Humanode

Whitepaper v. 0.9.6 "You are [not] a bot"

Dato Kavazi, Victor Smirnov, Sasha Shilina, MOZGIII, MingDong Li, Rafael Contreras, Hardik Gajera,Dmitry Lavrenov, and the Humanode Core

September 28, 2021

Abstract

The pursuit of new decentralized financial networks 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 are unable to overcome plutocratic governing systems that derive from the principles upon which Proof-of-Work (PoW) and Proof-of-Stake (PoS) heavily rely. 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 their various core technologies have their own advantages and disadvantages. This paper aims to describe an alternative to modern decentralized financial networks by introducing the Humanode network. Humanode is a network safeguarded by cryptographically secure bio-authorized nodes. Users will be able to deploy nodes by staking their encrypted biometric data. This approach can potentially lead to the creation of a public, permissionless financial network 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 network:

- a bio-authorization module based on cryptographically secure neural networks for the private classification of 3D templates of users' faces
- a private Liveness detection mechanism for identification of real human beings
- a Substrate module as a blockchain layer
- a cost-based fee system
- a Vortex decentralized autonomous organization (DAO) governing system
- a monetary policy and algorithm, Fath, where monetary supply reacts to real value growth and emission is proportional

All of these 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 liveness detection and internal multimodal biometric processing methods that, implemented properly, will 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 network that relies on the existence of human life.

Archived copy · cryp2nova.com

Contents

1 Introduction **4**

2 Humanode network **5**
2.1 Cryptobiometric blockchain protocol . . . 5

3 Humanode's goals and objectives **6**
3.1 Solutions for governments . . . 7
3.2 Shout-out to white hats . . . 8

4 Cryptobiometric blockchain protocol **8**
4.1 Rust . . . 8
4.2 Substrate . . . 8
4.3 Components . . . 9
4.4 Consensus agnosticism . . . 11
4.5 Residual increase in the number of human nodes . . . 11
4.6 Ethereum compatibility . . . 11
4.7 Slashing system . . . 11

5 Fath **12**
5.1 Transaction-based emission algorithm example . . . 16
5.2 Implications of the transaction-based Fath system for a distributed network economy 17

6 Biometric approach to user identification **17**
6.1 Humanode bio-authorization overview . . . 18
6.2 Convolutional neural network . . . 19
6.2.1 Convolution layer . . . 20
6.2.2 Pooling layer . . . 21
6.2.3 Fully connected layer . . . 22
6.2.4 Activation layers . . . 22
6.3 Cosine similarity for feature vector matching . . . 23
6.4 Active and Passive Liveness detection . . . 24
6.5 Merits and demerits of biometric identification . . . 25
6.6 Cryptobiometric search and matching operations . . . 26
6.6.1 Cosine similarity encryption . . . 27
6.6.2 Homomorphic encryption . . . 27
6.7 Extracting inner product from the encrypted value . . . 29
6.8 ZKP for verifiable computation . . . 30
6.8.1 Humanode approach to ZKP . . . 31
6.8.2 ElGamal Cryptosystem . . . 33
6.8.3 Zero-knowledge–proof system for liveness detection . . . 33
6.8.4 Collective Authority . . . 34
6.9 Humanode's multimodal biometric approach . . . 34
6.9.1 Neurosignatures and other emerging biometric modalities . . . 38
6.9.2 Biometric Identification Matrix . . . 38
6.9.3 Humanode Biometric Modalities Score . . . 41
6.10 Types of attacks on biometric systems and their solutions . . . 42
6.10.1 Attack on the sensor . . . 43
6.10.2 Replay attack . . . 46
6.10.3 Attack on the channel between the database and the matcher . . . 46
6.10.4 Attack on the database . . . 46

Archived copy · cryp2nova.com

6.10.5 Overriding the final decision . . . 46
6.10.6 Overriding the feature extractor . . . 47
6.10.7 Override matcher . . . 47
6.10.8 Synthesized feature vector . . . 47
6.10.9 Reconstruction attack . . . 47
6.11 Neurosignatures . . . 48
6.12 Humanode's approach to identity attack prevention . . . 50
6.12.1 Self-sovereignty . . . 51
6.12.2 Privacy-preserving . . . 51
6.12.3 Sybil resistance . . . 51

7 Transaction fee economics of the Humanode network **54**
7.1 Capital-based consensus mechanisms . . . 55
7.2 Cost-based fee system . . . 55

8 Vortex **56**
8.1 Tiers and proposal types . . . 59
8.2 Veto rights . . . 60
8.3 Proposal system . . . 60
8.4 Formation . . . 61
8.4.1 Assembling a team . . . 64

9 Discussion **64**
9.1 Gradual decentralization . . . 64
9.2 The iron law of oligarchy . . . 65
9.3 Vote delegation . . . 66
9.4 Populist tide and professional backslide . . . 68

CRYP2NOVA

Archived copy · cryp2nova.com

1 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 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 maintain privacy while liveness detection error probabilities decline by the day.

Humanode is a network based on cryptographically secure bio-authorized nodes. Using solutions that provide private search and matching operations and liveness detection algorithms, users will be able to deploy nodes to create a public permissionless financial network based on consensus between human nodes who share the fees and ownership of the network in an equal manner.

Modern decentralized verification systems rely on the concept of material obligations to prevent 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 in which 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 attack. The Humanode network will prevent malicious activity by blacklisting biometric data, meaning that your biometric identity becomes the stake.

Human nodes are created through cryptobiometric authentication, which is a combination of cryptographically secure matching and liveness detection mechanisms to verify the uniqueness and existence of real human beings. Thus, the user's pseudonymous biometric identity becomes the stake that gives access to the creation of a node 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 the right to launch human nodes is not entangled with a native token, it allows the implementation of any monetary system without the necessity of conforming to the requirements of capital-based Sybil-defense systems. With human nodes replacing staked assets, it is now possible to avoid a disproportion of token emission 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 a 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 who they are, can become a human node, as long as that person has access to devices that can conduct biometric processing (for example, a smartphone with a camera and biometric processing applications for recognition) or other verified hardware. The system delivers the equality of every single human node by deriving only one node from one biometric identity and mitigates any disproportion of power due to reward equality of individuals. As the system implements the Fath hypothesis, which negates the effect of devaluation on agents of the system, this narrows gaps between the users of the network as the emitted value is distributed proportionally to every participant.

Archived copy · cryp2nova.com

The main goal of Humanode is to create a stable and just financial network 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 deliver easy node creation flows and make it natural for any human to verify their unique existence privately in any digital service. 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.

2 Humanode network

The Humanode network is a protocol that can prove one's unique identity through private biometric authentication schemes and grant permission to launch a node and verify transactions running a public permissionless network based on collective human existence.

The core stack of technologies enabling human node technology include:

2.1 Cryptobiometric blockchain protocol

Substrate

- Single node per person invariant (bio-authentication consensus)
- EVM compatibility

Cryptobiometric neural networks

- Zero-Knowledge proven active and passive liveness Detection
- ZK-proven encrypted face feature extraction
- Distributed encrypted feature search and matching

Distributed economy

- Cost-based network fees
- Fath as the monetary policy and algorithm targeting real value growth and proportional emission.

Humanode/Vortex DAO

- Proposal pool system
- On-chain voting "Vortex"
- Formation

Archived copy · cryp2nova.com

3 Humanode's goals and objectives

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 problems connected to presentation attacks. If we consider that every year 3D (or even 4D) printing becomes more accurate, then sooner or later models will be able to emulate floating points even for top-notch neural networks and 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 modalities (iris scans, fingerprints, nose, palm, ears, etc.). Malicious actors may try to steal your biometric data, using a futuristic printer 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 signatures, and brain-computer interfaces (BCIs). 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 external multimodal biometric processing with liveness detection.

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 month then a malicious actor would be able to create many identities without additional challenges in terms of 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 processing 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 month, then if some human, unfortunately, ceases to exist, his node would still receive rewards until the end of that month.

Humanode's long-terms goals and objectives:

- Sybil resistance based on decentralized pseudonymous biometric identities
- secure, scalable, efficient, consistent, immutable, and sustainable Substrate mechanism
- creation, proliferation, and development of a strong and dedicated community of human nodes
- custom low-latency high-throughput Sybil-resistant consensus protocol
- privacy-preserving biometric processing protocols
- distributed encrypted biometric templates matching
- ZK-proven liveness check
- EVM compatibility with the Substrate pallet
- native Humanode applications (wallets, etc.)

Archived copy · cryp2nova.com

- biometric ownership;
- integration with EVM-compatible applications
- rich integration into Substrate ecosystem
- Humanode token (HMND) with Fath monetary system, equal fee distribution, and proportional emission distribution on the Humanode network
- Vortex, a DAO that regulates the existence of the 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 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
- cryptobiometric applications that deliver proper flows in UX/UI
- multimodal biometrics
- ability to deploy Fath-based monetary systems
- ability to deploy your own tokens on Humanode with different monetary policies and systems
- Humanode development framework with modular solutions
- judicial system framework;
- BCIs for liveness detection
- neurosignatures for signing on-chain transactions
- internal modalities-based biometrics (neurosignatures, DNA matching)
- real-time proof-of-human-existence
- biometric-based Autonomous Intelligent Agent
- ZK offchain commitment-based smart contracts

3.1 Solutions for governments

The reliance of human beings on governments is undisputed. We believe that many countries are willing to try and make their financial networks 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 unique existence can also become a solution in terms of funding a universal basic income. Governments that decide to make this 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.

Archived copy · cryp2nova.com

3.2 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. So please come and test our system's resolve, we will get stronger with each attack.

4 Cryptobiometric blockchain protocol

Humanode implementation is planned to be a maintainable, reliable codebase that will be under active development in the years to come. To build a high-quality system, a good foundation is needed, and the first thing to settle on is a programming language for the implementation.

4.1 Rust

We have evaluated Rust, Go, and C++ and chose Rust for our implementation, with Go being the second-best option. Rust offers a very expressive type system and a novel approach to memory safety, ultimately being the best choice for a long-term project with high demands on code quality and maintainability. Being a language that compiles to native code rather than a VM, it is also very efficient. Rust follows C++'s principle of "if you don't use it, don't pay for it" and powers developers with zero-cost abstractions. It doesn't use a garbage collector, and even async runtime is implemented in the user code, rather than being a part of the language. By modern standards, this is a very high degree of control. The downsides of Rust are that it is difficult to master, and the development process with Rust is slower than with, for instance, Go. Rust enables you to take control over many aspects of a system, and it takes knowledge and time to implement them right. We figured that for our use case, the benefits far outweigh the cost, and thus, we chose Rust.

4.2 Substrate

Every blockchain developer faces a choice: build the codebase from scratch or adopt an existing one for their needs. This decision is simple on the surface, but it is a tough one to resolve.

Substrate is a modular framework that enables the creation of purpose-built blockchains by composing custom or pre-built components. Since dismantling the involvement of the token in the consensus mechanism is one of our main goals as a project, we want to focus our development on building biometric-based consensus aspects on the network. And that is why the modular customization vision is a great ally on our path.

We chose Substrate after carefully evaluating the alternatives (build the code from scratch and using one of the other existing codebases) for several reasons:

- Substrate is designed to be used as a platform to build blockchains, i.e., it is by design a developer tool rather than a final product. Using it was more appealing than basing our development on a codebase that implemented a particular blockchain project.
- Substrate code quality is rather high, and it is clear that people working on it care about the quality.
- We decided that we want something that is a library rather than a framework, and with Substrate, the flexibility and modularity of the code are exactly where we needed them. If we were building the code from scratch, we'd go with a very similar approach to the one that Substrate developers have taken.

Archived copy · cryp2nova.com

- Substrate is being constantly worked on and improved by many people and this means that we can get a stable stream of improvements simply by building on Substrate. There is also a vibrant community around Substrate and many people we can talk to that can help us if we face any trouble with Substrate itself.
- Substrate has proven to be an excellent tool so far, and it allows us to focus on issues specific to Humanode, rather than spending time on the common ones of blockchain building.

4.3 Components

Here's an overview of our system on the component level. Only a subset of the most important pieces are represented here, and there's a lot more that wasn't included.

Below is the list of key components that covers the main Humanode requirements to achieve our goals.

Humanode App—an application that allows users to be a part of the Humanode network by exploring the network, submitting transactions, passing biometric identification, running a node, joining the block production, participating in the Humanode DAO.

Humanode Peer (substrate-based node)—a blockchain node in the Humanode network.

Humanode-runtime—a business logic that defines Humanode network behavior including storage, state transition logic, block, and transaction processing. Also, it enables one of the defining features of Substrate-based blockchains: forkless runtime upgrade.

Humanode-rpc—a component that allows blockchain users including the Humanode app and other dapps to interact with the Humanode network by HTTP and WebSocket RPC servers.

Consensus—a logic that allows Humanode network participants to agree on the state of the blockchain defining one of the key Humanode features: proof-of-human-existence.

Aura consensus—a deterministic consensus protocol that primarily provides block authoring by a limited list of authorities (validators) that take turns creating blocks. The authorities must be chosen before block production begins and all authorities must know the entire authority set. Time is divided up into "slots" of fixed length. During each slot, one block is produced and the authorities take turns producing blocks in order forever.

Grandpa consensus—deterministic consensus protocol that provides block finalization where each authority participates in two rounds of block voting. Once two-thirds of the authorities have voted for a particular block, it's considered finalized.

Bioauth consensus—an addition to deterministic consensus protocols that is responsible for validating whether block authors of proposed blocks have successfully passed biometric authentication (bioauth-authorized).

Frontier consensus—a component that provides an Ethereum compatibility layer that allows the running of Ethereum dapps natively by enabling the functionality of running EVM contracts, Ethereum block emulation, and transactions validation.

Main Pallets (runtime modules)

Bioauth—a component that defines required storage items and calls to manage authentication tickets that allow bioauth-authorized peers to participate in block production.

Fath—responsible for providing a Humanode monetary algorithm with a proportional distribution of issued tokens.

Cost-based fee—provides a logic to enable Humanode transaction fee economics of the network.

Ethereum—a module, combined with the RPC module, that enables Ethereum block emulation, validates Ethereum-encoded transactions, and allows existing dapps to be deployed on a Humanode network with minimal modifications.

Biometric Provider—a component that provides biometric registration and authentication that guarantees the image's privacy and resistance to various vectors of attack on biometrics.

Archived copy · cryp2nova.com

The scheme below illustrates communication and interaction between the components.

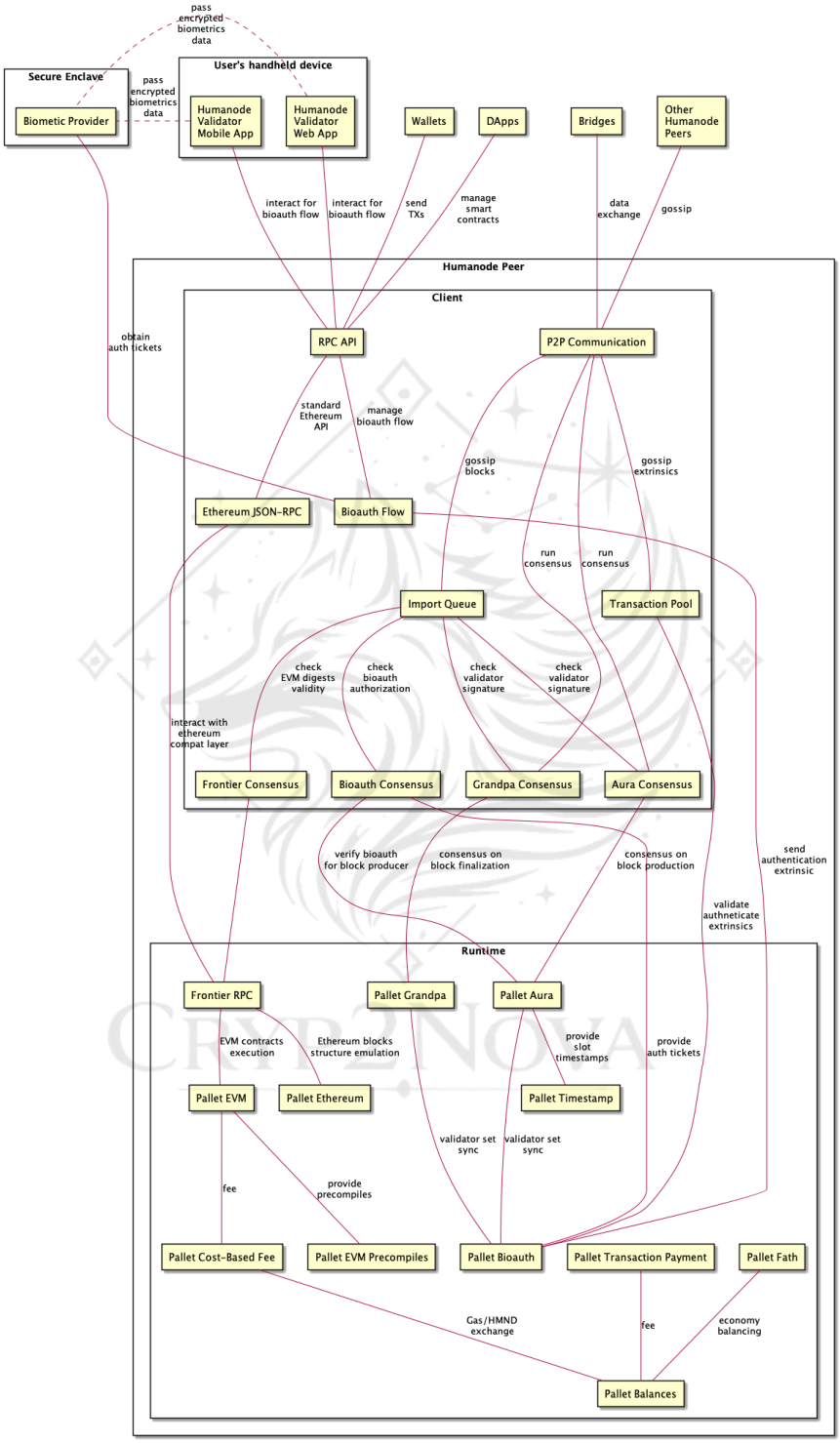


Figure 1: Humanode network components

Archived copy · cryp2nova.com

4.4 Consensus agnosticism

One of the interesting features of Humanode that we pursue is consensus agnosticism, the ability to change the consensus mechanism of the network if the Humanode DAO approves it. It derives from the necessity for constant research on the most suitable consensus for a leaderless system with equal validation power of nodes. Different consensus mechanisms have various pros and cons which constantly evolve, change, and shift due to the large amount of research done by thousands of scientists across the world on this topic. Swappable consensus mechanisms would allow the Humanode network to evolve and not be constrained by a framework of a singular consensus. Moreover, the Substrate ecosystem has ongoing attempts ([1], [2]) to support such a feature.

4.5 Residual increase in the number of human nodes

The limitation on the number of human nodes will be set following Vortex voting. When the limit is still low, it remains possible to attack the system by coordination among 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 for 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 network on the main net as nodes.

4.6 Ethereum compatibility

To bring cryptobiometric technology to existing protocols, the Humanode network includes an EVM pallet that allows it to run Solidity smart contracts and use existing developer tools. Its implementation is based on SputnikVM, which consists of four modules: evm, evm-core, evm-runtime, and evm-gasometer.

One of the goals of the Humanode network is to solve current issues of transaction fee pricing by making the fees stable in USD terms despite the volatility of the native token. Hence, the evm-gasometer is replaced with a cost-based fee system.

Unified accounts, first proposed by Moonbeam, solve the problem of account incompatibility between H256 Substrate addresses and H160 Ethereum addresses where the user is unable to send transactions directly and thus have to have two accounts and move assets between them to get access to both chains. With unified accounts, a single H160 is all the user needs to make the multichain experience seamless.

Moving a dapp or a smart-contract framework from Ethereum to Humanode will require minimal changes. Solidity smart contracts, block explorers, development tools, bridges, and frameworks for decentralized autonomous organizations are easily ported to the chain based on equal validators.

By bridging Humanode to other EVM-compatible chains, the network will be able to provide private biometric processing and Sybil resistance to dapps and protocols based on other chains. A biometric smart contract written in Solidity deployed on a needed chain will communicate with, for instance, a decentralized finance protocol, and then send the request to the Humanode network where biometric data is stored. Without revealing the user's identity, the Humanode network sends ZK liveness proof and identity checks back to the DeFi protocol to prove the user is the same real human being without using any PII (Personally Identifiable Information).

4.7 Slashing system

Any verification system requires executive tools that safeguard the 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 malicious actors for a period of time. If a malicious actor tries to harm the network in any way, the system will blacklist his biometrics. After being slashed, the perpetrator

Archived copy · cryp2nova.com

will remain blacklisted for a determined 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 the 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 perpetrations 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 predetermined by Vortex: 0.5 months (the basic length), 1 month, 2 months, 3 months, 6 months, 1 year, 2 years, 3 years, 10 years, 20 years, and 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 month	0	0.5	Human node is excluded from validator set 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
A node 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
Node 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

5 Fath

Humanode dismantles the involvement of tokens 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 (the Humanode Token).

Fath is a monetary algorithm with a proportional distribution of issued tokens. 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 issued tokens 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 its 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 networks and capital-based public blockchain networks operate.

Archived copy · cryp2nova.com

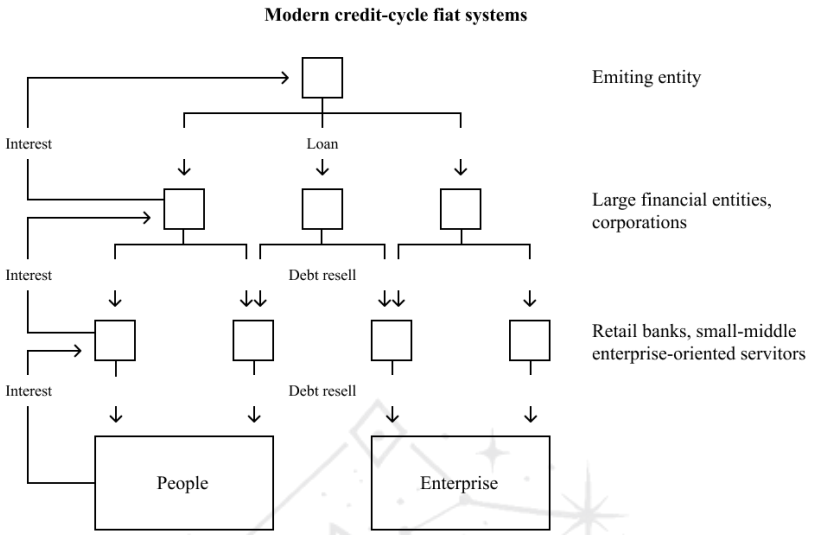


Figure 2: Issuance in modern credit-cycle fiat systems.

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 in 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, enterprises, and retail banks are the ones who are constantly cornered because they are the ones paying for those 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 monetary 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.

CRYP2NOVA

Archived copy · cryp2nova.com

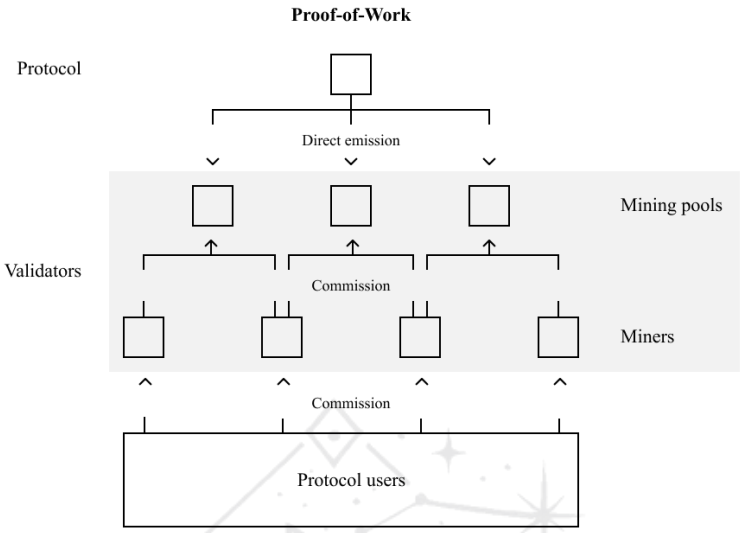


Figure 3: Issuance and commission in PoW blockchains

In PoW 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 18.8 million. With emission set in every block and the halving that happens every four years, it will take approximately 120 years to mint everything. Emission is received by miners not in the 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 ridiculously 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 does not line up with 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.

CRYP2NOVA

Archived copy · cryp2nova.com

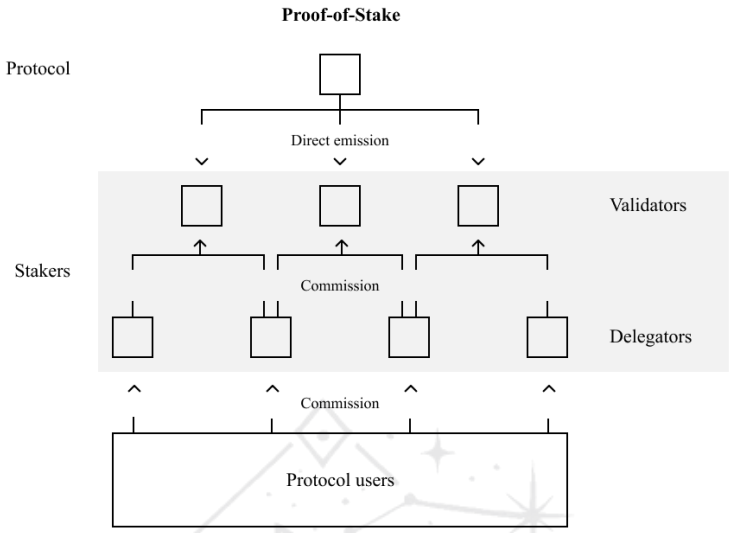


Figure 4: Issuance and commission in PoS blockchains.

As in PoW, in PoS the protocol acts as the issuance entity. In most cases, PoS have some kind of a 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 PoW, 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, which counterweighs the devaluation effect.

CRYP2NOVA

Archived copy · cryp2nova.com

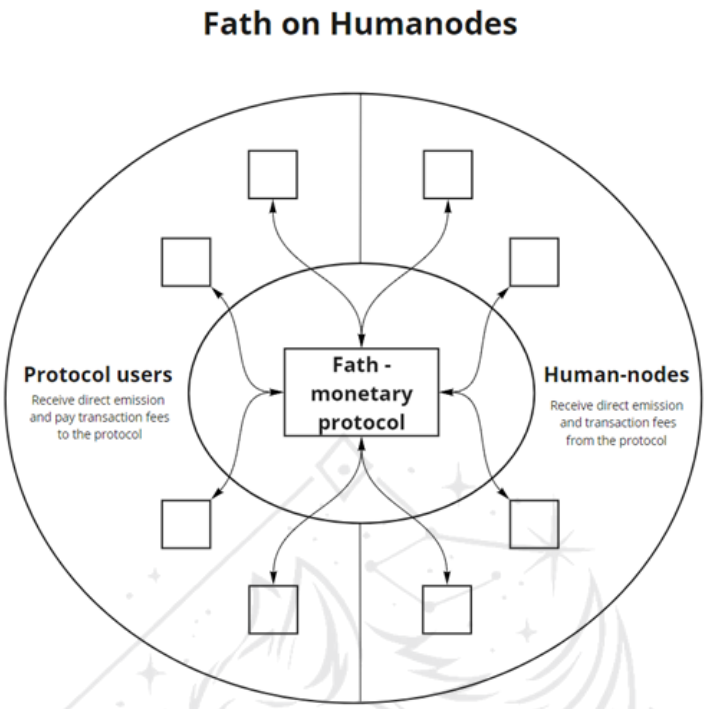


Figure 5: Issuance and commission in Fath

The emission of tokens in Fath behaves differently from the systems mentioned above. One of the hypotheses that are 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 (Gross Network Product; GNetP) in two different time periods. If GNetP in the second period is different from GNetP in the first then the algorithm calculates the difference and changes the monetary supply by the same percentage.

We consider the HMND token first of all to be a transaction-processing as well as a biometric network, which is why GNetP in the first implementation of Fath will be calculated based on the 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.

Two types of rebalances 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 the protocol proportionally burns excessive supply throughout every single wallet as well

5.1 Transaction-based emission algorithm example

End of Year 0

Archived copy · cryp2nova.com

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 burned and rebased proportionally.

New supply: 15,000,000 HMND
Your wallet: 1500 HMND
Such a rebalancing mechanism tries to:

- Mitigate the long-term effect of devaluation due to disproportional emission
- Negate macroeconomic shocks and structural inefficiencies that occur due to the monetary supply not satisfying the needs of the growing or shrinking GNetP. 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 them here.

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

If the total fees 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 opposite to the price change. The token issuance is tied to the change of total fees collected by the protocol. If the changes in quantity and size of the transactions are bigger than the asset price change, only then the protocol will initiate inFath.

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, the new Fath modules should be launched to account for new values created a nd 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 and contract types as are involved in the calculation of GDP.

6 Biometric approach to user identification

Rapid development in IT, DLT (Distributed Ledger Technology), and AI are prompting biometrics to constantly innovate and make the most of market demand. According to the latest reports, the global biometrics market is forecast to reach $82.8 billion [3] to nearly $100 billion [4] by 2027, growing at a $> 19.3\%$ compound annual growth rate (CAGR) from an estimated $ 24.1 billion in

Archived copy · cryp2nova.com

2020. According to these reports, the multimodal biometric systems segment is projected to increase in revenue at a significant CAGR during the forecast period.

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 [5].

In 2020, the global market for mobile biometrics was estimated at $18 billion, and it is projected to reach a size of $79.8 billion by 2027, growing at a CAGR of 23.7% over the analysis period 2020–2027 [6]. Growth in the scanner segment was readjusted to a 20.1% CAGR for the next seven-year period.

Furthermore, the post-COVID 19 global digital identity verification market is forecast to grow from $7.6 billion in 2020 to $15.8 billion by 2025, at a CAGR of 15.6%.

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 biohashing, biometric cryptosystems, and cancelable biometrics have not evolved enough to become efficient and secure for a hypothetical user ([7] ; [8], [9]; [10]; [11]; [12]; [13]; [14]; [15]).

Until not so long ago, biometric identification methods carried a heavy risk to personal privacy. Biometric data are considered to be very sensitive, as they can be uniquely associated with a human being. Passwords are not considered PII, as they can be changed and not associated with any person directly. The main risks associated with 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.

6.1 Humanode bio-authorization overview

The privacy and security of biometric data have been among the most critical aspects to consider when deciding on a biometric and cryptographic technology to use in Humanode. Biometric registration and authentication are carried out through a novel method based on cryptographically secure neural networks for the private classification of images of users' faces so that we can:

- guarantee the image's privacy, performing all operations without the biometrics of the user's face having to leave the device
- obtain a certificate or proof that the operations are carried out correctly, without malicious manipulation
- have resistance to different attacks, such as the Sybil attack and reply attack
- carry out all registration and authentication operations without the need for a central entity or authority that handles the issuance and registration of users' cryptographic keys
- compare the feature vector each time the user wants to authenticate in a cryptographically secure way

Let's now see how the different technologies that we use to perform the registration and authentication of users are broken down, guaranteeing privacy in a decentralized environment.

Traditionally, neural networks are used to identify an image. A neural network is a particular case of a machine-learning technique that consists of a series of so-called nodes structured in layers. These nodes or neurons are mathematical functions that perform a specific operation according to the layer they belong to.

For example, the convolutional layer is in charge of filtering the information to determine the similarity between the original image covered by a filter and the filter itself. The activation layer also determines if the filter pattern defined in the convolutional layer is present at a particular position

Archived copy · cryp2nova.com

in the image. There is also a layer called max pooling that modifies the data to make them easier to handle [16].

When the user logs into the system for the first time, the neural network gives us a unique feature vector that identifies the user. Once this vector is registered, we can store it for future comparisons when the user wishes to authenticate.

The main objective of the biometric registration and authentication system is to protect the images of users throughout the whole process and on the different layers of the neural network. It is required that the operations are carried out effectively and efficiently, preventing unauthorized access to the data, from the time when they are obtained on the user's device to when they are processed in the neural network and registered in the system [17].

A malicious user gaining access to the neural network should not be able to obtain any sensitive information. This is why Humanode biometric system architecture is designed to run neural networks locally on the user's device and only send the proof that all the neural network layers were executed. The user will also send the neural network's output in the form of an encrypted feature vector.

6.2 Convolutional neural network

Often referred to as CNNs or ConvNets, convolutional neural networks specialize in processing data that are grid-like in topology, such as images.

In a digital image, each pixel contains a binary value that denotes how bright it is and what color it should be. It contains a series of pixels that are arranged in a grid-like format.

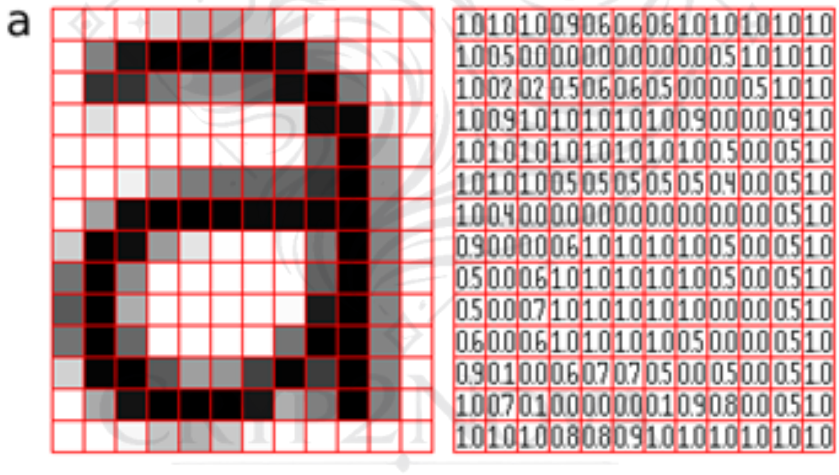


Figure 6: Representation of image as a grid of pixels ([18]).

Each neuron works in its own receptive field, interconnected with other neurons so that the entire visual field is covered. The human brain processes enormous amounts of information as soon as it sees an image.

In the same way that each neuron in the biological vision system responds to stimuli only in its receptive field, each neuron in a CNN also processes information only within its receptive field. With a CNN, one can enable computers to sense simpler patterns (lines, curves, etc.) at the beginning and more complex patterns (faces, objects, etc.) as they progress.

There are four main layer types of CNNs: a convolutional layer, pooling layer, fully connected layer, and one or more activation layers.

Archived copy · cryp2nova.com

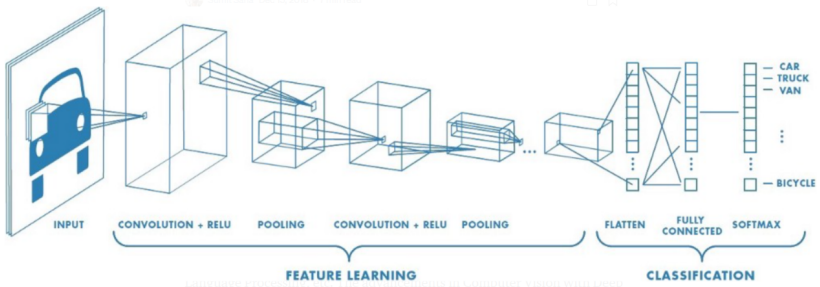


Figure 7: Architecture of a CNN ([19]).

6.2.1 Convolution layer

CNNs have a convolution layer that carries a vast amount of computations. Using this layer, we perform a dot product between two matrices, one that contains the set of learnable parameters, known as a kernel, and the other that contains the restricted portion of the receptive field.

In the case of an image composed of three (RGB) channels, the kernel height and width will be smaller than the image, but the depth will encompass all three channels.

When the forward pass is made, the kernel slides across the height and width of the image, creating an image representation of the receptive region. A kernel response is generated by computing an activation map in two dimensions, which results in a representation of the image for each spatial position. A stride refers to the size of the kernel as it slides. The size of the output volume can be calculated as follows if we have an input of size $W \times W \times D$ and a number of kernels of size F with a stride S and a padding P:

$$W_{out} = \frac{W - F + 2P}{S} + 1$$

This will yield an output volume of size $W_{out} \times W_{out} times D_{out}$.

CRYP2NOVA

Archived copy · cryp2nova.com

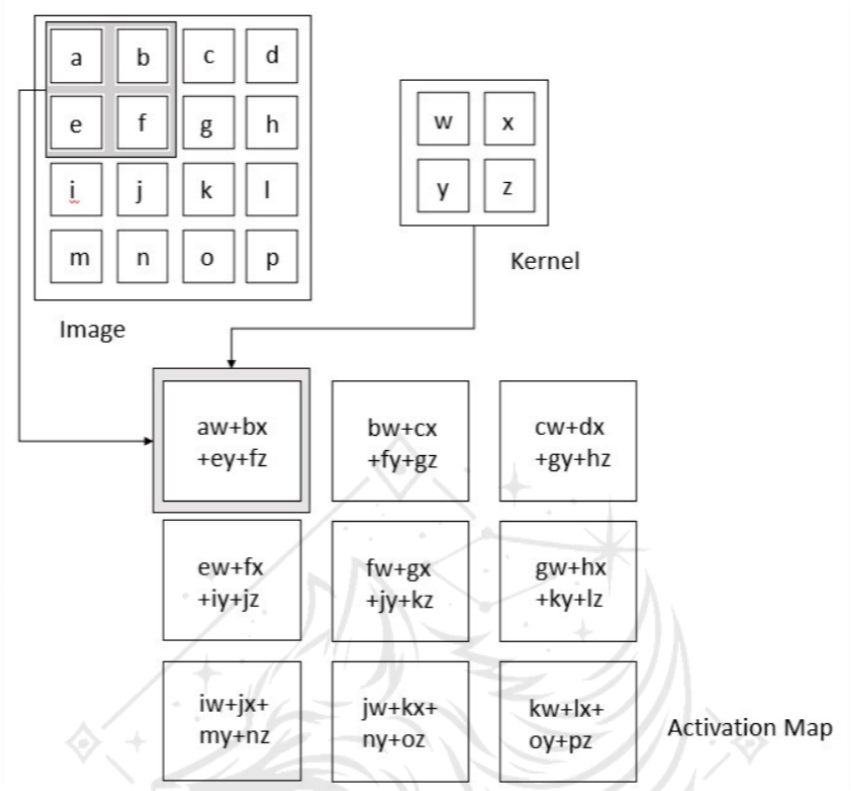


Figure 8: Convolution Operation ([20]).

6.2.2 Pooling layer

During the pooling layer, summary statistics are derived from the nearby outputs to replace certain outputs of the network. As a result, the size of the representation is reduced resulting in a decrease in computation and weights. The pooling operation is applied to every slice in turn.

In addition to the rectangular neighborhood average, there are several pooling functions such as the $L2$ norm of the rectangular neighborhood and the weighted average based on the distance to the central pixel. Max pooling, however, is the process most commonly used, which reports the max output from the neighbors.

Archived copy · cryp2nova.com

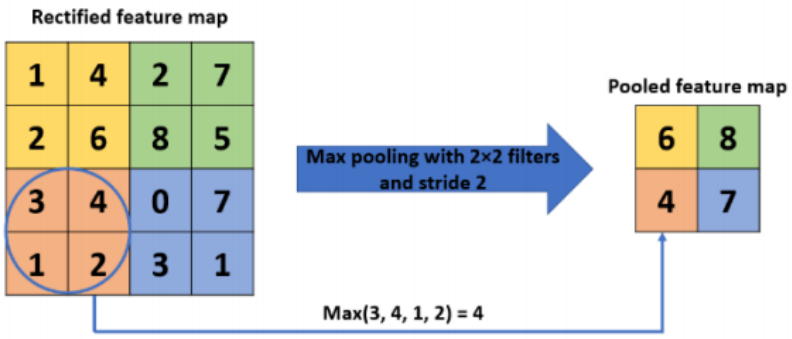


Figure 9: Example of a Max-Pooling Operation

The size of the output volume can be determined by this formula if we have an activation map with dimensions $W \times W \times D$, a pooling kernel with dimensions F and a stride:

$$W_{out} = \frac{W - F}{S} + 1$$

This generates an output volume of $W_{out} \times W_{out} times D_{out}$.

The translation invariance of pooling makes it possible to recognize objects wherever they appear in the frame regardless of their position.

6.2.3 Fully connected layer

As with regular FCNNs (Fully CNNs), neurons in this layer are fully connected to neurons in the preceding and following layers. Thus, it can be calculated as usual by a matrix multiplication followed by a bias effect. This layer enables mapping of inputs and outputs between representations.

6.2.4 Activation layers

Non-linear layers are often placed directly after the convolutional layer to introduce nonlinearity to the activation map, due to the linear nature of convolution and the non-linear nature of images.

1. Sigmoid

   The sigmoid nonlinearity has the mathematical form $\sigma(\kappa) = 1/(1+e^{-\kappa})$. This formula takes a real-valued number and "squashes" it between 0 and 1. However, the gradient of the sigmoid is almost zero when the activation is at either tail. In backpropagation, if the local gradient becomes very small, it will effectively "kill" the gradient. Furthermore, if the sigmoid is always positive, it will produce either all positives or all negatives, resulting in a zig-zag trend in gradient updates for the weights.

2. Tanh

   Tanh squashes a real-valued number between -1 and 1. The activation of sigmoid neurons saturates, but the output is zero-centered, unlike sigmoid neurons.

3. ReLUs

   In the last few years, Rectified Linear Units (ReLUs) have been very popular. They are computed with the function $f(\kappa) = \max(0, \kappa)$. In other words, the activation threshold is simply set to zero. With ReLUs, convergence is six times faster than the sigmoid and tanh non-linearities.

Archived copy · cryp2nova.com

The disadvantage of ReLUs is that they can be fragile during training. They can be updated by a large gradient in such a way that the neuron is never further updated. This can be addressed by setting an appropriate learning rate.

6.3 Cosine similarity for feature vector matching

Humanode facial recognition system uses modified ResNet architecture for facial feature extraction and uses cosine similarity for matching.

Cosine similarity is a measurement that quantifies the similarity between two or more vectors. It is measured by the cosine of the angle between vectors and determines whether two vectors are pointing in roughly the same direction. The vectors are typically non-zero and are within an inner product space. It is described as the division between the dot product of vectors and the product of the Euclidean norms or magnitude of each vector:

$$similarity = \cos(\theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{||\mathbf{A}||||\mathbf{B}||} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}}$$

and thus cosine similarities are constrained between 0 and 1. The similarity measurement is a measure of the cosine of the angle between the two non-zero vectors **A** and **B**.

Assume the angle between the two vectors is 90 degrees. The cosine similarity will be zero in that case. This indicates that the two vectors are orthogonal or perpendicular to each other. The angle between the two vectors **A** and **B** decreases as the cosine similarity measurement approaches 1. The image below illustrates this more clearly.

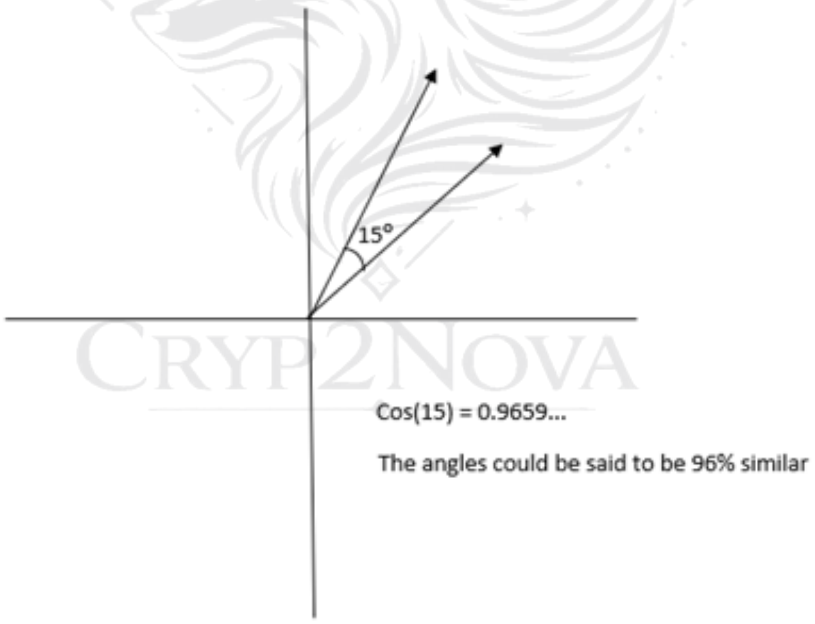


Figure 10: Two vectors with 96% similarity based on the cosine of the angle between the vectors.

Archived copy · cryp2nova.com

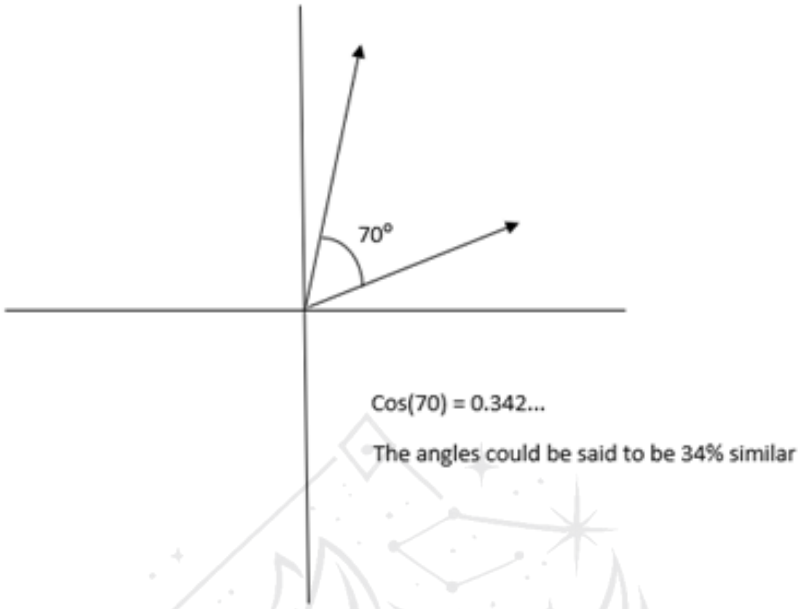


Figure 11: Two vectors with 34% similarity based on the cosine of the angle between the vectors.

Humanode uses cosine similarity in the facial feature vector matching part.

6.4 Active and Passive Liveness detection

Enterprises use face recognition for onboarding, validating, and approving customers due to its reliability and ease of use. The demand for liveness detection is growing rapidly. Liveness detection identifies presentation attacks like photo or video spoofing, deepfakes, and 3D masks or models, rather than matching the facial features.

This makes it much harder for an adversary to spoof an identity. Facial recognition determines whether the person is unique and the same whereas liveness detection determines whether the person is a living human being. Liveness detection confirms the presence of a user's identification credentials and that the user is physically present, whether on a mobile phone, a computer or tablet, or any camera-enabled device.

There are two methods in facial liveness detection: active and passive.

Active liveness detection asks the user to do something to confirm that they are a live person. A user would be normally asked to either change the head position, nod, blink their eyes or follow a mark on their device's screen with their eyes. Despite this, fraudsters can fool the active method using a so-called presentation attack, also known as the presentation attack detection (PAD) attack. Scammers can use various gadgets or "artifacts" to fool the system, some of which are remarkably low-tech.

The Humanode active liveness detection model asks the user to turn their face left or right, blink their eyes, or show emotions like happiness, anger, or surprise and determines whether the user is fake or real depending on the result.

With **passive liveness detection**, the user is not asked to do anything. This provides end-users with a modernized and convenient experience. It is an excellent method for determining whether the user is present without any specific movement or gesture. Passive methods use a single image, which is examined for an array of multiple characteristics to determine if a live person is present.

Archived copy · cryp2nova.com

The Humanode passive liveness detection model determines if a live person is present, based on texture and local shape analysis, distortion analysis, and edge analysis:

- Texture and local shape analysis—analyze the input image from a textural analysis point of view by image quality assessment, characterization of printing artifacts, and differences in light reflection
- Distortion analysis—analyze the input image using an image distortion analysis feature vector that consists of four different features, specular reflection, blurriness, chromatic moment, and color diversity
- Edge analysis—analyze the edge of the input to find out whether the edge component is presented or not

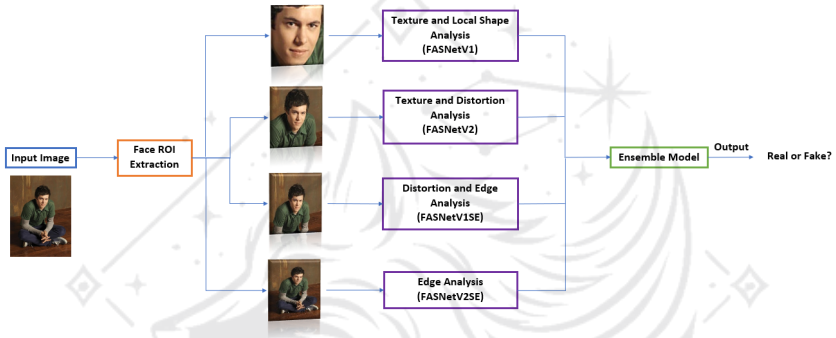


Figure 12: Analysis types in liveness detection.

While the active liveness detection process is going on, passive liveness detection is performed in the background.

By combining the advantages of active and passive liveness detection approaches, we made our liveness detection system more secure.

6.5 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.

Archived copy · cryp2nova.com

Table 2: Merits and demerits of biometric identification.

Merits	Demerits
• *High levels of security and accuracy* in contrast to passwords, as biometric data cannot be forgotten. • *Simplicity and convenience for the user* is a significant factor in the growing popularity of biometric authentication. • *Higher level of authenticity* for users prone to weak passwords that may be common to multiple users or easily shared. • *Affordability,* as biometric authentication is now possible in a wide range of common devices. • *Flexibility,* as users have their own security credentials with them, so they do not need to bother memorizing a complex password. • *Biometrics is trustable,* as reports from 2021 claim that the younger generations trust biometric solutions more than others. • Biometric solutions are *time conserving.*	• Sometimes *requires integration and/or additional hardware.* • *Delay,* as some biometric recognition methods may take more than the accepted time. • *Physical disability,* as some people are not fortunate enough to be able to participate in the enrollment process. • The need to *trust* your biometric provider that data are secure and private.

6.6 Cryptobiometric search and matching operations

When the user registers in the system, the executed private neural network allows the feature vector to be extracted from the user's face for the first time. It is essential to safely store this vector to evaluate the subsequent times that the user wants to authenticate in the system. But this storage must be encrypted. Moreover, to compare the new vector with the already stored one, we cannot decrypt the data. For this, there is the homomorphic encryption method.

Homomorphic encryption is nothing more than an encryption algorithm with the additional characteristic that operations can be defined so that they can be preserved by encryption. In mathematics, the preservation of an operation is obtained when we have an operation and a function between two spaces. The function that goes from one space to the other is said to preserve the operation if it is invariant under said operation.

Formally we say that the function f, from space A to space B, is an homomorphism if given two elements $a_1, a_2 \in A$, then the function f has the following property:

$$f(a_1 + a_2) = f(a_1) + f(a_2)$$

Archived copy · cryp2nova.com

This section will discuss a method used in neural networks to evaluate the similarity between two feature vectors. Then, we will define the homomorphic encryption method that will allow us to store the encrypted feature vector and perform the similarity operation without decrypting the vector.

6.6.1 Cosine similarity encryption

As mentioned above, one of the most efficient and natural ways to find the similarity between two feature vectors in neural networks is cosine similarity. Let $c = (c_0, \ldots, c_r)$ and $b = (b_0, \ldots, b_n)$ two vectors in

$$\mathbb{R}^n$$

, the cosine similarity between a and b is defined by the equation

$$cos(a, b) = \frac{a \cdot b}{||a||||b||}$$

where

$$||a||$$

is the norm of the vector a [16].

From the equation above, if we calculate the internal product between two vectors, we can determine if two vectors are similar directly. In simple terms, the cosine similarity of the angle of two vectors tells us whether two vectors point in the same direction.

If in addition the vectors are normalized, then it is evident that:

$$cos(a, b) = \frac{a \cdot b}{||a||||b||} = a \cdot b = \sum_{i=1}^{n} a_i b_i$$

In the cryptobiometric authentication system, we must define an encryption scheme that allows us to calculate the internal product between two vectors, which will give us the similarity between them. This calculation will be carried out on the encrypted vectors without the need to decrypt them.

It is natural to look for a homomorphic encryption scheme where the calculations to determine similarity are performed in the encrypted space.

In a traditional encryption scheme, which only encrypts the data to be sent, it would have to handle the private keys with which the user encrypted the data, decrypt the vectors, and then make the similarity calculation on clear data. From a decentralized perspective, this traditional approach has a flaw, as users' private keys are in an environment where peers are by nature untrusted. In a decentralized environment, there is no trusted third party to handle the keys securely.

6.6.2 Homomorphic encryption

There are different proposals for encryption schemes that preserve operations in a homomorphic manner through the encryption function. In particular, one of the most straightforward and most efficient is encryption based on learning with errors (LWE) [21]. In this section we will examine the mathematical preliminaries of this cipher and the algorithms that compose it, namely:

- Key generation
- Encryption
- Decryption
- Homomorphic operations

Archived copy · cryp2nova.com

Lattices

In group theory a lattice in $\mathbb{R}^n$ is an algebraic subgroup of $\mathbb{R}^n$ that spans the vector space $\mathbb{R}^n$ with integer coefficients in its basis.

Formally, let $n \in \mathbb{N}$,$B \in \mathbb{R}^{n\times n}$ be a matrix, and

$$b_i \in \mathbb{R}^n$$

the i-th row of B with $1 \leq i \leq n$. Then the linear combinations of b_i are defined as

$$\mathcal{L}(B) = \sum_{i=1}^{n} m_i b_i$$

is a subgroup of $\mathbb{R}^n$, where $m_i \in \mathbb{Z}$. If the

$$b_i$$

are linearly independent, we say that $\mathcal{L}(B)$ is a lattice in $\mathbb{R}^n$ of dimension n.

Lattice-based ciphers are some of the leading candidates for post-quantum cryptographic algorithms. If an efficient quantum computer is ever built, a post-quantum encryption scheme can resist attacks. In 1994, Shor theoretically demonstrated that a protocol could be built on a quantum computer that would break in polynomial time the problems on which most public-key ciphers such as the RSA, Diffie–Hellman, or cryptosystems of elliptic curves are based.

However, the computational complexity of the problem that shapes cryptosystems based on lattices ensures their quantum resistance. Furthermore, the LWE-based cryptosystem can be completely homomorphic: it possesses homomorphism in both operations of addition and multiplication. Which is very useful for the calculation of the inner product, and consequently for the similarity of the cosine [22].

Construction of the ring-LWE scheme

Let us now see in detail how the ring-LWE encryption scheme works and how the homomorphic operations are defined [23, 24].

Setup parameters First of all, we need to define certain general parameters to be used in the key generation algorithm:

- set $n \in \mathbb{N}$, a degree parameter.
- let q be a prime number, defining the ring $R_q = R/qR = \mathbb{F}_q[x]/f(x)$. This ring is the ciphertext space.
- take t as an arbitrary integer, with $t < q$, defining the ring $R_t = R/tR = \mathbb{F}_t[x]/f(x)$. This ring is the plaintext space.
- define the standard deviation σ, as the parameter for the discrete Gaussian distribution $\chi = D_{Z^n,\sigma}$.

Key generation First, we sample random elements as follows:

- sample s from the Gaussian distribution χ
- take a random $p_1 \in R_q$ and the error e sampled from χ.

Then the public key is defined as $pk = (p_0, p_1)$, where $p_0 = -(p_1 s + te)$, and the secret key is $sk = s$.

Archived copy · cryp2nova.com

Encryption After encoding the plaintext m as an element in R_t and given the public key $pk = (p_0, p_1)$, we sample u, f, g from the distribution χ and compute

$$Enc(m, pk) = (c_0, c_1) = (p_0 u + tg + m, p_1 u + tf)$$

Decryption If $c = (c_0, \ldots, c_r)$ is a ciphertext and $sk = s$ the private key, then the decryption is simply

$$Dec(c, sk) = [\widehat{m}]_q (mod t) \in R_t$$

where

$$\widehat{m} = \sum_{i=0}^{r} c_i s^i \in R_q$$

If we write the secret key vector S as $S = (1, s, s^2, \ldots, s^r)$, then

$$Dec(c, sk) = [\langle c, S \rangle]_q (mod t)$$

Homomorphic operations Now, if we have two elements in the encrypted space, $c = (c_0, \ldots, c_r)$, $c' = (c'_0, \ldots, c'_t)$ the homomorphic operations are given by

$$c + c' = (c_0 + c'_0, \ldots, c_{max(r,t)} + c'_{max(r,t)})$$

$$x * c' = (\widehat{c}_0, \ldots, \widehat{c}_{r+t})$$

where

$$\sum_{i=0}^{r+t} \widehat{c}_i z^i = \left(\sum_{i=0}^{r} c_i z^i \right) * \left(\sum_{i=0}^{t} c'_i z^i \right)$$

6.7 Extracting inner product from the encrypted value

The cosine similarity operation requires, as we saw, the calculation of the inner product in the encrypted space. It is evident then that if we define accordingly a transformation in the encrypted space, thanks to the homomorphic properties of the encryption scheme we can extract the inner product as a constant term from the encrypted result [25].

Thus, let P, Q be bit sequence representations of vectors and F a transformation onto the ring R_q such that $F(P) = \sum_{i=0}^{l-1} p_i 2^i$ and $F(Q) = \sum_{i=0}^{l-1} q_j 2^{n-j}$.

If we multiply $F(P) * F(Q)$, then

$$\begin{aligned} F(P) * F(Q) &= \sum_{i=0}^{l-1} p_i q_i 2^n + \cdots \\ &= \langle P, Q \rangle + \cdots \end{aligned}$$

Thus, if we encrypt $F(P)$ and $F(Q)$, thanks to the homomorphic properties of the encryption scheme, we can extract the inner product as a constant term from the encrypted result:

$$Enc(F(P) * F(Q)) = \langle P, Q \rangle + E(\cdots)$$

Archived copy · cryp2nova.com

6.8 ZKP for verifiable computation

In our setup, a node does not trust any other node in the system. This means that a node can be trusted to follow the protocol but may not be trusted with the computation of the feature extraction and liveness detection processes.

During the registration process, a node will extract a feature vector from the face image and then send it to a peer node. The problem is how does the peer node trust the feature vector? A node may or may not have followed the feature extraction process as required. In this situation, zero-knowledge–based verifiable computation comes to the rescue.

Verifiable computation is a technique to prove that the computation process was followed correctly by an untrusted party. Let $y = f(x)$ be the result of computation on input x. The prover generates a proof of computation, π, along with the result and sends x, y, π to the verifier. Using x, y and verification keys, the verifier verifies the correctness of the proof π.

Related work:

1. SafetyNet: Specialized interactive proof protocol for verifiable execution of a class of deep neural networks. It supports only quadratic activation functions, but in our neural network model, ReLU is necessary to achieve higher accuracy.

2. zkDT: Verifiable inference and accuracy schemes on decision trees. Decision trees are simple and quite different from neural network architecture.

3. vCNN: verifiable inference scheme for neural networks with zero knowledge. It only optimizes convolution. The vCNN scheme uses mixing of QAP (Quadratic arithmetic program), QPP (quadratic polynomial program), and CP-SNARK for making a connection between QAP and QPP. QAP works at the arithmetic circuit level and is costly in terms of computation.

4. ZEN: R1CS-friendly optimized ZK neural network inference scheme. Proposes an R1CS-friendly quantization technique. Uses an arithmetic-level circuit and Groth zero-knowledge–proof scheme.

5. zkCNN: Interactive zero-knowledge–proof scheme for a CNN. Proposes a new sum-check protocol. Uses the GKR protocol.

The vCNN, ZEN, and zkCNN procedures are most closely related to our scenario but all of these reduce the computation program to arithmetic circuit level and then use a Groth ZKP protocol for verification.

Any verifiable computation scheme utilizes the homomorphic property of the underlying primitive for verification. Therefore, it can support computation that involves either addition or multiplication. Since neural network computations are often complex and non-linear, researchers often convert the program to the arithmetic circuit level, which involves only addition and multiplication at the bit level, and then use a zkSNARK-type proof. This is a more generalized technique for any circuit. However, if the circuit involves only addition and multiplication at integer level then there is no need to convert it to the arithmetic circuit level.

Our idea is to break down the neural network model of feature extraction into different layers and then prove the computation of individual layers separately. There are four main layers: the convolution layer, Batch-normalization layer, ReLU layer, and average pooling layer. Out of these, only the ReLU layer is not in the form of addition and multiplication.

$$ReLU(x) = max(x, 0)$$

.

Archived copy · cryp2nova.com

So, to make it compatible with our idea, we replaced the ReLU function with the bit-decomposition of ReLU, which involves bit-level addition and multiplication. After this, we used Verifiable Private Polynomial Evaluation (PIPE) where an untrusted cloud server proves that the polynomial computation, $y = f(x)$, is correct without revealing coefficients of the polynomial f. We are aware of other similar schemes like Pinocchio, PolyCommit by Kate et al., and other Garbled circuit-based schemes, but PIPE is best suitable for our decentralized untrusted P2P network scenario.

Our scenario is similar but slightly different. We assume that the neural network parameters are available with each node. That means coefficients of the kernel in the convolution layer are available with each node. For input $(x_1, \ldots, x_n)$ and kernel $(a_1, \ldots, a_m)$, the output of convolution can be represented as:

$$y_j = \sum_i a_i x_{j+i}$$

In the PIPE scheme, a_i is kept secret from the verifier and in our scenario, x_i (which represents input image) is kept secret from the verifier. Moreover, in the PIPE scheme, both input and output are available in plain form for the verifier. However, we cannot reveal the input and outputs of the neural network as well as the intermediate layers due to privacy concerns. That means we had to modify the PIPE scheme in such a way that the verifier can still verify the correctness of computation using encrypted inputs and outputs.

Finally, here is what we have in a ZKP system for the feature vector extraction process.

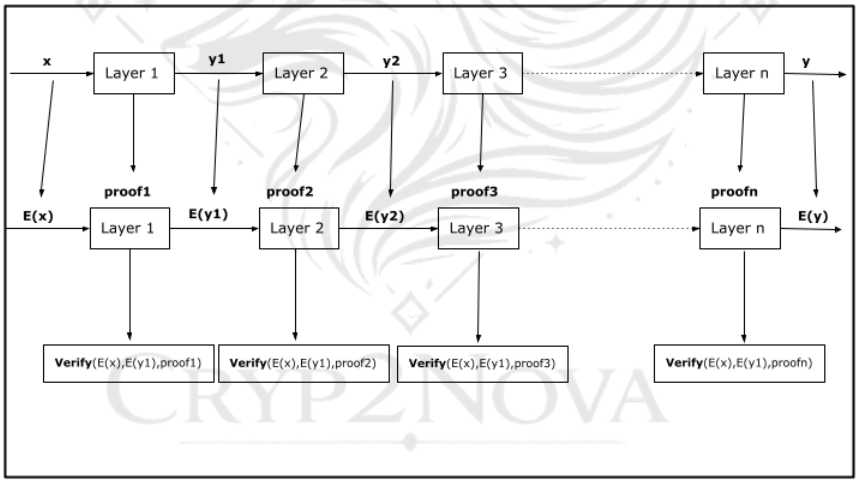


Figure 13: ZKP for the feature vector

6.8.1 Humanode approach to ZKP

Generalized problem: **Input:** $(x_1, \ldots, x_n)$

Computation: $y = \sum_i a_i x_i$

Prover picks an input and performs the computation. Since the verifier does not trust the prover, the prover needs to prove that the output y is computed correctly.

Archived copy · cryp2nova.com

Requirement: The coefficients of the computation, $\{a_i\}$ are public and known to verifiers. The prover can't disclose $\{x_i\}$ and y to the verifier due to privacy concerns.

To overcome this problem, we combined Feldman's Verifiable Secret Sharing (VSS), ElGamal Crypto system, and non-interactive ZK proof.

Feldman's Verifiable Secret Sharing scheme: Feldman's VSS is a secret sharing scheme where each share is a point $(x.y)$ on a secret polynomial f. In Feldman's VSS, given a share (a, b), anybody can verify the validity of the share using some public value corresponding to the secret polynomial f. This means anyone can check whether $a = f(b)$ without knowing the coefficients of the polynomial f.

Let $f(x) = \sum_{i=0}^{k} a_i x^i$ be a k-degree polynomial with $a_i \in \mathbb{Z}_p^*$.

Let G be a multiplicative group of a prime order p and g be a generator of G. For each a_i, set $h_i = g^{a_i}$.

Now make g and $\{h_i\}$ public. Given a share (a, b), one can check the validity of the share by verifying the following equation:

$g^b = \prod_{i=0}^{k} h_i^{a_i}$

Note: There are two concerns here. First, the share (a, b) is in plain form and hence, if we use this as is, then we have to reveal input and output to the verifier in our scenario. The second concern is that h_i hides a_i under the assumption that it is difficult to solve for a_i from h_i under the discrete logarithm assumption. However, if a_i is a small value, then it will be very easy to find a_i from h_i. In neural network computation, the values (input and weight parameters) are always small and cannot hide it properly.

Feldman's VSS with encrypted input and output: Input: $(x_1, \ldots, x_n)$

Computation: $y = \sum_i a_i x_i$

To hide input and output, we need to encrypt both in such a way that we can perform some operation over encrypted value. That means we have to use some homomorphic encryption scheme.

We use ElGamal encryption mainly because it is homomorphic with respect to plaintext multiplication as well as scalar multiplication, which suits our system perfectly.

ElGamal Key pair: $= (sk, pk) = (\alpha, h = g^\alpha)$

Encrypt input:= $Enc(g^{x_i}) = (c_i, d_i) = (g^{r_i}, h^{r_i} g^{x_i})$

Encrypt Output:= $Enc(g^y) = (g^r, h^r g^y)$

Compute

$$C = \prod_i c_i^{a_i} = \prod_i g^{r_i a_i} = g^{\sum_i a_i r_i} = g^{r'}$$

where $r' = \sum_i a_i r_i$ and

$$D = \prod_i d_i^{a_i} = \prod_i (h^{r_i} g^{x_i})^{a_i} = (\prod_i h^{r_i a_i})(\prod_i g^{x_i a_i}) = h^{r'} g^y$$

Finally, we have $(C, D) = (g^r, h^r, g^y)$, which is an ElGamal encryption of g^y. So now, the prover needs to convince the verifier that (C, D) computed from encrypted input is a valid ciphertext of g^y. Here, we use the Non-Interactive ZK Proof (NIZKP) of $(C/g^r) = (D/h^r g^y)$

Non-Interactive ZK Proof: If we generalize the above log equation, then we have $h_1 = h_2$ for some $g_1, h_1, g_2, h_2 \in G$. In 1993, David Chaum and T. P. Pedersen proposed the NIZKP to prove exactly this.

NIZKP LogEq:

Archived copy · cryp2nova.com

Let G be a multiplicative group of prime order p and H be a hash function. Let the language L be the set of all $(g_1, h_1, g_2, h_2) \in G^4$ where $h_1 = h_2$. The NIZKP $LogEq = (prove, verify)$ is as follows:

Prove $((g_1, h_1, g_2, h_2), w)$: Using the witness $w = h_1$, it picks a random r from $\mathbb{Z}_p^*$ and computes $A = g_1^r$, $B = g_2^r$, $z = H(A, B)$ and $t = r + w.z$. It outputs proof $\pi = (A, B, t)$.

Verify $((g_1, h_1, g_2, h_2), \pi)$: Using $\pi = (A, B, t)$, it computes $z = H(A, B)$. If

$$g_1^t = Ah_1^z \text{ and } g_2^t = Bh_2^z$$

Then it outputs 1, else it outputs 0.

We achieve the ZKP system for an individual layer of our NN model by combining Feldman's VSS, ElGamal cryptosystem, and NIZKP LogEq properly.

- Our ZKP system is unconditionally ZK-secure and UNF-secure under Random Oracle Model.
- Our ZKP system is also privacy-preserving under the DDH assumption in the Random Oracle Model.

6.8.2 ElGamal Cryptosystem

We generalize the input image as a higher-dimensional vector $(x_1, x_2, x_3, \ldots, x_n)$. Similarly, we assume the output of each layer is again a higher-dimensional vector $(y_1, y_2, \ldots, y_m)$. For each layer, we encrypt its input and output using ElGamal encryption.

The ElGamal public-key encryption scheme is defined as follows:

- $Gen(\lambda)$ - returns $pk = (G, p, g, h)$ and $sk = \alpha$ where G is a multiplicative group of prime order p, $g \in G$ and $h = g^\alpha$.
- $Enc_{pk}(m)$ - returns $(c, d) = (g^r, pk^r.m)$ where r is a randomly chosen integer between 1 and $(p - 1)$.
- $Dec_{sk}((c, d))$ - returns $m = \frac{d}{c^{sk}}$.

In our scheme, we use 1024-bit prime p to achieve the recommended security. Note that ElGamal encryption uses randomized encryption and is not deterministic. That means if the same message is encrypted twice then both ciphertexts will be different. Thus each transaction will be indistinguishable and preserve the privacy of the user. Moreover, ElGamal encryption is homomorphic with respect to plaintext multiplication and scalar multiplication.

$$Enc(m_1) * Enc(m_2) = Enc(m_1 m_2)$$

$$Enc(m)^\alpha = Enc(m\alpha)$$

6.8.3 Zero-knowledge–proof system for liveness detection

The result of liveness detection is proved by sending the output of the detection algorithm. This output comes in the form of a yes or no, a Boolean result.

In a centralized system, the algorithm runs in a controlled environment where the central authority manages the input and output. When the user is given the ability to run the liveness detection algorithm on their own there is the risk of a malicious user tampering with the result of the algorithm. Errors can also occur in the transmission of data or local failures in executing the algorithm and obtaining the results.

The system's decentralization includes the need to prove that the result is obtained through a correct execution of the algorithm. That is why in Humanode, we have an algorithm to generate

Archived copy · cryp2nova.com

proof of the correctness of each function of the liveness detection process. In addition, there will be a verification algorithm for the said proof, thus having a zero-knowledge–proof system suitable for decentralized testing of the correct execution of liveness detection.

6.8.4 Collective Authority

One of the most critical problems to solve when defining encryption schemes in decentralized environments is the handling of cryptographic keys, where in addition, the calculations are performed and verified by peers through multi-party computation.

In this sense, we will consider a subgroup of the Humanode network, which we will call the Collective Authority, whose objective is to generate the collective keys for homomorphic encryption and also verify the calculations performed by each peer.

In simple terms, the Collective Authority works as a trusted third party for key generation and verification but is also composed of several peers within the network.

During the Setup process, the Collective Authority is the one who defines generic parameters for the establishment of the cryptographic protocols [26]. The security that this Collective Authority provides us is that each peer takes these generic parameters and locally generates its public and private keys, as we saw above.

Each user keeps his private key secured locally but sends the public key to the Collective Authority. After collecting the public keys from each user, the Collective Authority constructs a collective public key and distributes it back to all users [26]. This collective public key is the one used to encrypt the feature vectors.

If a malicious user intercepts the public key in a traditional cryptosystem, obtaining the private key is computationally challenging. In our case, if the collective public key is intercepted, the perpetrator can't get the private keys, as he must know which partial element belongs to which peer. Thus we have an additional layer of security to the public-key cryptosystem, which we can call a lattice-based decentralized public-key cryptosystem.

6.9 Humanode's multimodal biometric approach

The Biometric Identification Matrix was created by the Humanode core to understand which of the existing biometric modalities 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* [27]:

- 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 patterns, signature, and gait [28].
- Some biometric traits 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 neurosignatures, 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

Archived copy · cryp2nova.com

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 [29], 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*" [30].

Based on Jain et al.'s classification and recent all-encompassing surveys on various biometric systems [31, 32], cancelable systems [33], and unimodal, multimodal biometrics and fusion techniques [34], we provide a comparative study of different biometric modalities, and propose a 'Biometric Identification Matrix', by studying and combining characteristics revealed in the above-mentioned 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 this space in more detail. To grasp how easy it is to collect biometric data on a person, we decided to add the 'Security' category, which refers to vulnerability to attack vectors, as paths or means by which attackers can gain access to biometric data to deliver malicious actions. 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 biometrics, their acceptance of the technology, and their readiness to have their biometrics trait captured and assessed.

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 authentication process using retina scanning [35]. Electrophysiological methods (EEG, ECG) and neurosignatures are not highly accepted nowadays, as they are intricate and not yet well-known or fully developed.

An active liveness detection technology may be uncomfortable for the average user if the trait acquisition method tends to be demanding or time-consuming. Even in the absence of physical contact with sensors, many users still develop a natural apathy for the entire liveness detection process, describing it as over-intrusive (K. Okereafor &Clement E. Onime, 2016).

- **Collectability**

'Collectability' refers to the ease of data capturing, measuring, and processing, as well as 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 [28]. Similarly, the advantages of face biometrics are that it is contactless, and the acquisition process is simple. An 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 stable over the long term. Such modalities have a low or medium level of permanence.

The same person can sign in different ways, as a signature is affected by physical conditions and feelings. Voice is not constant; it may change based on an individual's emotion, sickness, or age [36].

Facial traits are persistent but may change and vary over time, although heat generated by the tissues of the face has a measurable repeatable pattern. It can be more stable than the facial

Archived copy · cryp2nova.com

structure [37]. Finger and palm prints and vein patterns tend to remain constant. Hand geometry is more likely to be affected by disease, weight loss/gain, injury. However, the results of hand geometry recognition are not as much affected by skin moisture or textural changes depending on age. Ear size changes over time [28, 38]. DNA is highly permanent. The iris remains the same throughout life [27, 39]. However, diabetes and some other serious diseases can cause alterations. Likewise, retinal patterns can change during medical conditions like pregnancy, blood pressure, other ailments, etc. [27].

- **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 textures 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 [40]. Although at one time, neuroscientists thought brain activity was pretty much the same from one person to another [41, 42, 43], people display a distinct 'brain signature' when they are processing information, similar to fingerprints.

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 neurosignatures are to be one of the premier biometric technologies because 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 modality can tell individuals apart. This is partially determined by the amount of information gathered as well as the quality of the neural network resulting in higher or lower false acceptance and false rejection rates.

Two-dimensional (2D) facial recognition may give inaccurate results, as facial features tend to change over time due to expression, and other external factors. Also, 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.

Three-dimensional (3D) face recognition has the potential to achieve greater accuracy than its 2D counterpart by measuring the geometry of facial features. It avoids such pitfalls of 2D face recognition as lighting, makeup, etc. It is worth noting that 3D face recognition with liveness detection is considered the best in accuracy.

Archived copy · cryp2nova.com

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 [44].

The iris provides a high degree of accuracy (iris patterns match for 1 in 10 billion people; [45]), but still can be affected by wearing glasses or contact lenses. Similarly, retinal recognition is a highly accurate technology; however, diseases such as cataracts, glaucoma, diabetes, etc. may affect the results.

- **Security**

'Security' refers to vulnerability to attack vectors, i.e., paths or means by which attackers can gain access to users' biometric data to deliver malicious actions.

Vascular biometrics rank as the safest because of the many benefits it inherently offers, it is simple and contact-free as well as resilient to presentation attacks. This applies to both hand and eye vein recognition. The vein pattern is not visible and cannot be easily collected like facial features, fingerprints, voice, or DNA, which stay exposed and can be collected without a person's consent.

However, face recognition offers appropriate security if the biometric system employs anti-spoofing and liveness detection so that an impostor may not gain access with presentation attacks. 3D templates and the requirement of blinking eyes or smiling for a successful face scan are some of the techniques that improve the security of face recognition.

- **Processing Speed**

'Processing Speed' is 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 terms of the identification process. The time used by vein recognition systems is also very impressive and reliable, in terms of 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 0.5 seconds; [46]). Iris and retina recognition have a small template size, hence a promising processing speed (2 to 5 seconds). 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 can be processed fast. Signature, voice, and lip motion recognition take a few seconds. The EEG and ECG processes differ. Acquisition of a DNA sample requires a long procedure to return results [47].

- **Circumvention**

'Circumvention' relates to an act of cheating; thus, the identifying characteristic used must be hard to deceive and imitate using an artifact or a substitute.

Nearly every modality may become an easy subject for forgers. Signatures can be effortlessly mimicked by professional attackers; 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 without five levels of liveness detection can be fooled by sophisticated 3D masks [46]. Even vein patterns can be imitated by developing a hand substitute.

Having said that our DNA is left everywhere, and has no inherent liveness, it is believed to be the most difficult characteristic to dupe, as the DNA of each person is unique [46]. Brain activity and heartbeat patterns are also hard to emulate.

- **Hardware**

Archived copy · cryp2nova.com

'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 biometric recognition. Facial recognition and fingerprints are common features of smartphones. For 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 [48]. For eye vein identification, 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 [49, 50], as well as mobile apps with digital signatures [51].

In the meantime, electroencephalograms are needed for EEG, and electrocardiograms for ECG. Brain-computer interfaces (BCI) are needed for neurosignatures. Special expensive equipment and hardware are needed for DNA-matching procedures.

6.9.1 Neurosignatures and other emerging biometric modalities

We assume that a combination of the above-mentioned biometrics methods (and even multimodal biometrics) are not one hundred percent safe/secure. In the future, we plan to expand the system with this multimodal scheme, making neurosignatures 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 [52]: 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, and cognitive biometrics.

6.9.2 Biometric Identification Matrix

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

		Characteristics/Factors (L—Low, M—Medium, H—High)									
Measurements	Biometric Modality	Acceptability	Collectability	Permanence	Universality	Uniqueness	Accuracy	Security	Processing Speed	Circumvention	Hardware
External Physiological	2D Facial Recognition	H	H	M	H	M	M	M	H	H	H
	3D Facial Recognition	H	H	M	H	M	H	H	H	L	H
	Facial Thermography Recognition	H	H	M	H	H	H	H	H	L	L
	Fingerprint	H	M	H	M	M	L	L	H	H	H
	Palm Print / Footprint Recognition	M	M	H	M	M	M	L	H	M	M
	Finger/Hand Geometry Recognition	M	H	L	H	M	M	L	H	M	L
	Finger/Hand Vein Recognition	M	M	M	M	M	H	H	H	L	L
	Iris Recognition	L	H	H	H	H	H	H	M	L	M
	Retina Recogntion	L	M	H	H	H	H	H	M	L	L
	Eye Vein Recognition	L	L	H	H	H	H	H	M	L	M
	Ear Shape	H	M	H	M	L	L	L	M	M	M
	Body Odor	M	L	H	H	L	L	M	M	L	L
	DNA Matching	L	L	H	H	H	H	L	L	L	L
Physiological + Behavioral	Brain Activity (EEG)	L	L	M	H	H	H	H	L	L	L
	Electrocardiography (ECG)	L	L	M	H	M	H	H	L	L	L
Internal Physiological + Behavioral	Neurosignatures	L	L	H	H	H	H	H	H	L	L
Behaviormetrics	Gait	M	H	M	M	M	L	L	M	M	L
	Keystroke Dynamics	H	H	L	L	L	L	M	M	M	M
	Lip Motion Recognition	H	H	M	H	L	L	M	H	L	H
	Signature Recognition	H	H	L	L	L	M	L	H	H	M
	Voice Recognition	H	H	L	M	M	M	L	H	H	H

Archived copy · cryp2nova.com

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.

Measurements	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 impostor attacks, errors: lighting, age, glasses, hair
	3D Facial Recognition	easy, fast, and accurate	Potential attacks of lifelike dolls, realistic 3D masks that may bypass the system
	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 is 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.

Archived copy · cryp2nova.com

	Eye Vein Recognition	long-term stability, the technology works even with glasses or contact lenses	quality of images 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 Odors	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
	DNA Matching	provides high accuracy, does not suffer from system performance issues	complex method, requiring a physical sample that 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	Neurosignatures	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
Behaviometric	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 the 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

Archived copy · cryp2nova.com

6.9.3 Humanode Biometric Modalities Score

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

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

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

To evaluate every above-mentioned biometrics modality technique, we proposed the 'Humanode Biometric Modalities Score', based on the 'Biometric Identification Matrix' analyzed in Table 4.

The study revealed that the 3D facial recognition technique has the highest score (198), with facial thermography recognition (192) and iris recognition (190) not far behind. Retina recognition (176) and eye vein recognition (178) also got quite high scores, as well as neurosignatures (173), which are not so highly scored because they are not yet fully developed or widely adopted.

Table 5: 'Biometric Identification Matrix': Modalities Scores.

Biometric Modality	Characteristics/Factors (1—Low, 2—Medium, 3—High)										Modalities Score
	Acceptability (6)	Collectability (6)	Permanence (5)	Universality (5)	Uniqueness (10)	Accuracy (8)	Security (10)	Processing Speed (3)	Circumvention (10)	Hardware (8)	
Facial Recognition	3	3	2	3	2	2	2	3	1	3	160
3D Facial Recognition	3	3	2	3	2	3	3	3	3	3	198
Facial Thermography Recognition	3	3	2	3	3	3	3	3	3	1	192
Fingerprint	3	2	3	2	2	1	1	3	1	3	136
Palm Print / Footprint Recognition	2	2	3	2	2	2	1	3	2	2	140
Finger/Hand Geometry Recognition	2	3	1	3	2	2	1	3	2	1	133
Finger/Hand Vein Recognition	2	2	2	2	2	3	3	3	3	2	170
Iris Recognition	1	3	3	3	3	3	3	2	3	2	190
Retina Recognition	1	2	3	3	3	3	3	2	3	1	176
Eye Vein Recognition	1	1	3	3	3	3	3	2	3	2	178
Ear Shape	3	2	3	2	1	1	1	2	2	2	125
Body Odor	2	1	3	3	1	1	2	2	3	1	130
DNA Matching	1	1	3	3	3	3	1	1	3	1	147
Brain Activity (EEG)	1	1	2	3	3	3	3	1	3	1	146
Electrocardiography (ECG)	1	1	2	3	2	3	3	1	3	1	152
Neurosignatures	1	1	3	3	3	3	3	3	3	1	173
Gait	2	3	2	2	2	1	1	2	2	1	122
Keystroke Dynamics	3	3	1	1	1	1	2	2	2	2	126
Lip Motion Recognition	3	3	2	3	1	1	2	3	3	3	162
Signature Recognition	3	3	1	1	1	2	1	3	1	2	117
Voice Recognition	3	3	1	2	2	2	1	3	1	3	131

Archived copy · cryp2nova.com

* When calculated, we swapped the levels (numbers) for the 'Circumvention' factor so that it could be correlated with other factors, since a 'High' level of circumvention means it is easy to imitate the body part, the modality, by using an artifact or substitute, while a 'Low' level of circumvention means this is practically impossible to do. In our model 'Low' is assin a value of 3 while 'High' is assigned the value -1.

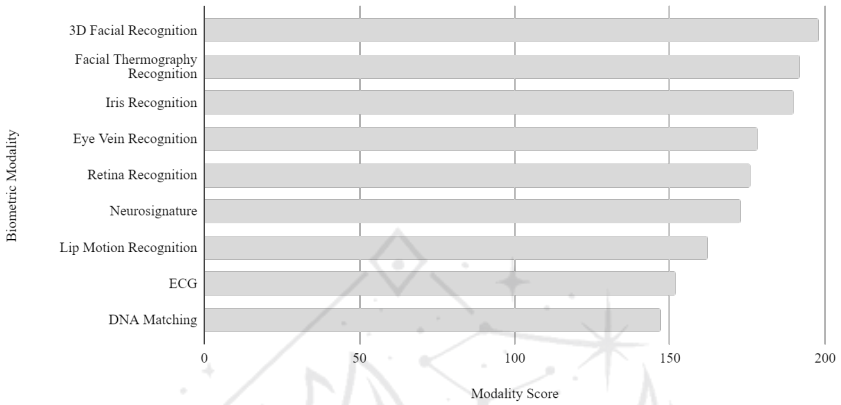


Figure 14: 'Biometric Identification Matrix': Modalities Scores

To create a human node, only those modalities will be used that have score points above the median value (> 147), i.e., 2D facial recognition, 3D facial recognition, facial thermography recognition, iris, retina, finger/hand vein recognition, eye vein recognition, ECG, DNA matching, and neurosignatures (in the future).

Due to the possible development of methods of attack on the current biometric security setup in the future, the Humanode network will require human nodes to provide additional biometric data during network upgrades. For instance, once iris verification is shown 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 [53] 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 permission to launch a human node. Starting only with 3D facial recognition and liveness detection, later on one will have to go through multimodal biometric processing.

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.

6.10 Types of attacks on biometric systems and their solutions

Currently, there are eight possible attacks against biometric systems, which are discussed below.

Archived copy · cryp2nova.com

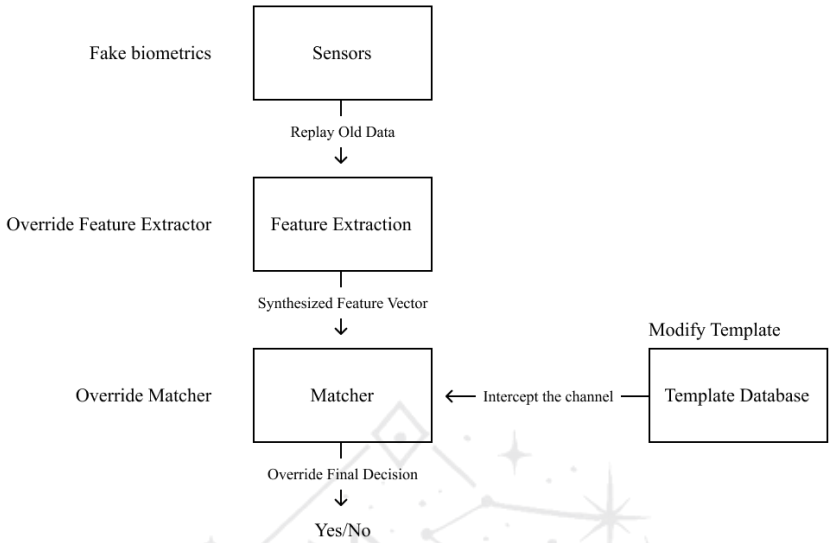


Figure 15: Possible attacks on biometric verification systems.

6.10.1 Attack on the sensor

Attackers can present fake biometrics to attempt to fool sensors [54]. For example, someone can make a fake hand with fake vein patterns, or a finger with a fake wax fingerprint; wear special-made lenses to bypass the iris scanner; and 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 [55].

Multimodal biometrics is the main technique 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 (see the 'Humanode Biometric Modalities Score' section for more information).

Liveness detection uses different physiological properties to differentiate between real and fake characters. An AI computer system can determine that it is interfacing with a physically present human being and not an inanimate spoof artifact.

A non-living object that exhibits human traits is called an 'artifact'. The goal of the artifact is to fool biometric sensors into believing that they are 4 interacting with a real human being instead of an artificial copycat. When an artifact tries to bypass a biometric sensor, it is called a 'spoof'. Artifacts include photos, videos, masks, deepfakes, and many other sophisticated methods of fooling the AI. Another method of trying to bypass sensors is by trying to insert already captured data into a system directly without camera interaction. The latter is referred to as 'bypass'.

In the biometric authentication process, liveness data should only be valid for a set period of time (up to several minutes) and then is deleted. As this data is not stored, it cannot be used to spoof liveness detection with corresponding artifacts to try and bypass the system.

The security of liveness detection is very dependent on the amount of data it is able to detect. That is why low-resolution cameras might never be totally secure. For example, if we take a low-res

Archived copy · cryp2nova.com

camera and put a 4k monitor in front of it, then weak liveness detection methods such as turning your head, blinking, smiling, speaking random words, etc. can be easily emulated to fool the system.

In 2017, the International Organization of Standardization (ISO) published the ISO/IEC 30107-3:2017 standard for presentation attacks and went over ways to stop artifacts such as high-resolution photos, commercially available lifelike dolls, silicone 3D masks, etc. from spoofing real identities. Since then, sanctioned PAD (presentation attack detection) tests for biometric authentication solutions have been created so that any new solutions meet the specified requirements before hitting the market. The most famous of them all is the iBeta PAD Test. It is a strict and thorough evaluation of biometric processing solutions to see whether they can withstand the most intense presentation attacks. Four years have passed since then and this standard is condemned as outdated by many specialists in the field, and iBeta PAD tests have gradually become easier to pass with modern sophisticated spoofing methods.

FaceTec, one of the leading companies in liveness detection, divides attacks into five categories that go way beyond those stated in the 30107-3:2017 standard and represent real-world threats much more precisely.

Depending on the artifact type, there are three levels of PAD attacks:

Level 1—Hi-Res digital photos, HD videos, and paper masks

Level 2—Commercially available lifelike dolls, latex and silicone 3D masks

Level 3—Ultra-realistic artifacts like 3D masks and wax heads

Furthermore, depending on the bypass type, FaceTec researchers identify Level 4 & 5 biometric template tampering, and virtual camera and video injection attacks:

Level 4—Decrypt & edit the contents of a 3D template to contain synthetic data not collected from the session, having the server process and respond with 'Liveness Success'.

Level 5—Take over the camera feed and inject previously captured video frames or a deepfake puppet that results in the AI responding with 'Liveness Success'.

CRYP2NOVA

Archived copy · cryp2nova.com



Figure 16: 5 levels of liveness.

Almost all liveness detection methods as well as those described above in the Humanode approach to user identification are *software-based* and available on any modern smartphone. In *hardware-based methods*, 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

Archived copy · cryp2nova.com

by an artificially created human node minus the costs to run the node.

The Humanode network implements 3D facial liveness detection from the testnet.

6.10.2 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 older recorded data to bypass the feature extraction module [54].

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. It is a way to combat replay attacks, but only if that data has been seen before or the watermark cannot be removed.
- A challenge-response system, in which a task or a question is given to the person as a challenge and the person responds to the challenge voluntarily or involuntarily [55].

6.10.3 Attack on the channel between the database and the matcher

The attacker intrudes on 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 [56].

6.10.4 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
- *Cryptobiometrics*, where all data are 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 of template protection scheme.

6.10.5 Overriding the final decision

As the software application may have bugs, an intruder can override the actual decision made by the matcher.

Humanode ensures that nobody knows the actual decision result of matching but the protocol before this decision is executed. This kind of attack can be prevented using soft biometrics as well [55].

Archived copy · cryp2nova.com

6.10.6 Overriding the 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. The human node encrypts the embedded feature vector using the public key and gets the encrypted feature vector. Further, it provides ZKP proof that the feature vector is extracted through the system's feature extraction process only, as a result the attacker is unable to override it.

6.10.7 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 impostor.

In Humanode, the matching score is computed over an encrypted feature vector. Moreover, the matcher is required to provide proof of correctness for the matched score. As a result, the attacker cannot override matchers to generate a high matching score for a target feature vector.

6.10.8 Synthesized feature vector

The route from the feature extractor to the matcher is intercepted to steal the feature vector of the authorized user. Using the legitimate feature vector, the attacker then iteratively changes the false data, retaining only those changes that improve the score until an acceptable match score is generated and the biometric system accepts the false data. The legitimate feature sets are replayed later with synthetic feature sets to bypass the matcher [56, 54, 55].

In the Humanode system, there is a private channel between the feature extractor and the matcher while the feature vector is always kept in encrypted form and is never available in a plain form to the attacker. Therefore these kinds of attacks are not possible.

6.10.9 Reconstruction attack

Recently, Mai G. et al. [57] proposed a neighborly de-convolutional neural network (NbNet) to reconstruct face images from their deep templates. In a distributed P2P network, a node can have access to a biometric template database, and it can use NbNet to reconstruct corresponding 2D or 3D masks with a very high success probability for verification.

A robust liveness detection prevents the use of a reconstructed 2D or 3D mask, but it does not protect the privacy of the corresponding user. For protecting privacy, there are several solutions based on user-specific randomness in deep networks and user-specific subject keys. Along with using robust liveness detection, Humanode stores all biometric templates in the encrypted form and these are never available in the plain form to the attacker.

Archived copy · cryp2nova.com

Table 6: Attacks on biometric systems and their possible solutions

Attacks	Humanode's approach
Attack on the sensor	Liveness detection, multimodal biometric systems, soft biometrics
Replay attack	Steganography, watermarking techniques, challenge-response systems
Attack on the channel between the matcher and database	Steganography, watermarking techniques, challenge-response systems
Attack on the database	ElGamal Cryptosystem and BFV lattice-based encryption for biometric data
Override final decision	Soft biometrics
Override feature extractor	Impossible due to ZKP
Override matcher	Encrypted Matching process
Synthesized feature vector	A private channel between the feature extractor and the matcher
Reconstruction Attack	Liveness detection, encrypted biometric templates

6.11 Neurosignatures

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 BCI development, rapidly approaching adoption. Companies, like BrainGate and Neuralink, [58, 59] have manufactured working prototypes of invasive and non-invasive BCIs that build a digital link between brains and computers. In 2014, Brainlab [60] 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 [61], 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 [62] that set a new benchmark for decoding speech directly from brain activity. Even with the immeasurable complexity of neurons and ridiculous entanglements 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.

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 including 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.

Archived copy · cryp2nova.com

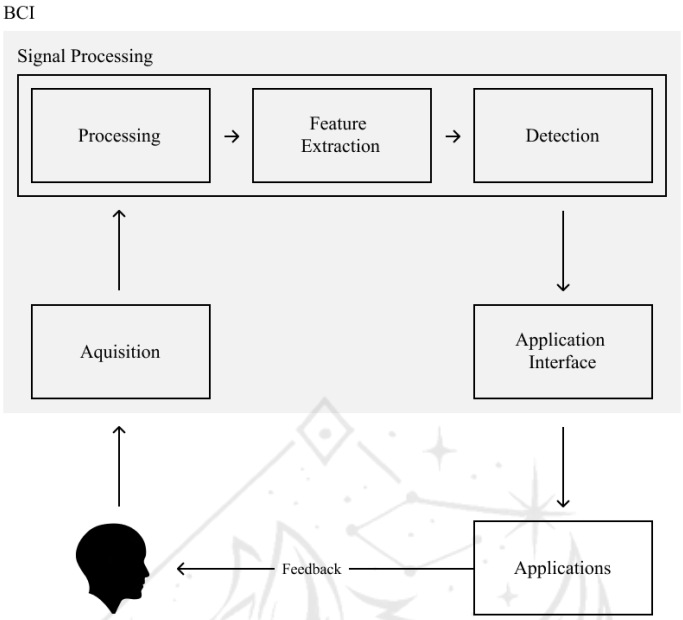


Figure 17: Block diagram of a BCI system.

Table 7: Summary of signal acquisition method [63].

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	Electrical	Portable	Low	Mediate
	MEG	Magnetic	Non-portable	Mediate	Mediate
	fMRI	Metabolic	Non-portable	High	Low
	fNIRS	Metabolic	Portable	Mediate	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, p rove it [64, 65, 66, 67]. These hBCI systems are categorized according to the type of signal combined as well as 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 [68]. In general, the essential goal of combining signals is to increase detection accuracy, enhance system speed, improve the user experience, and overcome the disadvantages of BCI systems [69]. 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:

Archived copy · cryp2nova.com

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.

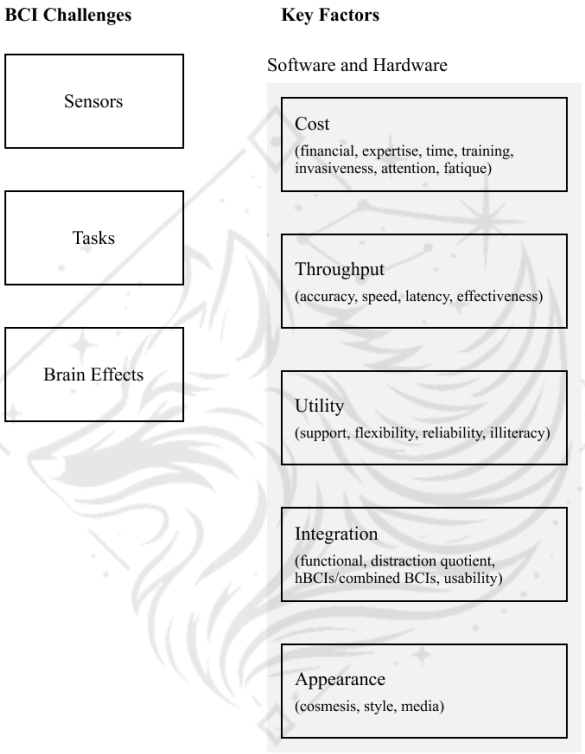


Figure 18: Factors that influence adoption.

Researchers are making great strides toward 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 [70, 71, 72, 73, 74]. There is a relevant body of work addressing not only technology improvements [75] but also the fact that BCI design and development should become more user-friendly to achieve successful mainstream applications [76, 77].

6.12 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 [78, 79, 80, 81], along with studies combining these systems with biometrics [82, 83, 84].

Archived copy · cryp2nova.com

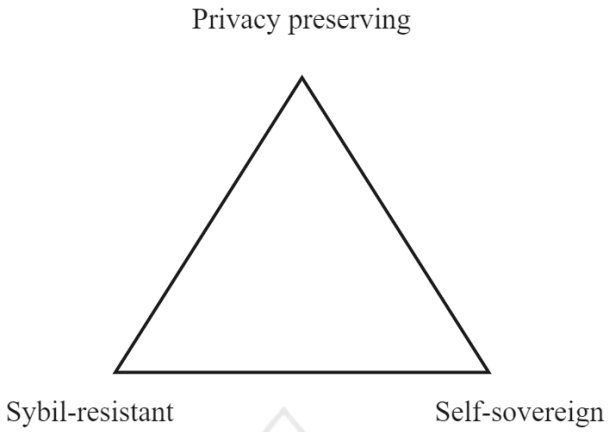


Figure 19: Decentralized Identity Trilemma [85].

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 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 [86, 87, 88, 89].

None of the existing solutions are privacy-preserving, self-sovereign, and Sybil-resistant at the same time [85]. We at Humanode propose the following solutions to break the trilemma.

6.12.1 Self-sovereignty

The Humanode protocol applies principles of self-sovereign identity, requiring that users be the rulers of their own ID [90]. In Humanode, there is no centralized third party to control one's ID, thus ID holders can create and fully control their identities.

6.12.2 Privacy-preserving

In order to meet the security requirements of protecting highly private biometric information on a truly global decentralized system that is run on nodes by everyday people, simply encoding the information using cryptography (no matter how high the encryption) is not enough. We also need to consider the integrity of the information, preventing malicious actors from accessing the information and the network as a whole, preventing Sybil attacks, deepfakes, and an endless number of various possible and potential attacks. This is where the concept of cryptobiometrics comes into play.

Obviously, in order to safeguard the information while allowing the necessary information (such as if this is a registered user or not, or what account is he or she tied to), cryptobiometrics is based on a combination of various technologies and exists at the intersection of the disciplines of mathematics, information security, cybersecurity, Sybil resistance, biometric technology, liveness detection, zero-knowledge–proof (ZKP) technologies, encryption, and blockchain technology.

6.12.3 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 [91, 92]. In recent years, attempts in the field were made by blockchain-based initiatives like HumanityDAO, POAP, BrightID,

Archived copy · cryp2nova.com

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 8: 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

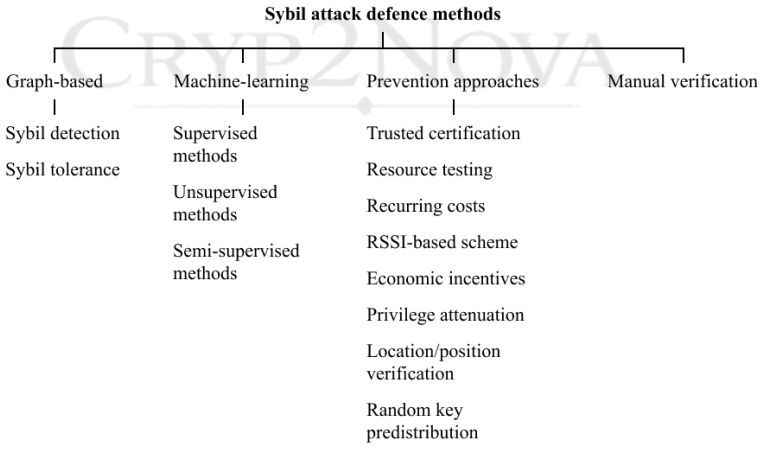


Figure 20: Main Sybil attack defense methods.

Archived copy · cryp2nova.com

- *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 [93, 94].

- *Machine-learning methods*

These methods fall into the following categories:

1. Supervised, which use regression models, support vector machine (SVM) [95], and decision tree models
2. Un-supervised, which use fuzzy logic, Markov models [96], 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 9: Main techniques for preventing Sybil attacks.

Technique	Application Domain	Description
Cryptobiometrics	General	A combination of cryptographically secure matching and liveness detection mechanisms to verify the uniqueness and existence of real human beings.
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 [97, 98, 99]. 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 [100].
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 [101, 102, 103]. The main disadvantage is that it may encourage attackers economically.

Archived copy · cryp2nova.com

From the very start, Humanode uses the above-mentioned 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.

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; [104])
- *Existing* (the person behind the ID is alive and well)

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 periodic verification of identity
- Biochemical biometrics—direct DNA screening and neurosignature biometrics through BCI

***

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.

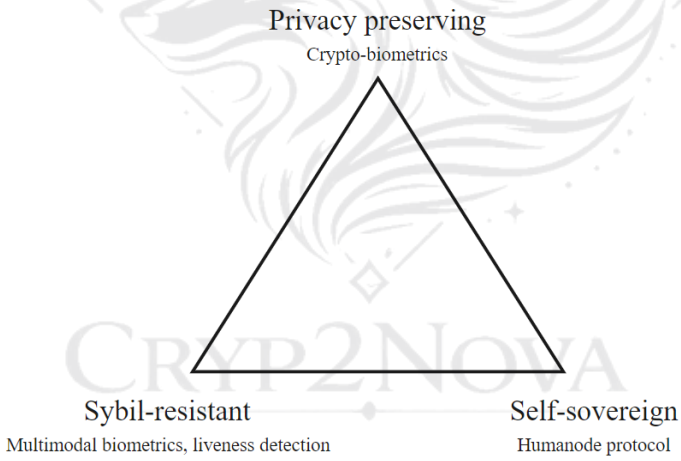


Figure 21: Humanode's approach to identity attack prevention

7 Transaction fee economics of the Humanode network

This part of the paper describes important considerations when selecting an optimal fee strategy for a public cryptonetwork. It is proposed that the Humanode network will have a cost-based fee policy that differentiates it from the existing public permissionless systems based on the internal gas market.

Archived copy · cryp2nova.com

7.1 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 [105] 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 node.

7.2 Cost-based fee system

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 making it more stable over time.

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 are spent on renting computing resources from the largest web service provider in a certain period determines the amount of HMND tokens the user pays after submitting the transaction. 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.

The protocol gets the computational cost in USD quoted by major cloud computing and storage providers through an oracle-checked API. The largest price for renting hardware will be set as the base computational cost of the node.

Instead of having an internal gas token with its own market, in a cost-based fee system the currency most used by cloud service providers becomes the internal non-tradable fee token. For US dollars we use gusd as an internal gas token. It is used only for determining the protocol's fees at an exact moment in time. Actual fees are paid in HMND, and the amount is defined by the exchange rate provided by the oracles including decentralized exchange data.

In order to define a user's fee, we multiply the validator's cost of computation by the number of validators involved in processing the data.

Now after agreeing on the transaction, human nodes have to store the updated ledger 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, we set the base cost for a set time period.

We know the storage costs for a given month. However, the price of the storage resources does not stay the same over a longer time frame. Hence, we have to define a formula that determines the cost of permanent storage over time. This formula is based on the data sources, methodology and, eventually, rate of cost decline and is agreed upon in the Vortex.

Over the past 50 years, the cost of commercially available storage has been decreasing at an annual rate of 30.57% [106]. Extrapolating from this data, the costs of perpetual data storage can be presented as the infinite sum of the declining storage costs over time:

$$Pstore = \sum_{i=0}^{\infty} (Data_{size} * P_{GBH}[i])$$

where
$PStore$ = The perpetual price of storage
$P_{GHB}[i]$ = The cost of storing 1 GB for an hour at time i
$Data_{size}$ = The quantity of data to store

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.

Archived copy · cryp2nova.com

Submitting the transaction, the user pays the cost of perpetual storage multiplied by the number of nodes storing the data at the moment. After receiving the fees, the protocol distributes them equally among the human nodes. This mechanism ensures that the fee the protocol gets is higher than the actual cost for storing data, which includes its future storage. This creates an incentive to continue operating a Humanode server, ensuring the network's long-term stability.

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 encrypt, process, and store biometric data, send transactions with on-chain assets, execute smart contracts, and connect to other ledgers and databases.

8 Vortex

The concept of a "Decentralized Autonomous Organization" (DAO) was proposed by Daniel Larimer ([107]) and implemented in Bitshares [108] in 2014. In 2014, Vitalik Buterin, the founder of Ethereum 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 [109]. 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 [110], that is "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" [109].

Governance in the Humanode network will be decentralized from genesis and is known as Vortex—the Humanode DAO, to propose and decide on changes to the Humanode network. 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. *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.
3. *Delegator*—a Governor who decides to delegate his voting power to another Governor.

The Governors will have different rights according to their tiers. Tiers 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. Tiers do not give any additional voting powers to their holders; instead, they are given the ability to make and promote proposals on crucial matters. If a human node wants to become a Governor, they must have their proposal accepted by the Vortex DAO. All proposals are submitted to the proposal pool anonymously.

Table 10: 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
Run a node	Required	Required	Required	Required
Have one of your proposals approved by Vortex	Required	Required	Required	Required

Archived copy · cryp2nova.com

The combination of PoT and PoD in Humanode governance means that a Governor progresses through tiers based on the time their node was considered governing and the amount of devotion a Governor channeled into the network. On top of that, to progress to a Legate or higher, a Governor must participate in Formation, a proposal-based grant mechanism. Even if a Governor participates in Formation during the first days of his node's existence, he will still be required to govern for another three years to become a Legate.

Table 11: Governor rights.

Rights	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 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% of the Governors within the quorum vote to approve a proposal, then Vortex will consider it approved. This means that 22% of the Governors will be the necessary minimum to approve a proposal. Human nodes that do not participate in governance are not counted in reaching 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.

CRYP2NOVA

Archived copy · cryp2nova.com

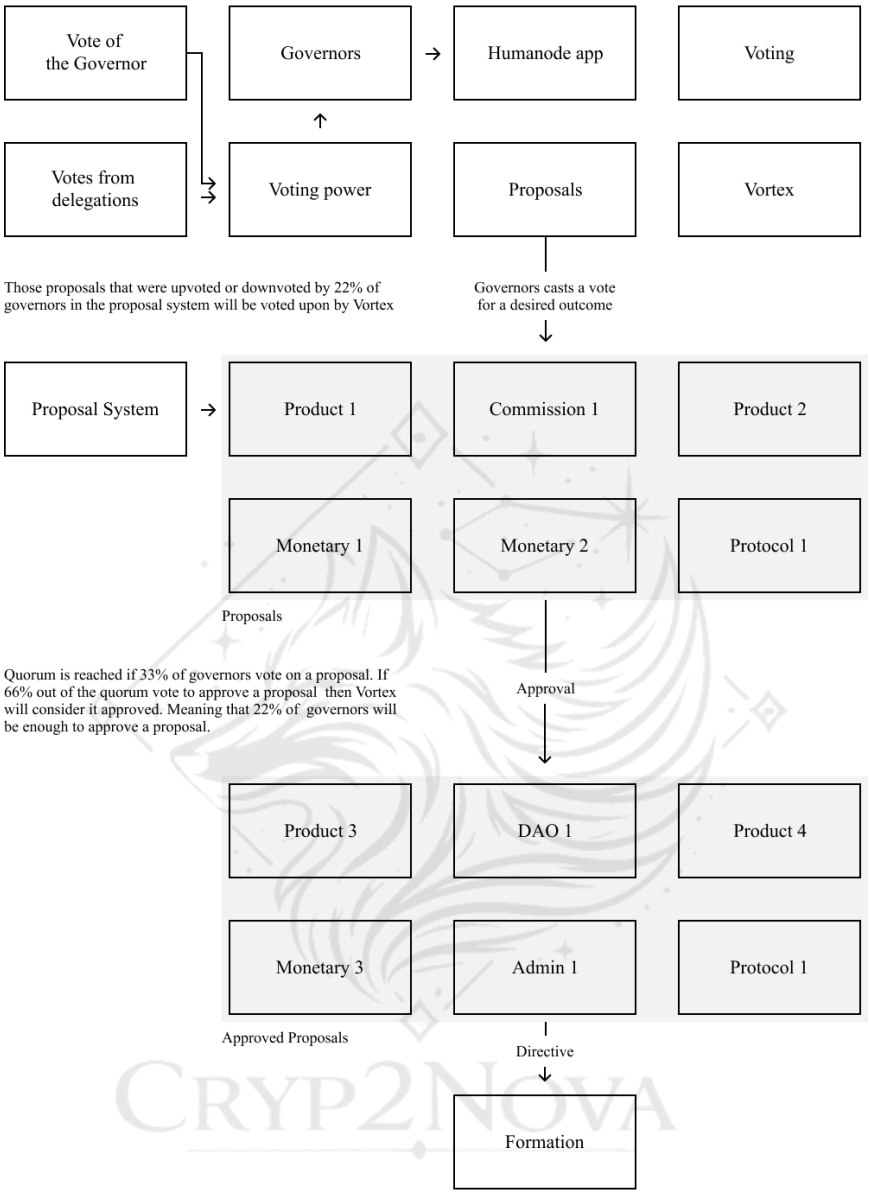


Figure 22: Vortex voting procedures.

Becoming a part of Vortex gives access to different governing tools based on the user's Governor tier. Hypothetically, separation of voting powers 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.

Archived copy · cryp2nova.com

8.1 Tiers and proposal types

Tiers give various proposal rights to the Governors. The higher the tier the more crucial a proposal a Governor can make.

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

Tier 1 Citizen

Product Changes in the products. Max time in proposal pool: 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

Tier 2 Senator

Fee distribution Vortex can change fee distributions. Maximum time in the proposal pool: 1 month.

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

Monetary Modifying Humanode's monetary system and its principles via DAO. Max time in proposal pool: 1 month.

- Creation of HMND tokens
- Implementation of Fath on the Humanode main net
  - Proportional emission distribution
  - Monetary Supply Balancing mechanisms
- Equality of fee distribution among human nodes

Tier 3 Legate

Protocol HUPs are the way to create enforceable changes to the Humanode protocol. Max time in proposal pool: 2 months.

- Combination of biometrics through multimodal biometric processing in node creation
- Substrate blockchain
- Consensus mechanism (Aura, Snowball, Grandpa, Nakamoto, Agnostic)
- Sybil defense through decentralized cryptobiometrics
- Equality between peers in decisions on a global state
- Delegation mechanics

Archived copy · cryp2nova.com

Administrative Max time in proposal pool: 3 months.

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

Tier 4 Consul

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 HUPs to do anything possible on the DAO. Simply by submitting proposals, Vortex can go wherever the imagination takes proposers. Maximum time in the proposal pool: 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 above-mentioned characteristics will be implemented on top of the Humanode network at the deployment stage.

8.2 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 two times for a particular decision.

8.3 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 while 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 five proposals at the same time. All proposals are submitted to the proposal pool anonymously.

Archived copy · cryp2nova.com

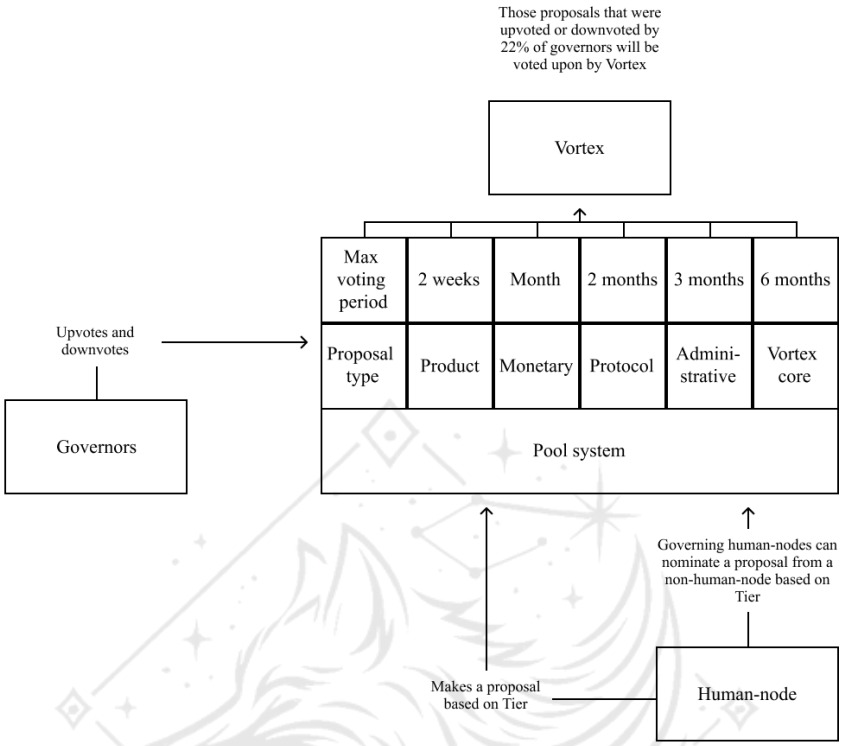


Figure 23: Proposal pool system and voting periods.

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.

8.4 Formation

Vortex governs the Humanode by deciding on key parameters through the voting power of human nodes.

Archived copy · cryp2nova.com

Formation is a part of the Humanode. It is a special grant-based development system providing grants, investments, service agreements, and projects to build. 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:

Archived copy · cryp2nova.com

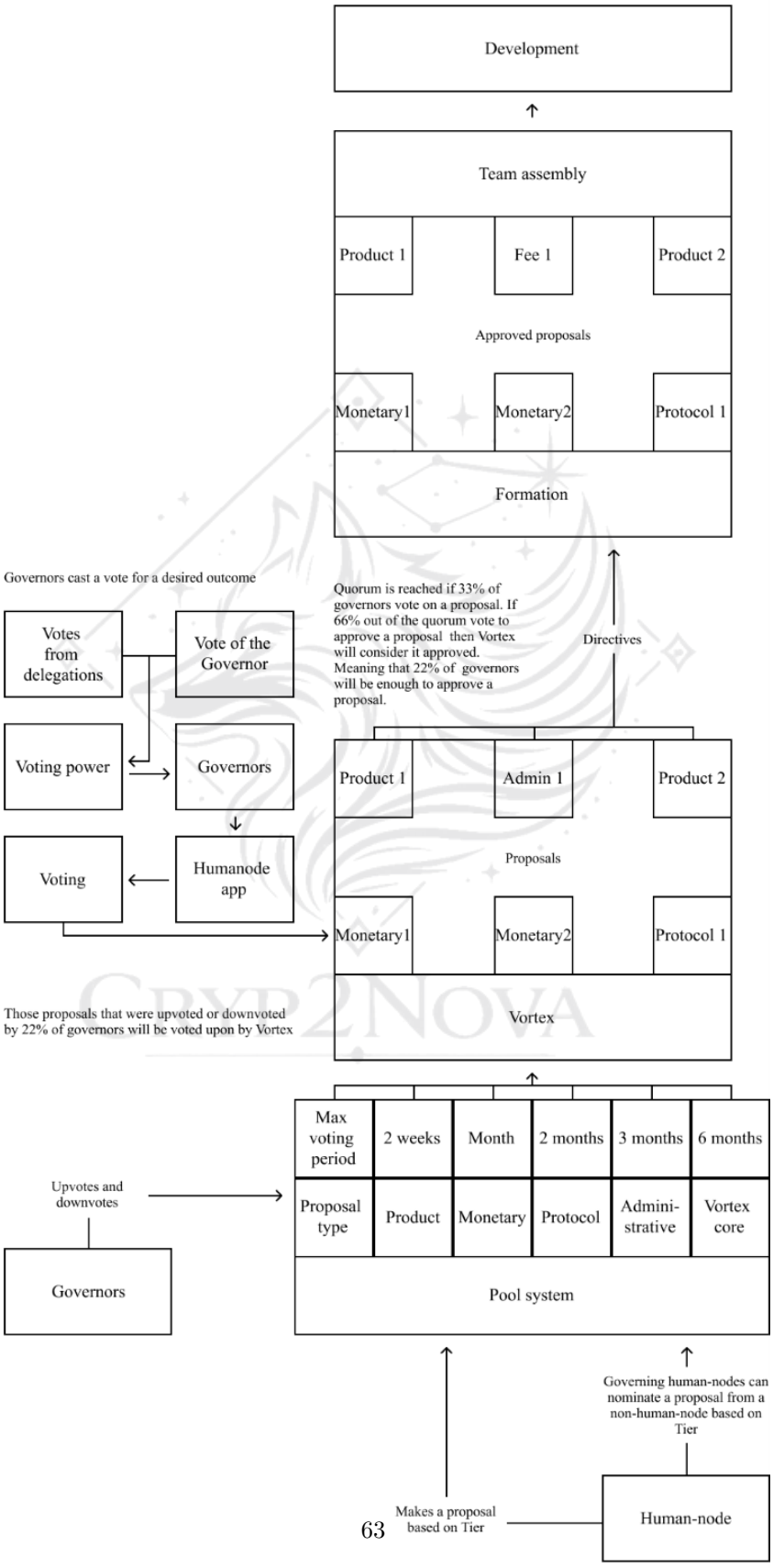


Figure 24: Proposal pool, Vortex, and Formation processes.

Archived copy · cryp2nova.com

Human nodes create proposals, allocate funds for their implementation, and take coordinated action to see the proposals implemented properly. 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 cryptobiometrics, cryptographic primitives, distributed systems, consensus mechanisms, smart-contract layers, biometric modalities, liveness detection, encrypted search, and matching operations.
- Development and Product: Development turns research into software, while Product turns it into user experiences. Formation is primarily interested in technologies that expand the Humanode network, its potential, capabilities, and security, as well as the ecosystem, from decentralized finance and non-fungible tokens to decentralized courts.
- Social Good & Community: Formation supports community members to bring awareness to open-source, decentralized networks, and biotechnologies, and scale community outreach for the Humanode network.

The Formation funds are mainly used to maintain the network.

8.4.1 Assembling a team

We 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 grant proposal in Formation does not include the team, its members might be selected from the human nodes who are interested in the proposed project.

9 Discussion

9.1 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:

Archived copy · cryp2nova.com

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 in proposals and voting from Governors and proof of existence from all human nodes. Those Governors who do not fulfill monthly governing conditions (either they did not make proposals 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. The necessity to have your proposal approved before becoming a Governor acts as a Proof-of-Devotion step that uplifts the quality of Governors and acts as an important layer of defense against Sybil attacks.

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. Governing 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+ the number 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 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 the 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 weight of Humanode's initial group will be diluted. Another authoritarian point is that in the first four 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.

9.2 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

Archived copy · cryp2nova.com

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 truly 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 [111].

This law is directly applied to modern elites. The financial network is always a complex multilayer 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, unbiased intellectual barriers, direct delegation, Proof-of-Time, Proof-of-Devotion, 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. The 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.

9.3 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 arsenals and have democratic political systems. The vote on the

Archived copy · cryp2nova.com

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 the 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, 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. Natural autocracy rises in the chokepoints of strategic value.

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 of using 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 DAO 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 PoS (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 the commission size, uptime, and security of the delegate's server might reflect on the 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 the system from manipulated panic-based

Archived copy · cryp2nova.com

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.

9.4 Populist tide and professional backslide

It is commonly acknowledged that any voting system faces the problem of too much populism. Hypothetically there are two major approaches to how populism is perceived:

- 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.
- 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. 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 number 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. This is slightly balanced out by the fact that human nodes must have an accepted proposal before they become Governors. Thus Governors should be less affected by populist media, as they have a confirmed intellectual skill set that allowed them to create a useful proposal accepted by the Governors of Humanode.

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 the direct and active participation of human nodes in governing processes. The more Governors 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.

Archived copy · cryp2nova.com

References

[1] Habermeier R., "Swappable Consensus." https://github.com/paritytech/substrate/issues/1304, 2018. Online; accessed 26 September 2021.

[2] Tang, W., "Re-Genesis." https://github.com/paritytech/substrate/issues/7458, 2020. Online; accessed 26 September 2021.

[3] Research and Markets. , "Biometrics - Global Market Outlook (2018-2027)." https://www.researchandmarkets.com/reports/5017531/biometrics-global-market-outlook-2018-2027?utm_source=dynamic&utm_medium=BW&utm_code=b4k3kn&utm_campaign=1381747+-+Global+Biometrics+Market+Outlook+to+2027%3a+Impact+of+COVID-19&utm_exec=joca220bwd, 2018. Online; accessed 26 September 2021.

[4] Emergen Research. , "Global Biometrics Market Size to Reach USD 99.63 Billion in 2027." https://www.prnewswire.com/news-releases/global-biometrics-market-size-to-reach-usd-99-63-billion-in-2027--increasing-penetration-of-smartphones-around-the-world-and-increasing-integration-of-biometric-systems-with-iot-devices-are-some-key-factors-driving-industry-deman-301350996.html, 2021. Online; accessed 26 September 2021.

[5] Apple Support. , "About Face ID advanced technology." https://support.apple.com/en-us/HT208108, 2021. Online; accessed 26 September 2021.

[6] Global Industry Analysts, Inc, "Mobile Biometrics - Global Market Trajectory & Analytics." https://www.researchandmarkets.com/reports/5027979/mobile-biometrics-global-market-trajectory-and#rela4-5117598, 2021. Online; accessed 26 September 2021.

[7] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in *Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No.98CB36186)*, pp. 148–157, 1998.

[8] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[9] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002. Pattern Recognition in Information Systems.

[10] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[11] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.

[12] A. B. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, 2008.

[13] U. A. Rathgeb C., "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. on Info. Security*, no. 3, 2011.

[14] M. A. Syarif, T. S. Ong, A. B. J. Teoh, and C. Tee, "Improved biohashing method based on most intensive histogram block location," in *Neural Information Processing* (C. K. Loo, K. S. Yap, K. W. Wong, A. T. Beng Jin, and K. Huang, eds.), (Cham), pp. 644–652, Springer International Publishing, 2014.

Archived copy · cryp2nova.com

[15] B. J. Jisha Nair and S. Ranjitha Kumari, "A review on biometric cryptosystems," *A Review on Biometric Cryptosystems*, vol. 6, no. 1, pp. 46–53, 2015.

[16] H. Kikuchi, K. Nagai, W. Ogata, and M. Nishigaki, "Privacy-preserving similarity evaluation and application to remote biometrics authentication," in ., pp. 3–14, 10 2008.

[17] R. Belguechi, E. Cherrier, V. Alimi, P. Lacharme, and C. Rosenberger, *An Overview on Privacy Preserving Biometrics*. IntechOpen, 07 2011.

[18] , "Representation of image as a grid of pixels." http://pippin.gimp.org/image_processing/images/sample_grid_a_square.png, 2021. Online; accessed 26 September 2021.

[19] Shyamal Patel and Johanna Pingel, "Introduction to Deep Learning: What Are Convolutional Neural Networks?." https://www.mathworks.com/videos/introduction-to-deep-learning-what-are-convolutional-neural-networks--1489512765771.html, 2021. Online; accessed 26 September 2021.

[20] H. Gholamalinezhad and H. Khosravi, "Pooling methods in deep neural networks, a review," 2020.

[21] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Advances in Cryptology – CRYPTO 2013* (R. Canetti and J. A. Garay, eds.), (Berlin, Heidelberg), pp. 75–92, Springer Berlin Heidelberg, 2013.

[22] T. Dinh, R. Steinfeld, and N. Bhattacharjee, "A lattice-based approach to privacy-preserving biometric authentication without relying on trusted third parties," in *Information Security Practice and Experience* (J. K. Liu and P. Samarati, eds.), (Cham), pp. 297–319, Springer International Publishing, 2017.

[23] A. Abidin and A. Mitrokotsa, "Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-lwe," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 60–65, 2014.

[24] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages," in *Advances in Cryptology – CRYPTO 2011* (P. Rogaway, ed.), (Berlin, Heidelberg), pp. 505–524, Springer Berlin Heidelberg, 2011.

[25] J. Chotard, E. Dufour-Sans, R. Gay, D. H. Phan, and D. Pointcheval, "Decentralized multi-client functional encryption for inner product." Cryptology ePrint Archive, Report 2017/989, 2017. https://ia.cr/2017/989.

[26] D. Froelicher, P. Egger, J. S. Sousa, J. L. Raisaro, Z. Huang, C. Mouchet, B. Ford, and J.-P. Hubaux, "Unlynx: A decentralized system for privacy-conscious data sharing," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, pp. 232 – 250, 2017.

[27] G. Kaur and C. K. Verma, "Comparative analysis of biometric modalities," in ., 2014.

[28] S. Jaiswal, S. S. Bhadauria, and D. S. Jadon, "Biometric: Case study," *Journal of Global Research in Computer Sciences*, vol. 2, pp. 19–49, 2011.

[29] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. Norwell, Massachusetts: Kluwer Academic Publishers, 1999.

[30] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 14, pp. 4 – 20, 02 2004.

Archived copy · cryp2nova.com

[31] A. Weaver, "Biometric authentication," *Computer*, vol. 39, pp. 96–100, feb 2000.

[32] V. P. Venkatesan and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," in ., 2018.

[33] B. Choudhury, P. Then, B. Issac, V. Raman, and M. Haldar, "A survey on biometrics and cancelable biometrics systems," *International Journal of Image and Graphics*, vol. 18, p. 1850006, 01 2018.

[34] A. Raju and V. Udayashankara, "A survey on unimodal, multimodal biometrics and its fusion techniques," *International Journal of Engineering and Technology(UAE)*, vol. 7, pp. 689–695, 12 2018.

[35] F. Sadikoglu and S. Üzelaltınbulat, "Biometric retina identification based on neural network," *Procedia Computer Science*, vol. 102, pp. 26–33, 12 2016.

[36] L. Rabiner and B.-H. Juang, *Fundamentals of Speech Recognition*. USA: Prentice-Hall, Inc., 1993.

[37] M. Hanmandlu and S. Vasikarla, "Online biometric authentication using facial thermograms," in ., pp. 1–6, 10 2012.

[38] A. Abaza, A. Ross, C. Hebert, M. Harrison, and M. Nixon, "A survey on ear biometrics," *ACM Computing Surveys (CSUR)*, vol. 45, 02 2013.

[39] K. Bowyer, K. Hollingsworth, and P. Flynn, "Image understanding for iris biometrics: A survey," *Computer Vision and Image Understanding*, vol. 110, pp. 281–307, 05 2008.

[40] M. Shu, Y. Liu, and H. Fang, "Identification authentication scheme using human body odour," *2014 IEEE International Conference on Control Science and Systems Engineering*, pp. 171–174, 2014.

[41] S. D. Finn E., Shen X., "Functional connectome fingerprinting: identifying individuals using patterns of brain connectivity," *Nat Neurosci*, vol. 18, p. 1664–1671, 2015.

[42] F. E. H. L. and J. D.C., "Layer-dependent activity in human prefrontal cortex during working memory," *Nat Neurosci*, vol. 22, p. 1687–1695, 2019.

[43] A. Demertzi, E. Tagliazucchi, S. Dehaene, G. Deco, P. Barttfeld, F. Raimondo, C. Martial, D. Fernández-Espejo, B. Rohaut, H. U. Voss, N. D. Schiff, A. M. Owen, S. Laureys, L. Naccache, and J. D. Sitt, "Human consciousness is supported by dynamic complex patterns of brain signal coordination," *Science Advances*, vol. 5, no. 2, p. eaat7603, 2019.

[44] A. Kong, D. Zhang, and M. S. Kamel, "A survey of palmprint recognition," *Pattern Recognition*, vol. 42, pp. 1408–1418, 07 2009.

[45] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[46] Chien Le and Raj Jain, "A Survey of Biometrics Security Systems." https://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf, 2011. Online; accessed 26 September 2021.

[47] S. Bhable, S. Kayte, R. Maher, J. Kayte, and C. Kayte, "Dna biometric," *IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*, vol. 5, pp. 2319–4200, 11 2015.

[48] R. Garcia-Martin and R. Sanchez-Reillo, "Vein biometric recognition on a smartphone," *IEEE Access*, vol. 8, pp. 104801–104813, 2020.

Archived copy · cryp2nova.com

[49] S. Bargal, A. Welles, C. Chan, S. Howes, S. Sclaroff, E. Ragan, C. Johnson, and C. Gill, "Image-based ear biometric smartphone app for patient identification in field settings," *VISAPP 2015 - 10th International Conference on Computer Vision Theory and Applications; VISIGRAPP, Proceedings*, vol. 3, pp. 171–179, 01 2015.

[50] A. F. Abate, M. Nappi, and S. Ricciardi, "Smartphone enabled person authentication based on ear biometrics and arm gesture," in *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 003719–003724, 2016.

[51] E. Rahmawati, M. Listyasari, A. Aziz, S. Sukaridhoto, F. A. Damastuti, M. M. Bachtiar, and A. Sudarsono, "Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone," in ., pp. 234–238, 09 2017.

[52] G. Goudelis, A. Tefas, and I. Pitas, "Emerging biometric modalities: A survey," *Journal on Multimodal User Interfaces*, vol. 2, pp. 217–235, 12 2009.

[53] Samsung, "Security." https://www.samsung.com/latin_en/smartphones/galaxy-s8/security/, 2021. Online; accessed 26 September 2021.

[54] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, 03 2008.

[55] K. A. Professor, "A review of various attacks on biometrics system and their known solutions," in ., 2011.

[56] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002. Pattern Recognition in Information Systems.

[57] G. Mai, K. Cao, P. C. Yuen, and A. K. Jain, "Face image reconstruction from deep templates," *CoRR*, vol. abs/1703.00832, 2017.

[58] Braingate, "braingate, turning thought into action." https://www.braingate.org/, 2021. Online; accessed 26 September 2021.

[59] Neuralink, "Breakthrough Technology for the Brain." https://neuralink.com/, 2021. Online; accessed 26 September 2021.

[60] Brainlab, "Brainlab." https://www.brainlab.com/, 2021. Online; accessed 26 September 2021.

[61] Facebook, "F8 2017: AI, Building 8 and More Technology Updates From Day Two." https://about.fb.com/news/2017/04/f8-2017-day-2/, 2017. Online; accessed 26 September 2021.

[62] M. D. . C. E. Makin J.G., "Machine translation of cortical activity to text with an encoder–decoder framework," *Nat Neurosci*, vol. 23, p. 575–582, 2020.

[63] S. Mudgal, S. Sharma, J. Chaturvedi, and A. Sharma, "Brain computer interface advancement in neurosciences: Applications and issues," *Interdisciplinary Neurosurgery*, vol. 20, p. 100694, 02 2020.

[64] G. Pfurtscheller, B. Allison, C. Brunner, G. Bauernfeind, T. Solis-Escalante, R. Scherer, T. Zander, G. Müller-Putz, C. Neuper, and N. Birbaumer, "The hybrid bci," *Frontiers in neuroscience*, vol. 4, p. 30, 04 2010.

[65] G. Müller-Putz, R. Leeb, J. d. R. Millan, P. Horki, A. Kreilinger, G. Bauernfeind, B. Allison, C. Brunner, and R. Scherer, *Principles of Hybrid Brain–Computer Interfaces*, pp. 355–373. ., 01 2013.

Archived copy · cryp2nova.com

[66] I. Choi, I. Rhiu, Y. Lee, M. H. Yun, and C. S. Nam, "A systematic review of hybrid brain-computer interfaces: Taxonomy and usability perspectives," *PLOS ONE*, vol. 12, pp. 1–35, 04 2017.

[67] D. Yang, H. Nguyen, and W.-Y. Chung, "A synchronized hybrid brain-computer interface system for simultaneous detection and classification of fusion eeg signals," *Complexity*, vol. 2020, pp. 1–11, 06 2020.

[68] K.-S. Hong and M. Khan, "Hybrid brain–computer interface techniques for improved classification accuracy and increased number of commands: A review," *Frontiers in Neurorobotics*, vol. 11, 07 2017.

[69] S. Sahar and A. Maleki., "Recent advances in hybrid brain-computer interface systems: A technological and quantitative review.," *Basic and clinical neuroscience*, vol. 9, pp. 373–388, 2018.

[70] T. Blum, R. Stauder, E. Euler, and N. Navab, "Superman-like x-ray vision: Towards brain-computer interfaces for medical augmented reality," in *2012 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, pp. 271–272, 2012.

[71] X.-S. Hu, T. D. Nascimento, M. C. Bender, T. Hall, S. Petty, S. O'Malley, R. P. Ellwood, N. Kaciroti, E. Maslowski, and A. F. DaSilva, "Feasibility of a real-time clinical augmented reality and artificial intelligence framework for pain detection and localization from the brain," *Journal of medical Internet research*, vol. 21, p. e13594, June 2019.

[72] S. Park, H. Cha, J. Kwon, H. Kim, and C. Im, "Development of an online home appliance control system using augmented reality and an ssvep-based brain-computer interface," in *8th International Winter Conference on Brain-Computer Interface, BCI 2020*, 8th International Winter Conference on Brain-Computer Interface, BCI 2020, Institute of Electrical and Electronics Engineers Inc., Feb. 2020. Publisher Copyright: © 2020 IEEE.; null ; Conference date: 26-02-2020 Through 28-02-2020.

[73] D. Friedman, ""brain art: Brain-computer interfaces for artistic expression"," *Brain-Computer Interfaces*, vol. 7, no. 1-2, pp. 36–37, 2020.

[74] A. Benitez-Andonegui, R. Burden, R. Benning, R. Möckel, M. Lührs, and B. Sorger, "An augmented-reality fnirs-based brain-computer interface: A proof-of-concept study," *Front Neurosci*, vol. 14, 2020.

[75] G. Liberati, A. Pizzimenti, L. Simione, A. Riccio, F. Schettini, M. Inghilleri, D. Mattia, and F. Cincotti, "Developing brain-computer interfaces from a user-centered perspective: Assessing the needs of persons with amyotrophic lateral sclerosis, caregivers, and professionals.," *Applied ergonomics*, vol. 50, p. 139–146, 2015.

[76] K. A, H. EM, and R. A, "The user-centered design as novel perspective for evaluating the usability of bci-controlled applications.," *PLoS One.*, vol. 9, 2014.

[77] F. Nijboer, "Technology transfer of brain-computer interfaces as assistive technology: Barriers and opportunities," *Annals of Physical and Rehabilitation Medicine*, vol. 58, no. 1, pp. 35–38, 2015. Brain Computer Interfaces (BCIs) / Coordinated by Jacques Luauté and Isabelle Laffont.

[78] D. Baars, "Towards self-sovereign identity using blockchain technology," October 2016.

[79] Ori Jacobovitz, "Blockchain for Identity Management." https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf, 2016. Online; accessed 26 September 2021.

Archived copy · cryp2nova.com

[80] Andrew Tobin and Drummond Reed, "The Inevitable Rise of Self-Sovereign Identity." https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf, 2016. Online; accessed 26 September 2021.

[81] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[82] J. S. Hammudoglu, J. Sparreboom, J. I. Rauhamaa, J. K. Faber, L. C. Guerchi, I. P. Samiotis, S. P. Rao, and J. A. Pouwelse, "Portable trust: biometric-based authentication and blockchain storage for self-sovereign identity systems," 2017.

[83] P. Garcia, "Biometrics on the blockchain," *Biometric Technology Today*, vol. 2018, no. 5, pp. 5–7, 2018.

[84] A. Othman and J. Callahan, "The horcrux protocol: A method for decentralized biometric-based self-sovereign identity," in *2018 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–7, 2018.

[85] Maciek Laskus, "Decentralized Identity Trilemma." http://maciek.blog/dit/?cookie-state-change=1574327093444, 2018. Online; accessed 26 September 2021.

[86] J. R. Douceur, "The Sybil Attack." https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf, 2002. Online; accessed 26 September 2021.

[87] R. John, J. P. Cherian, and J. J. Kizhakkethottam, "A survey of techniques to prevent sybil attacks," in *2015 International Conference on Soft-Computing and Networks Security (ICSNS)*, pp. 1–6, 2015.

[88] A. M. Bhise and S. D. Kamble, "Review on detection and mitigation of sybil attack in the network," *Procedia Computer Science*, vol. 78, pp. 395–401, 2016. 1st International Conference on Information Security & Privacy 2015.

[89] D. Siddarth, S. Ivliev, S. Siri, and P. Berman, "Who watches the watchmen? A review of subjective approaches for sybil-resistance in proof of personhood protocols," *CoRR*, vol. abs/2008.05300, 2020.

[90] Christopher Allen, "The Path to Self-Sovereign Identity." http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, 2016. Online; accessed 26 September 2021.

[91] V. Buterin, "Problems." https://github.com/ethereum/wiki/wiki/Problems/89fd07ffff8b042134e4ca67a0ce143d574016bd, 2014. Online; accessed 26 September 2021.

[92] V. Buterin, "Hard Problems in Cryptocurrency: Five Years Later." https://vitalik.ca/general/2019/11/22/progress.html, 2019. Online; accessed 26 September 2021.

[93] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. M. M. Rahman, and M. S. Hossain, "Sybil defense techniques in online social networks: A survey," *IEEE Access*, vol. 5, pp. 1200–1219, 2017.

[94] A. Alharbi, M. Zohdy, D. Debnath, R. Olawoyin, and G. P. Corser, "Sybil attacks and defenses in internet of things and mobile social networks," in ., 2019.

[95] P. Gu, R. Khatoun, Y. Begriche, and A. Serhrouchni, "Support vector machine (svm) based sybil attack detection in vehicular networks," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2017.

Archived copy · cryp2nova.com

[96] K. Zhang, X. Liang, R. Lu, K. Yang, and X. S. Shen, "Exploiting mobile social behaviors for sybil detection," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 271–279, 2015.

[97] Y. Muliadi, M. Baker, D. Rosenthal, P. Maniatis, M. Roussopoulos, and T. Giuli, "Preserving peer replicas by rate-limited sampled voting in lockss," ., 03 2003.

[98] B. Awerbuch and C. Scheideler, "Group spreading: A protocol for provably secure distributed name service," in *ICALP*, 2004.

[99] P. Maniatis, D. S. H. Rosenthal, M. Roussopoulos, and M. Baker, "Lockss: A peer-to-peer digital preservation system," *ACM Transactions on Computer Systems*, vol. 23, p. 2005, 2003.

[100] B. Levine, C. Shields, and N. Margolin, "A survey of solutions to the sybil attack," *Technical Report of Univ of Massachussets Amherst*, vol. 2006–052, 11 2005.

[101] N. Margolin and B. Levine, "Informant: Detecting sybils using incentives," in ., vol. 4886, pp. 192–207, 02 2007.

[102] M. B. Shareh, H. Navidi, H. H. S. Javadi, and M. HosseinZadeh, "Preventing sybil attacks in p2p file sharing networks based on the evolutionary game model," *Information Sciences*, vol. 470, pp. 94–108, 2019.

[103] M. B. Shareh, H. Navidi, H. H. S. Javadi, and M. Hosseinzadeh, "A new incentive mechanism to detect and restrict sybil nodes in p2p file-sharing networks with a heterogeneous bandwidth," *Journal of AI and Data Mining*, 2020.

[104] F. Wang and P. De Filippi, "Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion," *Frontiers in Blockchain*, vol. 2, p. 28, 2020.

[105] B. Ford and R. Böhme, "Rationality is self-defeating in permissionless systems," 2019.

[106] S. A. Williams, V. Diordiiev, and L. Berman, "Arweave: A protocol for economically sustainable information permanence," in ., 2019.

[107] Daniel Larimer, "The Hidden Costs of Bitcoin." https://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security, 2013. Online; accessed 26 September 2021.

[108] Bitshares, "Bitshares." https://bitshares.org/, 2021. Online; accessed 26 September 2021.

[109] V. Buterin, "DAOs, DACs, DAs and More: An Incomplete Terminology Guide." https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/?source=post_page, 2014. Online; accessed 26 September 2021.

[110] V. Buterin, "Ethereum Whitepaper." https://ethereum.org/en/whitepaper/, 2013. Online; accessed 26 September 2021.

[111] J. Hyland, *Democratic Theory: The Philosophical Foundations*. Manchester: Manchester University Press, 1995.

Archived copy · cryp2nova.com