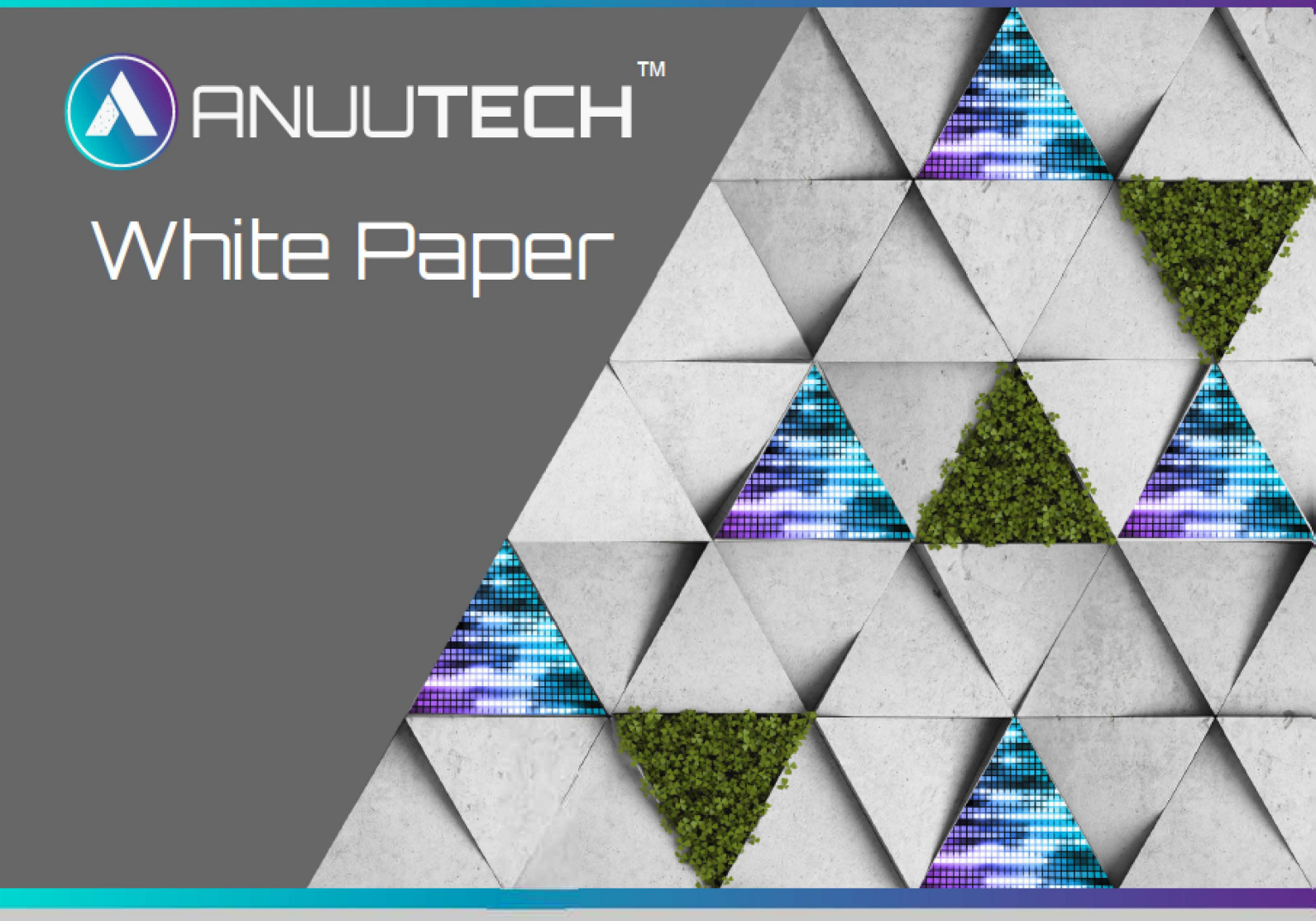
ANUUTECH™

# White Paper



# AnuuTech Ltd.

An ecosystem utilizing the highest integrity protocols and safety standards with a unique consensus algorithm, Proof of Hash.

*(Technical WhitePaper December 14, 2021*
*The AnuuTech Ltd. Team*
*https://www.anuutech.com*

## I Abstract

AnuuTech is a next-gen distributed ledger platform [1] that allows dApps [2] to be programmed in any language. Whereas standard blockchain environments are susceptible to centralization vulnerabilities, AnuuTech rectifies these limitations by creating a truly decentralized network of 3-tier nodes.

AnuuTech's most radical notion is the idea that not everything needs to occur on-chain. Whereas data storage, data protection, and data validation are achieved on-chain in a classic blockchain [3] AnuuTech disaggregates these components into three separate off-chain processes.

AnuuTech proposes a fast and ecological consensus algorithm called ***Proof of Hash***, or **PoH**.

Proposal- Proof of Hash (PoH) consensus algorithm can serve as the basis for a decentralized data integrity protection service. Anyone seeking to protect their data can make use of this service (provided they conform to the requirements that are set out by the node network).

The proposed PoH consensus protocol is not used to validate any data, it is only used to provide proof of integrity and existence of (any type of) data.

AnuuTech platform will allow third-party developers to access its core modules as a means for creating external (server-side) modules - and in whatever programming language they choose.

AnuuTech Network brings a new dimension to traditional networks. Its layered structures, dynamic gateways, trusted connections and network consensus optimizes the communication, security and speed of the network.

Our functional layers make the scalability infinite, the more entities join our network the faster it becomes. AnuuTech Network is the next generation of networks.

## 1 Introduction

### 1.1 General

While most blockchain projects in the cryptocurrency industry only focus on conducting peer-2-peer payment transactions, we have designed PoH to handle all types of data transactions. As a result, we're bringing the benefits of blockchain to a variety of industry sectors that have not been able to fully implement this technology (particularly those who seek to improve and/or secure their data transactions like Healthcare [4], Online Gaming [5], Legal Forms & Documents [6], Voting [7], Supply Chain [8], Hosting [9], Internet of things [10] and more [11]).

Proof of Hash brings the advantages of blockchain to data processes not yet associated with blockchain technology. Accordingly, data that is not stored in public ledgers can benefit from our decentralized data integrity protection service. Data that cannot be placed on public ledgers due to their private and/or secretive nature will be able to reap the benefits of distributed ledger technology.

PoH is able to employ a combination of various hashing [12], encryption and signature schemes [13], thus making it highly flexible and easily adaptable to the latest technological advancements. This combination allows us to provide security against the various threats that quantum computing will bring. By combining various security schemes we're able to eliminate any one of these schemes from becoming a single point of failure.

PoH's proposed multi-level security provides a safe, fast, and extremely reliable service to anyone seeking to protect their data, regardless of data type or how such data is stored.

The network's nodes (which ensure data integrity) do not require any specialized hardware. AnuuTech recommends a x64 platform with 2Ghz processor, 2Gb of RAM and 10Gb of diskspace as minimum for a node.

## 1.2 General Aspects

AnuuTech designed it's innovative solution with these challenging aspects in mind:

### 1.2.1 Decentralization

Among the most important features of a good blockchain is its level of decentralization. Sufficient decentralization ensures that it's impossible for a single user or faction to take control of the network.

For another, decentralized systems do not have a single point of entry – and thus not a single point of failure. [14]

### 1.2.2 Speed

AnuuTech is aiming for not only the highest tps amount possible but is also seeking optimised performance for distributed state machine. [15]

### 1.2.3 Security

Allowing secure transactions and preventing any attacks based on known attack vectors. (This will be described in III Threat Model). [16]

### 1.2.4 Scalability

AnuuTech can scale when it retains the ability to offer its services as the number of users grows [17]

### 1.2.5 Optional ownership

AnuuTech's design incorporates private chains to meet the wish of stakeholders who are bounded by local or international law. (This will be later discussed in chapter 3 "Private chains").

## 1.3 Proposal

To overcome the challenges mentioned above the AnuuTech team started to find solutions to overcome and comply with these. The proposal for this solution is PoH, AnuuTech Network and Private Chains.

### 1.3.1 Proof of Hash

AnuuTech proposes PoH which stands for Proof of Hash, it is a network consensus protocol that provides trustable unalterable proof of the existence of a data subset at a given moment in time.

The PoH consensus protocol is not used to validate any data, it is only used to provide proof of integrity and existence of (any type of) data which enables the integrity validation of off-chain data.

### 1.3.2 AnuuTech network proposal

For the AnuuTech Network we propose a different approach to current networks by using a solution that makes sure that all of the necessary connections are already pre-built. The proposed solution acts as a support structure for the PoH mechanism.

Leveraging of pre-authenticated and pre-established connections means there is no need to continuously build authenticated new connections that depend on a number of external factors which lead to faster overall end to end requests/replies and faster initial application communication.

In addition to this we propose a solution to properly identify the entities inside of this network by introducing the AnuuTech ID. It is a collection of smart data properties for a giving network entity, that provides identification, application specifics and virtual geographical position within the ecosystem which is represented via the ID #. The AnuuTech ID number can be thought of as the "GEN2 IP Address" of the virtual entity.

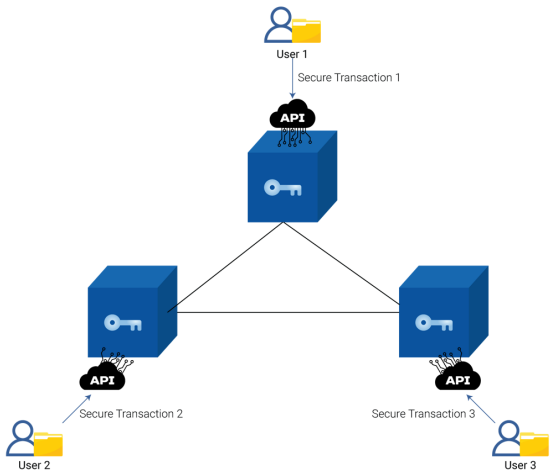
#### 1.3.3 Private Chains proposal

In contrast to traditional blockchain networks where every user can be connected to every other user, AnuuTech proposes an option to create a private chain. The transactions that are sent through the network will be exclusive between two parties. AnuuTech private chains will make use of the cornerstone techniques Proof of Hash and it's integrated support structure AnuuTech network. Private chains' promise to an exclusive two-party transaction will be helpful for users that are bound by local or international law.

# II Architectural Overview

## 1. Entities

The entities that exist in the AnuuTech ecosystem consist of users, API interfaces and nodes. Users can send and receive secure transactions using API interfaces and have the transaction signed by the consensus mechanism executed by the nodes.




PoH consensus mechanism relies on a network of trusted nodes executing the various tasks that make up the consensus protocol [18]. In the AnuuTech network the nodes are divided in 3 different levels each responsible for a part of the consensus protocol.

### 1.1 Address verification

AnuuTech proposes an optional process during enrollment of the user. This enables a KYC procedure using a zero-knowledge proof protocol which connects users to wallet address(ses), this information will be stored in the AnuuTech ID of the user. AnuuTech ID enables the implementation of decentralized identity verification. Third party network entities can utilize this information to determine if a user is in compliance with a rule set they need to comply with. For example country of origin.

## 2. AKEY

AKEY is an intrinsic utility token and plays an important role in filling the node network, as AKEY tokens will be needed to register a node and also is the mode of payment for the users to pay to utilize the revolutionary technology, services and to pay for transaction fees on the AnuuTech platform.

# III Threat Model

AnuuTech works on the basis of a byzantine adversarial model in which at least 2/ 3 n+1 of the nodes are trustworthy. The system stops attackers to delay or transmit contradicting messages, compromise other nodes, have defects, or collaborate among themselves, as long as 2/ 3 n+1 of the AnuuTech network's eligible validators are not compromised and the protocol can establish consensus for every layer.

# 1. Attack vector prevention

## 1.1 Denial of Service

Given the limitations and status of current techniques, plus the ever-increasing sophistication of DDoS attacks, there is a demand and need for more efficient detection and mitigation solutions based on new technologies. Because of our network's tiering and decentralized nature, any external attack on the network's inner, more vital components, is impossible and futile. Non-members have no access to the protected inner layers (level 1 nodes, for example). L1 nodes are required to adhere to our connection and communication protocols. A DDoS attack on the network would have a minimal impact because of the layered structure, each hosting its own node workgroups. Network and communication violations will be detected by our decentralized watchdog. DDOS and flooding assaults rely on a single or a small number of attack locations. By combining a decentralized network with access verification, we can avoid such attacks. In other words, while DDOSing a single server is possible, DDOSing thousands of nodes at once is exponentially more difficult. DDOSing is especially difficult if you have no idea where nodes are located on the network. If a node is attacked it is removed from the network until the communication has stabilized. Only then can the node rejoin the network.

## 1.2 Sybil attack

Because the nodes are connected using certificates the risk of a compromised trust is impossible.

## 1.3. 51% attack

AnuuTech uses a three-tiered node structure, with each tier playing a specific role in the Proof of Hash process. As a result, attacking and taking over a node on a tier will result in that node failing to follow its consensus within its task, such as creating/validating a block that does not use the anticipated template, resulting in the node losing trust and having to reconnect to the network.  A bad actor, transactions will be rejected until the compromised node generates a new signature. Because PoH uses node functions across three tiers of nodes, performing 51% percent attacks is impossible. More details on this in IV AnuuTech Network.

# 2. Proof of Hash

## 2.1 Proof of Hash proposal

AnuuTech proposes PoH which stands for Proof of Hash, it is a network consensus protocol that provides trustable unalterable proof of the existence of a data subset at a given moment in time.
The PoH consensus protocol is not used to validate any data, it is only used to provide proof of integrity and existence of (any type of) data.

## 2.2 The node network

PoH relies on a network of trusted nodes executing the various tasks that make up the consensus protocol. In the AnuuTech network the nodes are divided in 3 different levels each responsible for a part of the consensus protocol. These levels are created to create physical layer separation between layers and functionalities, enhancing the network security, and to differentiate the network node hardware requirements, optimizing every step of the process.
In the AnuuTech network the third level of nodes is the collection layer, users that want to use the PoH service will interact with the nodes on this layer.
The second level of nodes is the aggregation layer where all the data collected by the third layer is compressed into smaller packages. In the first layer the nodes will reach a consensus on the data collected by the third layer and aggregated by the second layer, and the result of the consensus will be made available for the rest of the network.

The operations that need to be executed are done by virtual “checkpoints” hosted on the node network. Each checkpoint's hosting is assigned in a pseudo-random manner, based in part on the previous consensus round's outcome and the certificates issued to the nodes after each consensus round. If there aren't enough physical nodes for all of the checkpoints, multiple checkpoints can be assigned to the same physical node.

### 2.2.1. Level 3 - collection phase

When a user wants to use the PoH service, they will present a subset of data to the third node level.  Based on the checkpoint's unique certificate and the current network time, the checkpoint will create a time stamped fingerprint for the data, add it to its collection and shared temporary storage for the current time period, and provide this fingerprint to the network user.

The user will present this time stamped data fingerprint to a second checkpoint on the third level, which will verify if the time stamped data fingerprint was created by the correct checkpoint on the third level and if it exists in the shared storage, which will be chosen based on the fingerprint. Depending on the network's consensus rules, the number of secondary checkpoints that will collect/verify the time stamped data fingerprint can vary.
For the duration of the specified time period, all checkpoints on the third level will collect the timestamped data fingerprints they either generated or verified (n).

Once a user receives a timestamped data fingerprint, he or she has a temporary proof of data integrity; however, to get full confirmation, the master hash for the time period of the time stamped data fingerprint must be added to the PoH consensus protocol's shared storage, and the time stamped data fingerprint must be used in the calculation of the master hash. The total amount of time required for complete confirmation is n x 4.

### 2.2.2. Level 2 - aggregation phase pt. 1

The time stamped data fingerprints collected by all third-level checkpoints during the time period (n) will be aggregated and hashed. The collection hash will be sent from the third level checkpoints to a checkpoint on the second level that has been chosen based on the collection signature. Based on the unique certificate of the second level checkpoint and the current network time, the second level checkpoints will verify the consensus for the time stamped data fingerprints included in the collection and provide a collection fingerprint. This collection fingerprint will be added to the checkpoint on the second level's collection for the current time period and shared storage, as well as provided to the checkpoint on the third level that sent the collection.

The collection fingerprint will be sent from the checkpoint on the third level to a second checkpoint on the second level, which will verify if the collection fingerprint was created by the correct checkpoint on the second level and if it exists in the shared storage.

Depending on the network's consensus rules, the number of secondary checkpoints that will collect/verify the collection fingerprint can vary.

*For the duration of the specified time period, all second-level checkpoints will collect all collection fingerprints they either created or verified (n).*

### 2.2.3. Level 1 - aggregation phase pt 2

The collections collected during the time period (n) and the hash of the new collection will be aggregated by all checkpoints on the second level. The second-level checkpoints will send the new collection hash to a first-level checkpoint that has been chosen based on the new collection signature. The first-level checkpoints will verify the consensus for the new collection's collections as well as the consensus for the digital fingerprints in the collection, and provide a consensus fingerprint based on the first-level checkpoint's unique certificate and the current network time.

This consensus fingerprint will be added to the checkpoint on the first level's collection for the current time period and shared storage, and this collection fingerprint will be provided to the checkpoint on the second level that sent the new collection.The checkpoint on the second level will send the consensus fingerprint to a second checkpoint on the first level, which will verify if the consensus fingerprint was created by the correct checkpoint on the first level and if it exists in the shared storage, based on the created consensus fingerprint.

Depending on the network's consensus rules, the number of secondary checkpoints that collect/verify the consensus fingerprint can vary.
For the duration of the specified time period, all first-level checkpoints will collect all consensus fingerprints they either created or verified (n).

### 2.2.4. Level 1 - Signing phase round 1

Based on the previously generated masterhash, all of the checkpoints in the first level are ordered in a pseudo random fashion into a number of groups with equal members. All of the checkpoints within each group will be in a specific order as well.

All of the groups will work at the same time to create an aggregated collection of unique time stamped data fingerprints that will be included in all of the new collections for which the group's first-level checkpoints either created a consensus fingerprint or verified one during the previous phase. The first group member will be given a

time limit in which to add all of the unique time stamped data fingerprints included in the new collection for which it created or verified a consensus fingerprint during the previous phase to the group's shared storage and sign the entries.

The other checkpoints of the groups will sync with the shared storage and add the entries to their collection if they can confirm the consensus for each time stamped data fingerprint. After the first checkpoint's allotted time frame has expired, the group's second checkpoint will sign all of the unique time stamped data fingerprints included in new collections for which the checkpoint either created or verified a consensus fingerprint and which have not yet been added to the group's shared storage during the allotted time frame. If the remaining checkpoints of the groups can confirm the consensus for each digital fingerprint, they will sync with the shared storage and add the entries to their collection. The third checkpoint will follow suit, followed by the rest of the group's checkpoints.

#### 2.2.5. Level 1 - Signing phase round 2

When all checkpoints have added their digital fingerprints to the group’s shared storage, each member of the first group will send their collection of digital fingerprints to their counterpart in the second group (G1C1 -> G2C1; G1C2->G2C2; …). The second group's checkpoints will compare the collection of digital fingerprints they each received to the rest of the group. If they received the same, they will continue with the collection they received; if not, they will continue with the collection that includes the majority of digital fingerprints for which they can confirm the consensus. The second group's checkpoint will verify the consensus for each digital fingerprint and add the collection of digital fingerprints generated in the previous phase. The combination of digital fingerprints collected by the first and second groups is transmitted to the counterpart in the third group. (G2C1-G3C1; G2C2-G3C2; …). The third group's checkpoints will compare the collections they each received with the rest of the group. If they received the same, they will continue with the collection they received; if not, they will continue with the collection that includes the majority of digital fingerprints for which they can confirm the consensus. The second group's checkpoint will verify the consensus for each digital fingerprint and add the collection of digital fingerprints generated in the previous phase. The combination of digital fingerprints collected by the second and third groups is sent to the fourth group's counterpart. (G3C1->G4C1; G3C2-G4C2; …). Next the fourth group will do the same followed by the other groups.

#### 2.2.6. Level 1 - Adding phase

When the last group has finished adding the last group's digital fingerprints. The last group's checkpoint will compare their collections, and the checkpoint with the highest priority will generate a master hash of all the digital fingerprints for which the consensus can be confirmed. This checkpoint will display the master hash to the controllers of the decentralized storage location chosen to store the master hash for that time period.

Before storing the master hash, all controllers check if the checkpoint presenting the master hash has the highest priority in the previous group and verify the created master hash. If one of the controllers rejects the master hash, new controllers are chosen at random. And the process will be repeated at the checkpoint with the highest priority. If no master hash is added within the time limit, an empty hash is added.

### 2.3. How does PoH provide trustable proof

The level 3 checkpoints generate a digital fingerprint based on the hashed value of the data requesting PoH integrity protection, the current network time, and the unique certificate of the level 3 checkpoint for that time period. As a result, the digital fingerprint provides third-party verification of the data content at the time the digital fingerprint was requested. The master hash is a hash value generated from all of the digital fingerprints for that time period that proves the existence of the digital

signature during that time period. Each time period can only have one master hash, and the master hashes are linked to each other in the same way that blocks in a regular blockchain are.

When a user connects to the network, they will sync with the network, adding all of the master hashes to their chain.
After the master hash for that time period has been created, a user will be unable to change the data protected by a digital fingerprint.

# 3 Private chains

## 3.1 Why private chains

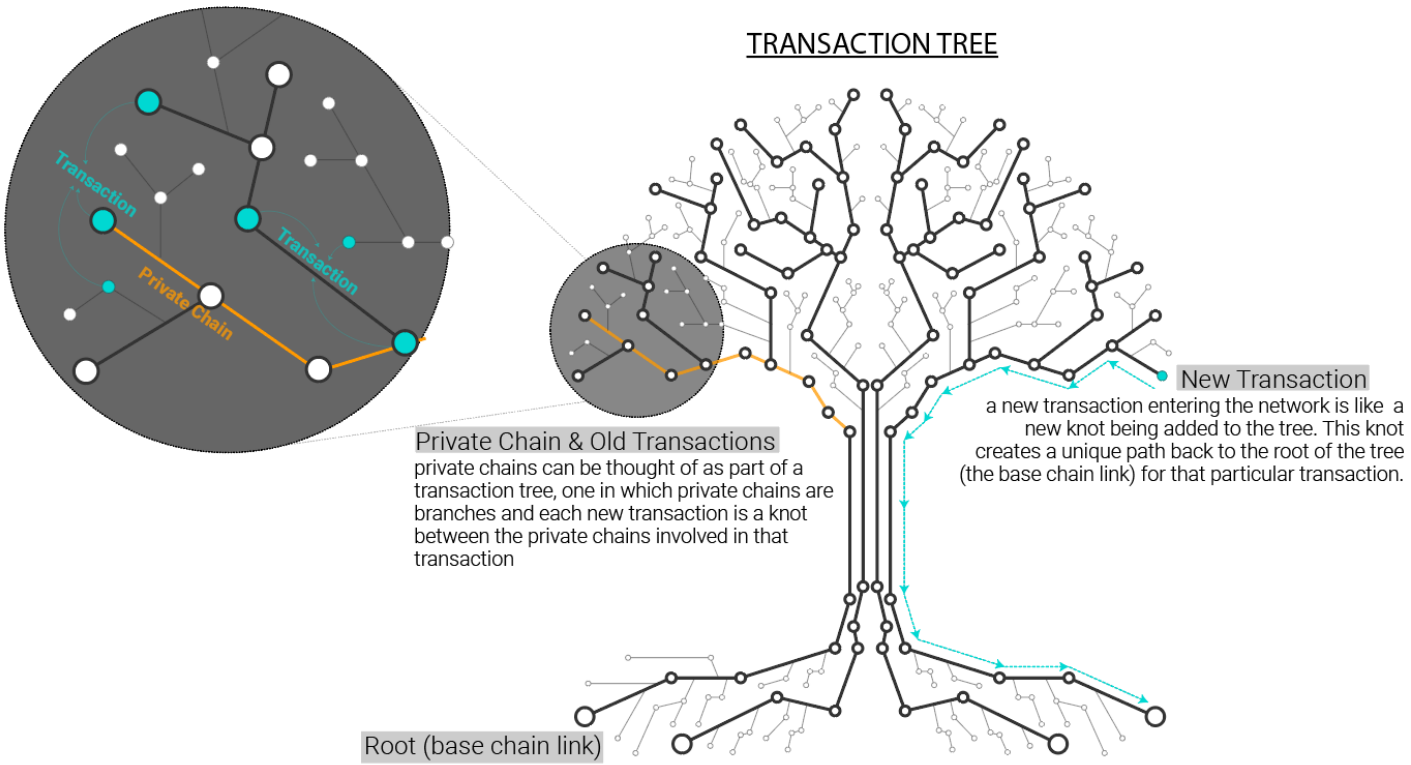
In classic blockchain networks, a single “master” chain records all transactions and shares the data with users of the network. However, users must constantly sync with the entire chain and store all transactions that occur on the network. As this requires a vast amount of storage space, master chains end up limiting network throughput and scalability.

AnuuTech proposes private chains in which, in contrast to classic blockchains, only contain transactions directly related to the user's address(es) eliminating much of the throughput and scalability issues currently found in “traditional” blockchains.
Private chains provide additional privacy to users since transaction data is only shared between users and not the entire network.

## 3.2 The principle of a private chain

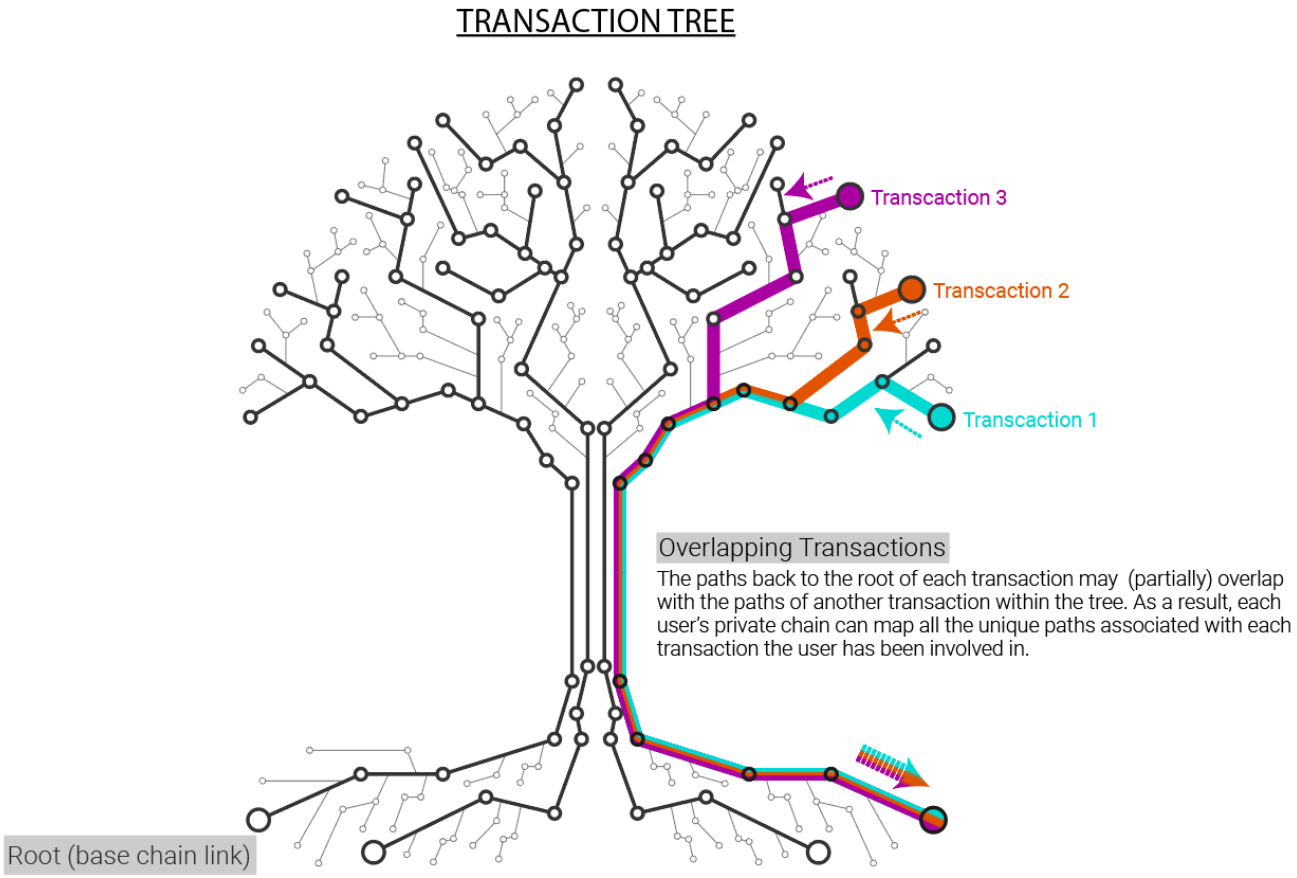
In a private chain network, every user is responsible for mining their own chain and providing the evidence for the origin of the data that is being transacted. The entire network consists of an unlimited number of private chains that interlink during each individual transaction.

The private chains are part of the transaction tree where the private chains are the branches and with each new transaction a knot between the private chains involved in that transaction gets added to the tree, creating a unique path back to the root of the tree (base chain link for that particular transaction.




The paths back to the root for a transaction can (partially) overlap with the path of another transaction in the tree.

A user’s private chain is in fact a map of all the unique paths for each transaction the user was involved in.




When a user wants to transact data to another user, they will show the other user that they are in fact the owner of the data's path endpoint at that time of the transaction as well as provide the proof for the origin of the data. Meaning that every user receiving data in a transaction will be able to verify the sender is allowed to "spend" this data as well as trace the data back to its origin proving its existence. In a private chain network, the burden of proof lies solely with the person sending the data. Accepting invalid data in turn will also lead to invalidating one's private chain as it will be impossible to spend the invalid data since the required proof for the valid origin of the data will not exist.

## 3.3 Creating transactions

In order to create a transaction, the user needs to mine a new block to his private chain which includes the transaction.

## 3.4 Chain syncing

Before a user can mine a new block, they need to sync their private chain within the network. This requires the user to add all Masterhashes created by the PoH process since the last time the user was synchronized with the network. To get these Masterhashes the user will connect to the node network where the user can download the missing Masterhashes. When the user has synced their private chain, the user can now mine a new block to their chain.

For comparison, a year's worth of Masterhashes will require +/-16 MB compared to the dozens of GB in a traditional blockchain network. Not only will this make the syncing process exponentially faster than a classic blockchain network, it will also cut down significantly on the storage required to keep in sync with the rest of the network.

## 3.5 Block mining

To mine a new block to a private chain the user must use a valid block template that was created when the previous block was mined. A valid block template contains a backwards pointer to the previous block and a unique template validator that can be found in the previous block which serves as a forward pointer from the last block to the block template. The first phase of the block mining is to acquire a new unique block template validator for the next block template.

This new unique block template validator is generated by the node network based on the last validated block in the private chain. The last validated block in the private chain proves the user has paid the fee for a new block template validator and this block will be added to the private chain of the reward pool. By adding the block to the private chain of the reward pool it is impossible to get a second unique block template validator using this block.

If the user did not pay the required fee for the previous block, the user will not receive a new unique block template validator and it will be impossible for the user to mine a new block to their private chain.

Next, the user will add the acquired unique block template validator to the active template which will serve as a forward pointer to the new block template. The user will also add all the transactions intended for this block and create a block hash, “locking” the content of the block. It is important to note that a user can add an unlimited amount of transactions in each block and that the fee for 1 block is a fixed amount regardless of the number of transactions included in the block. With this newly created block hash, the user will acquire a PoH consensus hash from the node network.

Once the PoH consensus hash has been acquired and the Masterhash containing this PoH consensus hash has been generated by the node network, the new block is unchangeable, and the block template is spent.

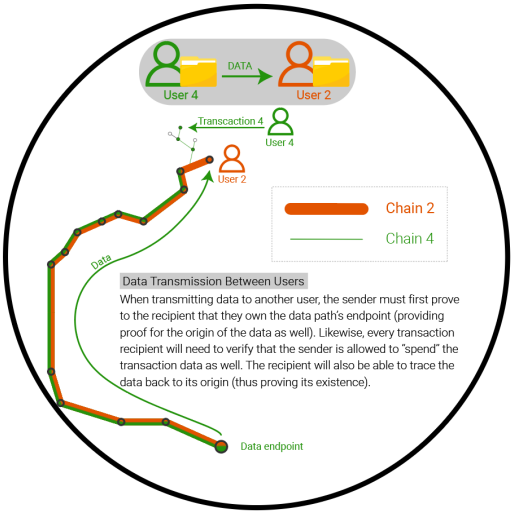
By creating a new block, a new block template has been generated as well containing the blockhash of the newly created block which serves as a backwards pointer and the newly created unique block template validator which was included in the newly created block and serves as a forward pointer from the newly created block to the new block template.

## 3.6 Sending transaction

Once the user has successfully mined a new block, the user can now send this notification of this new block to all the recipients of the transactions included in this block. This can be done by either directly sending notification to these recipients or by using the decentralized messaging service offered by the node network. Because cryptocurrency tokens on the AnuuTech chain can have multiple states, users will be able to recall a transaction request, for example if there is an error, such as a wrong address or amount.

## 3.7 Block seeding

Since every user is required to provide the necessary proof for the origin of the data used in the transactions the user has the option to either provide this information directly to the recipients of the data in the transactions or by using the decentralized block seeding service offered by the node network.



## 3.8 Accepting transactions

### 3.8.1. Receiving transaction notifications

Transaction recipients will receive notification of an imminent transaction either from the sender or from the decentralized messaging services offered by the node network. This notification will contain the blockhash of the block included which includes the transaction.

### 3.8.2 Chain syncing

Before a user can accept a transaction, they must first sync their private chain with the network. Again, this will require the user to download all  by downloading all the new Masterhashes that were generated since the last time  the user was synchronized with the network.

### 3.8.3. Block validation

#### *3.8.3.1. PoH validation*

Before validating the transaction, the user will first verify the integrity of the block containing the transaction. While blockhash will provide proof for the integrity of the block itself, the PoH consensus hash related to the blockhash will provide proof of the integrity of the blockhash. The Masterhash created for the time period in which the PoH consensus hash was created will provide proof of the integrity of the PoH consensus hash itself.

#### *3.8.3.2 Chain integrity validation*

Secondly, the user will verify the chain integrity of the sender's private chain ensuring that the transaction is included in a valid block of the sender's private chain. The user can use both forward and backward pointers included in theblocks to verify the chain integrity of the sender's private chain. The user only needs to check the chain integrity of the chain from the block containing the transaction to the block that included the previous transaction received from the same sender.

#### *3.8.3.3. Data ownership validation*

In order for someone to be able to "spend" data, a user only needs to sign it with the private key for the address holding the data at the moment of the transaction.The receiver of the data can verify with the public key for that address if the data was signed with the correct private key. The receiver will trace back the data using the transactions related to the origin of the data and verify if the inputs and outputs of the connected transactions found in the traceback are valid. In order to check if the coins are not the result of a double spending, the receiver would verify if the inputs used in the transactions related to the origin of the data have not been used in more than one block of the chains involved in the various transactions related to the origin of the data.

When a receiver detects that a sender is using data for which no complete origin verification can be done, they will report this sender to the network's decentralized network, which can then take action towards the untrustable sender. If the receiver can validate the data ownership and can validate the data origin the recipient can use the received data for future transactions.The receiver will also store the collected validation proof to provide proof for future transactions with the received data.
If the receiver can not validate the data ownership and/or the data origin it will be impossible for the receiver to use this data in a future transaction since they will be unable to provide the necessary proof of ownership and origin of the data.

As long as the receiver does not use the received data in a new transaction, the received data will not be visible on the chain of the receiver.

#### *3.8.3.4. Data origin validation*

A receiver of data will also check the origin of the data to make sure that the data originated from a valid source and that the sender was the valid owner of the data. Therefore, the receiver will need to back trace the data to the last known shared knot for the data.

If there is no shared knot for the data, then the origin needs to be traced back all the way to the root of the transaction tree.

The receiver will trace back the data using the transactions related to the origin of the data and verify if the inputs and outputs of the connected transactions found in the traceback are valid. In order to check if the coins are not the result of a double spending, the receiver would verify if the inputs used in the transactions related to the origin of the data have not been used in more than one block of the chains involved in the various transactions related to the origin of the data.

When a receiver detects that a sender is using data for which no complete origin verification can be done, they will report this sender to the network's decentralized network, which can then take action towards the untrustable sender. If the receiver can validate the data ownership and can validate the data origin the recipient can use the received data for future transactions. The receiver will also store the collected validation proof to provide proof for future transactions with the received data.

If the receiver can not validate the data ownership and/or the data origin it will be impossible for the receiver to use this data in a future transaction since they will be unable to provide the necessary proof of ownership and origin of the data. As long as the receiver does not use the received data in a new transaction, the received data will not be visible on the chain of the receiver.

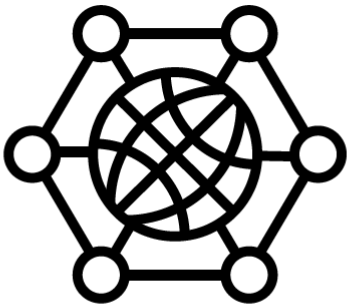
# IV Anuutech Network

## 1. The Anuutech network in depth

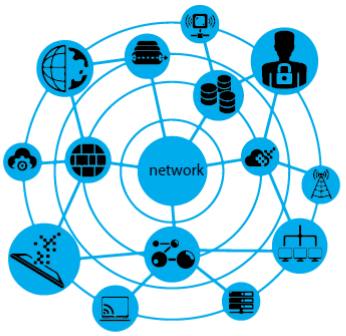
On the AnuuTech Network, all of the necessary connections are already pre-built. Data can be sent instantly which makes the whole process way faster than on a traditional network.

AnuuTech Network will leverage pre-authenticated and pre-established connections which allows data communication and transfers to take place immediately – removing the need to continuously build authenticated new connections that depend on a number of external factors. This allows a high level of efficiency leveraging prebuilt encrypted tunnels between applications resulting in immediate execution of data communication and data transmission between functional application groups.

An additional feature of the AnuuTech Network is the so called AnuuTech ID. This is what we call the next generation of IP addresses. It is a collection of smart data properties for a giving network entity, that provides identification, application specifics and virtual geographical position within the ecosystem which is represented via the ID #. The AnuuTech ID number can be thought of as the “GEN2 IP Address” of the virtual entity.



≠




### Traditional Networks

- classic IP-level connections structures
- build the connection when required (encrypted connections before data is able to send)
- application/web components geographically dispersed in different servers

Speed of network convergence between network entities is very slow

High number of independent connections to various destinations

Slowing down the overall connection and processing of data

Degraded network and application performance

Longer initial connection generation

Latency

### AnuuTech Network

- all of the necessary connections are already pre-built
- leveraging of pre-authenticated and pre-established connections
- no need to continuously build authenticated new connections that depend on a number of external factors
- faster overall end to end request/reply
- faster initial application communication

Speed of network convergence between network entities is very fast

Faster initial application communication generation times

Data can be sent instantly

**The result is a more secured and trusted communication between multiple AnuuTech ID identified entities.**

AnuuTech Network, is a specialized network that allows for VPN-like P2P communication via UDP packets, between authorized peers and functional application service layers (also service-groups) involved in the ecosystem leveraging AnuuTech ID encrypted properties.

These functional application service layers will be comprised of the following:

1) Entry/Connection Layer

2) Routing/AnuuTech ID Adjacency Map Layer

3) Transport Layer

4) Functional Application Service Group Layer

5) PARLEY – communication language

The AnuuTech ID gateway groups towards other functional group layers exist out of multiple entities, not only making it a redundant setup at all time but also making the throughput scalable to the needs of the network.

This makes the AnuuTech Network suited for many new services that can't be provided using a traditional network such as download boosting and offline receiving similar to our e-mail systems, but with other services.

## 1.1. Consensus

The base of the AnuuTech Network is the network map or routing layer. On this layer, every entity has an AnuuTech ID number and every connection (gateway) to reach another layer exists. The Transport Layer provides logical PARLEY communication between entities, and their associated functional application service groups, leveraging the adjacency map provided by AnuuTech Network routing layer.

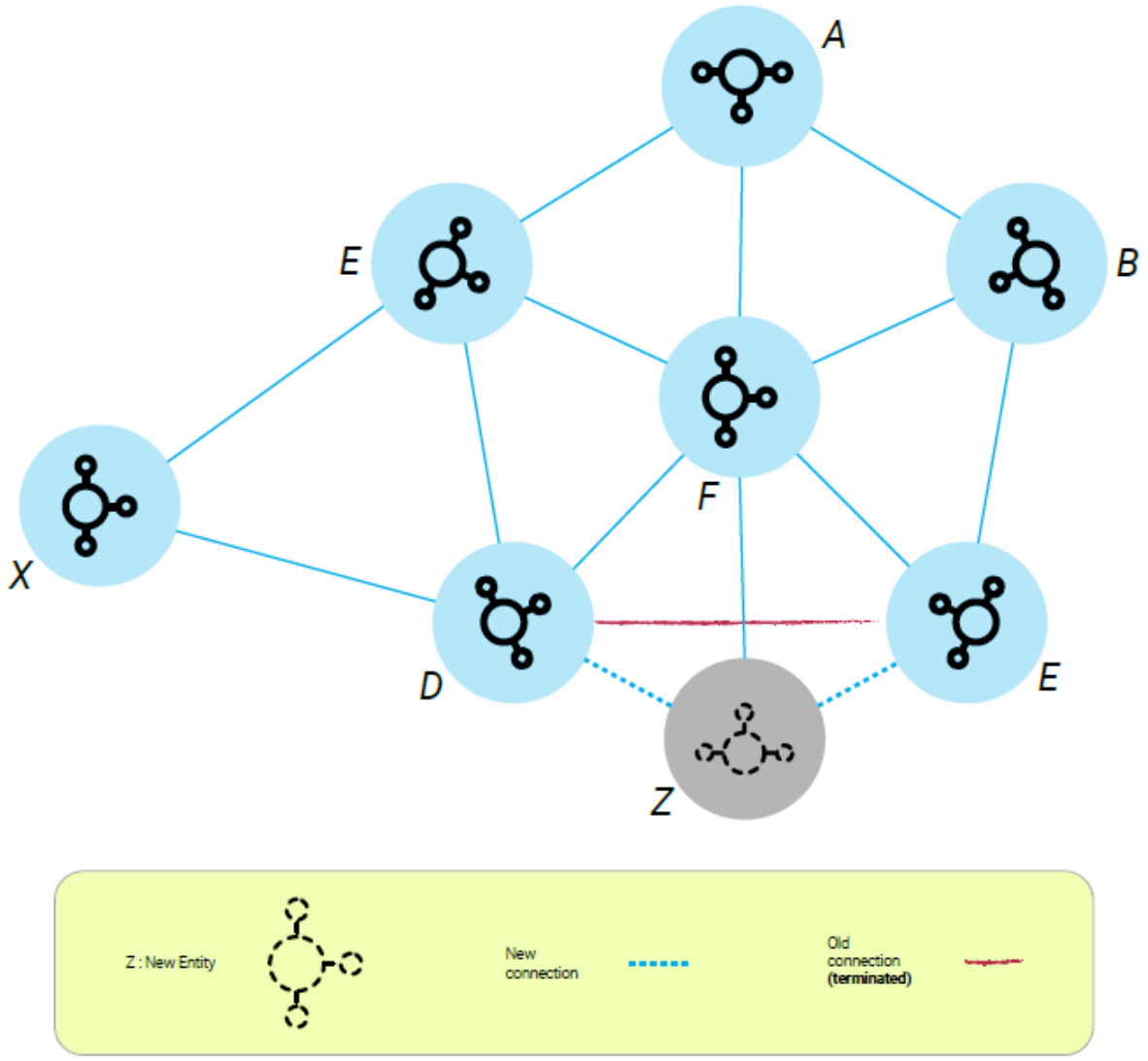
Within the layer, responsibility for communication management will involve error correction during the send and receive actions for each entity over the AnuuTech Network.

The network map is updated every time a client or entity enters or leaves the network. It's important to notice here that only a small part of the network map needs to be refreshed whenever an event takes place.

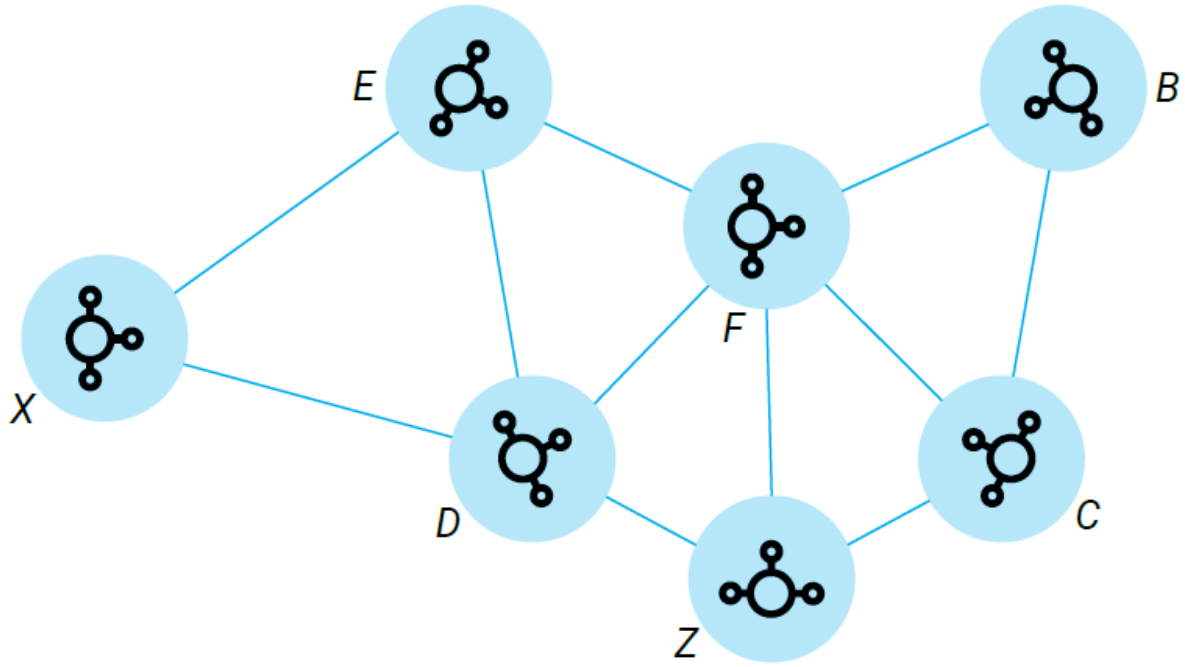
The routing layer leverages AnuuTech Network. When the routing layer process is initiated, nodes establish information gathered via the AnuuTech ID certificate profile, which contains geographical location position information. When this geographical location is shared between trusted entities, it will know and keep record of each entity's physical position – establishing an entity neighbor position map. When establishing the routing path, the routing layer will ensure that only the best-known paths are in place to get proper PARLEY communication via the transport layer. This suggests that each entity will have a direct AnuuTech Network connection to each other without path entanglement – forming a connection consensus.

As new entities join the network and connections are made, it could happen that these connections cross the existing ones. The consensus forbids connections crossing each other and prioritizes the shortest connection between the entities.

The entity is now connected to the AnuuTech Network, but the connection between F and Z is crossing the connection between D and E. Because the connection between D and E is longer than the one between F and Z, this connection (red line) is terminated.




This means that every new connection to the network can cause a change to the network map. The big advantage is that these structural changes only affect a very small part of the network, being the neighbors of the new or disconnecting entity. In the next drawing, you'll see entity A leaving the network.




With entity A having left the network, this could be a client closing its ANUU app or a node going offline, the neighbors re-evaluate and/or rebuilding their connections to the other neighbors. At this point, the network map is changed but only a slight part of the entities are affected by this.

The tunnels that existed when entity A was connected to the network are cached. When the entity comes online again it will try to use the cached tunnel information to rebuild its new tunnels, if no consensus rules are broken. With AnuuTech Network connection consensus algorithm, changes in adjacencies get handled in an efficient way that establishes those connections quickly and without connection entanglement.

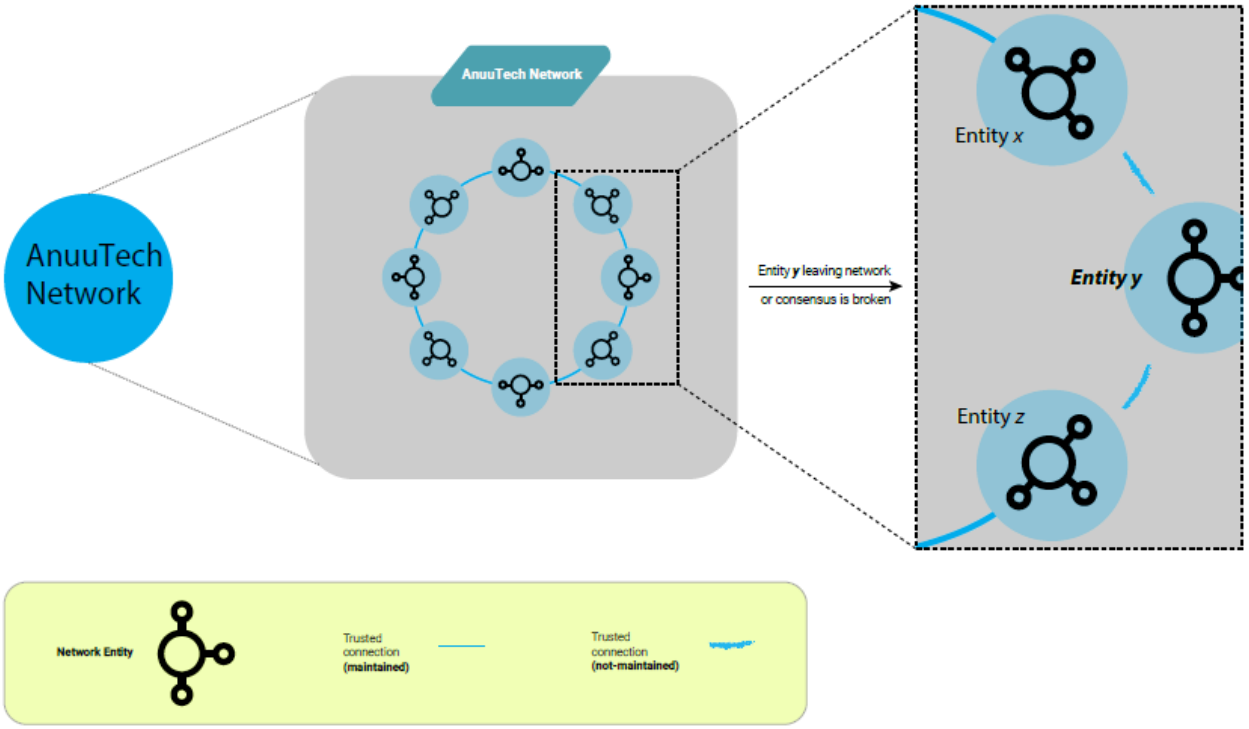
## 1.2. Interchangeable cryptographic layers

We propose an interchangeable cryptographic layer. In case there is need for upgrading or switching cryptographic methods this would be possible. Early development cycles will make use of the SHA-512 method which is detailed in Federal Information Processing Standards (FIPS) 180-4.

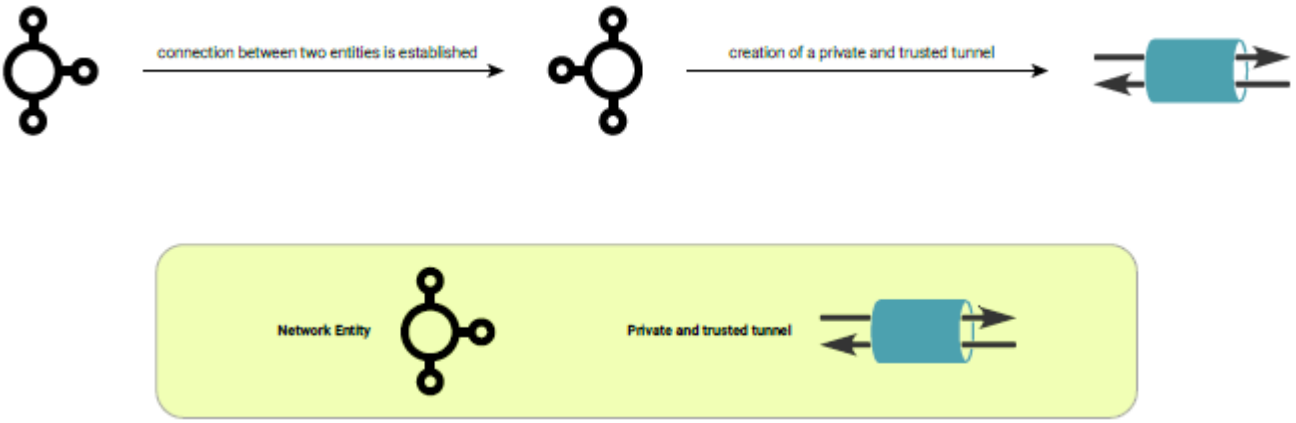
## 1.3 Interaction between the layers and the relation with signed data.

The entities in the network can be nodes, Node service providers, ANUU clients, storage servers, applications and other various virtual elements and groups.

The AnuuTech Network is made out of entities connected to their closest neighbors. These are trusted connections and are maintained until a neighboring entity leaves the network or the consensus rules are broken.

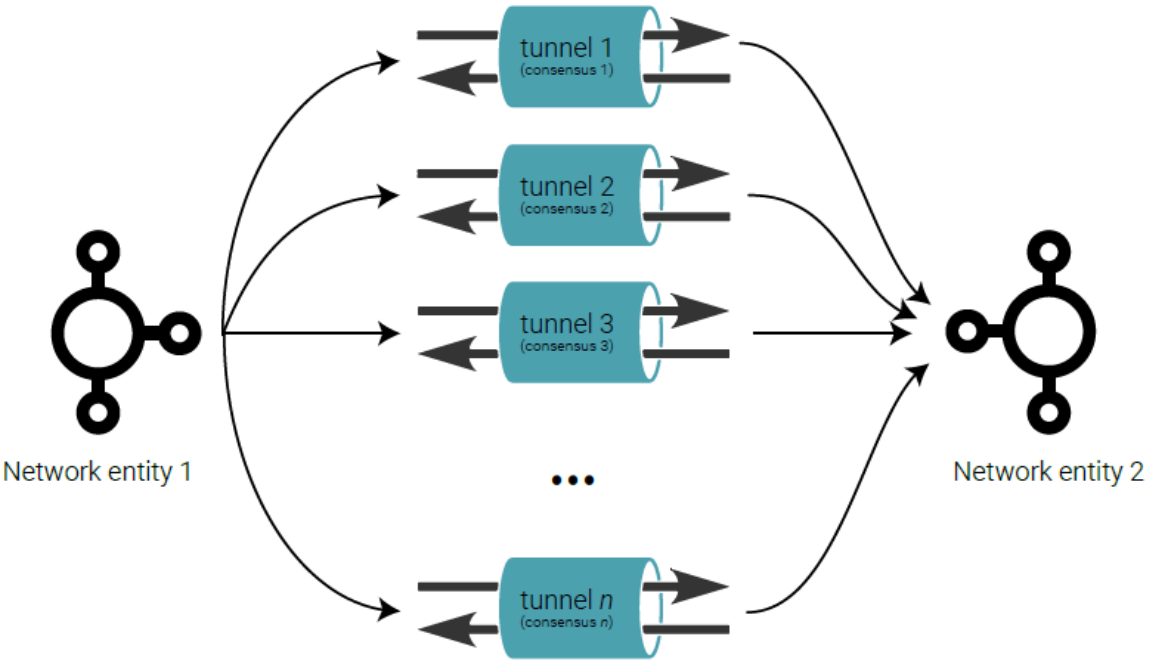



When a connection between 2 entities is established, this becomes a private and trusted tunnel.




Multiple tunnels exist between 2 entities, each respecting their own consensus. The consensus of each tunnel controls the usage of it. A “routing message tunnel” to transmit other types of data as these are on other layers may not be available. Having these trusted connections between entities makes for much faster transmissions throughout the network, as there’s no need to constantly create and authenticate these tunnels.

The required keys for these secure, encrypted connections are stored in the AnuuTech ID's.



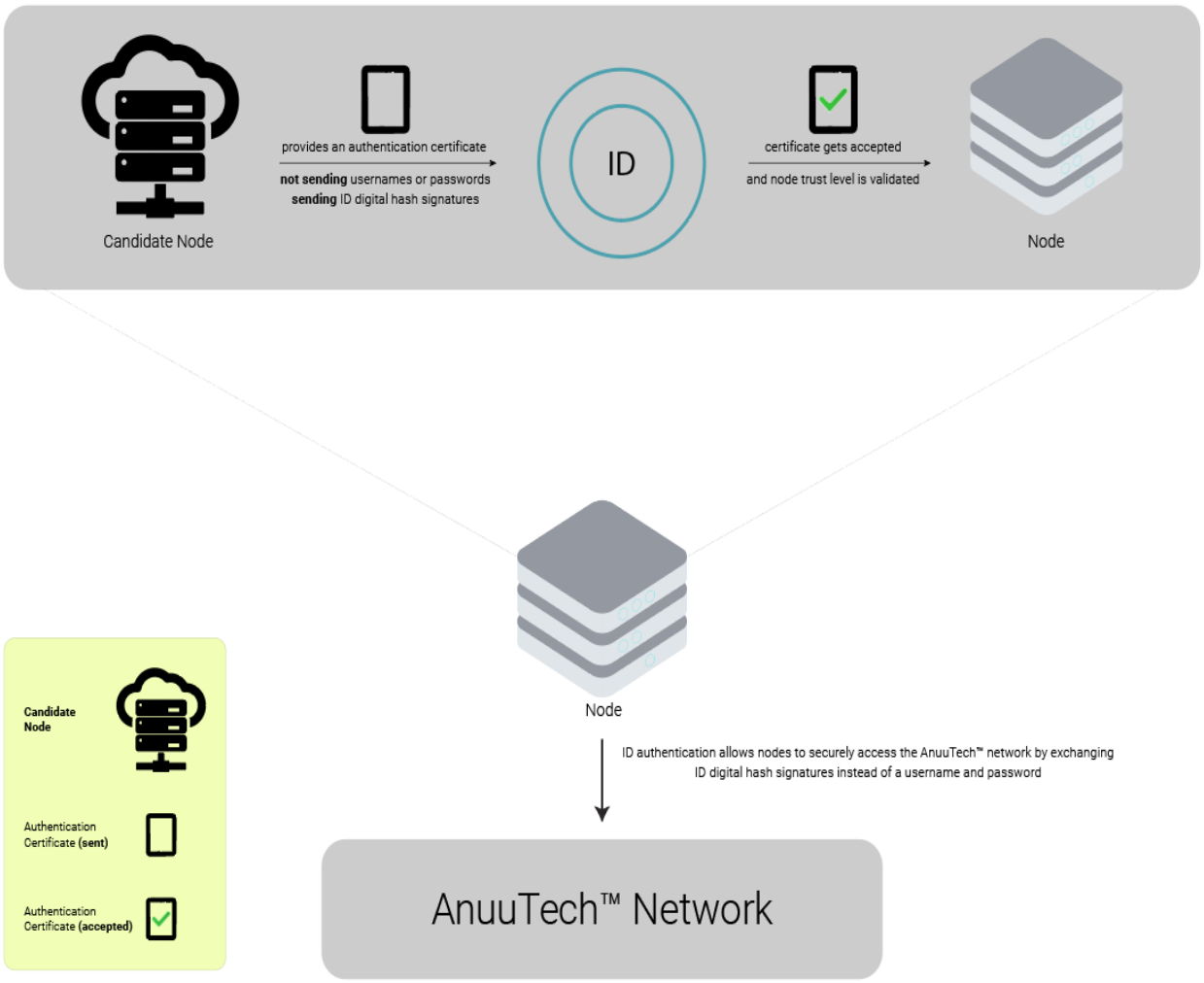

## 1.4 Entry layer

This layer provides strict authentication and authorization processes for users and node service providers. This process includes various validation steps to determine if a new or returning node can be trusted. To establish its trustworthiness, the remote host must provide an acceptable authentication certificate which is then validated to form a chain of trust.

The entry layer leverages an authentication technology known as AnuuTech ID protocol.

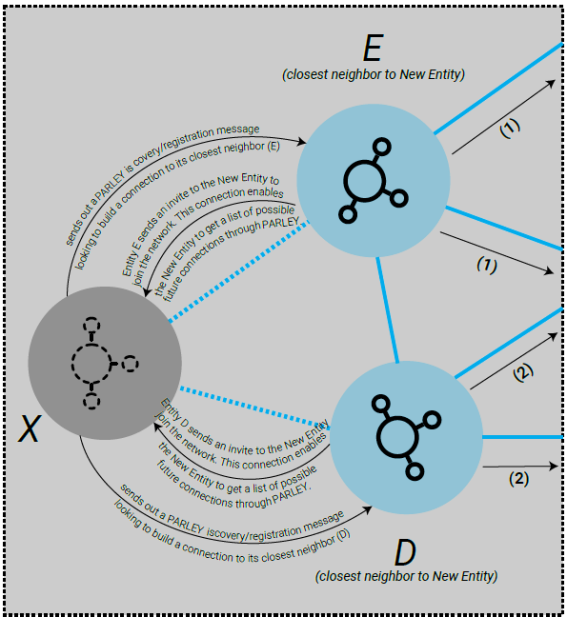
AnuuTech ID maintains multiple fields that are used to validate a node trust level.

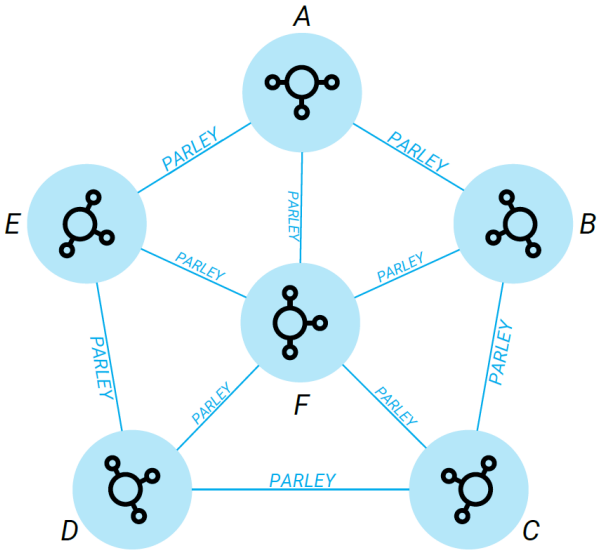
This form of authentication allows nodes to securely access the network by exchanging AnuuTech ID digital hash signatures instead of a username and password. This means the candidate node is not sending a username or password to the server which helps in preventing phishing, keystroke logging and man-in-the-middle (MITM) attacks among other common problems with password-based authentication.




It's within this layer where new and returning nodes will provide identity credentials in the form of a hash to the entry protocol to validate the candidate node's signature to join the network. The result is forming the nodes AnuuTech ID trustworthiness.

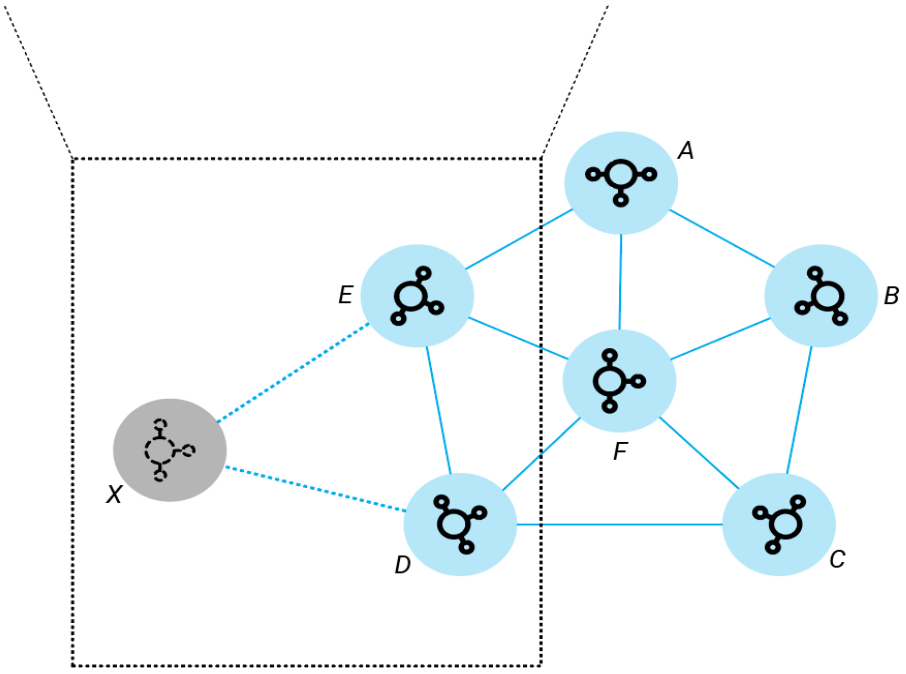
In this drawing, you see a network of 6 entities connected to each other. Each entity has a connection to its closest neighbor. They use the PARLEY language for the communication between entities.




When a new entity joins the network, it sends out a PARLEY discovery/registration message looking to build a connection to its closest neighbors. These requests are forwarded by the other entities to its future closest neighbor. After the others receive this message, the procedure for new connections will be initiated.

In this example, X is the new entity and the blue lines are the new connections. The closest neighbor in the network will initialize the connection. This existing member entity will send an invite to the new entity to join the network. This connection enables the new entity to get a list of possible future connections through PARLEY.




X : New Entity

New connection

**(1)** request is forwarded by Entity E to New Entity's future closest neighbors (A,F)
**(2)** request is forwarded by Entity D to New Entity's future closest neighbors (F,C)

## 1.5 Processing between the layers

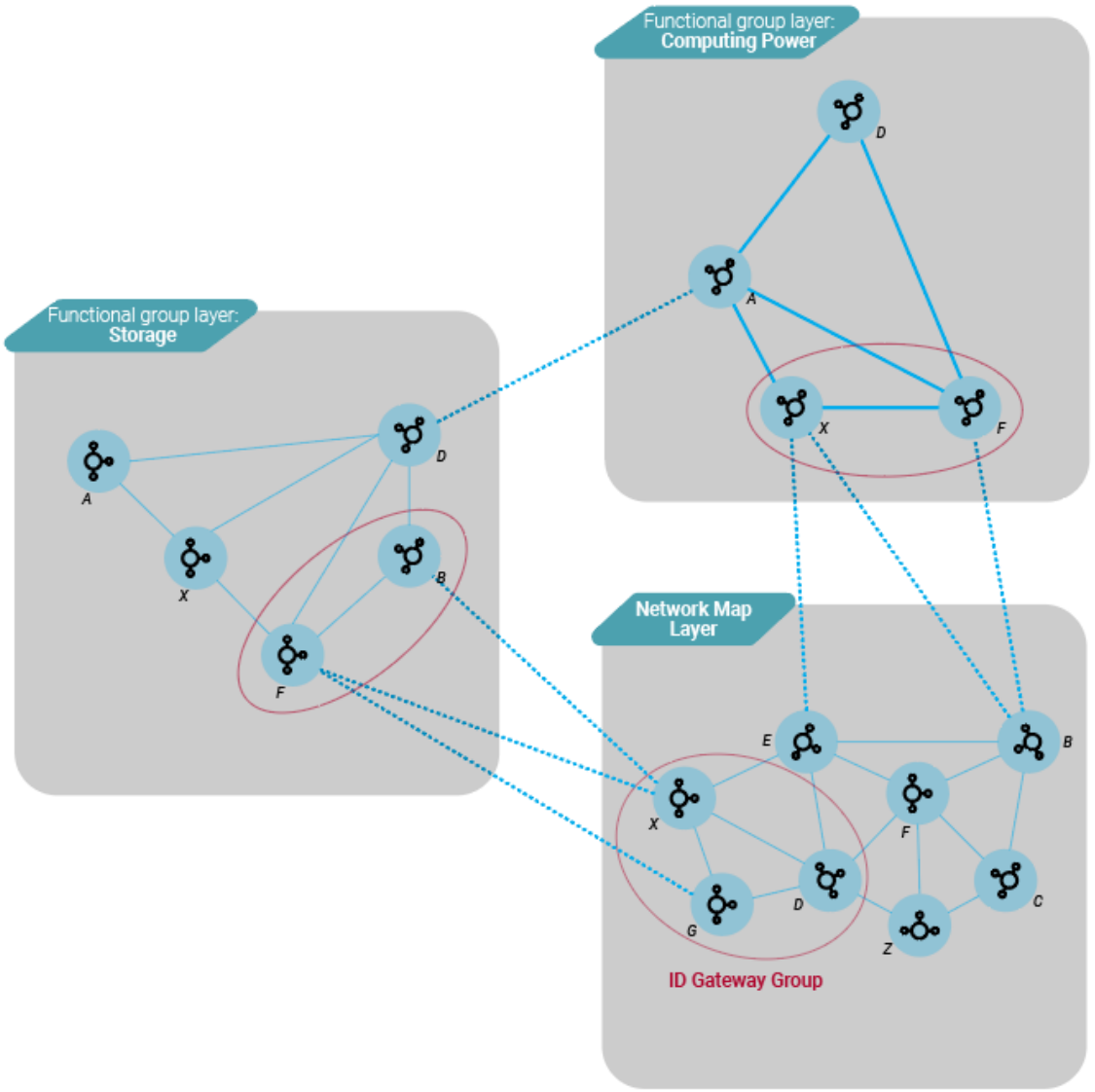
### 1.5.1 Transport layer

A client requesting a specific service is routed to the correct layer via AnuuTech ID gateway groups. These layers are called Functional layers and will be explained later on in this document.

An AnuuTech ID gateway group exists out of multiple entities that have connections between layers. This AnuuTech ID gateway group is used by entities that require a passthrough to another functional group layer. The AnuuTech ID gateway groups have an AnuuTech ID number of their own. When a connection is directed towards the AnuuTech ID number of a gateway group, one of the members inside the AnuuTech ID gateway group handles the connection.

Within this layer, all authentications and tunnel connections are established during the routing adjacency layer stage between entities, allowing the elimination for communication initialization.

Each functional group layer has its own network map. On this map, entities are connected to each other using the nearest neighbor and respecting the AnuuTech Network consensus. As a whole new layer, the connections between entities may vary from the initial layer they connected on as their position on this layer is different. The map and all of its layers are permanently connected to each other through neighboring trusted tunnels.

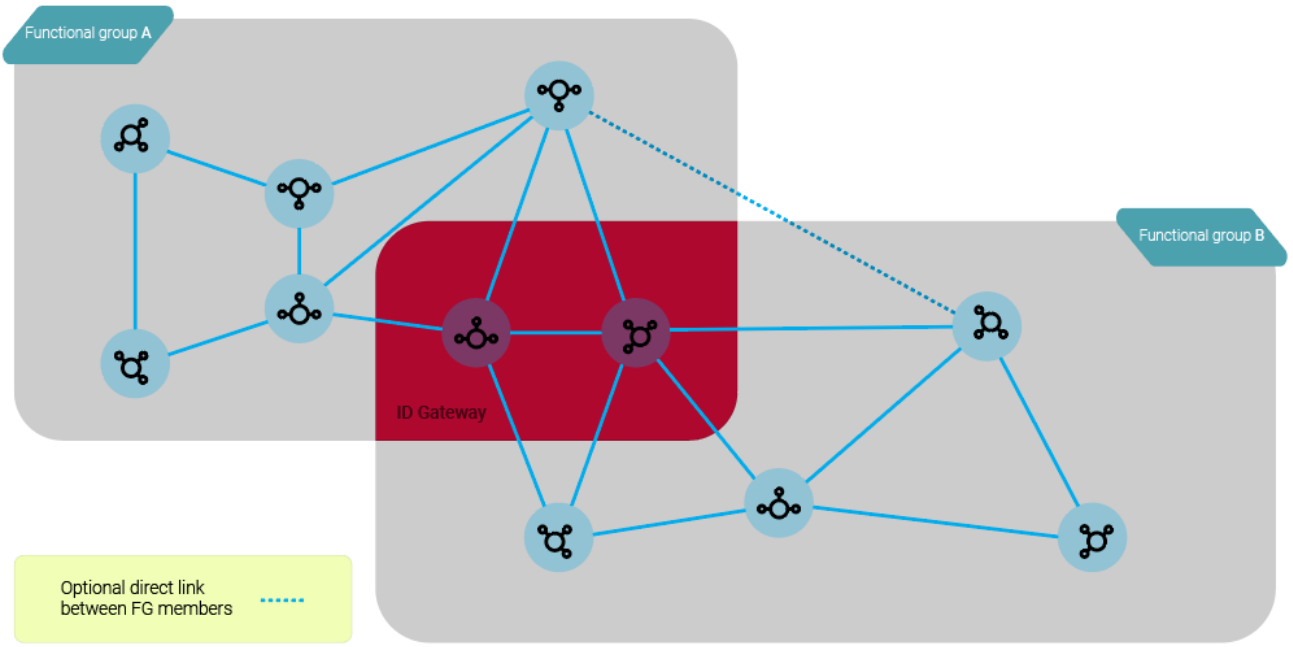


### 1.5.2. Functional Application Service Group Layer

The various services within the dApp ecosystem are organized in functional groups within different AnuuTech Network function layers.

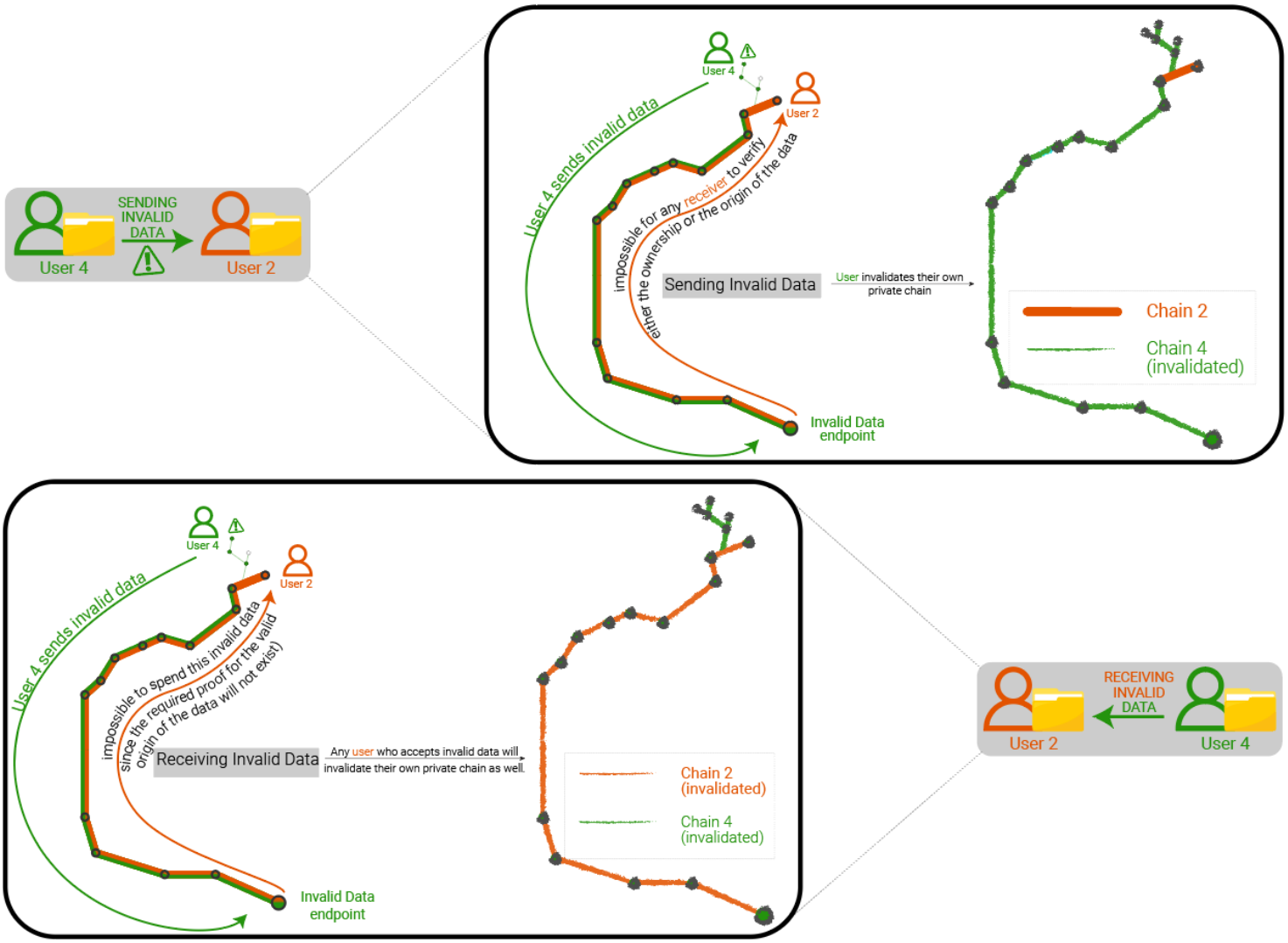
Each layer has its own consensus and AnuuTech ID data. The access to a layer is controlled by both the consensus rules active on the layer and the data stored in the AnuuTech ID, dependent on for example the dApp a client wants to use.

Each functional layer is grouped by functionality, resulting in private functional groups that are paired together via layer-gateways. These functional groups each have AnuuTech ID properties that allow AnuuTech Network entities, belonging to different functional layers, to send PARLEY messages to other AnuuTech Network entities residing in different functional groups - leveraging the functional group address information found in the AnuuTech ID certificate.




## 1.6 Compromised node

If a node fails to sign a transaction within a specified time frame owing to hardware or software failure or network connectivity challenges, the routing map marks the node as inactive. This state is saved in the node's Anuutech ID, letting other nodes know not to expect any more output until the node is synced up again. However, the node continues to receive block information so that it may catch up as soon as the node is restored and back online. Because the routing map is dynamic, these changes in node state have no effect on the rest of the network.




## 1.7 Being Code Agnostic

AnuuTech proposes a platform that allows third-party developers to access its core modules as a means for creating external (server-side) modules - and in whatever programming language they choose. A core module for  smart contracts will soon be in the planning stages. Thus, it's entirely conceivable that third-party developers will create several external modules for smart contracts.

As they're limited only by imagination, developers can create modules dedicated to decentralized storage, instant messaging, decentralized exchanges, or any other conceivable application.

Modules are best understood as extensions of the AnuuTech core and its functionality. Modules implement the major use cases for AnuuTech , whether it be decentralized storage, instant messaging, decentralized exchanges, or any other conceivable applications a developer might create. The AnuuTech core, along with the PARLEY API, allows programmers the freedom to create their own modules using many different popular programming languages ranging from Visual Basic, Java, to C++ and many others. The opportunity for developers to create agnostic coded modules makes the AnuuTech platform not only extremely flexible but also allows the creation of modules by third-party developers of any programming ability.

The PARLEY API is a language application for the core programming interface through which external modules connect to AnuuTech's core via API. It extends the core's functionality and versatility, thus enabling all single programming language barriers and overly complicated user guides to be removed.

# V Performance

AnuuTech has been testing its ideas in an experimental network environment that is not yet optimized for performance but resembles the same architectural structure and tier levels. In preliminary tests, AnuuTech reached a transaction speed of 12,000 tps. That transaction speed was reached using a limited number of nodes. The technology achieves its speed by upscaling the number of nodes utilized by private chains. A higher tps number will be realized using additional nodes. AnuuTech targets a stable 50,000 tps. for its testnet.

# VI Conclusion

AnuuTech’s unique approach to blockchain technology enables users to make use of the advantages of the disaggregation of on-chain and off-chain data. To make setting up a transaction easy AnuuTech provides code agnostics, making  dApps coding in nearly any programming language possible. Our technology can also integrate several existing technologies (hardware, blockchains, etc.), thus elevating their functionality and security in the process.

AnuuTech combines four components seamlessly: **Private Chains**, allowing each user to create their chain. **PoH** (our algorithm) decentralized data integrity protector service running on our node network. **AnuuTech Network's**, network consensus is configured to optimize communication security and speed by incorporating layered structures, trusted connections, and a dynamic gateway. **AnuuTech ID**, (our identifier protocol) facilitates this layered network, identifies entities within a network. The adaptable cryptographic layers ensure endurable use of AnuuTech’s technology to its users in the long term.

# 10 References


1. Mohammad Jabed Morshed Chowdhury, Md. Sadek Ferdous, Kamanashis Biswas, Niaz Chowdhury (2019) "*A Comparative Analysis of Distributed Ledger Technology Platforms*"
2. Ilham Ahmed Qasse; Josef Spillner; Manar Abu Talib; Qassim Nasir (2020) "*A Study on ĐApps Characteristics*"
3. Xiaoshu Wang (2021), *"Research on Data Integrity Verification Technology Based on Blockchain"*
4. Anton Hasselgren, Jens-Andreas Hanssen Rensaa, Katina Kralevska, Danilo Gligoroski, Arild Faxvaag (2021), "*Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study"*
5. Shang Gao, Ying Li (2021) "*An empirical study on the adoption of blockchain based games from users' perspectives"*
6. *Jaliz Maldonado (2018), "10 Ways Blockchain Technology Will Change The Legal Industry" National Law Review, Volume VIII, Number 323*
7. *Connor Young, Yanyan Li, and Hector Fernandez (2021), "The Economist Case Study: Blockchain-based Digital Voting System"*
8. *Ahmad A. A. Khanfar, Mohammad Iranmanesh, Morteza Ghobakhloo, Madugoda Gunaratnege Senali and Masood Fathi (2021), "Applications of Blockchain Technology in Sustainable Manufacturing and Supply Chain Management: A Systematic Review"*
9. *Gagan Varshney, Kaushal Pratap Singh, Tejesh Bhalla, Saumya (2021), "Comparative study of centralized and decentralized web-hosting Solutions using blockchain"*
10. *Sanjeev Kumar Dwivedi, Priyadarshini Roy, Chinky Karda, Shalini Agrawal, and Ruhul Amin (2021), "Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey"*
11. *Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, Jun Zhao (2021), "A Survey of Blockchain Applications in Different Domains"*
12. *Alexandr Kuznetsov , Inna Oleshko, Vladyslav Tymchenko, Konstantin Lisitsky, Mariia Rodinko and Andrii Kolhatin (2021), "Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain"*
13. Sheping Zhai, Yuanyuan Yang, Jing Li, Cheng Qiu and Jiangming Zhao (2019 "Research on the Application of Cryptography on the Blockchain"
14. Balázs Bodó, Jaya Klara Brekke, Jaap-Henk Hoepman(2021), "Decentralisation in the blockchain space"
15. Vivek Bagaria, Sreeram Kannan, David Tse, Giulia Fanti, Pramod Viswanath (2019), "Deconstructing the Blockchain to Approach Physical Limits"
16. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen (2017), "A Survey on the Security of Blockchain Systems"
17. Dodo Khan, Low Tang Jung, Manzoor Ahmed Hashmani (2021), "Systematic Literature Review of Challenges in Blockchain Scalability"
18. Lewis-Pye, Andrew (2020) "Cryptocurrencies: protocols for consensus"