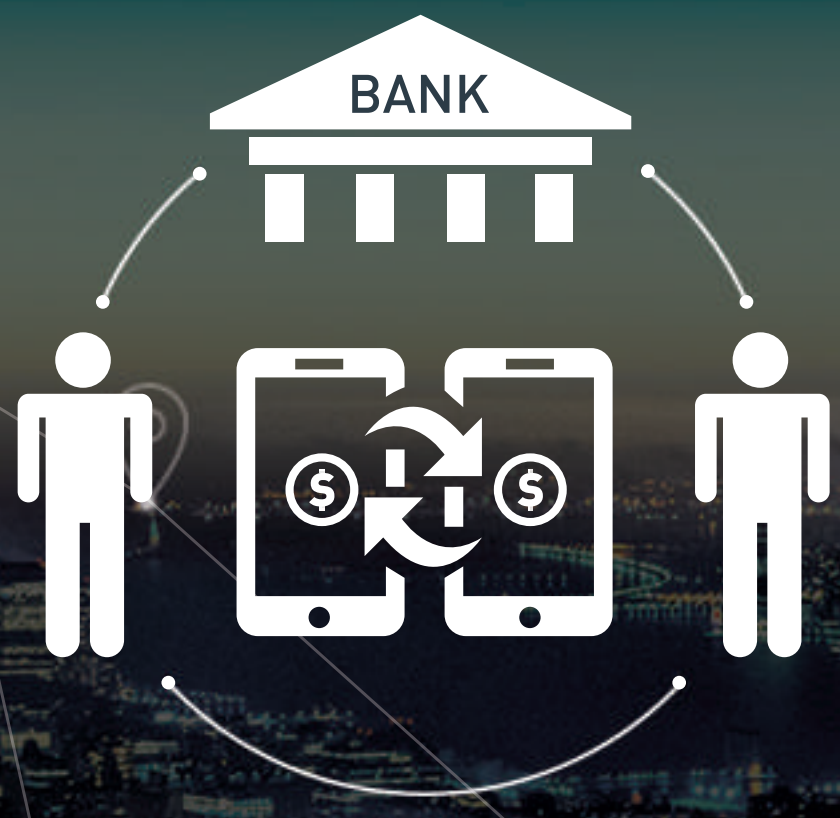
GRUUT
A FULLY DECENTRALIZED P2P PUBLIC LEDGER

Gruut Networks

GRUUT NETWORKS
fairly decentralized, people oriented

01 GRUUT VISION



An online recording of transactions by peers (not a third party) that is impossible to forge is necessary if it is not technically, economically, or politically possible to set up a trusted third party that secures transactions. Also, even though there is already a trusted third party, it is preferable to use a P2P ledger wherever possible if the cost of maintaining the third party is too high; not because it is technically or economically unavoidable, but because the third party makes undue profits. Our vision is not just to introduce yet another cryptocurrency, but to also dismantle business models that rely on trusted third parties. It can be summarized as follows:

PEER-TO-PEER

To replace ledgers managed by third parties with peer-to-peer public ledgers that provide high levels of trust, and to distribute fees to peers evenly that cannot be centralized.

DECENTRALIZED APPLICATIONS

To provide various decentralized applications (DApp) with a versatile / flexible / scalable platform for on/offline payments as well as remittances.

FRIENDLY ECOSYSTEM

To build up a government-friendly ecosystem that is compatible with legacy / legal financial systems.

02 ISSUES WITH CURRENT BLOCKCHAIN TECHNOLOGY

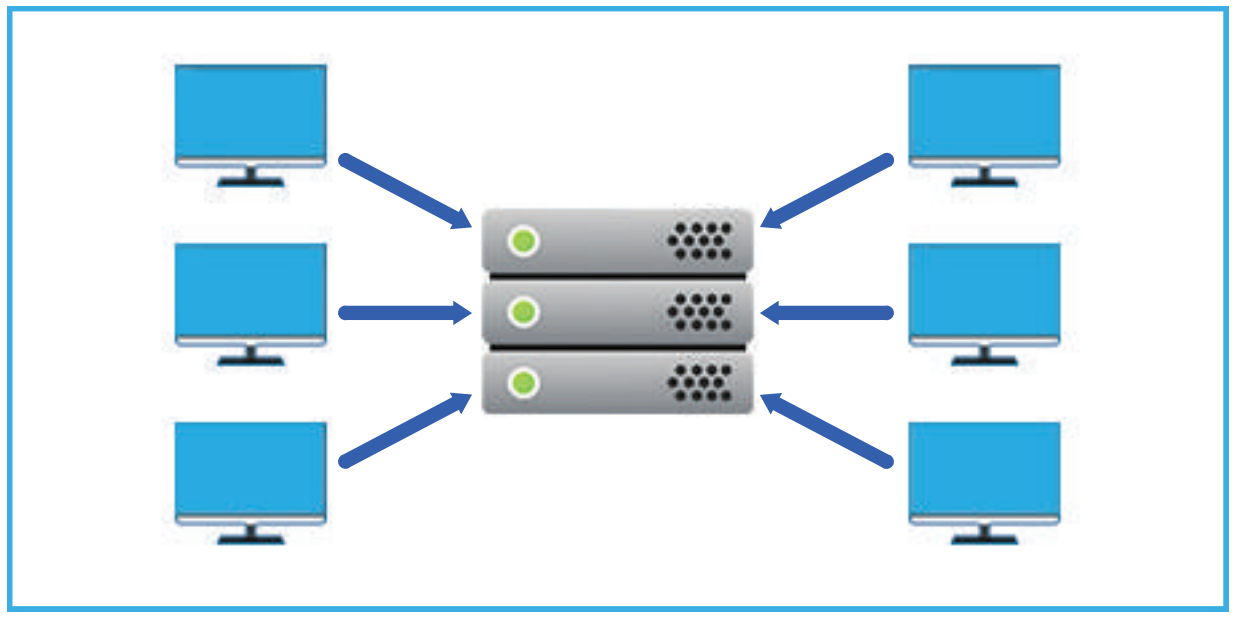
Current blockchain technologies have two critical issues: anonymity and decentralization.

No decentralization

Hashing powers or stakes have been dominated by small groups of people.

No economic transparency

All transactions are processed under random addresses whose owners are not identifiable, which can allow money laundering and tax evasion.



Also, most of them cannot be used for buying a pizza due to the following

Closed ecosystem

Cryptocurrency is for rewards and transactions are made only with the cryptocurrency.

Mining cost

Current blockchain ledgers are ill-suited for processing small-value transactions because of their high mining costs.

There are also several technical limitations in current PoW-based cryptocurrency systems

Energy

According to Bitcoin energy consumption index by Digiconomist, the number of U.S. households that could be powered by Bitcoin is 4,049,860.

4,049,860
powered by Bitcoin

Slow confirmation

Theoretically, it takes at least 60 mins for a block to be finalized.

60min
Block Complete

Scalability

TPS is only between 4 and 20, which is not scalable enough for a global transaction network.

4-20
TPS

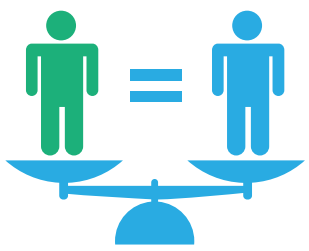
03 GRUUT'S APPROACH AND BENEFITS

How to construct a fully-decentralized and low mining-cost public ledger?

When a node behaves like Sybil in PoW/PoS networks, it has a lower probability to receive rewards because its hashing power is divided into multiple forks (for multiple votes) and the chance to add its block decreases. Therefore, PoW (similarly PoS) can be seen as a mechanism to enforce an entity to behave as a single node instead of many Sybils. Our mechanism for this is to identify nodes before they join the network. Gruut uses a PoP (proof-of-population)-based voting, where generating proof to make a block is to gather some number of signatures generated by multiple identified nodes. The benefits are:

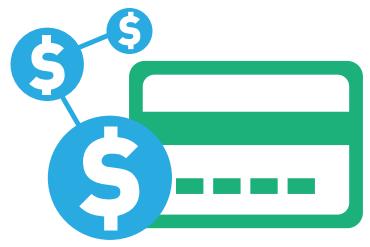
True decentralization

One entity has only one voting power irrespective of its hash power / stake, and the benefits are evenly distributed to peers.



Micropayment

Thanks to low mining costs, small value transactions can be processed efficiently in the network.



Go green

Even a smartphone can run our GruutApp as a node.

How to deploy Gruut in mainstream business areas that require economic transparency?

Our suggestion for economic transparency is customer identification. Considering that financial transactions must be conduct with identification in almost every country in the world, we do not need to stick to anonymous transactions. The benefits are quite obvious: Economic transparency and a countermeasure for tax evasion and money laundering.

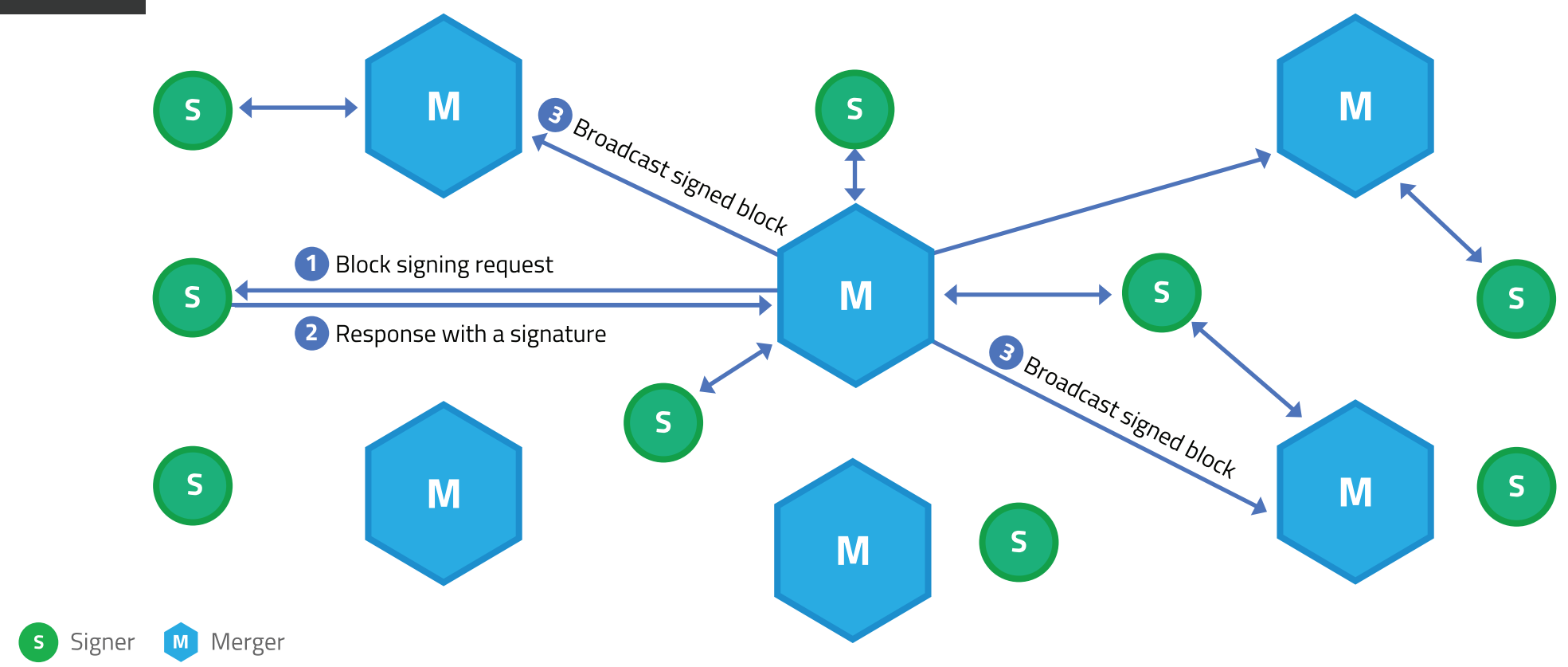
How to deal with price volatility for running real financial platforms?

To cope with this, our suggestion is to use a fiat currency as the main currency in our ledger. This design choice offers many benefits: Money control by government, immunity to price volatility, and a fiat-based economy.

What about scalability to accommodate all P2P transactions?

The answer to the scalability issue is to use multiple local blockchains in parallel and to adopt inter-chain protocol. Another interesting idea on this is to introduce interchain transaction protocols that process transactions occurring from one chain and going to another.

Figure 1

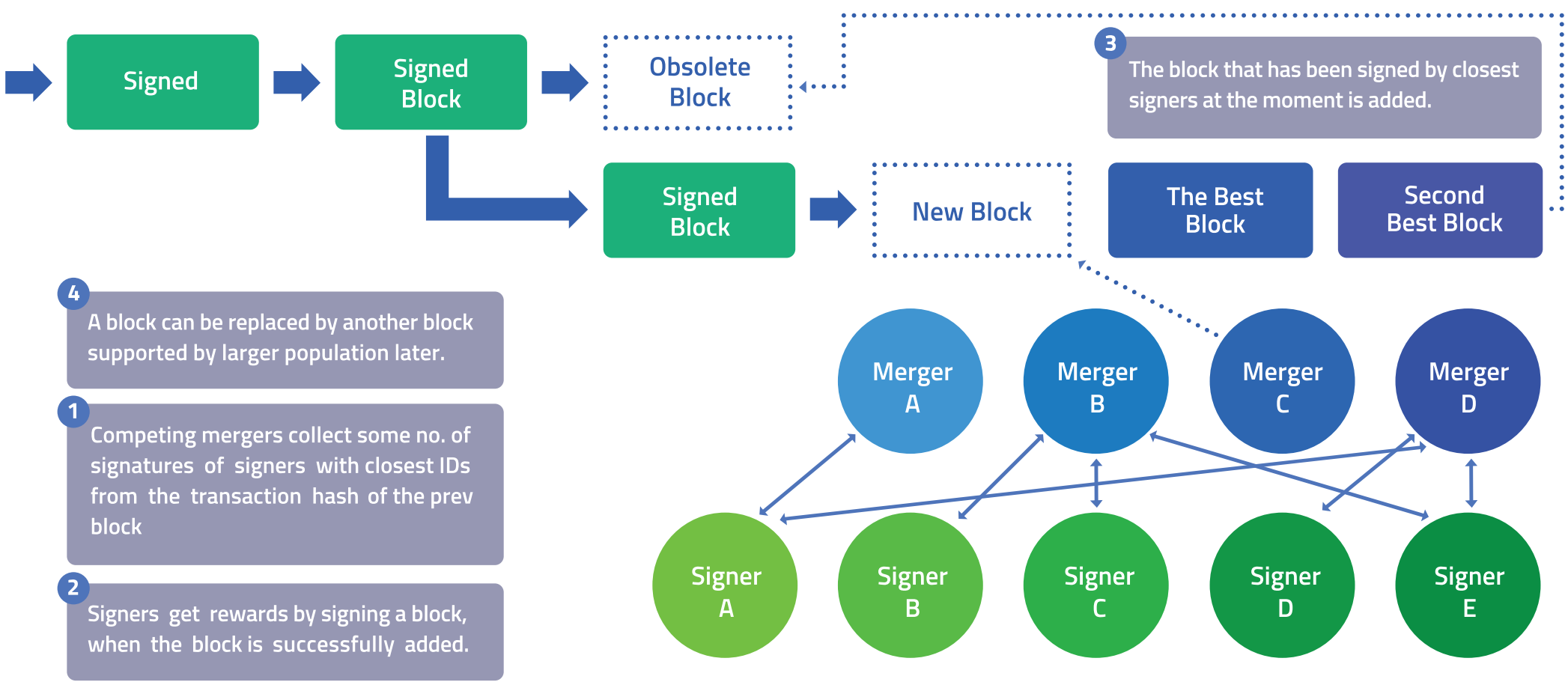


1 A merger requests signatures of a block to signers.

2 A signer responds with a signature.

3 Adding a block to the chain is the game that the first merger who gathers some pre-determined number of signatures for the block wins.

Figure 2



A block is signed by signers who have the closest IDs from the hash of transactions in the last block upon the request of the merger.

How is Gruut's smart contract different?

Our strategy is to run a blockchain per DApp type. Heavy smart contracts slow down network throughput and, even worse, they even affect non-contract transactions. We are going to divide into two types of smart contracts and run them on separate chains.

04 GRUUT ARCHITECTURE

To realize the new blockchain

To realize the new blockchain, PoP using digital signatures is used instead of PoW or PoS, which is a realization of explicit voting by individuals. There are two types of nodes in Gruut

A signer is prompted to allow a PoP wallet to generate a signature when it receives a signing request for a transaction block.

A merger collects and validates a certain number of transactions to compose a transaction block. Also, each transaction block must collect a number of valid signatures for the block from signers and insert them into the blockchain.

Processing transactions in Gruut

1. A transaction is broadcast to the merger's network, and mergers wait until some amounts of transactions are collected.
2. A merger who has not produced any blocks for some time collects transactions into a block, computes signer ID's, finds the closest signers among the queue of signers registered on their cache roster, and sends the block to the signers.
3. A signer checks the validity of the block and responds with its signature on the block to the merger.
4. A merger waits until it gathers a number of signatures on the block. If successful, the merger signs the block and broadcasts the multi-signed block to all mergers.
5. Mergers accept a block only if it is valid and not double spent and if the sending merger is eligible.
6. Mergers notify their acceptance of a block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

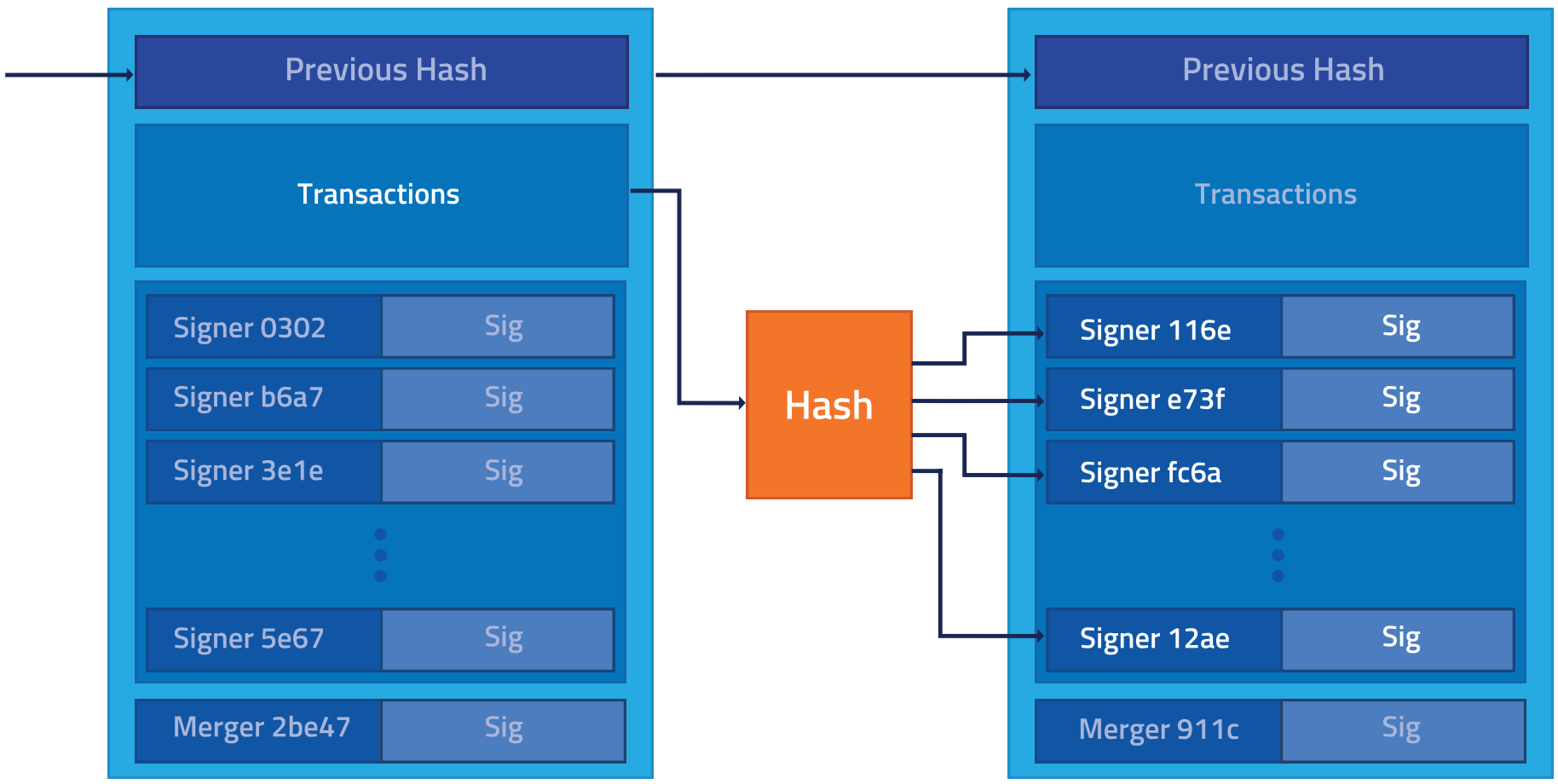
Taking a fork supported by the largest number of voters

In a PoP network, choosing the proper chain is done by voting. When two or more forks are competing with each other to become the main chain, mergers choose the fork that has the larger accumulated number of signatures, which means that there are more people who support this chain.

Size Scalability by local blockchains and inter-operation

To make Gruut scalable, every regional area has its own local blockchain. Obviously, it is possible to remit across borders money from an account in a chain in one country to one in another country.

Figure 3



A block in can a PoP network is signed by signers and then by mergers. The signer group is determined randomly by the hash of transactions of the previous block.

05 BUSINESS DEVELOPMENT IN THE FINANCIAL SECTOR

Two business models

Replacing the centralized trust with a decentralized one will make it possible to spread the profits fairly to network participants through the following business models

P2P bank paying operational fees to peers.
Any bank can run its business on a Gruut ledger. They advertise their financial instruments, recruit customers through various promotions, let customers open accounts on the ledger, and manage accounts.

P2P credit / debit card payment. In general, card payment system fee rates ranges from 1.7% to 3.3% in Korea. Initially, we thought that with the spread of the Gruut payment system, it would be possible to lower the payment fee rate to somewhere around 0.5%.

Two strategies to deal with fiat money

The cryptocurrency economy is not linked to the real economy (they are linked only at an exchange), so the matter regarding the cryptocurrency system boils down to the belief among participants within the ecosystem. However, the Gruut ledger connects and binds to a fiat currency in the real economy. We must therefore spread and disseminate the belief that a transaction made on a Gruut ledger is safely bound to a transfer of the corresponding value in the real economy. To resolve the issue, we propose two strategies: one is to establish an operating company to provide customers with payment guarantees , and the other is to make transaction recorded on Gruut ledgers be regarded as legal contracts between the sender and recipient.

Local mining and Gruut business deployment

Unlike current blockchain projects, Gruut makes use of node identification and local chains. This limits a node to work or mine on a local Gruut ledger in its country of residence. This limitation is fundamentally different from the case of blockchains out there, where any node can contribute to the global chain irrespective of its residency. Gruut's business strategy, therefore, is not to make one global single ledger all at once, but to launch local Gruut ledgers incrementally over regions.