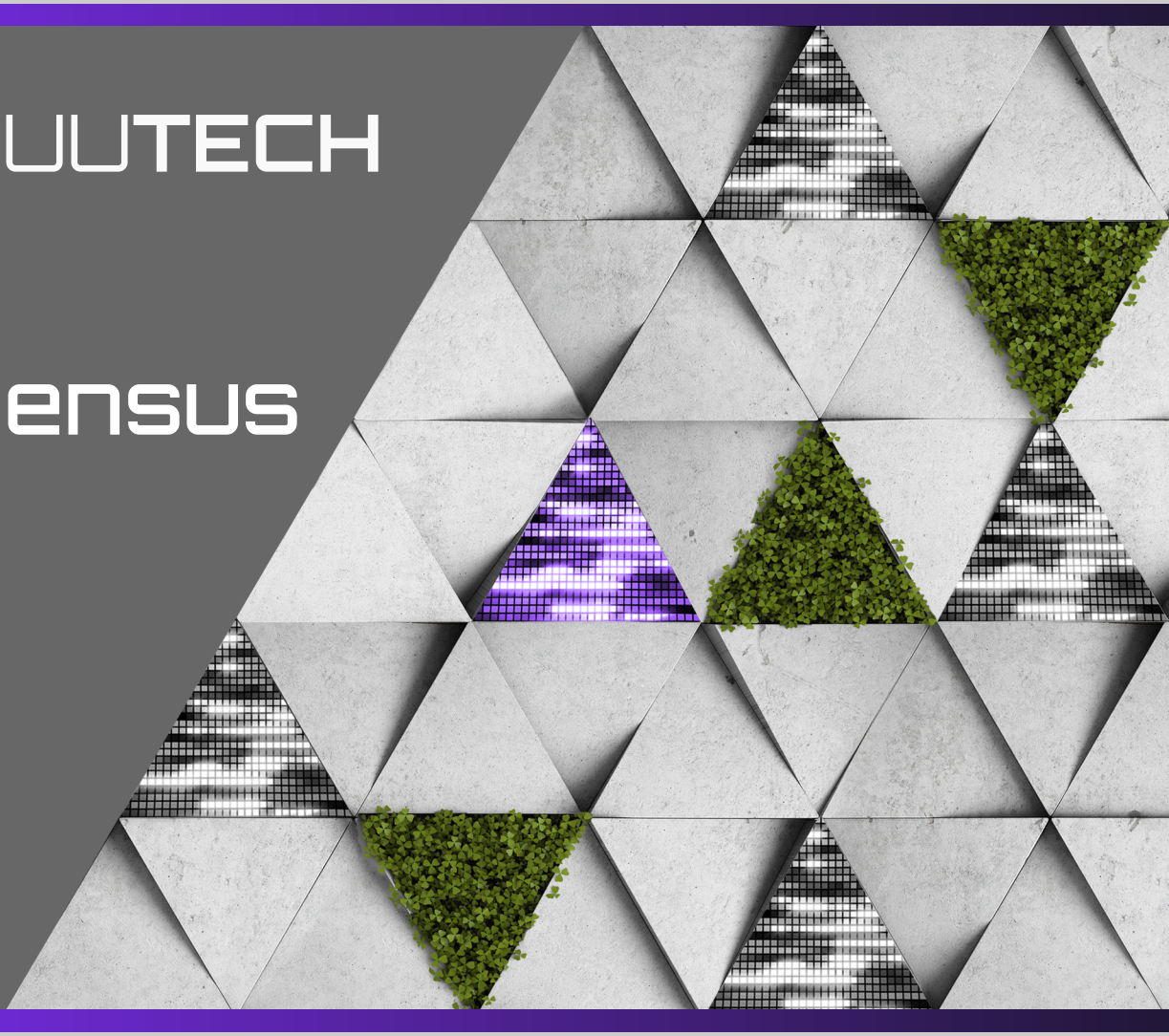
ANUUTECH

PoH Consensus

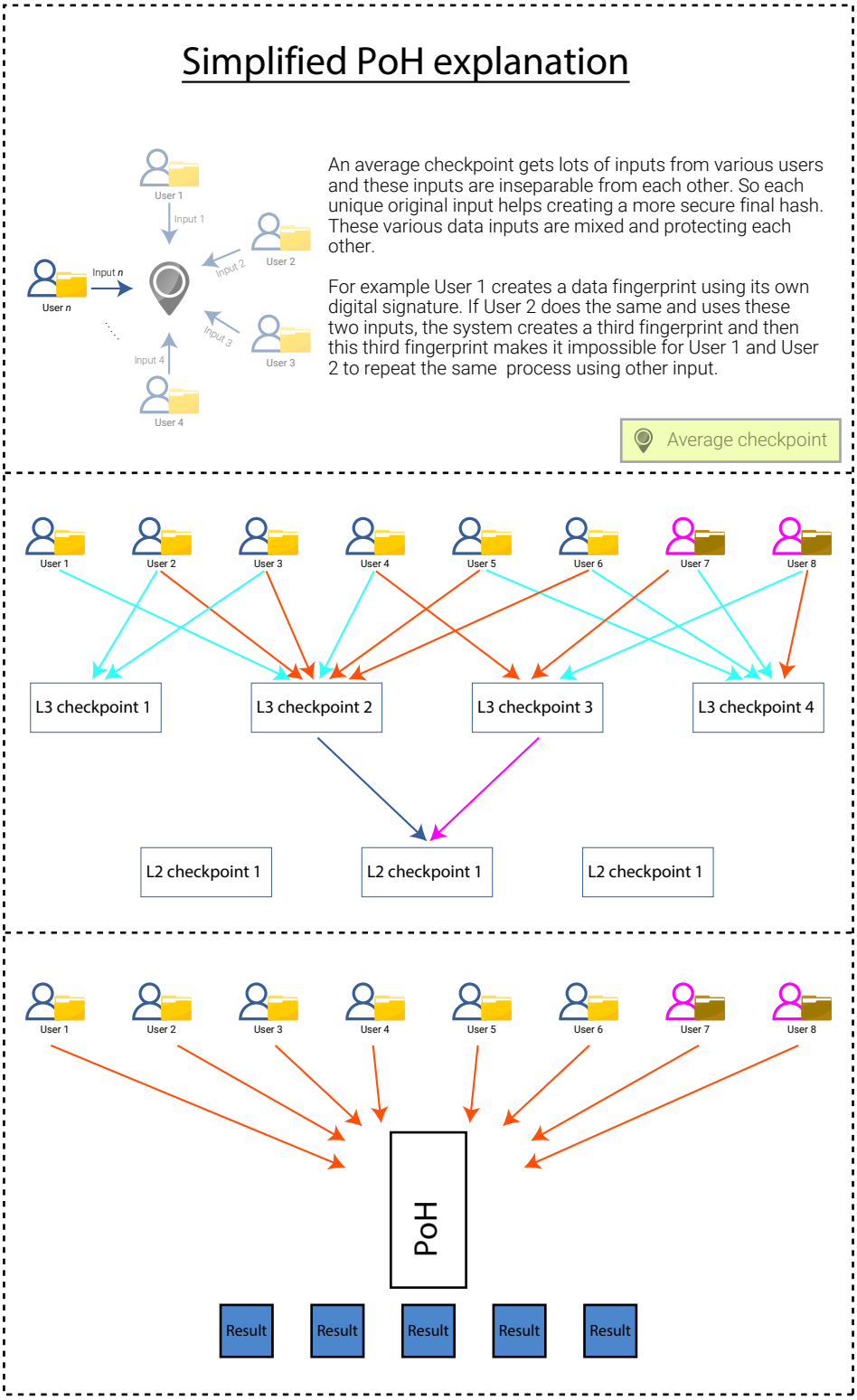


PoH Consensus

Table of Contents

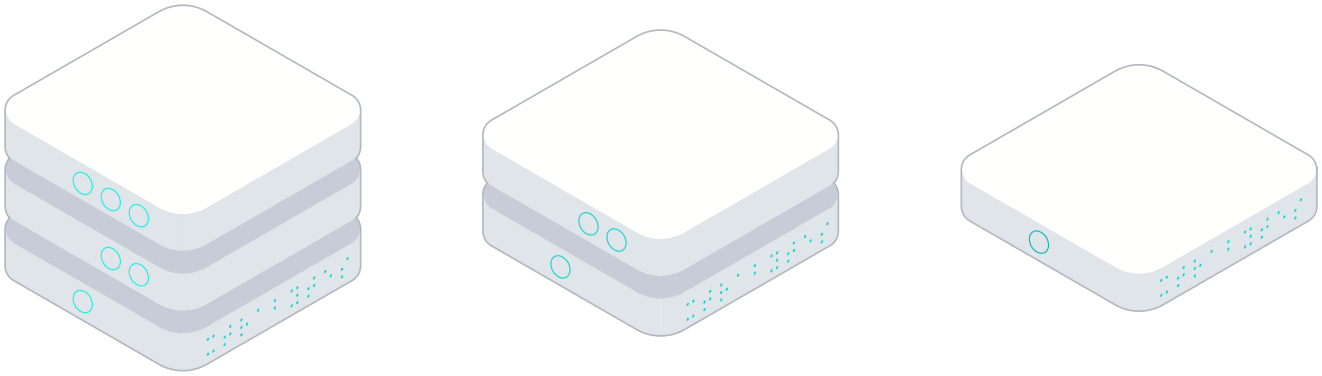
PoH consensus

What is PoH PoH 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.



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. 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. This layer also serves as a barrier between the third layer which is accessible by the network users and the first layer where the eventual consensus is reached. This will help prevent the possibility for network users to interfere with the consensus process. 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.
The hosting of each checkpoints is assigned in a pseudo random fashion, partially based on the result of the previous outcome of the consensus round and the certificates issued to the nodes, after each consensus round. Multiple checkpoints can be assigned to the same physical nodes should there not be enough physical nodes for all the checkpoints.



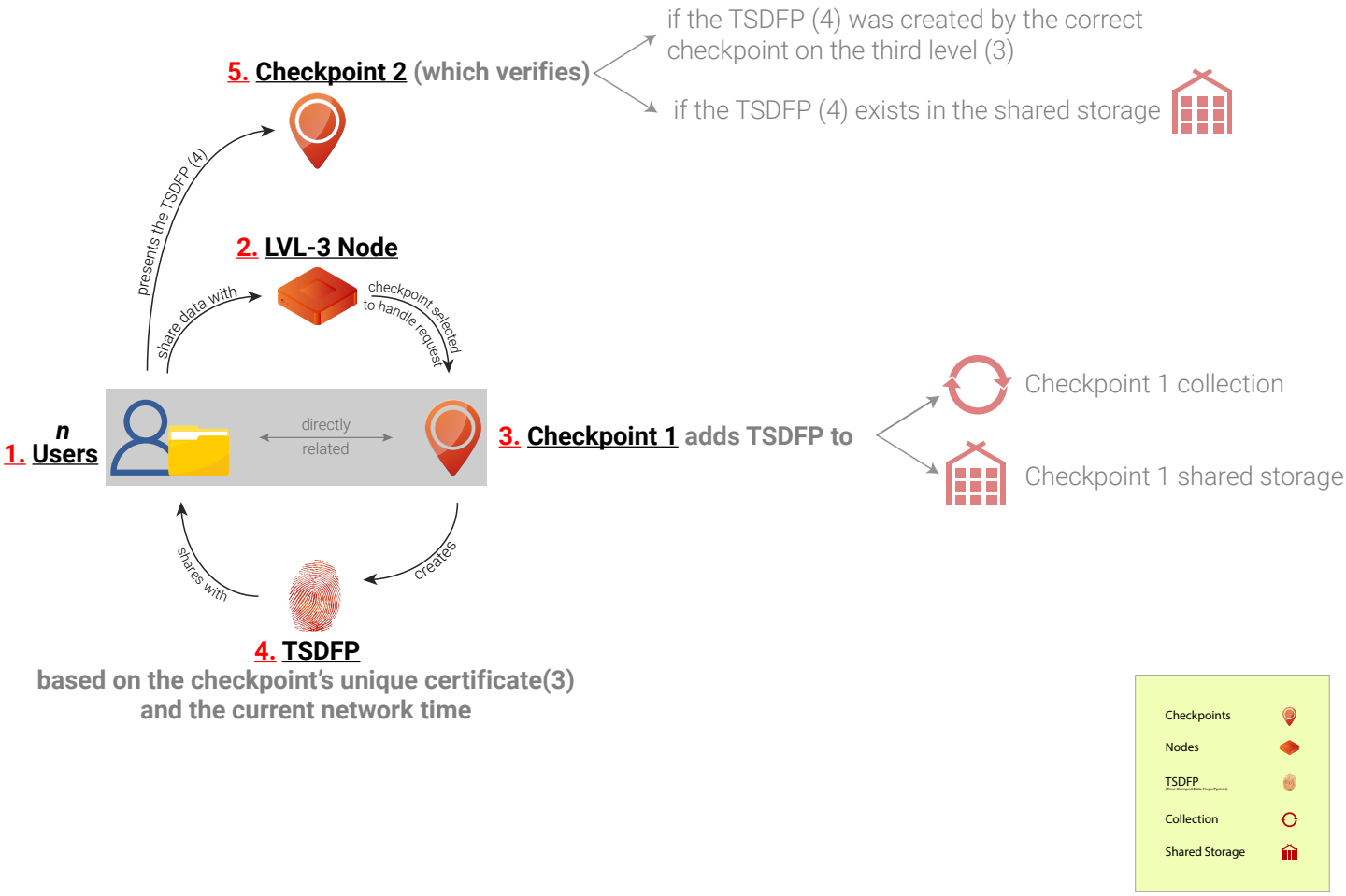
How does it work?

Consensus phase

Level 3 - Collection phase

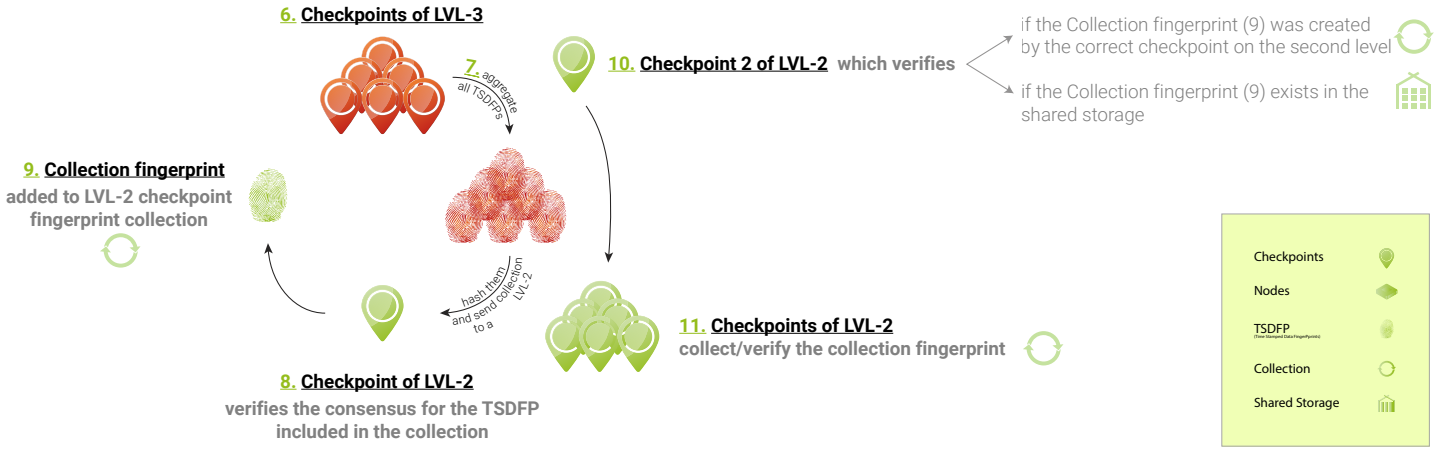
When a user wants to use the PoH service, they will present a subset of data to the third node level. The checkpoint selected to handle this request is directly related to the data. The checkpoint will create a time stamped data fingerprint for the data based on the checkpoints unique certificate and the current network time, add this time stamped data fingerprint to its collection and the shared temporary storage for the current time period, and provide this fingerprint to the network user. The user (1) will present this time stamped data fingerprint to a second checkpoint (5), selected based on the fingerprint , on the third level which will verify if the time stamped data fingerprint was created by the correct checkpoint (3) on the third level and if it exists in the shared storage. The number of secondary checkpoints that will collect/verify the time stamped data fingerprint can vary depending on the consensus rules for the network. All checkpoints on the third level will collect the timestamped data fingerprint (4) they either generated or verified for the duration of the specific time period (n).

Once a user (1), receives a timestamped data fingerprint , they will have a temporary proof of data integrity, however, to get full confirmation the master hash for the time period of the time stamped data fingerprint needs to be added to the shared storage for the PoH consensus protocol and the time stamped data fingerprint needs to be used in the calculation of the master hash. The time required for full confirmation is n x 4.



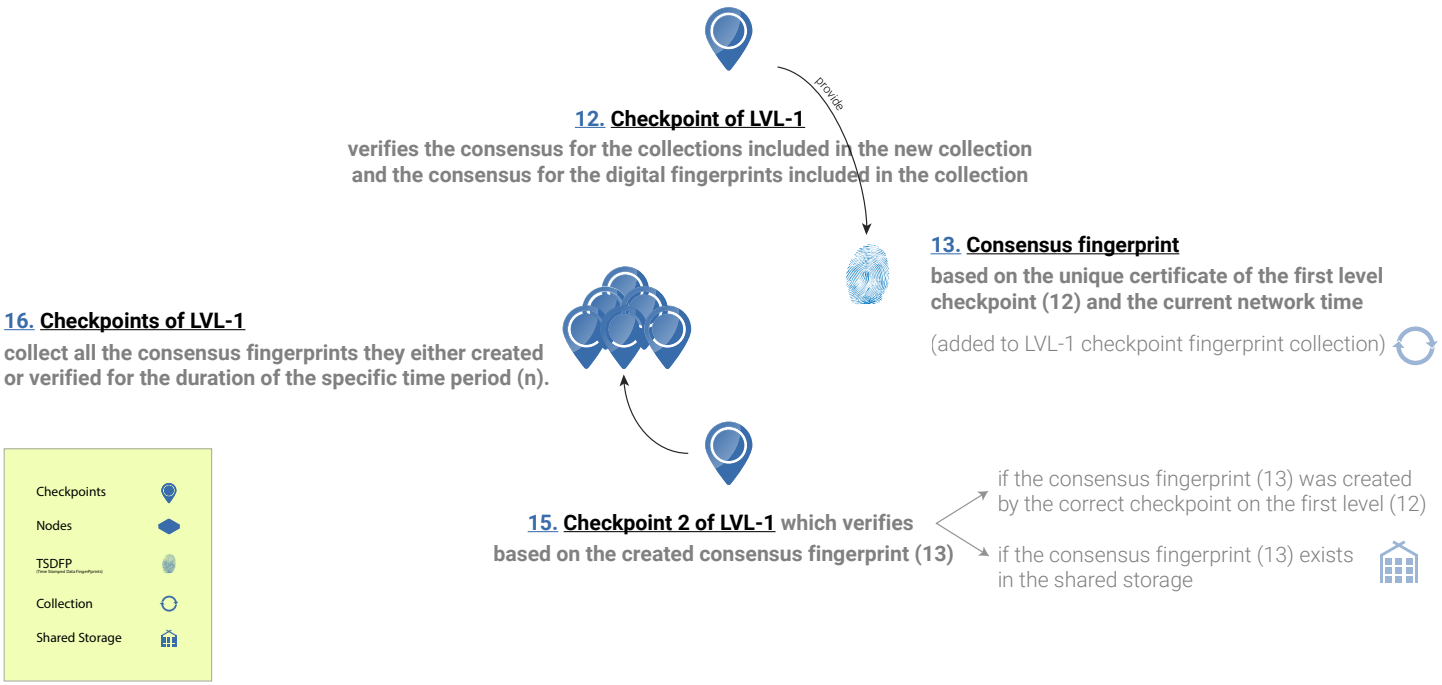
Level 2 - Aggregation phase part 1

All checkpoints on the third level will aggregate (6) the time stamped data fingerprints they collected during the time period (n) and hash the collection. The checkpoints on the third level will send the collection hash (7) to a checkpoint on the second level, selected based on the collection signature. The checkpoints on the second level will verify (8) the consensus for the time stamped data fingerprints included in the collection and provide a collection fingerprint, based on the unique certificate of the second level checkpoint and the current network time. The checkpoint on the second level will add this collection (9) fingerprint to its collection for the current time period and the shared storage and provide this collection fingerprint to the checkpoint on the third level that had sent the collection. The checkpoint on the third level will send the collection fingerprint to a second checkpoint on the second level (10), selected based on the created collection fingerprint, 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. The number of secondary checkpoints that will collect/verify the collection fingerprint can vary depending on the consensus rules for the network.
All checkpoints of the second level will collect all the collection fingerprints (11) they either created or verified for the duration of the specific time period (n).

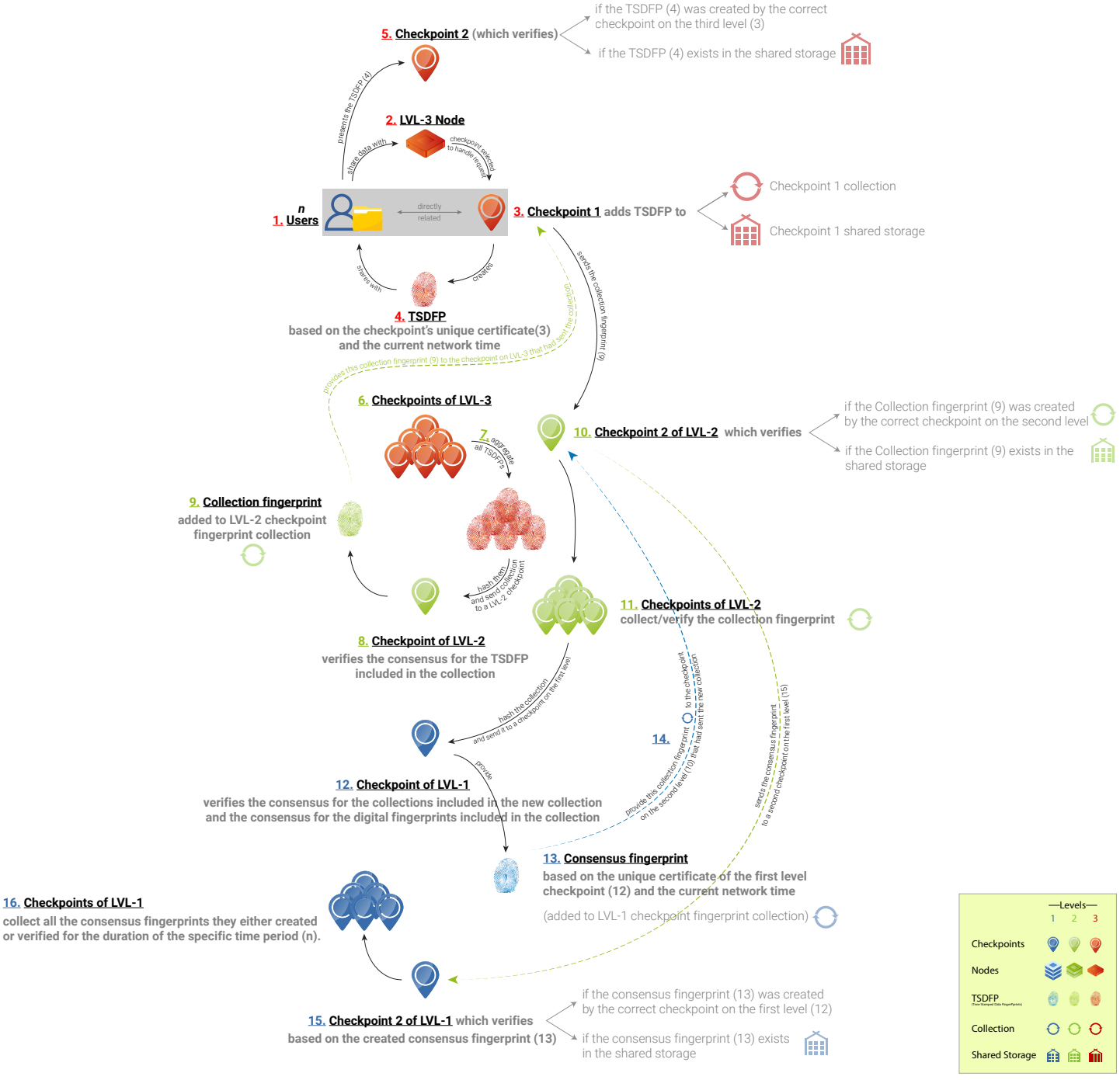


Level 1 - Aggregation phase part 2

All checkpoints on the second level will aggregate the collections they collected during the time period (n) and hash of the new collection (12). The checkpoints on the second level will send the new collection hash to a checkpoint on the first level, selected based on the new collection signature. The checkpoints on the first level will verify the consensus for the collections included in the new collection and the consensus for the digital fingerprints included in the collection, (13) and provide a consensus fingerprint, based on the unique certificate of the first level checkpoint and the current network time. The checkpoint on the first level will add this consensus fingerprint to its collection for the current time period and the shared storage and provide this collection fingerprint to the checkpoint on the second level (14 Page 9) that had sent the new collection. The checkpoint on the second level will send the consensus fingerprint to a second checkpoint on the first level, selected based on the created consensus fingerprint, 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 (15). The number of secondary checkpoints that will collect/verify the consensus fingerprint can vary depending on the consensus rules for the network.
All checkpoints of the first level will collect all the consensus fingerprints they either created or verified for the duration of the specific time period (n) (16).



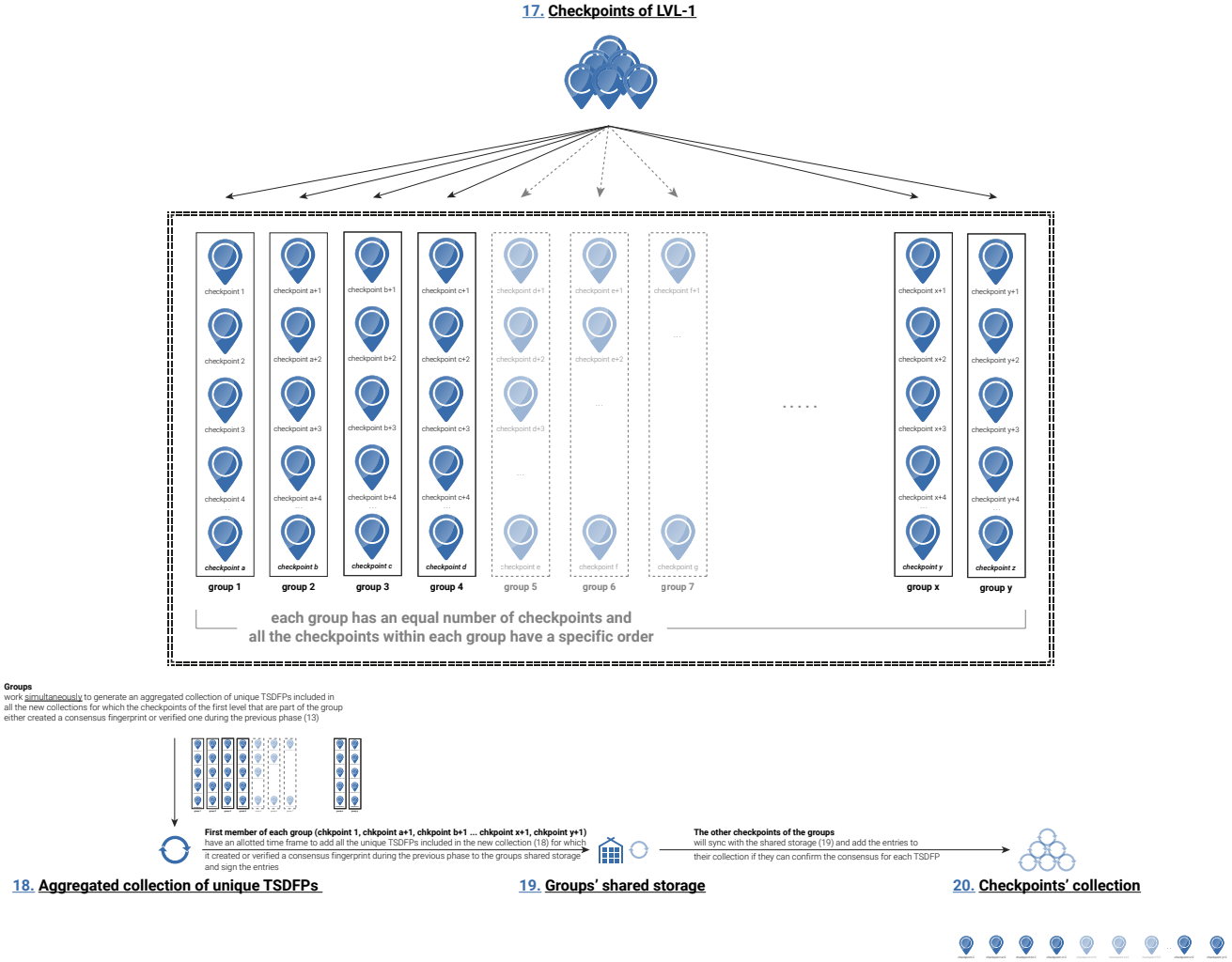
PoH Full Explanatory Diagram Part 1



Master hash phase

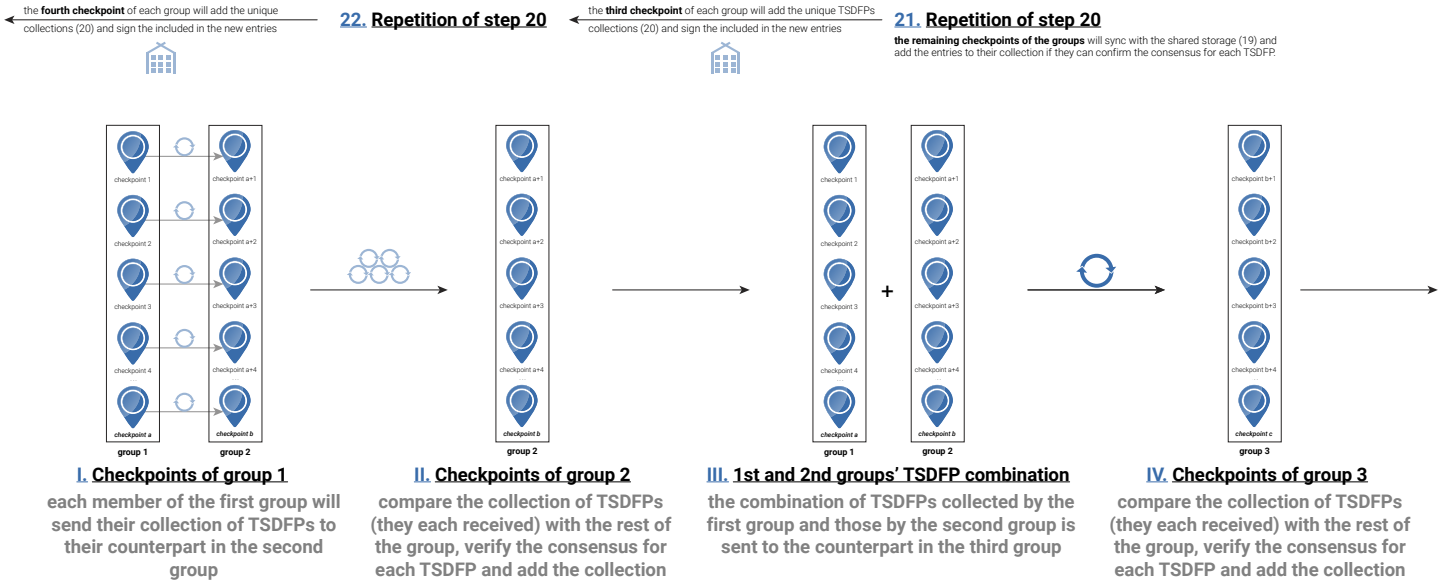
Level 1 - Signing phase round 1

All the checkpoints of the first level (17) are ordered in a pseudo random fashion, based on the previously generated masterhash, in a number of groups with equal members.
Within each group all the checkpoints will have a specific order as well.
All the groups will work simultaneously to generate an aggregated collection of unique time stamped data fingerprints included in all the new collections for which the checkpoints of the first level that are part of the group either created a consensus fingerprint or verified a one during the previous phase. The first member of the groups will have an allotted time frame to add all 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 groups 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 allotted time frame for the first checkpoint has expired, the second checkpoint of the group (18) will add all the unique time stamped data fingerprints, included in the 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 its allotted time frame and sign the entries. Again, the remaining checkpoints (19) of the groups will sync with the shared storage and add the entries to their collection if they can confirm the consensus for each digital fingerprint. Next (20) the third checkpoint will do the same followed by all other checkpoints in the group.



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 (I) will send their collection of digital fingerprints to their counterpart in the second group (G1C1 -> G2C1; G1C2->G2C2; …). The checkpoints of the second group (II) will compare the collection of digital fingerprints 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 with most digital fingerprints for which they can confirm the consensus. The checkpoint of the second group will verify the consensus for each digital fingerprint and add the collection of digital fingerprints for the second group generated in the previous phase. The combination of digital fingerprints collected by the first group and those by the second group is sent to the counterpart in the third group (G2C1->G3C1; G2C2-G3C2; …). The checkpoints of the third group (III) 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 with most digital fingerprints for which they can confirm the consensus. The checkpoint of the second group will verify the consensus for each digital fingerprint and add the collection of digital fingerprints for the third group generated in the previous phase. The combination of digital fingerprints collected by the second group and those by the third group is sent to the counterpart in the fourth group (G3C1->G4C1; G3C2-G4C2; …). Next the fourth group (IV) will do the same followed by the other groups.



I. Checkpoints of group 1
each member of the first group will send their collection of TSDFPs to their counterpart in the second group

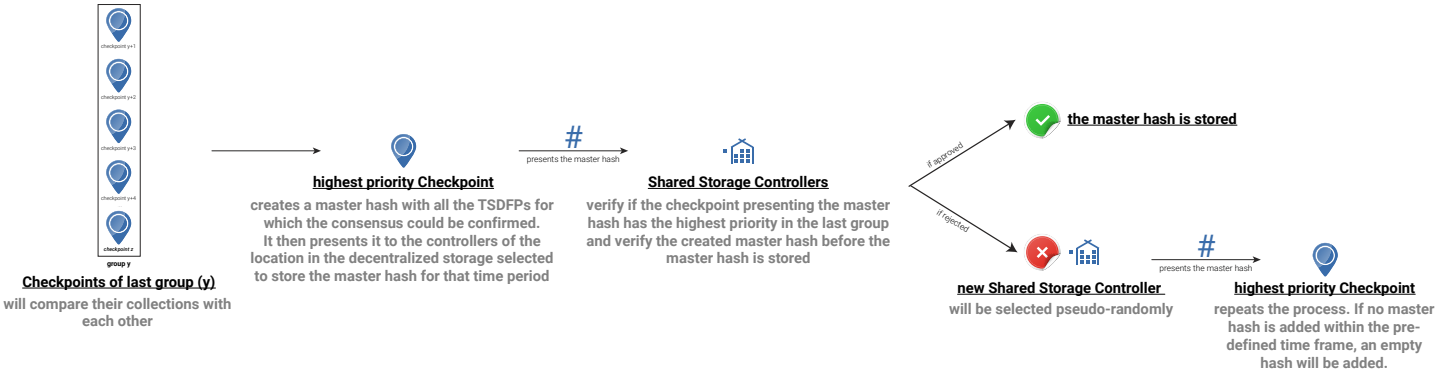
II. Checkpoints of group 2
compare the collection of TSDFPs (they each received) with the rest of the group, verify the consensus for each TSDFP and add the collection

III. 1st and 2nd groups' TSDFP combination
the combination of TSDFPs collected by the first group and those by the second group is sent to the counterpart in the third group

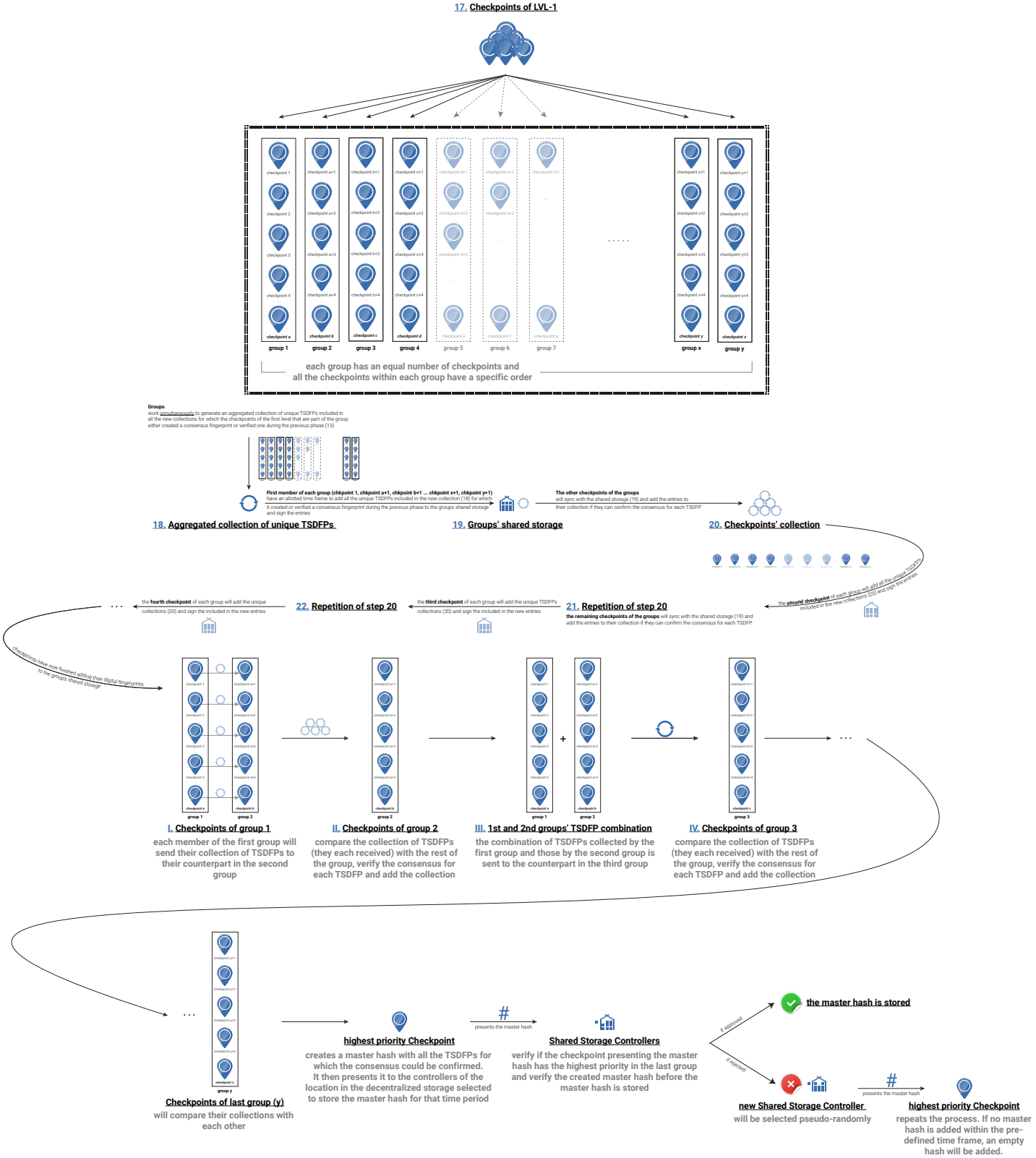
IV. Checkpoints of group 3
compare the collection of TSDFPs (they each received) with the rest of the group, verify the consensus for each TSDFP and add the collection

Level 1 - Adding phase

When the last group has finished adding the digital fingerprints for the last group. The checkpoint of the last group will compare their collections with each other and the checkpoint with the highest priority will create a master hash with all the digital fingerprints for which the consensus could be confirmed. This checkpoint will present the master hash to the controllers of the location in the decentralized storage selected to store the master hash for that time period. All the controllers verify if the checkpoint presenting the master hash has the highest priority in the last group and verify the created master hash before the master hash is stored. If one of the controllers rejects the master hash, new controllers will be selected pseudo-randomly. And the checkpoint with the highest priority will repeat the process. If no master hash is added within the pre-defined time frame, an empty hash will be added.



PoH Full Explanatory Diagram Part 2



How does PoH provide trustable proof

The digital fingerprint created by the level 3 checkpoints uses the hashed value of the data requesting the PoH integrity protection, the current network time and the unique certificate of the level 3 checkpoint for that time period. This way the digital fingerprint provides 3rd party verification of the data content for the data at the moment the digital fingerprint was requested. The master hash is a hash value created from all the digital fingerprints for that time period and provides proof for the digital signature's existence in that time period. Only 1 master hash can exist for each time period and the master hashes are also linked to each other much like the blocks in a regular block blockchain.
Every user will sync with the network the moment they connect to the network adding all the master hashes to their chain.
It will be impossible for a user to change the data protected by a digital fingerprint after the master hash for that time period has been created.

Glossary

Aggregated Collection:	Collection of everything from the previous nodes.
Collection Fingerprint:	Fingerprint made from in the level 2 checkpoint from the collection hash received from the second node and its own unique certificate and the current network time.
Collection Signature:	The hash of all the current node level collections.
Consensus Protocol:	A specific algorithm that ensures how and according to which rules transactions on a blockchain are approved.
Controller:	The Entity that will verify if the master hash is coming from the correct check point and will eventually store it.
Data Fingerprint:	Something that is created for a specific piece of data with extra unique parameters to make it possible to identify a piece of data.
Digital Fingerprint:	A unique identifier for the checkpoints.
Master Hash:	The Master hash is the result of running true all phases of the PoH consensus before being stored.
Node:	The collection of nodes (dedicated computers) forms the infrastructure of a blockchain. AnuuTech has 3 levels of 3584 nodes.
PoH:	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.
TSDFP:	Time Stamped Data FingerPrint based on the checkpoints unique certificate and current network time.
Virtual Checkpoints:	Part of nodes that execute the operations from the collection of the previous level of nodes.