TECHNICAL WHITEPAPER

ico@sphere.ee

TABLE OF CONTENTS

ABSTRACT

Sphere is a decentralized network for smart-contracts execution and digital commodities management. It ensures immediate transaction execution, provides real scalability, guarantees network synchronisation and resilience, and eliminates the need of mining.

As an open-source software, Sphere can be engaged as a scalable and resilient fintech tool for internal (B2B) and external (B2B, B2C, C2C) intelligent transactions (smart-contracts):

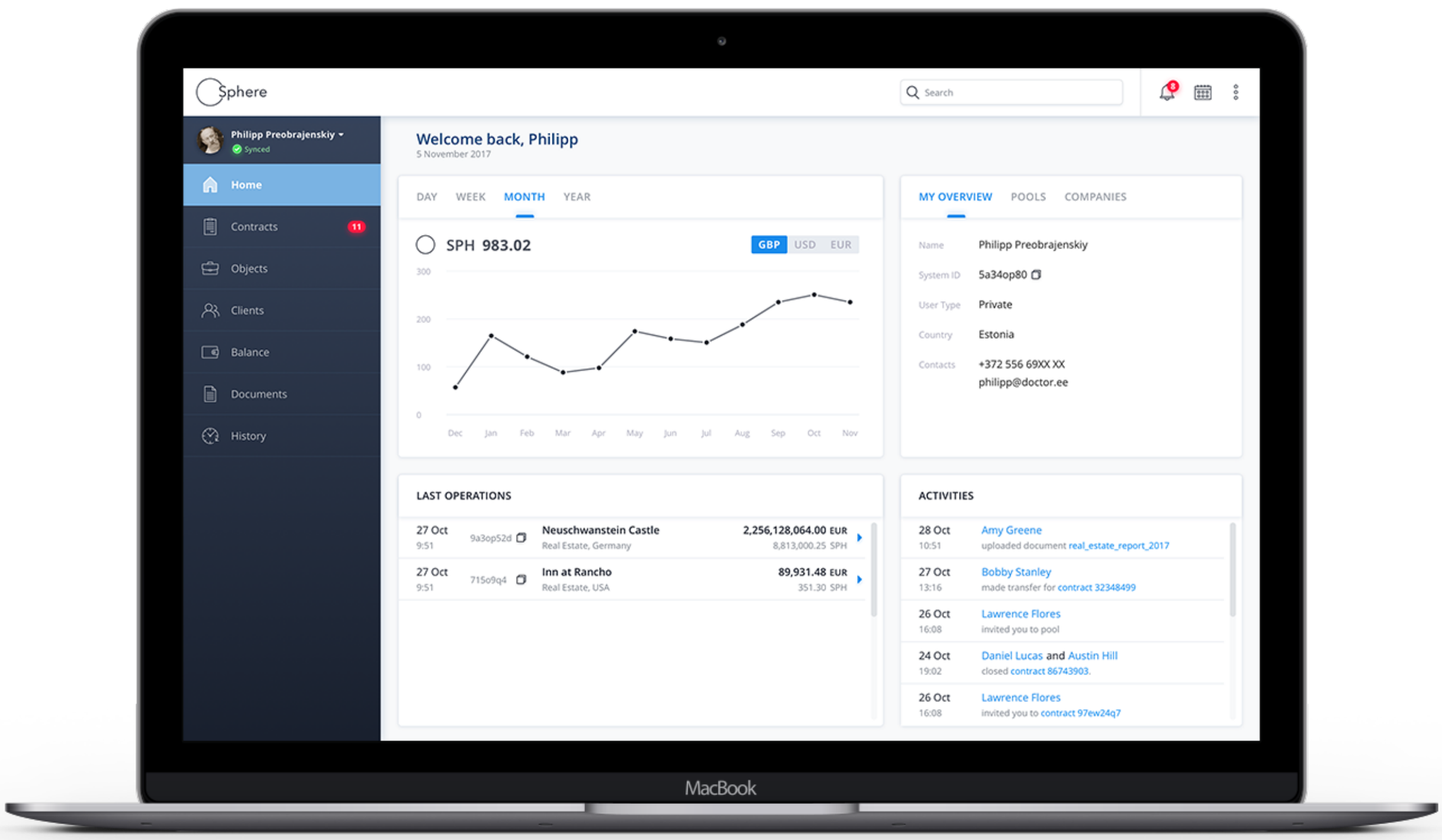
- **B2B.** Organizations can issue their own Sphere-compliment tokens over Sphere networks spawned in a private cloud. It may be used internally (for transactional costs reducing, financial control, accounting simplification and automatization) or externally (for mutual settlements, smart-contracts, etc).
- **B2C and C2C.** Sphere Platform (see the next chapter) is the reference implementation of B2C and C2C with Sphere, however, one can also deploy own Sphere-based online platform with own Sphere-compliment token to create a new marketplace.

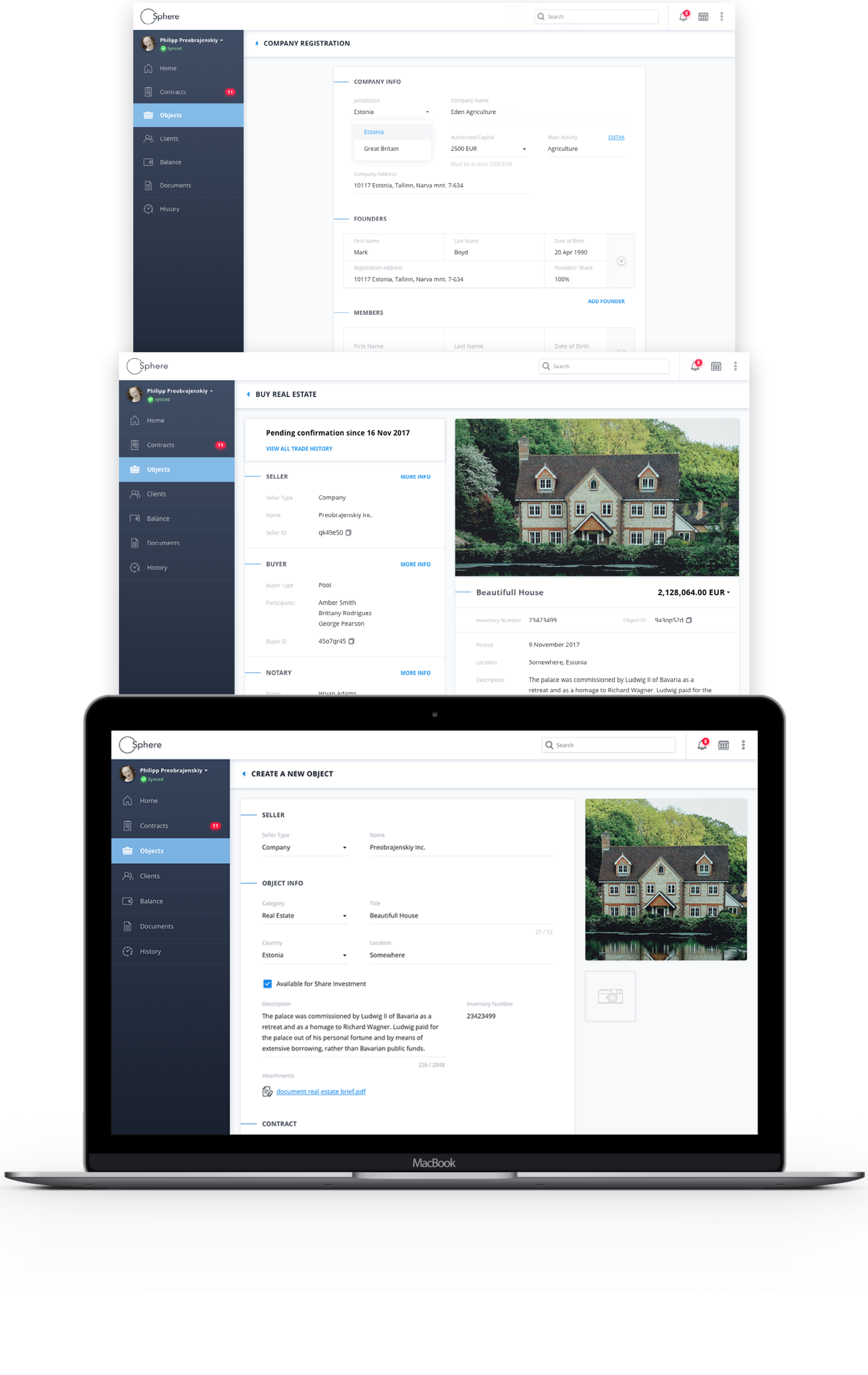
Current whitepaper covers theoretical foundations and technical implementation of Sphere. Key concepts: blockchain, cloud computing, clustering, network mesh, async Proof of authority (aPoA) consensus algorithm, concurrent transactions evaluation and verification, adaptive block size, elimination of mining, SPVs with committed Bloom filter, deterministic smart-contracts written in Scala.

For wider economical and legal rationale, please, check Legal whitepaper.

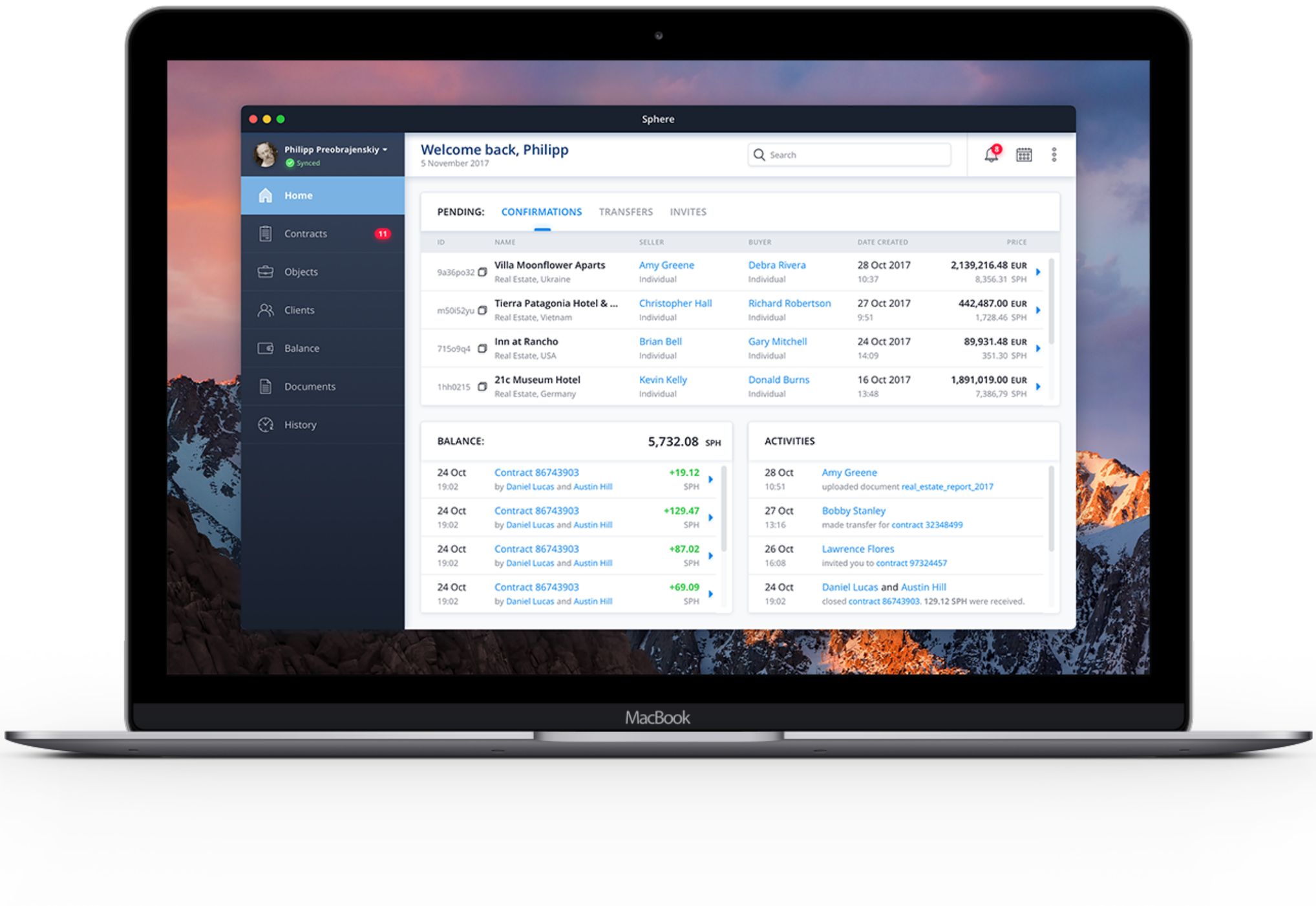
SPHERE PLATFORM

Sphere Platform is a free public application, designed for digital commodities management, e.g. buying, selling, crowdfunding, etc. Client can both set any kind of service or good for sale or to buy it. For example, real estate, company incorporation, consulting services, currency exchange.
It also includes crypto-currencies and FIAT stock exchange facilities, lawyers and notary officers freelance market, Sphere IT consulting, etc.




Sphere
Search
Philipp Preobrajenskiy
Synced
Home
Contracts
11
Objects
Clients
Balance
Documents
History
COMPANY REGISTRATION
COMPANY INFO
Jurisdiction
Estonia
Great Britain
Company Name
Eden Agriculture
Authorized Capital
2500 EUR
Must be at least 2500 EUR
Main Activity
EMTAK
Agriculture
Company Address
10117 Estonia, Tallinn, Narva mnt. 7-634
FOUNDERS
First Name
Mark
Last Name
Boyd
Date of Birth
20 Apr 1990
Registration Address
10117 Estonia, Tallinn, Narva mnt. 7-634
Founders' Share
100%
ADD FOUNDER
MEMBERS
First Name
Last Name
Date of Birth
BUY REAL ESTATE
Pending confirmation since 16 Nov 2017
VIEW ALL TRADE HISTORY
SELLER
MORE INFO
Seller Type
Company
Name
Preobrajenskiy Inc.
Seller ID
qk49e50
BUYER
MORE INFO
Buyer Type
Pool
Participants
Amber Smith
Brittany Rodriguez
George Pearson
Buyer ID
45o7qr45
NOTARY
MORE INFO
Beautifull House
2,128,064.00 EUR
Inventory Number
23423499
Object ID
Posted
9 November 2017
Location
Somewhere, Estonia
Description
The palace was commissioned by Ludwig II of Bavaria as a retreat and as a homage to Richard Wagner. Ludwig paid for the
CREATE A NEW OBJECT
SELLER
Seller Type
Company
Name
Preobrajenskiy Inc.
OBJECT INFO
Category
Real Estate
Title
Beautifull House
21 / 72
Country
Estonia
Location
Somewhere
Available for Share Investment
Description
The palace was commissioned by Ludwig II of Bavaria as a retreat and as a homage to Richard Wagner. Ludwig paid for the palace out of his personal fortune and by means of extensive borrowing, rather than Bavarian public funds.
226 / 2048
Inventory Number
23423499
Attachments
document real estate brief.pdf
CONTRACT
MacBook

The Client can engage notary officers and law advisors for his/her deals. Notary officers and advisors have their own application to validate all deals deployed on Platform effectively. All acts validated by notary officers or law advisors mirrored in smart-contracts are considered as legally valid acts in Estonia and EU.



TOKEN

Sphere token (SPH) is an internal currency for Sphere Platform.
It is an investment gold backed token fixed by investment gold price on LBMA (London Bullion Market Association). SPH is both a risk hedging and good crypto-investment tool:

- **80% of investments will be immediately converted into physical gold or gold Exchange Traded Funds (ETFs) with repaying possibility in one year.**
- **20% of will be gathered for development and service costs (see ICO chapter).**

Investor's interest is based on commission executed across the network.
Commissions are calculated and processed by Full Nodes (see Rewards chapter).

SPH token gold guarantee is provided by Eclat Capital OU. Eclat Capital OU (Tallinn, Estonia, registry number 14291703) has following licenses:

- Operating as a financial institution FFA000216
- Service of alternative means of payment FIA000063
- Currency exchange VVT000380
- Financial services, Buying up and wholesale of precious metals and precious stones FVV000187

Eclat Capital OÜ is registered in the US, Foreign Account Tax Compliance Act FATCA ID 3M1BD2.

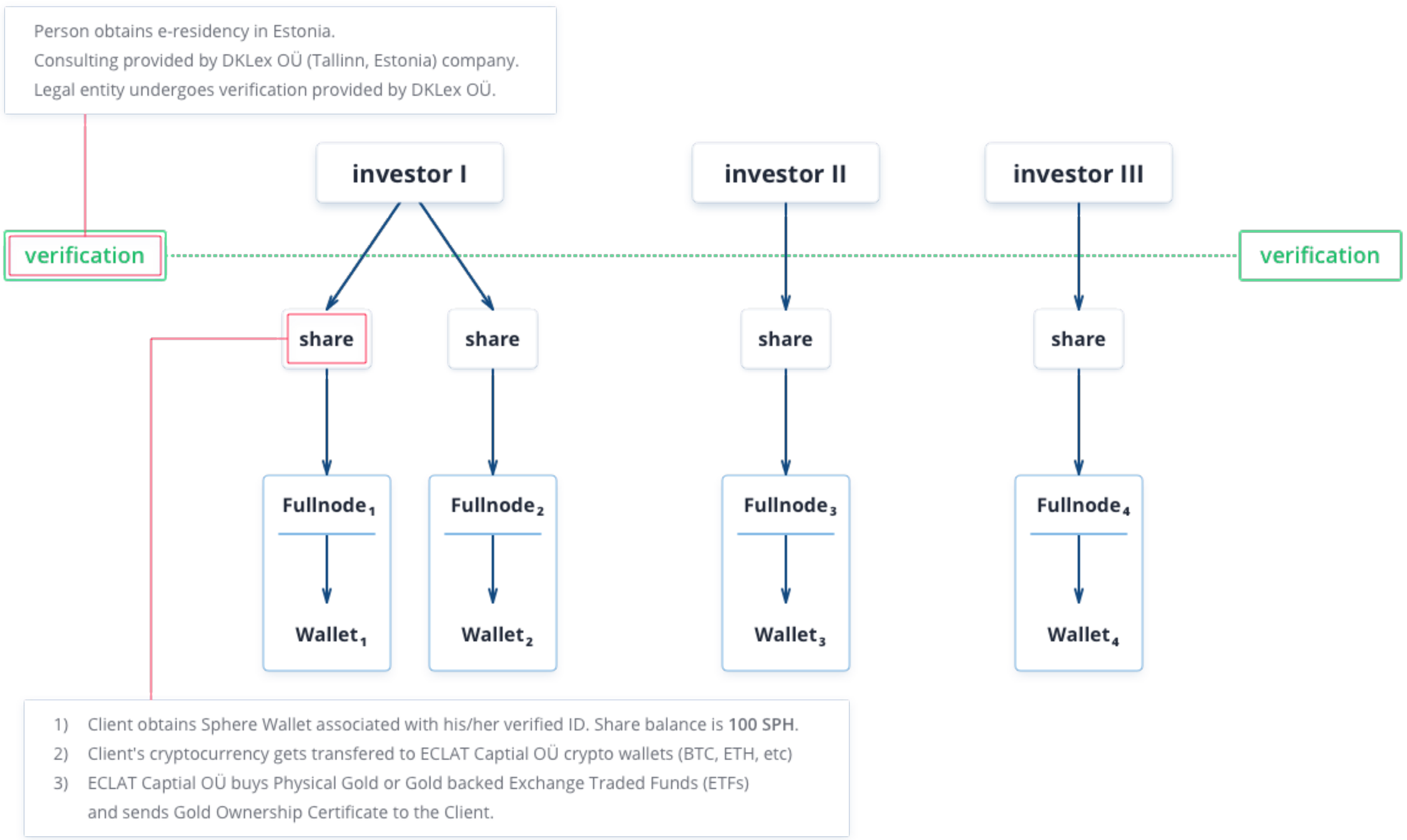
You can check more about SPH in Legal whitepaper.

ICO

During the ICO, **the Investor who bought N shares** will join stakeholders pool and **obtains a cluster of server machines (Full Nodes) in a quantity proportional to the share**. The picture below describes all the step from crypto-investment to gold ownership certificate issue and spawning a Full Node.

Full Node can be provided as a service in a cloud (Google Cloud, AWS) by Sphere core team, or launched manually by Investor's own IT team in a private cloud.

Investor should undergo identification procedure according to EU law. It includes AML (anti money laundering) and KYC (know your client) procedures.



ICO

There are two investments seeding rounds: pre-ICO and ICO.

Eclat Capital OÜ adds additional Full Nodes in equivalence of 20% of general Full Nodes resources after the ICO. That nodes will be evenly distributed across 5 geographical zones (Europe, North America, South America, Asia, Australia) to guarantee full Sphere Platform coverage over the Earth.

More information about the economical program of the ICO can be found in the Legal whitepaper.

HISTORY

Since blockchain technology has been introduced, it had 2 major issues: scalability and trust (consensus). Persisting massive real-time data for million clients in distributed network implies massive async messaging over the wire and eventual data log consistency, which causes scalability problems in classic blockchain approach.

In classical Proof of Work (PoW) model, there's an existential scalability restriction, a mining. As block creation requires more computational resources, its issuing speed is confined with worldwide mining powers and network throughput.

In addition, PoW miners competition is absolutely inefficient, it causes ecological problems and appears to be pseudo-random mining race winner takes all merits for block, but in fact, larger mining pools will always apprehend. Sometimes even a block size is not optimal, but dictated by historical or economical reasons.

Proof of State consensus model, from the other hand, switches from «hashing race» mining to «wallet mining» - nodes, that carry wallets with largest amounts, are «heavier» and thus are more trusted. It leads rewards centralization and network problems due to unbalanced traffic towards «heavier» nodes.

SPHERE NETWORK

Sphere effectively resolves following modern blockchain networks issues:

- **Efficient trust sharing** over the network. Sphere utilizes async Proof of Authority (aPoA) consensus algorithm to ensure transactions validations e.g. proof-by-challenging by selecting identified Full Nodes from random Client Nodes.
- **Proven scalability** up to 30k transactions per second. Sphere relies on top industrial technologies for highly concurrent asynchronous communications (Scala, Akka, Akka Cluster) and deployed in the cloud. This comes with following benefits like: auto-scaling and load balancing, self-healing, concurrent networking with no idle time, adaptive block size, deterministic concurrent transactions evaluation and verification.
- **Fair participation rewards.** Each Investor receives his/her fee for transactions verification and execution.
- **Safety.** All Full Nodes are legally identified entities or persons, verified by Estonian police and government and authorized by Sphere's legal partners. All operations, including consensuses gathering and challenging are happening under regular clients surveillance.
- **Legality.** Sphere network requirements are synced up to date with current EU laws. You can check more in Legal Whitepaper.

HOW SPHERE NETWORK WORKS

Smart-contracts. Smart-contracts in Sphere are merely extended functionality transactions with certain conditions. They are stateless micro-applications written in Scala with some restrictions to perform impure IO. Functional statelessness and IO purity matters - it serves of efficient parallelization and intelligent resources utilization.

There are two fundamental entities in **Sphere Network**: Full Nodes (challengers) and Clients Nodes (clients).

All Node to Node connections are under TLS/SSL encryption.

Clients Nodes could be installed anywhere - PC, mobile phone, bare metal server, cloud, etc. It requires only a Sphere wallet to become a Client Node.

Full Nodes are an auto-scaled clusters of dedicated servers. To obtain a Full Node, one must participate on ICO.

Joint network of Full Nodes conforms an internal network mesh. Sphere network relies on actor-based concurrency model (Akka) and carries Sphere Core, a software written in Scala that operates Akka actors. Communication between nodes relies on Akka Cluster.

Basic kinds of services (actors) in Sphere Core:

- state service (controls memory pool, keeps memory pools equally loaded, listens to transactions emitted by Clients, see Stage 0 and Stage 1)
- quorum service (gathers quorum across Sphere network, see Stage 1)
- calculation service (verifies and calculates transactions, see Stage 2)
- NTP service (time synchronisation across the network)
- AI service (a connector to Big Data service for Neural Network or statistical ML)

Typically, Full Node operates all the services mentioned above.

Full Node may play different roles as a Full Node or Archive Node (carries transactions history and assigns blocks to blockchain) depending on network needs.

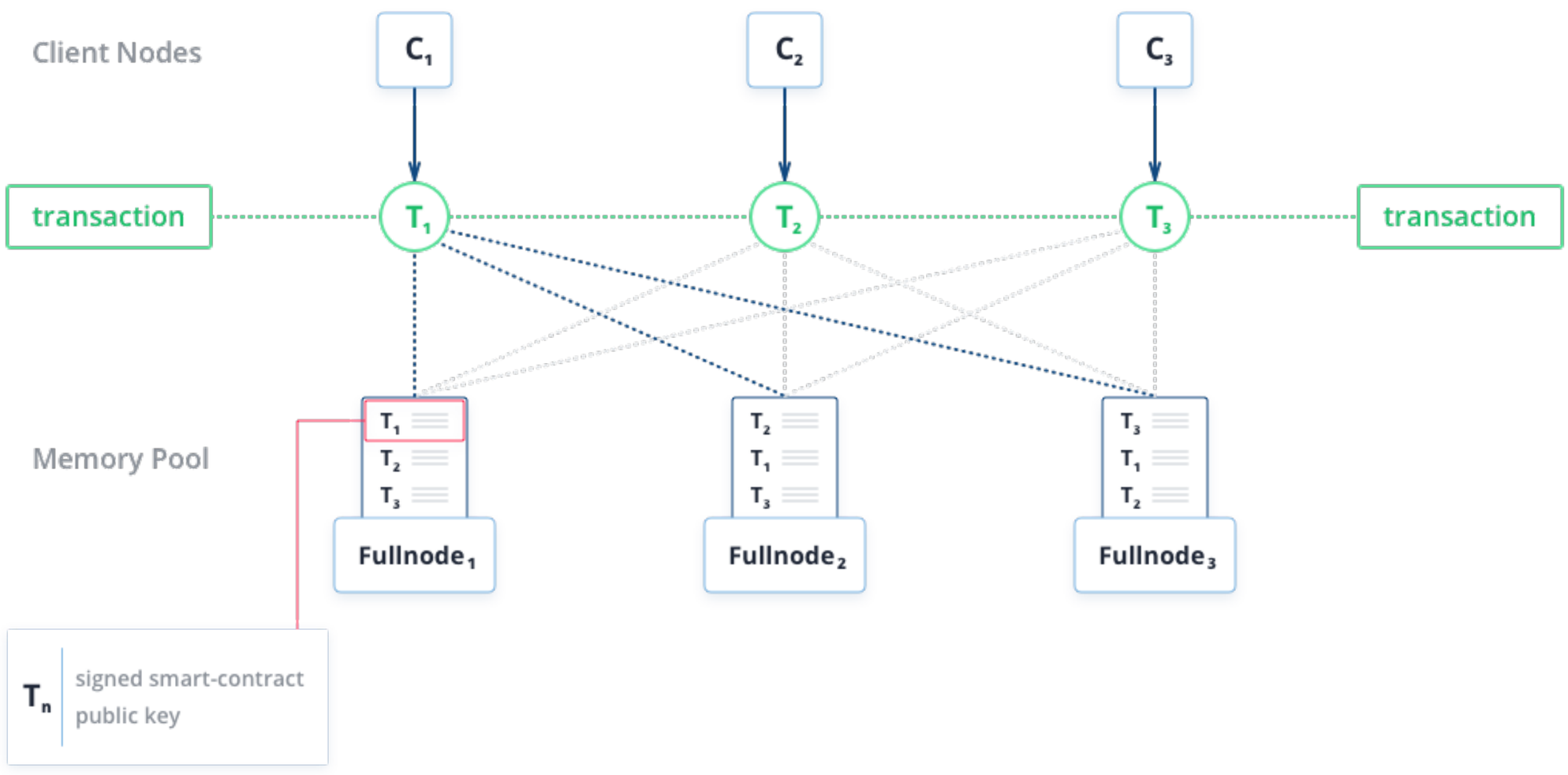
Each Full Node joins designated **geo-cluster**. Geo-cluster means reducing network overhead. A transaction between geo-zones is always bound to the recipient locality. For example transaction from the US to the UK, are served by Europe geo-cluster.

In the next chapters we will see full smart-contract lifecycle in Sphere: from issuing to recording into the blockchain and additional services use cases.

Stage 0

The very core of it is trust sharing is gained by **async Proof of Authority** (aPoA) consensus.

Process. On Stage 0 Clients' transactions fill the memory pools of Full Nodes concurrently (see the picture below). Memory pools (sets of transactions stored in in-memory DB) are versioned with timestamp. Each transaction payload is a public key, signed smart-contract and smart-contract code to be executed.



Transactions topology

Sidenote. The important feature is transactions throttling - one client can issue only 6 transactions a minute e.g. one per second. This prevents malicious network spamming.

Stage 1

The first step is **Transactions count window moment.**

In Sphere, transactions count window - an event triggering Delegates Selection process - is equivalent of «block size» in blockchain. Its size is auto-adjustable by AI service. Full node has built in AI actor, which can be integrated with a broad range of (Big) Data platform.

Stage 1: Transactions count window moment

AI and data platform integrations. Transactions count window optimization is just a reference implementation of AI actor, but one can integrate AI actor with own data platform to write analytics for private Sphere Network quickly and easily, so one can rapidly scale virtually any big data application including data warehousing, fraud and malicious operations detection, event-driven ETL, batching and real-time predictions based on statistical analytics or/and neural network tool, depending mainly on network size and its requirements.

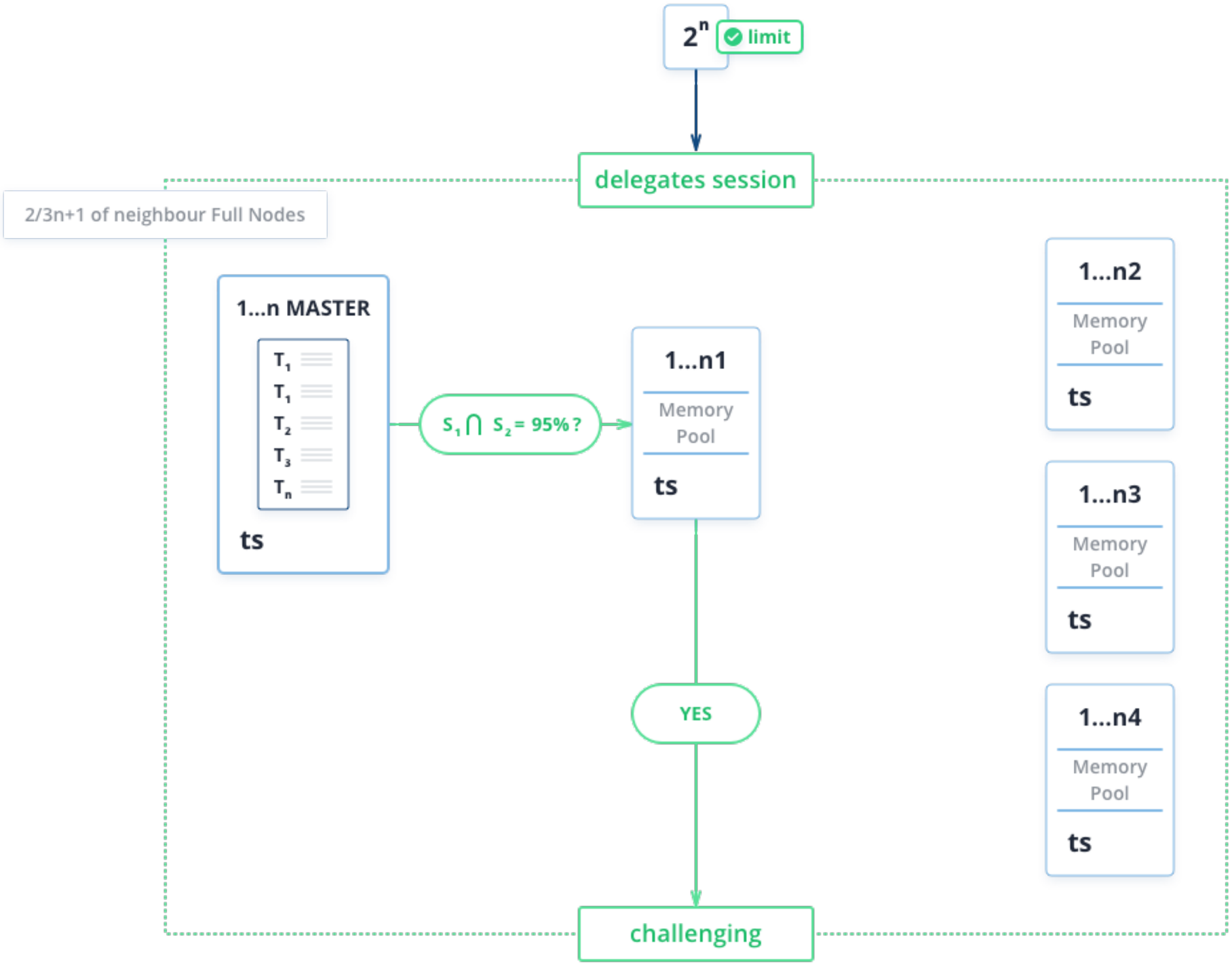
Stage 1.1

Next step is **Delegates Selection**.

Process. Once some Full Node meets transactions count limit window, it becomes Master Node for this round. It starts gathering at least 2/3 N+1 (e.g. Byzantine quorum) of Full Nodes (Stage 1.2) assigned to the same geo-cluster. If less than 2/3 N+1 Full nodes responded, it might mean that cluster is damaged or compromised. In this case, the closet neighbour geo-clusters takes all suspended geo-cluster's transactions.

Problem. In an ideal case mempools are equal per each Full node, but in real world high-load network has some degree of entropy, e.g. different transactions will appear in different nodes more and more often over the time.

Solution. Full node stores smart-contracts in mempools as a Set to prevent duplicates and to facilitate intersection and difference calculations.
Intersection Function (IF) tests whether certain Full Node will join Master or not. If mempools intersection is 95% or higher (an optimal number IF threshold is adjusted by AI service), Full Node (whit mempool set S2) will join Master's quorum and will become a Challenger for Master's mempool set (S1). Full Node's mempool and Master's difference set will be merged with next Full Node's mempool. Otherwise, Full Node will flush mempool Sets intersection from own mempool, keeping S1 - S2 difference.



Stage 1.1: Delegates Selection

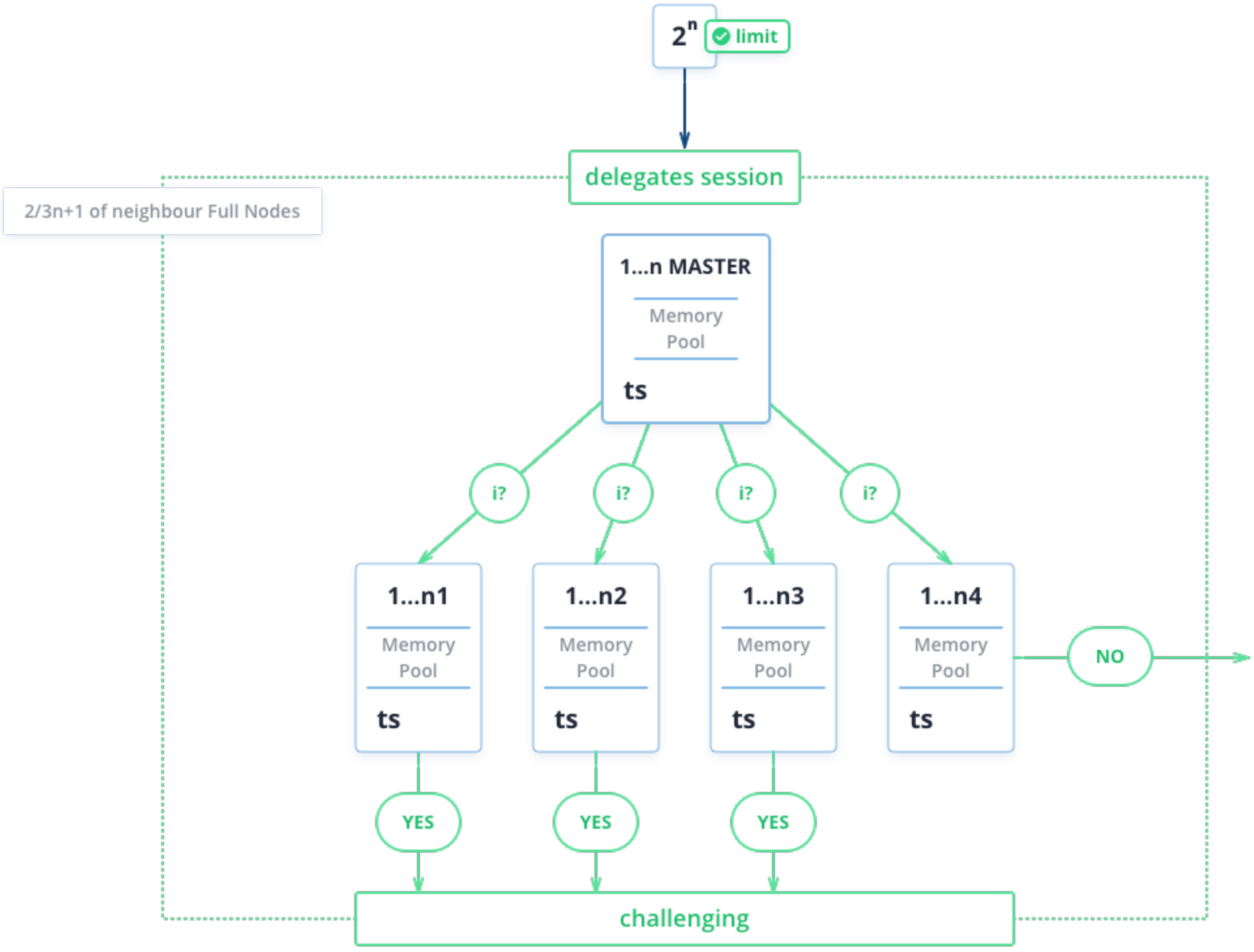
Stage 1.2

Problem. All Node-to-Node operations are async and concurrent, which means, new transaction may come to the Node before previous mempool calculations are finished (see Stage 2).

Solution. Thus, Full Node selected as a Challenger has multiple mempools - current one sealed mempool (the one against which Challenging will be performed) and future mempools (could be one or multiple), which are never locked and are keeping listening to Clients' transactions. Future mempools are balanced: at first within the geo-cluster and then across all geo-clusters. Mempools rebalancing is provided by state service.

Problem. What if there are two Master simultaneously?

Solution. To resolve this each Full node has NTP actor that provides time synchronization and a timestamp (TS) versioning for mempool. The Master Node carrying earlier TS for sealed mempool remains as a Master, while the second node has an options depending on IF function result: if it returns true, the second node will join Master and so its Challenging Node will do (e.g. quorums will be merged), otherwise it will flush own mempool, keeping s1 / s2 difference and so its Challenging Nodes will do (e.g. quorum will be dismissed)



Stage 1.2: Quorum Synchronization

Stage 2

Next step is **Challenging** - transactions verification, calculation and singing.

Verification. Each Node does signatures verifications. Then it verifies each transaction code in parallel. If the code is valid and conforms:

- statelessness and IO purity,
- content length,
- SphereContract class inheritance
- allowed methods restrictions

and there are no double-spending, overspending and other fraud operations, the smart-contract will be compiled. Also, on this step Rewards (Investors fees) block is calculated. Rewards block is just a code added into each smart-contract, which describes service fees distribution across Full Nodes.

Calculation. Compilation is executed in parallel. Once every contract is compiled, quorum Nodes start sequential contracts execution with simultaneous building of three SHA3 Merkle trees:

- transaction tree (history of payments)
- state tree (wallets state after transactions are done)
- event tree (populated once smart-contract met some requirements)

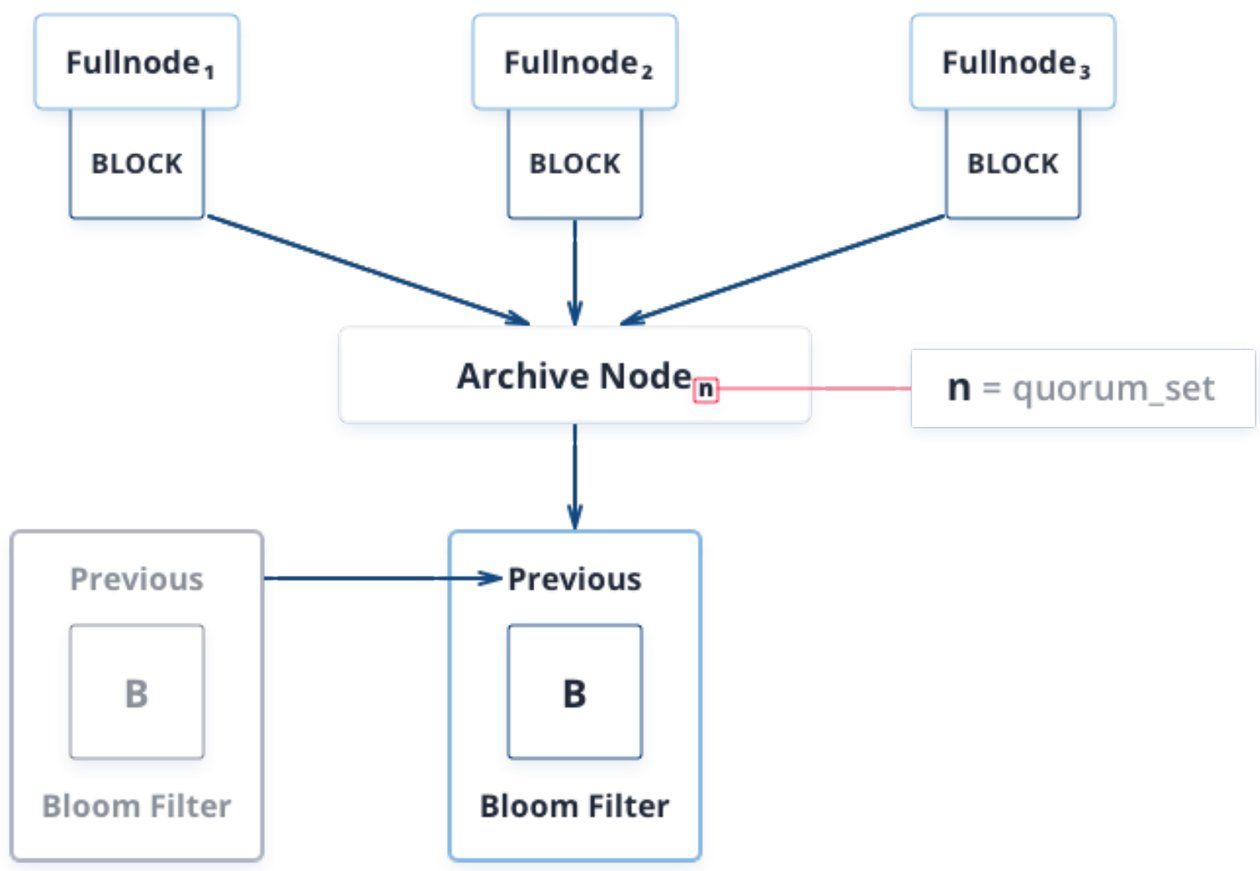
Singing. Finally, each quorum Node signs full transactions block and emits it into the network back.

Stage 3

The last step is **Chaining** - adding transactions block into blockchain.

Archive Node listens to blocks emission and then:

- verifies block headers and block stream drain (e.g. all Challengers successfully emitted same block),
- checks rewards transactions to be valid and fair,
- and finally adds the block padded by committed Bloom filter for Clients (for faster access to wallet balance) to the blockchain.



Stage 3: Block emission and chaining

Block validation period is 16 blocks, once Archive node digested the block and ensured its presence across internal network, the block itself becomes fully trustworthy and thus visible to clients when there are 16 blocks ahead of it.

REWARDS

Full Nodes holders will receive rewards for Challenging. Commissions held from all transactions are explicitly listed in blocks as separated smart-contracts and are accumulated on each Investor’s wallet, associated with a Full Node.

For Sphere Platform there’s reference set of Investor’s wallets, so even if it appears to be a fraud Full Node among valid ones, it will never get any reward and will be immediately spotted.
If Investor decides to quit Sphere Platform and redeem its share as a gold or ETF, his/her wallet will be suspended and removed from reference set of Investor’s wallets.

Also, network executes a special smart contract, that and covers network infrastructure expenses, like cloud services, data analytics services, etc.

ico@sphere.ee