public address of the potential member, and it should state working objectives and conditions and have a smart contract that locks some part of the grant for that person in particular.
Proposers—the team (public key-role).

- Full team
- The team is partially assembled
- No one in the team yet

If the proposal for grant in Formation does not include the team, it may be selected from the human nodes who are interested in the proposed project.

13.4.2 Slashing

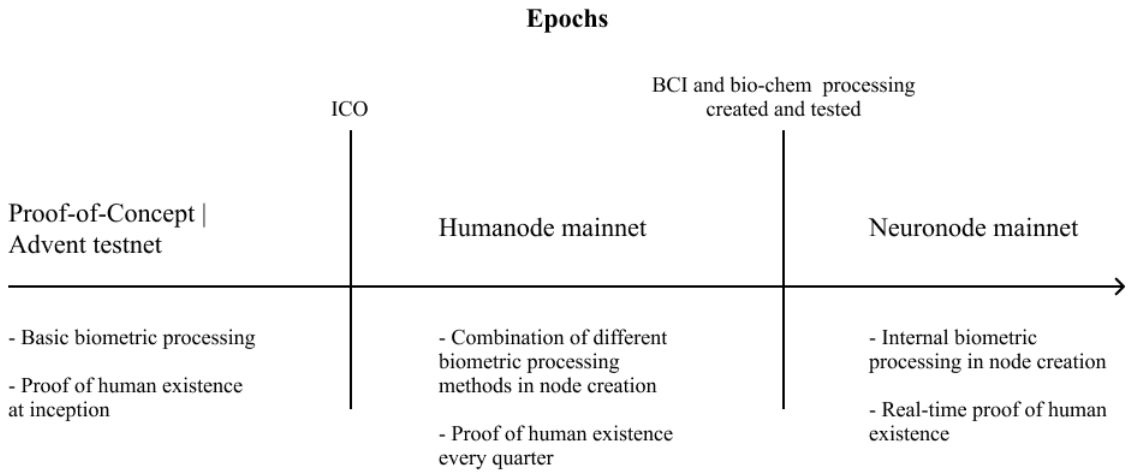
If the recipients of the Formation's grant do not fulfill their obligations they are slashed.
We believe that it is essential to establish a system to prevent and punish behavior that could be malicious and to ensure a complete balance in the system. Slashing has therefore been put in place to provide a durable solution while guaranteeing the integrity and durability of the system.
Slashing periods:

- 2 weeks
- 1 month
- 3 months
- 1 year
- 3 years
- 10 years
- Forever

Slashing mechanisms and conditions are presented in the 'Slashing system' sub-paragraph of the Merkle-CRDT mechanism between equal human nodes leveraging IPFS.

14 Strategic roadmap

Figure 23: Epochs in the Humanode network



In our research, the Humanode core came to agree that the Humanode network should have two main epochs that are defined by two factors: the external existence of keys and how often proof of human existence occurs. In our opinion, these two factors also shape the way people accept becoming a part of the Humanode network.

The first factor is derived from the problem connected to 3D-printers. If we consider that every year 3D-printing becomes more accurate, then sooner or later models will be able to be printed that can emulate floating points even for top-notch neural networks and they will not be expensive to produce. Since the very first creation of keys as a tool to store something that you do not want to easily fall into the hands of strangers or malicious actors, keys have always existed externally. Even when humanity learned to digitize keys, we still used some virtual plane of existence to store them. Modern biometrics are also based on keys stored externally because most companies use external floating points (iris scans, fingerprints, nose, palm, ears, etc.). Malicious actors may try to steal your biometric data and use a futuristic 3D printer to print all those floating points to bypass the biometric processing protocol. We can mitigate this angle of attack by removing the key from the external world per se and putting it inside a human body. There are a lot of ways to do so, but the most common are biochemical, DNA-signature, and brain-computer Interfaces (BCI). If the network is built so that node creation is possible only through internal biometric processing, where keys do not exist externally then the mechanism becomes tremendously impenetrable. At some point, Humanode will have to transcend to this kind of verification of human existence. Before the implementation of internal biometric processing protocols is complete, Humanode will use multimodal biometric processing with liveness detection and soft biometrics, which also make such an attack nearly impossible.

The second factor consists of two main sub-factors: real proof of human existence and fee distribution. Let us imagine that somehow we create tech that emulates internal biometric processing with such accuracy that it bypasses the system and is able to generate an artificial proof of human existence. If the Humanode network demands verification every quarter then a malicious actor would be able to create many identities without additional challenges in bandwidth and computing power. But if the Humanode network requires proof of existence every, let us say, half a minute, then it would be very hard and costly to carry out such types of attacks, considering that the biometric process protocol itself has an incorporated neural network that distinguishes emulations from real data by detecting liveliness. The second sub-factor is all about fees. Fees are built in such a way that they are equally distributed among every node that exists in the network. If Humanode requires proof every quarter then if some human, unfortunately, ceases to exist, his node would still receive rewards until the end of a quarter.

Table 13: Humanode strategic road map

2020	2021	2022	2023
• Whitepaper • Basic biometric processing • CRDT consensus mechanism • HMND testnet • Client application • Human-node creation • Fully homomorphic encryption for biometric data	• ICO • Humanode network • HMND Fath on human nodes • Combination of biometrics in node creation • Vortex creation • BCI biometric processing research and tests • Support of Wasm-based smart-contracts	• BCI neurosignatures for biometric processing in node creation • Bio-chemical biometric processing • Ethereum interoperability • Modular development framework • Regulatory compliance framework	• Real-time proof of human existence • Internal biometric processing in node creation • Private computations on Humanode consensus • Biometric avatars • Multi-purpose microchip implant compatibility

14.1 2020

In the first year, the Humanode team will focus on delivering a working concept in a form of a testnet–based mobile application that allows early testers to deploy human nodes with biometrics and participate in Merkle-CRDT consensus to verify transactions on the Humanode network. We are to use fully homomorphic encryption for biometric data. We will concentrate on finding early backers that will help us build and grow.

14.2 2021

Before conducting the ICO, the Humanode team must build an HMND token based on Fath monetary policy, a multi-modal biometric processing method that combines different biometrics in replica creation, a working DAO called 'Vortex', as well as several types of applications that safely conduct biometric processing. Humanode will hold an ICO during which most of the tokens will be sold to the public. After the ICO, the Humanode network will be initialized and the Humanode team will deliver a proposal to Vortex containing all the tasks and objectives mentioned in this paper, and if Vortex approves it, further development will commence. We also plan to start conducting BCI biometric processing experiments and integrate the support for WASM-based smart contracts and Inter-Blockchain Communication.

14.3 2022

The Humanode team will concentrate its efforts to finalize the creation of BCI neurosignatures and other types of internal biometric processing such as DNA-signatures and biochemical solutions. This transcendence, as mentioned above, will strengthen the protection of the Humanode network. Besides biometric processing, the team will continue upgrading and researching the Merkle-CRDT consensus mechanism to understand its limitations, try to overcome them, and also provide Ethereum-interoperability. Another very important task is to create a modular development framework so that any developers that would like to create something on top of the Humanode network will be able to do so with greater ease. Somewhere by the end of the year, we will be rolling out regulatory compliance frameworks that will provide interaction between human nodes and different judicial systems of the world.

14.4 2023

The Humanode team will focus on delivering the tech that makes real-time human existence verification possible and approaching the goal of node creation only through internal biometric processing protocols. Besides this, we will implement a private computational layer run by human nodes. We plan on developing a biometric avatar that might become a new method of signing transactions and explore and research multi-purpose microchip implant projects to deliver Humanode network compatibility, broadening available authentication schemes.

15 18 month "Road to Mainnet"

15.1 2020

November

- Whitepaper
- Basic biometric processing
  - Face
  - Voice
- Private smart-contracts for biometric search and matching
- Website

December

- Merkle-CRDT consensus mechanism
- Humanode mobile app private alpha testing
- Humanode forum deployment
- FHE biometric processing
- HMND token testnet
- Web app
- Early backer community development

15.2 2021

January

- Transactional Fath protocol
- Proposal pool system
- Desktop app
- DAO forums in Humanode app

February

- Convolutional neural network biometric processing training protocols
- Governor tier system
- Passive neurosignature biometric protocol

March

- Vote delegation
- WASM-based smart-contracts
- User domains on the Humanode network
- Fath emitting algorithm

April

- Human-node creation
- Fath on human nodes

May

- Vortex DAO testing
- Voting system and procedures testing

June

- Formation in app
- Team assembly mechanism
- Formation vault

July

- Fath HMND token on human nodes testnet
- Slashing mechanism implementation

August

- Multi-modal biometric processing

September

- Humanode mainnet
- Multi-level biometric wallet keys

October

- Vortex mainnet
- Private smart-contracts for identification

November

- Formation deployment
- Neurosignature node creation tests

December

- Community development programs
- Private HMND network creation
- Token creation on HMND network

15.3 2022

January

- DNA biometric processing protocols
- Ethereum interoperability

February

- Modular development framework

March

- HMND Fath testnet on neurosignature human nodes

April

- Regulatory compliant framework for HMND Fath token
- Internal multi-modal biometric processing

16 Discussion

16.1 Gradual decentralization

Obviously, the Humanode network relies on the activity of its Governors. Besides building the technological solutions stated in this paper, the Humanode core will promote full transparency of governing processes and transactions, design and deploy decentralized governing processes, participate heavily in the Humanode community, and make development proposals. The Proposal Pool System– Vortex–Formation governance stack was designed by the Humanode core to create a hybrid Proof-of-Time/Proof-of-Devotion/Proof-of-Human-Existence safeguarded network. This implementation allows us to lower the influence of the problems that affect any system that tries to integrate democratic procedures:

1. Voter apathy is a very widespread problem that entangles every single voting system. The biggest part of this problem is the inability to reach a quorum. The Humanode network demands governance participation from Governors and proof of existence from all human nodes. Those Governors who do not fulfill quarterly governing conditions (either they did not make proposals that were approved or declined or did not vote on any proposal) are automatically converted to non-governing. Quorum is reached if 33% of Governors vote upon a proposal, so it means that only voices of those who actively participate in governance are calculated to reach a quorum.

2. Masses are often mistaken. It is common sense that a small, dedicated group of professionals with years of experience would be able to give a more precise and correct opinion on a particular voting matter than a mass of people with different backgrounds and education. To balance the democratic approach with professional education and experience, Humanode core came up with a hybrid Proof-of-Time/Proof-of-Dedication governance system named "Vortex", in which Governors have different tiers. They can be promoted in tiers if certain requirements are met. This way the protocol gives more tools and proposal rights to those who have more experience and have proven their devotion through Formation.

3. Inability to directly delegate your vote to any other voter in a system creates many different forms of how the voting procedures take place. The very systems of how electoral delegates are chosen have loopholes that allow political tricks such as gerrymandering and filibustering. Human nodes are designed to be equal in voting power; at the same time the voting mechanisms allow you to delegate your vote to any other human node without boundaries. A Governor's voting power equals 1+ amount of delegations he has.

As we try to balance freedom with safety and quality we were faced with two options: to either be a centralized company that just does everything on its own until it is working optimally or decentralizing it and building on a devoted community. The first approach surely has its advantages in terms of coordination and speed, but it is authoritarian, and Humanode is not. But if we chose the second option, the Humanode network would be at a larger risk, as it is going to be quite small at first. So to solve this dilemma, instead of choosing one out of the two approaches we came up with a third solution. We decided that all members of Humanode core will receive a Consul tier at the deployment phase so that we as founders and developers would have the ability to lead a more centralized approach in governance at first. Decentralization is guaranteed because of two reasons: 1) In four years other Consuls will emerge; 2) Any decision still has to be voted upon by Governors. This way we can concentrate on development and deliver everything that we laid out in this paper, but at the same time, the protocol guarantees that the system itself will definitely become more and more decentralized and the Humanode core's weight will be diluted. Another authoritarian point is that in the first two years of Humanode's existence proposals that require grants from Formation must be voted upon by 66% of the Consuls to be approved. This precaution is taken to defend the Formation vault from many angles of attacks that persist in decentralized permissionless public networks.

16.2 The iron law of oligarchy

"Who says organization, says oligarchy".
"Historical evolution mocks all the prophylactic measures that have been adopted for the prevention of oligarchy."

-Robert Michels

This hypothesis was developed by the German sociologist Robert Michels in his 1911 book, 'Political Parties.' It states that any organizational form inevitably leads to oligarchy as an 'iron law'. Michels researched the fact that large and complex organizations cannot function efficiently if they are governed through direct democracy. Because of this, power within such organizations is always delegated to a group of individuals.
In Michels's understanding, any organization eventually is run by a class of leaders regardless of their morals or political stance. Monarchies and republics, democracies and autocracies, political parties, labor unions, and corporations, etc. have a nobility class, administrators, executives, spokespersons, or political strategists. Michels stated that only rarely do representatives of these classes really act as servants of the people. In most cases, people become pawns in never-ending games of power balancing, networking, and survival. Regardless of the inception principles, the ruling class will always emerge and in time it will inevitably grow to dominate the organization's power structures. The consolidation of power occurs for many different reasons, but one of the most common ways is through controlling access to information.
Michels argues that any decentralized attempts to verify the credibility of leadership are predetermined to fail, as power gives different tools to control and corrupt any process of verification. Many different mechanisms allow serious influence on the outcome of democratically made decisions like the media. Michels stated that the official goal of representative democracy of eliminating elite rule was impossible, that representative democracy is a façade legitimizing the rule of a particular elite,

and that elite rule, which he refers to as oligarchy, is inevitable (J. L. Hyland, 1995, p. 247).
This law is directly applied to modern elites. The financial system is always a complex multi-layer construct that requires a great deal of administrative and organizational power. According to Michels, such a system would inevitably become oligarchic. While designing the basic principles of the Humanode network and Vortex, the Humanode core was faced with a challenge to find a delicate balance between organizational efficiency and the democratic involvement of the masses. We believe that a combination of voting power equality, direct delegation, Proof-of-Time, Proof-of-Dedication, and Proof-of-Human existence would make a very balanced and just system, but it will not solve the problem of 'Iron Oligarchy,' as a leadership class will definitely emerge.
Fiat credit-cycle systems have large financial entities, PoW networks are faced with miner cartels, PoS systems have validator oligopolies, and Humanode has Consuls and research groups. Governors have different proposal rights based on different tiers. Consuls have absolute freedom in proposal creation as they can put forth an idea of any type and they wield a right to veto any decision that is approved by Vortex twice. Legate and Consul freedom of authority is balanced out by the voting mechanism that requires a quorum and an absolute majority of those voting for a proposal to be approved. As the absolute majority of Governors is required for a decision to be approved it negates the ability of Legates and Consuls to approve something against the will of the majority of voters.
In a perfect world where all participants of the network actively govern, this balancing effort should be just enough to minimize the influence of any type of oligopoly that might emerge in the Humanode network, but we do not live in a perfect world. Apathy of voters is a scourge to most of the voting systems that exist and creates the necessity of vote delegation, which has its own advantages and disadvantages.

16.3 Vote delegation

Problems of vote delegation have always accompanied any large democratic system. The core problem of democracies in their purest form is that they are very vulnerable to the Byzantine Generals Problem (BGP). Any system has a critical point of failure. Large systems tend to have several or dozens. Because of this, any democratic system requires institutions built on top to protect those critical points. These institutions limit the direct voting of the masses on crucial matters. There are four main reasons why these limitations are a necessity.

1. *Strategic resources, critical points, and stability.* Any system has a sensitive part. For example, some countries wield nuclear bombs and have democratic political systems. The vote on the deployment of nuclear weaponry is commonly restricted to a very small group of individuals. It makes sense that such an important spectrum would be heavily guarded against any angle of attack, especially BGP. That is why this part of the system requires consolidation of power, and an autocratic approach in decision-making. Besides weapons of mass destruction (WMDs) there are financial, energetic, military, trading, diplomatic, intelligence, etc. chokepoints that unless safeguarded can be used by the enemies of that system to cause catastrophic events and lead to destabilization.

2. *Apathy of voters and effectiveness.* Lack of caring among voters in voting procedures can lead to a halt in governance, as most voting requires some kind of a quorum. If apathy is strong enough to stop a quorum from being raised then the governance process stops until a quorum is reached. Some operations and decisions require the constant active involvement of voters, which is where delegation comes in hand. Ordinary people do not want or have time to participate in governance, which is why in representative democracies citizens can cast their vote to elect representatives that are actively involved in decision-making. The fewer people participate in voting, the easier it is to coordinate.

3. *Technological limitations.* Before the digital era, there was no effective way to conduct voting procedures, as communications were not as developed as they are now. Without proper confirmation of identity and support of modern tech, it was hard to imagine a way to conduct large direct voting without putting strain on administrative resources. Delegating to a politically active person negates the necessity to use sophisticated technologies to conduct legislative procedures.

4. *Misrepresentation.* In most democracies your vote is restricted by the region you are geographically located in, meaning that you can cast a vote for a nominee tied to your constituency, but he might not get elected, meaning that your vote was practically burned and a person that you did not vote for might be representing you. Most governing systems lack the freedom of vote delegation, as you cannot directly delegate your voice to a particular person.

While devising the voting procedures for Vortex, the Humanode core has kept in mind the principles mentioned above. The Governor tier system safeguards critical points by limiting the abilities of the electorate to create proposals but at the same time, the autocratic chokepoint is balanced out by requiring a quorum of Governors to approve created proposals. The influence of apathy of voters is limited by demanding voting activity from human nodes to be counted as Governors. This way only active participants of the network are counted in reaching a quorum. The technological progress in decentralized autonomous organization deployment and biometric processing in the last decade has brought forward a way to overcome the obstacles of the past connected to direct voting procedures and the uniqueness of voters. Delegation of voting power is permissionless meaning that any human-node can delegate its vote to any Governor in the Humanode network. We acknowledge that even with modern approaches to voting and technological breakthroughs, a delegation mechanism in the Humanode network is a natural necessity.

The digital revolution has paved the way for technologies that allow us to create systems with liquid representative democracies. Compared to traditional representative democracies, a voter can re-cast his vote any time he wants, without the necessity to wait for years to do it again. Vote delegation can be changed anytime. Delegated Proof-of-Stake (DPoS) protocols implemented liquid democracy for delegating transaction validation operations to professional entities. As the validators are safeguarding the protocol and receive a commission for their operation, the voter's choice is usually driven by economic incentives: how commission size, uptime, and security of the delegate's server might reflect on voter's earnings. Is that enough to choose an opinion representative in a decentralized network? Most DPoS networks have a strict unbounding period that can last up to two weeks or even months. This measure is a necessity to safeguard from manipulated panic-based market crashes where delegators undelegate their tokens and sell them in fear of losing value. In the Humanode network, voting power is not entangled with a token, which is why there is no need for unbounding periods. Any time a human-node wishes to re-cast or simply retrace its delegation it can be done instantly.

16.4 Populist tide and professional backslide

It is commonly acknowledged that any voting system is faced with populism.
Hypothetically there are two major approaches to how populism is perceived:

1. Populism poses a threat to democratic stability. According to recent studies, conducted by Jordan Kyle and Yascha Mounk of the Tony Blair Institute for Global Change, one of the key findings they have had is that Populists are far more likely to damage democracy. Overall, 23 percent of populists cause significant democratic backsliding, compared with 6 percent of non-populist democratically elected leaders(J. Kyle & Y. Mounk, 2018). In other words, populist governments are about four times more likely than non-populist ones to harm democratic institutions.

2. Populism is a necessary corrective mechanism that addresses popular problems and limits the power of elites.

Regardless of which view is more accurate populism is acknowledged to be a very powerful tool to gather the support of the masses in democratic systems. The main danger perceived by the Humanode core is the rise of populists in that individuals that know how to be popular do not necessarily have the intelligence, professional qualities, experience, or profound knowledge on the subjects they have to make decisions upon on a regular basis.

In the Humanode network, every human node has a voting power of 1. Voting delegation in Humanode allows for any human node to delegate their voting power to any governor in the network. Governor power equals 1 + the amount of delegations from other human nodes. Such a system allows limitless crowdsourcing possibilities as delegation is liquid and not regionally bound. As in any other democratic system, individuals that possess oratory, diplomatic skills and are backed by influential media sources have an advantage in the Humanode network. An introvert with sociopathic tendencies possessing a very professional skill set for decision-making operations will most likely receive less support than a good negotiator, orator, and crowd controller that possesses a mediocre skill set.

In Vortex voting procedures, Governors have disproportionate voting power and those governors that have more delegations have more power. The professional backslide in our understanding poses a threat to the effectiveness, progressiveness, and constant optimization of governance. We fear that without Proof-of-Devotion, which is in a way a proof of having some kind of professional skill set, any democratic system faces becoming a plutocracy, where the wealthiest members control influential and credible media sources to direct the opinion of masses and drive support to candidates of their choosing.

Proof-of-Devotion might bring a small balance to populism upheaval, as it demands participation in Formation to receive proposal rights on critical matters. Nevertheless, consuls wielding huge delegations will inevitably emerge and their stance in decision-making mechanisms will be very strong. The only way to limit their influence is direct and active participation of human nodes in governing processes. The more overnors that do not delegate their vote and actively participate in governance the less authority can be accumulated in the hands of those that seek it.

17 Conclusion

In this paper, we have introduced an alternative to modern decentralized financial systems—the Humanode network safeguarded by private biometrically encrypted human nodes. Using FHE of feature vectors for biometric processing and the Merkle-CRDT algorithm, the Humanode protocol achieves strong eventual consistency and causality of events. Anyone can deploy a human node by staking their encrypted biometric data.

The proposed approach can potentially lead to the creation of a public, permissionless financial system based on human existence with algorithm-based emission mechanisms targeting real value growth and proportional issuance distribution.

Before we can deploy the Humanode network, many challenges must be overcome. The creation of a public and permissionless protocol based on the Merkle-CRDT mechanism might introduce a new way of transacting value in a decentralized manner. Much work and many tests on multi-modal FHEd biometric processing will be carried out before we consider them to be safe enough for users. Vortex as a DAO governing layer should provide enough flexibility and precision in decision making, but there are many more tweaks that should be addressed before Vortex becomes optimized for large and simultaneous governing processes. The Fath monetary protocol hypothetically should lower the long-term effects of devaluation but as we converge from transactional-based Fath to real value creation-based Fath, many improvements must be made before the latter can be implemented. We hope that with Humanode's community effort we will be able to overcome any challenges that stand in the way of creating a decentralized, public permissionless financial network based on Proof-of-Human existence through biometrically encrypted human nodes with equal fee distribution, algorithm-determined issuance, and proportional distribution of emission.

Strength comes with the unity of passionate but rational minds. Change should not be associated with violence. You can be the change itself if you are willing to dedicate yourself to a higher purpose. When you finish reading this paper the only question we sincerely ask you to answer, but only to yourself, is whether you are willing to become a human node, or not?

18 References

Almeida P. S., Shoker A., and Baquero C. (2015) Efficient State-based CRDTs by Delta-Mutation.
Benet J. (2014) IPFS - Content Addressed, Versioned, P2P File System.
Blau T. (2020) Verifying Strong Eventual Consistency in δ-CRDTs.
Bolle R.M., Connel J.H., Ratha N.K.(2002) Biometrics perils and patches.
Buterin V. (2013) Ethereum Whitepaper.
Choudhury B., Then P., Isaac B., and Raman V. (2018) A Survey on Biometrics and Cancelable Biometrics Systems.
Davida G., Frankel Y., Matt B.J.(1998) On enabling secure applications through off-line biometric identification.
Douceur J. R. (2002) The Sybil Attack.
Ford B. and Bohme R. (2019) Rationality is Self-Defeating in Permissionless Systems.
Goudelis G. et al. (2009) Emerging biometric modalities: A survey.
Jaiswal S. et al. (2011) Biometric: Case Study. Journal of Global Research in Computer Sciences.
Jain et al. (1999) Biometrics. Personal Identification in Networked Society.
Jin A.T.B, Ling D.N.C, Goh A. (2004) Biohashing: Two factor authentication featuring fingerprint data and tokenised random number.
Jisha Nair B.J., Ranjitha Kumari S. (2015) A Review on Biometric Cryptosystems.
Kamaldeep (2011) A Review Of Various Attacks On Biometrics System And Their Known Solutions.
Kaur G. et al. (2014) Comparative Analysis of Biometric Modalities.
Kleppmann M. (2015) A Critique of the CAP Theorem.
Kyle J. and Mounk Y. (2018) The Populist Harm to Democracy: An Empirical Assessment.
Merkle R. C. (1998) A digital signature based on a conventional encryption function.
Raju A.S., Udayashankara V. (2018) A Survey on Unimodal, Multimodal Biometrics and Its Fusion Techniques.
Rathgeb C. & Uhl A. (2011) A survey on biometric cryptosystems and cancelable biometrics.
Sabhanayagam T., Prasanna Venkatesan V., and Senthamaraikannan K. (2018) A Comprehensive Survey on Various Biometric Systems.
Sanjuan H., Poyhtari S., Teixeira P., Psaras I. (2020) Merkle-CRDTs: Merkle-DAGs meet CRDTs.
Sadeghi S. & Maleki A. (2018) Recent Advances in Hybrid Brain-Computer Interface Systems: A Technological and Quantitative Review.
Shapiro M. et al. (2011) Conflict-free Replicated Data Types.
Schroff F., Kalenichenko D., Philbin J. (2015) FaceNet: A Unified Embedding for Face Recognition and Clustering.
Streit S., Streit B. and Suffian S. (2017) Privacy-Enabled Biometric Search.
Syarif M.A., Ong T.S., Teoh A.B.J., Tee C. (2014) Improved Biohashing Method Based on Most Intensive Histogram Block Location.
Teoh A.B.J., Kuan Y.W., Lee S. (2008) Cancellable biometrics and annotations on BioHash.
Weaver A.C. (2006) Biometric Authentication.
Williams S. (2018) Arweave: A Protocol for Economically Sustainable Information Permanence.
Zyskind G., et al. (2015) Enigma: Decentralized Computation Platform with Guaranteed Privacy.