Smart Ledger Technology (SLT)

Discover what Smart Ledger Technology is and the problems it aims to solve.
See how blockchains and cryptocurrencies fit into the picture.
Get an idea of the opportunities SLT offers, as well as the challenges to be resolved.

Menu

- Cryptocurrencies: The Popularisers of SLT
- What is SLT ?
- What is Blockchain ?
- SLT beyond Cryptocurrencies
- Opportunities and Challenges for Financial Services

Cryptocurrencies: The Popularisers of SLT

Cryptocurrency

A cryptocurrency is a digital currency that relies on cryptography (encryption and hashing) to verify transactions and to control the generation of new currency units.

The value of cryptocurrencies is determined by supply and demand, not by a central third party, such as a central bank.

Bitcoin is the first major and best-known cryptocurrency.

Digital currency

Relies on encryption and hashing

No central third party

Cryptocurrency and SLT

Cryptocurrencies rely on SLT technology to provide an indestructible record of transactions to prevent theft, forgery, and double-spending.

Digital currency

Relies on encryption and hashing

No central third party

Managed through SLT
(Smart Ledger Technology)

What is SLT ?

What is a Ledger?

A ledger is a list of entries, often taking the form of a registry, where transactions between parties are recorded by a third party.

There can be ledgers of:

- Financial instruments, such as currency and credit data.
- Public records, such as birth certificates.
- Semi-private records, such as university degrees.
- Private records, such as contracts.

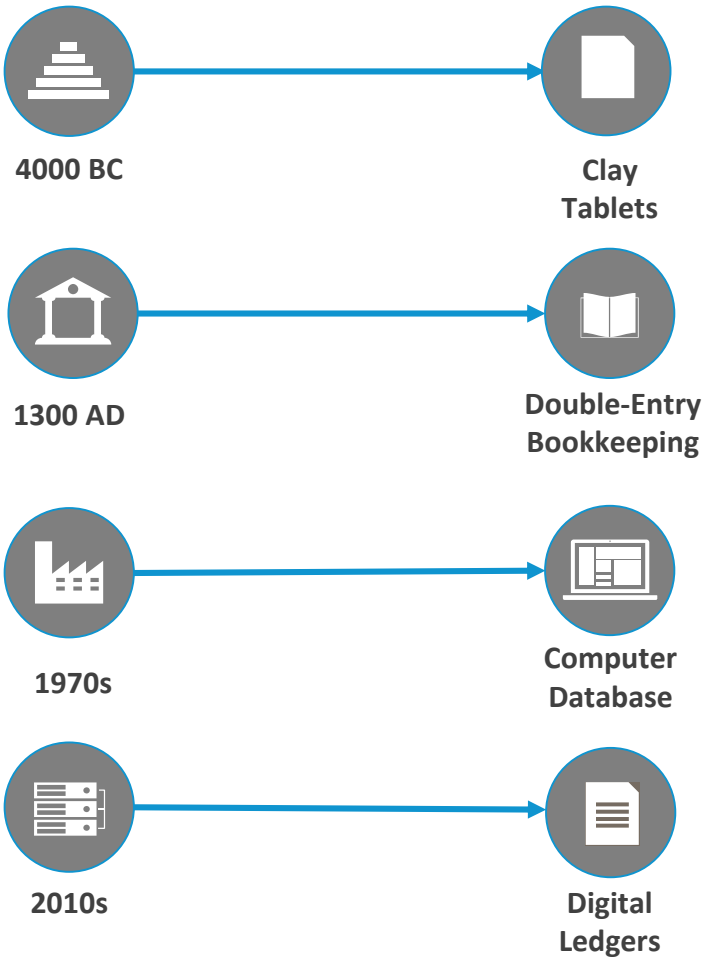
Financial Ledgers

In the financial market, a ledger is a record of financial transactions.

The first documented ledgers were the Sumerians' cuneiform clay tablets dating back to the 4th millennium BC, followed by tally sticks, and papyri.

Double-entry bookkeeping was introduced around 1300, with the first known use of the word 'ledger' recorded in 1588.

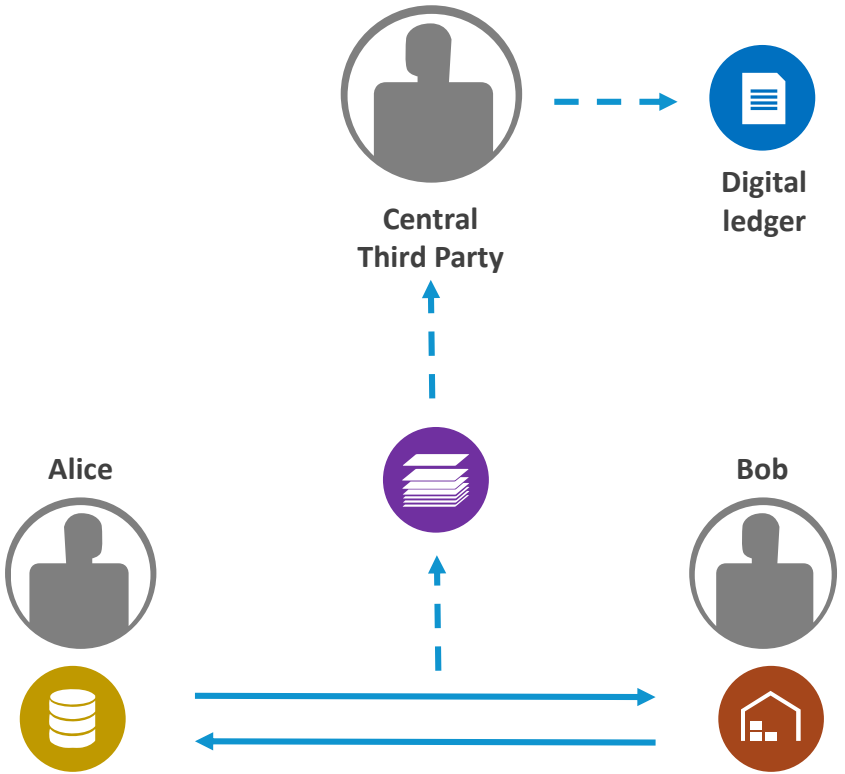
In the 1970s, computer databases became the ledgers of preference.



Traditional ledgers

In traditional ledger systems, third parties are usually relied upon to:

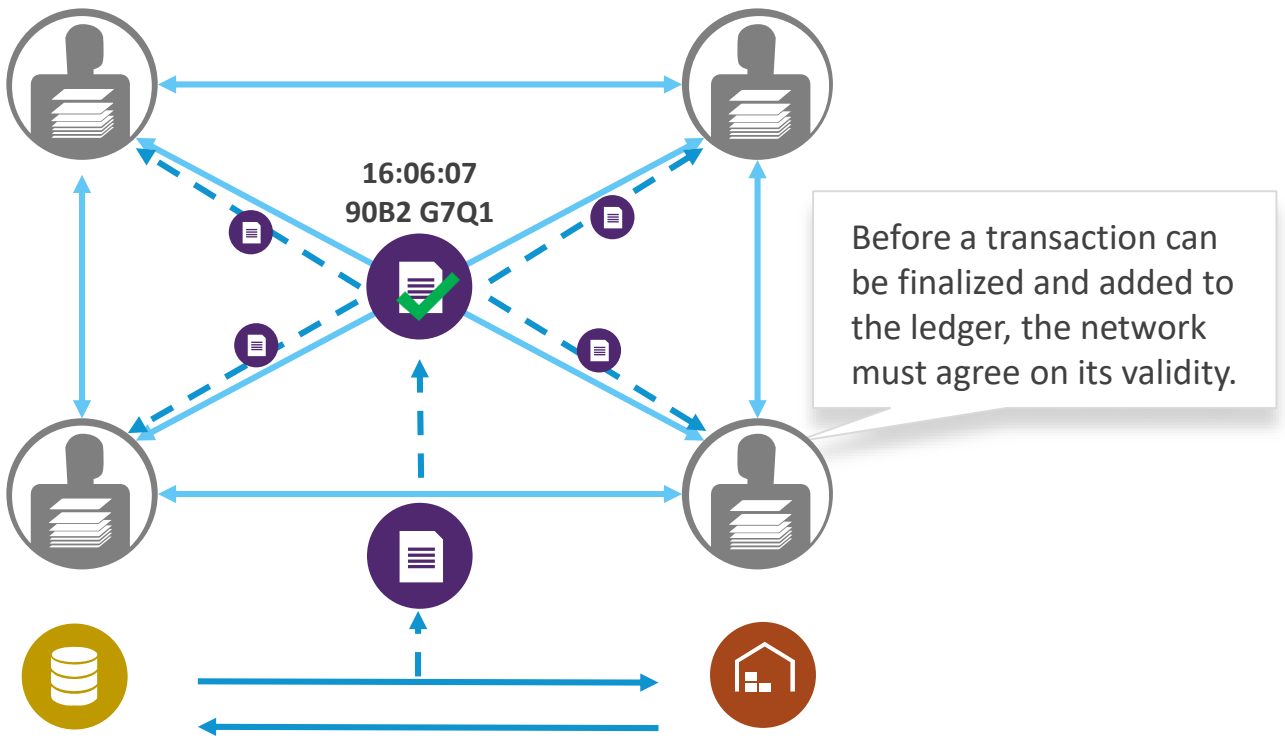
- validate entries
- safeguard transactions
- preserve historic records.



What is SLT? (1)

Smart Ledgers are multi-organisational databases with a super audit trail. Instead of relying on a central third party to witness and record transactions, they rely on a consensus mechanism of validation.

Once a transaction has been validated, it is assigned a cryptographic signature and recorded on the ledger. That record is timestamped. A copy of the amended ledger is distributed to all nodes, making the ledger hard to destroy.

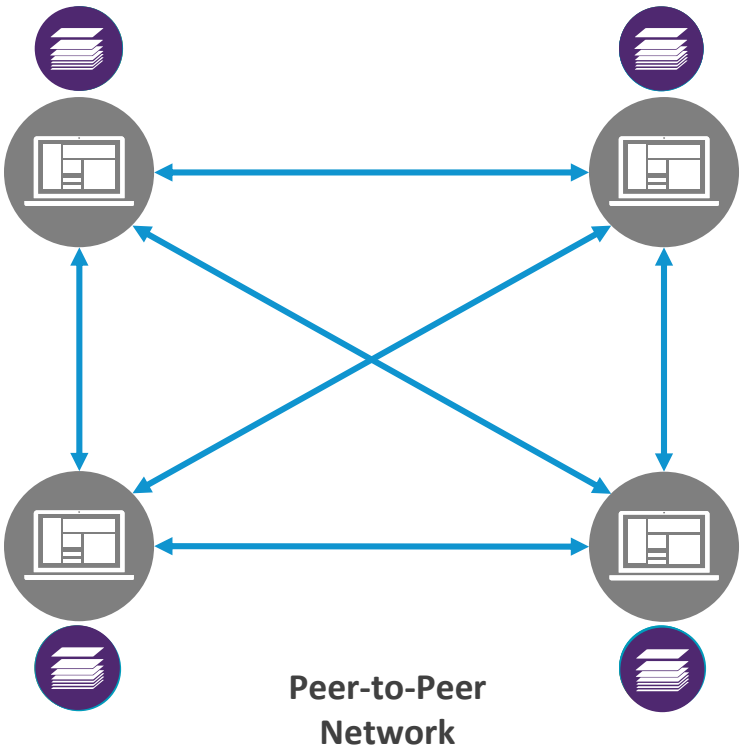


What is SLT? (2)

In a distributed ledger system, each member of the network (node) holds a local, synchronized copy of the ledger.

Distributed ledgers are characterised by resilience and immutability, as tampering or destroying one node doesn't affect the entire system, nor the continuity of the ledger.

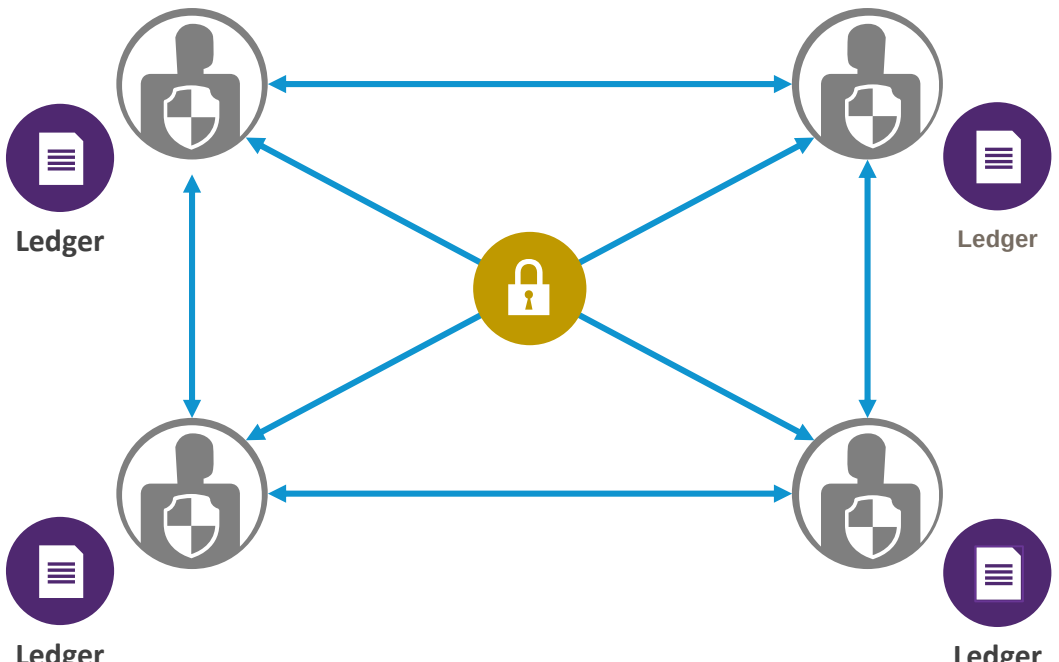
On the downside, distributed networks can be markedly slower, as any updates must be agreed upon by most, if not all, nodes.



What are the Benefits of SLT?

SLT has a number of advantages, including:

- Built in authentication
- Selective and built in data distribution
- Tamper proof history recording built in
- Smart contracts allow business processes and data validation in the shared space
- Built in resilience

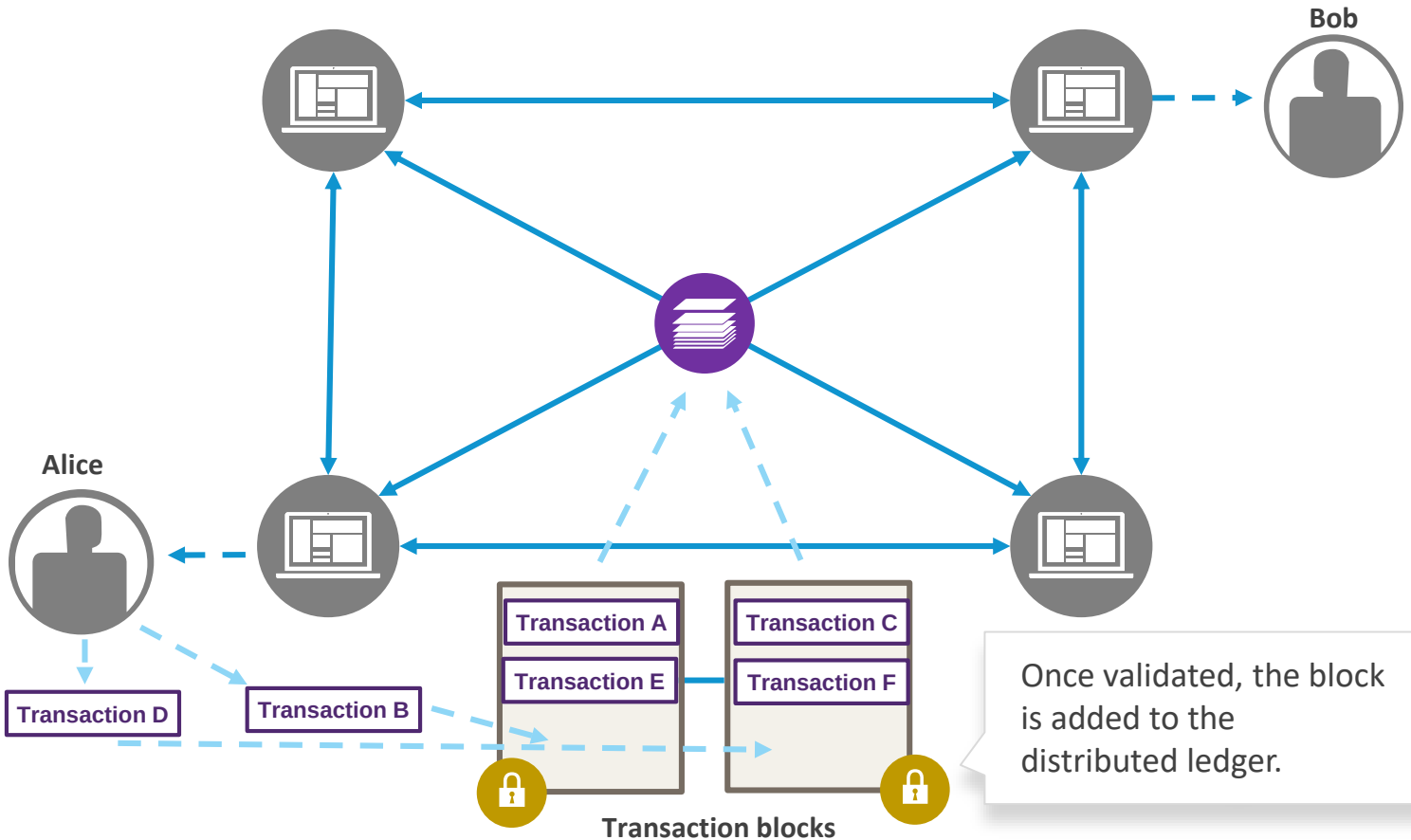


What is Blockchain ?

What is Blockchain ?

Blockchain is one way to implement distributed ledgers, and underpins today's cryptocurrencies.

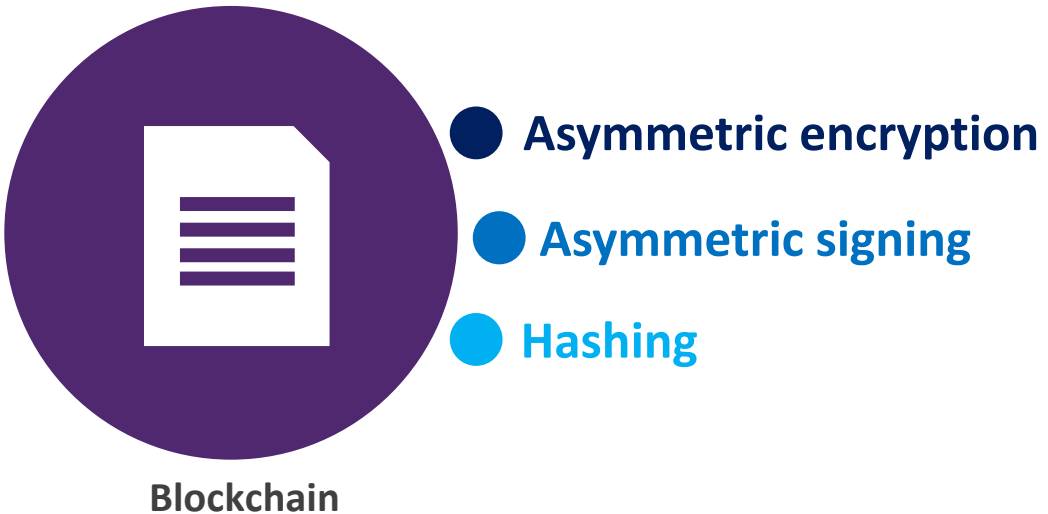
A blockchain consists of concatenated **blocks** of transactions and allows counterparties to share a distributed ledger across a network of computers.



Technologies Related to Blockchain

In blockchain and more generally in digital ledgers, no single party has the power to tamper with the records: the math keeps everyone honest.

Privacy and safe storage of ledger entries can be handled with technologies such as asymmetric encryption, asymmetric authentication, and hashing.

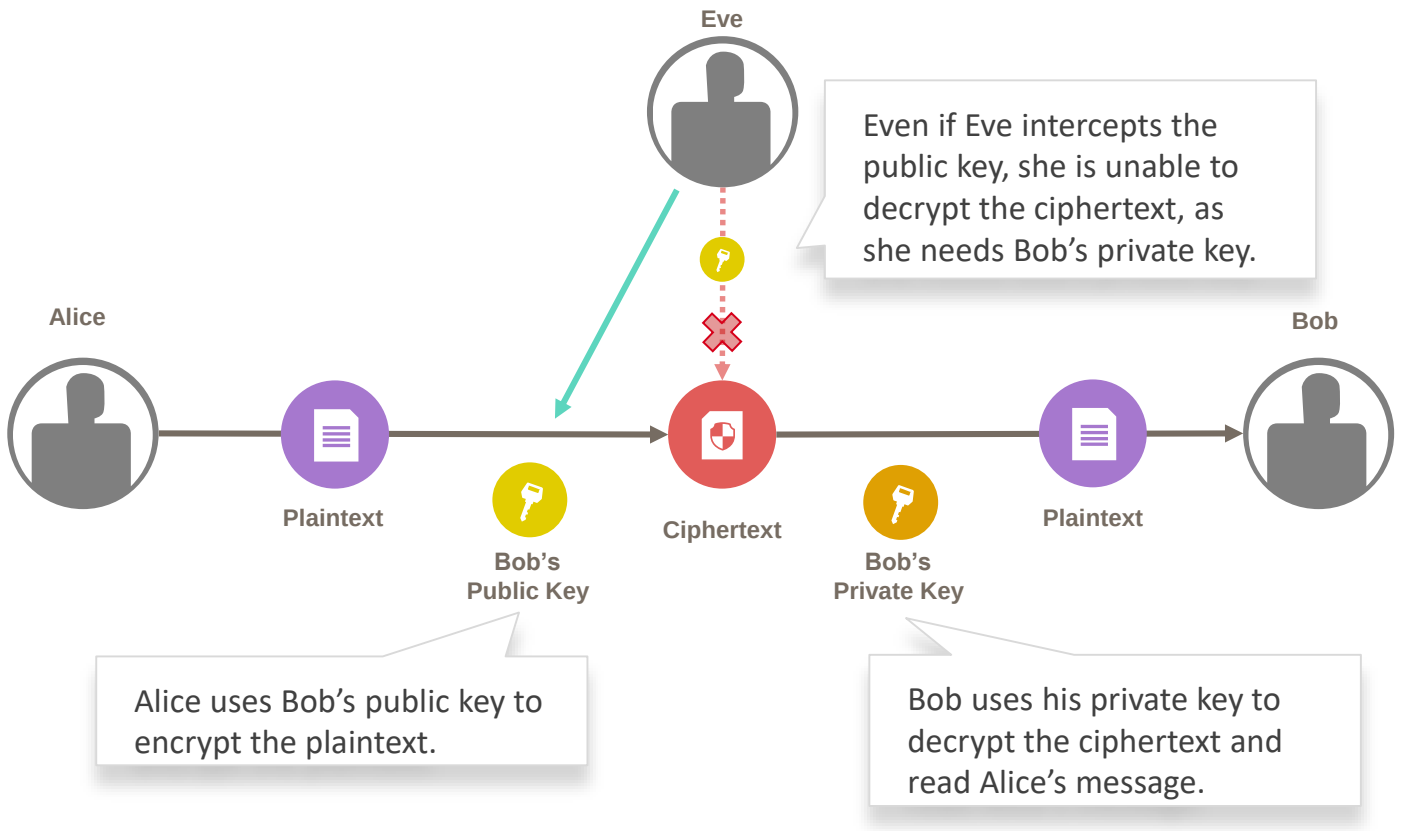


Asymmetric Encryption

Asymmetric, or public key, encryption uses two keys: a private key and a public key.

Important note: the public key is computed based on the private key, so the two keys are linked. However, it is impossible to infer the private key from the public key.

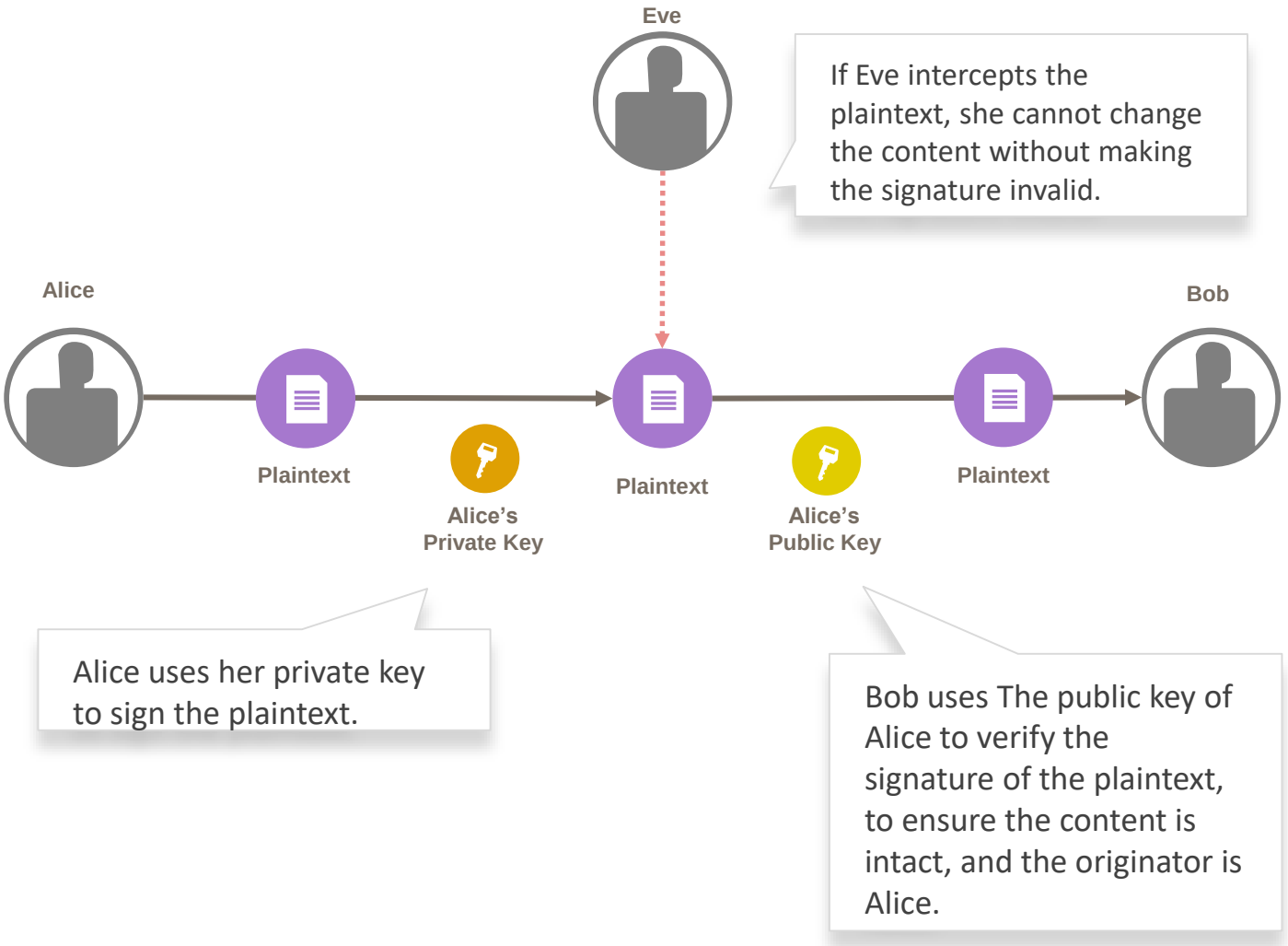
The public key is given to anyone that wants to send you a message, so they can encrypt it. In order to decrypt the message, you then use your private key, which is only known to you.



Asymmetric Signing

Asymmetric signing allows the receiver of a data set to validate that the originator of the data set is genuine, and that the data has not been altered.

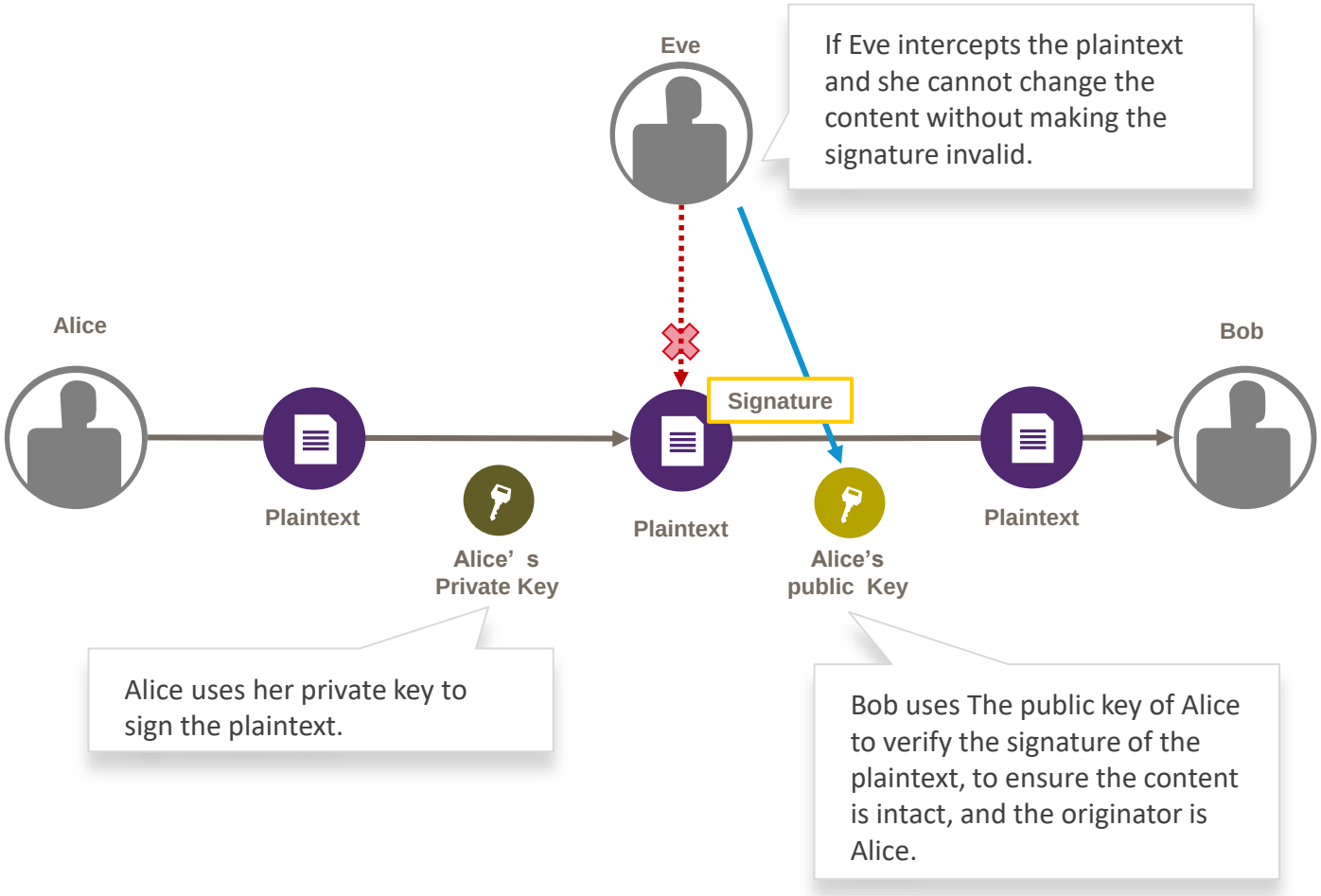
Like hashing, The result of an authentication is a string of characters, the signature, but it's content is not only based on the data set, but also on an authentication key. The smallest change to the data set creates a completely different signature.



Asymmetric Signing

Asymmetric signing allows the receiver of a data set to validate that the originator of the data set is genuine, and that the data has not been altered.

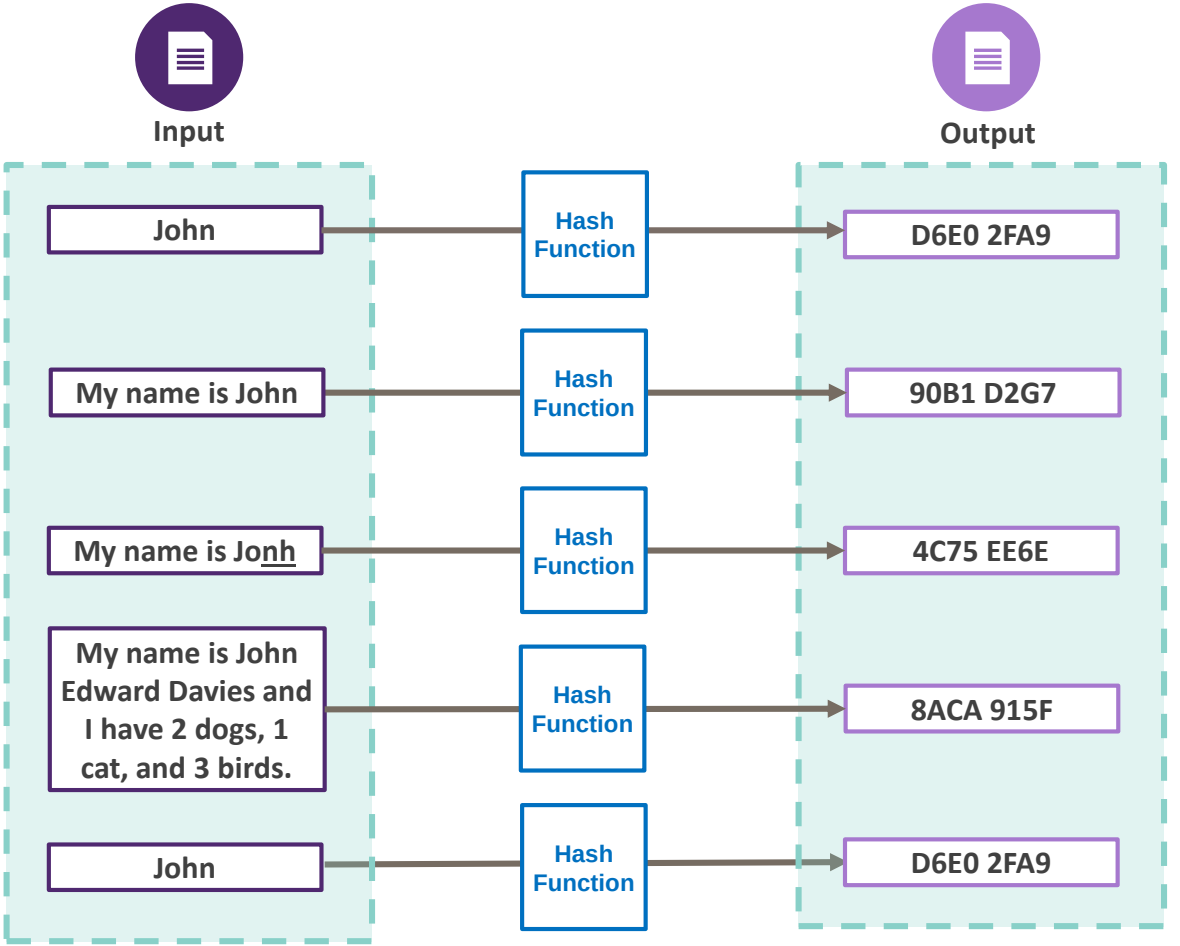
Like hashing, the result of an authentication is a string of characters, the signature, but it's content is not only based on the data set, but also on an authentication key. The smallest change to the data set creates a completely different signature.



Hashing

Hashing means taking a set of data of arbitrary size and using an algorithm to transform it into a string of characters of fixed length. The smallest change in the input will create a completely different hash output.

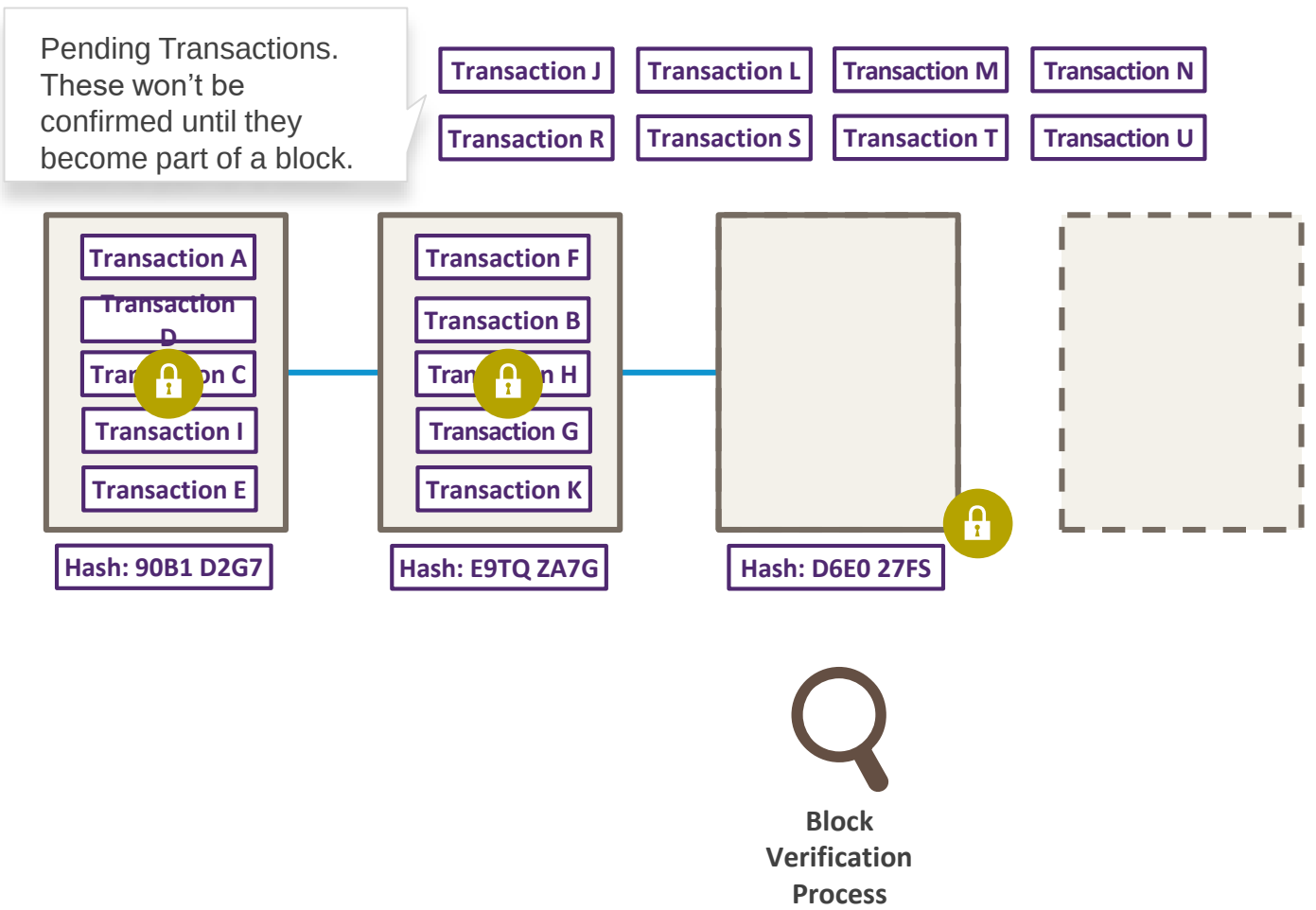
Unlike encryption, hashing is a one-way street: the input of a hash cannot be recovered from the output. However, a specific algorithm applied to a specific set of data will always produce the same hash. This is what makes hashing a powerful tool.



How Blockchain Works

A blockchain is a type of SLT, with a specific way of storing transactions.

Transactions are distributed across all nodes and each node can take a number of pending transactions and add them to a block. Through a verification process , such as mining, the block is verified, ‘locked’, assigned a hash, and then distributed to all nodes. If the block is validated through the consensus mechanism in place, it is added to the blockchain.

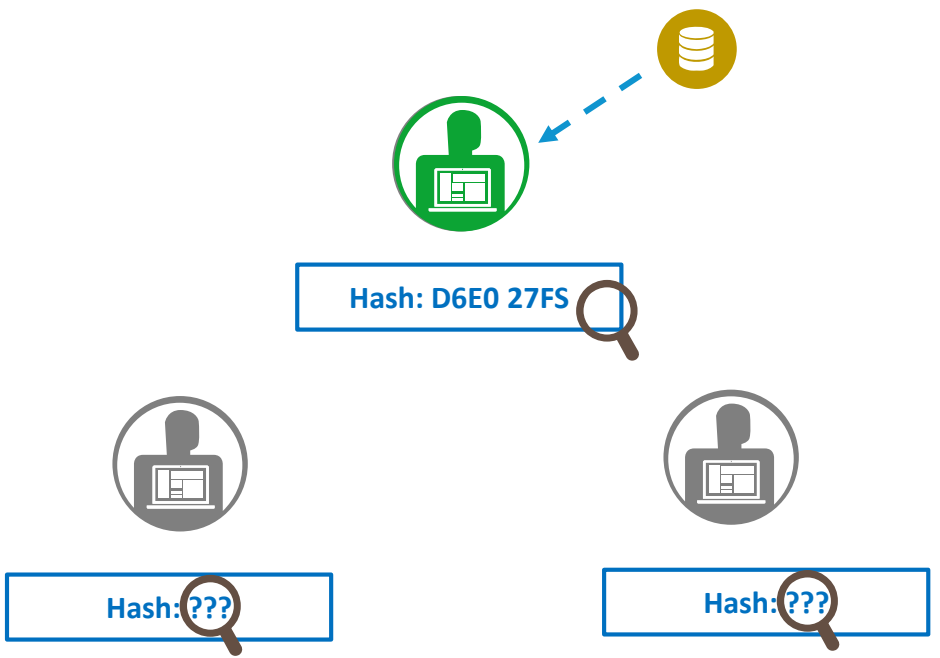


Blockchain Validation

The Bitcoin blockchain depends on a Proof of Work (PoW or mining) process to validate new blocks.

In PoW, several nodes try to algorithmically find an appropriate hash to seal the block. The first to do so wins a cryptocurrency reward.

PoW is both time- and energy-consuming. This limits the scalability of a blockchain.

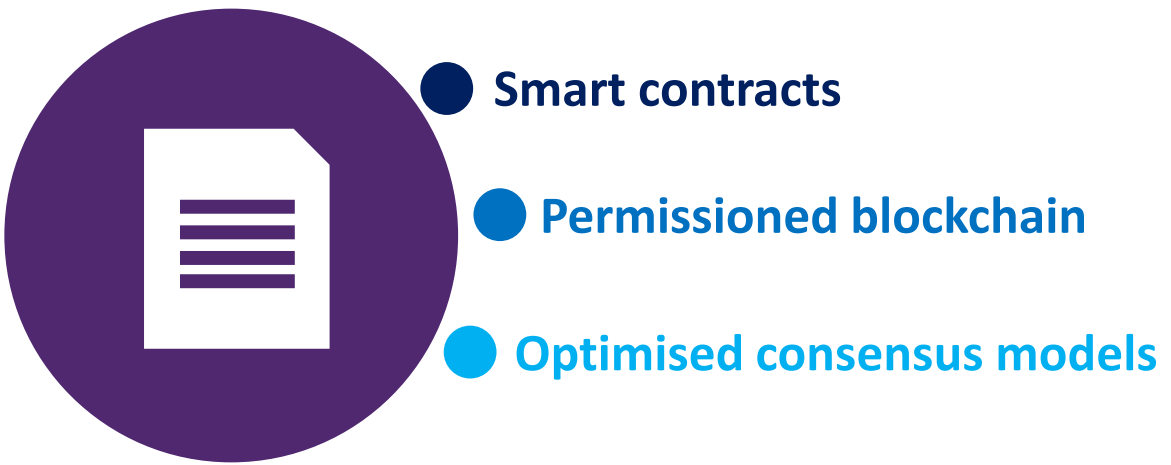


SLT beyond Cryptocurrencies

SLT Evolution to Support Other Use Cases

Many industries developed new use cases underpinned by SLT.

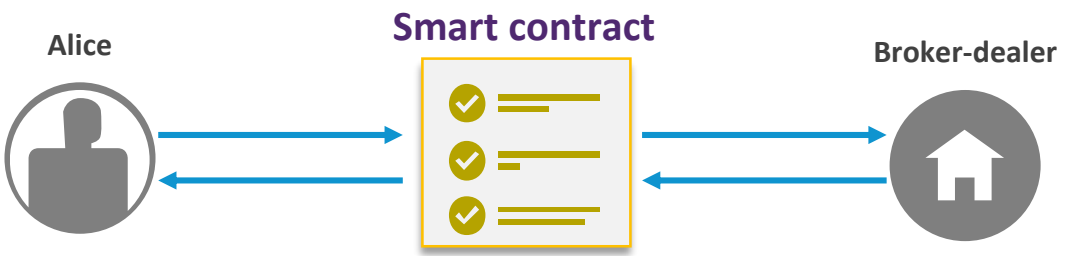
This leads to the evolution of SLT technology, and introduces a number of new concepts.



Smart Contracts on Blockchain

A **smart contract** is stored and executed on the blockchain. Smart contracts enable the creation of new transactions, according to the business logic programmed in the smart contract.

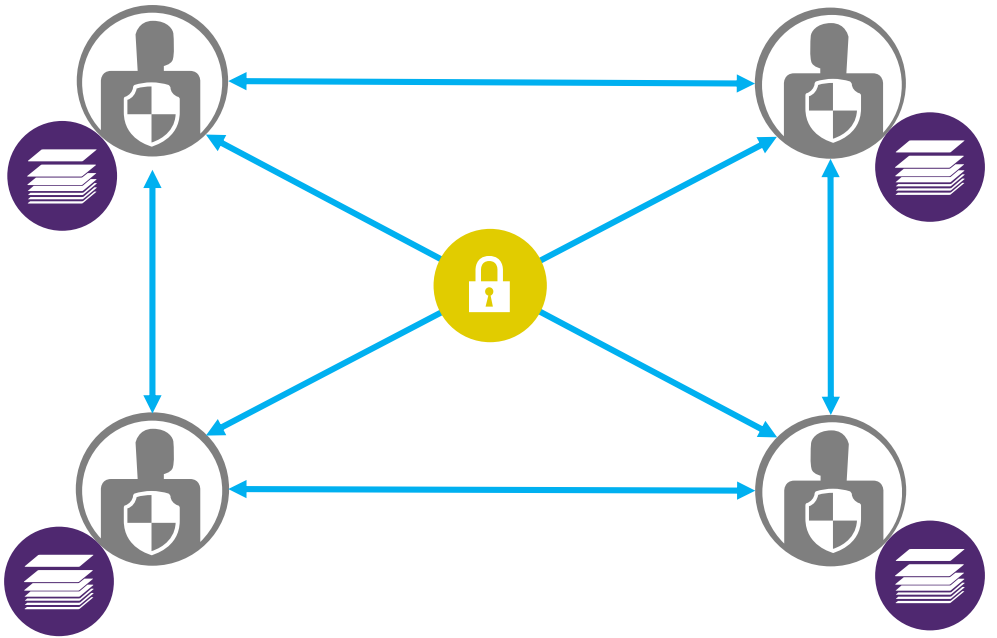
For example, the **smart contract** can check that the minimal subscription amount is submitted, fulfilling the related clause specified in the prospectus of a bond. It will not create the transaction if the requirement is not met.



Permissioned Blockchain

In a permissioned blockchain, the access to the distributed ledger is not open to anyone who wants to participate, as it is for cryptocurrencies, but controlled, and participants are authenticated.

By combining data distribution techniques, together with authentication and encryption, permissioned blockchains allows to selectively distribute data to those parties that have access rights to the data.

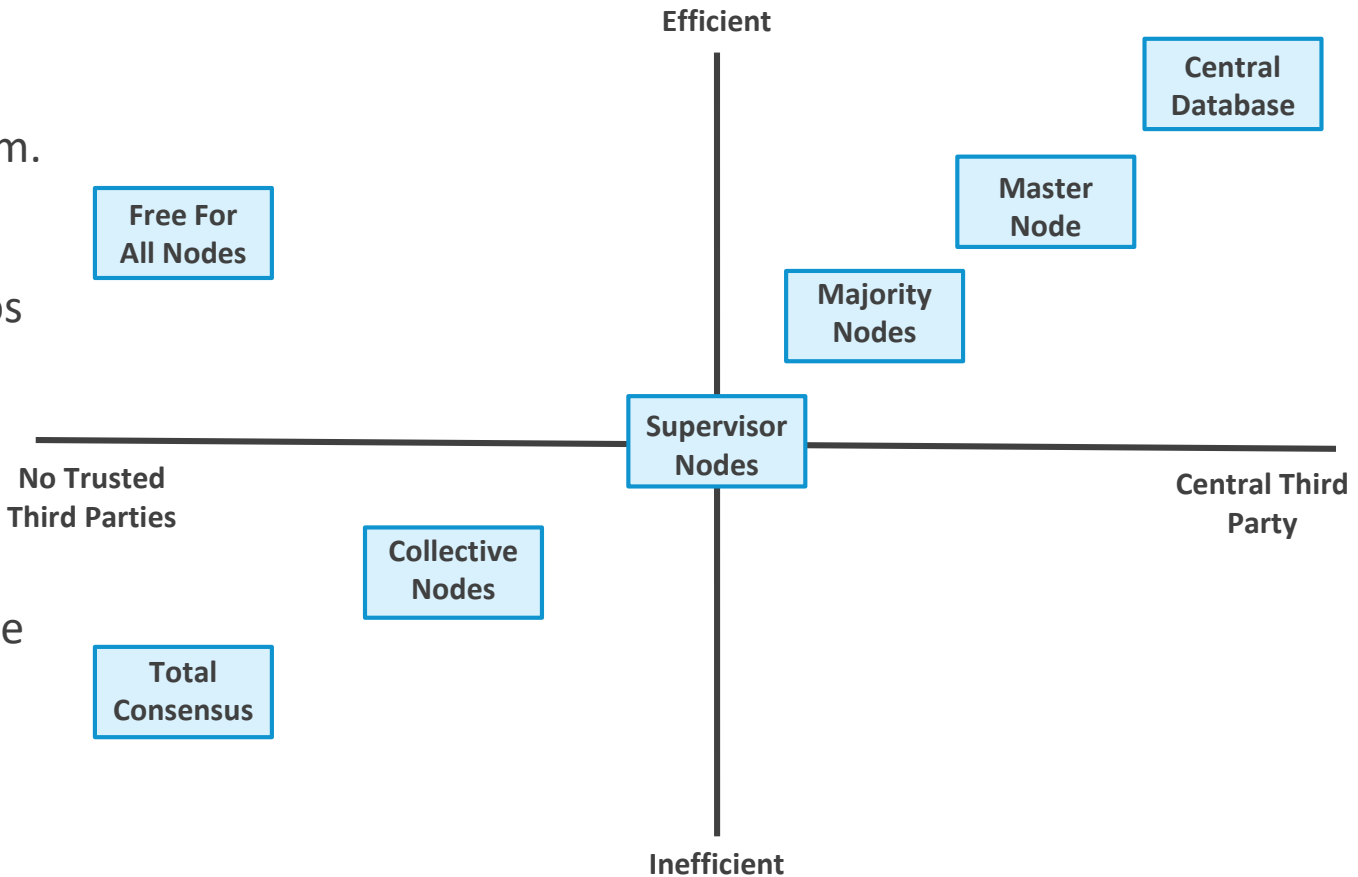


Optimised Consensus Models

The validation process is key to the structure of a SLT. Most SLTs depend on some sort of consensus mechanism.

The percentage of nodes needed for validation varies, and comes with pros and cons: the higher the percentage, the more difficult it is to falsify transactions, but the slower the process becomes.

Because permissioned blockchains are accessed controlled, the validation mechanisms can be optimised depending on the use case, and no longer requires the proof of work mechanism.



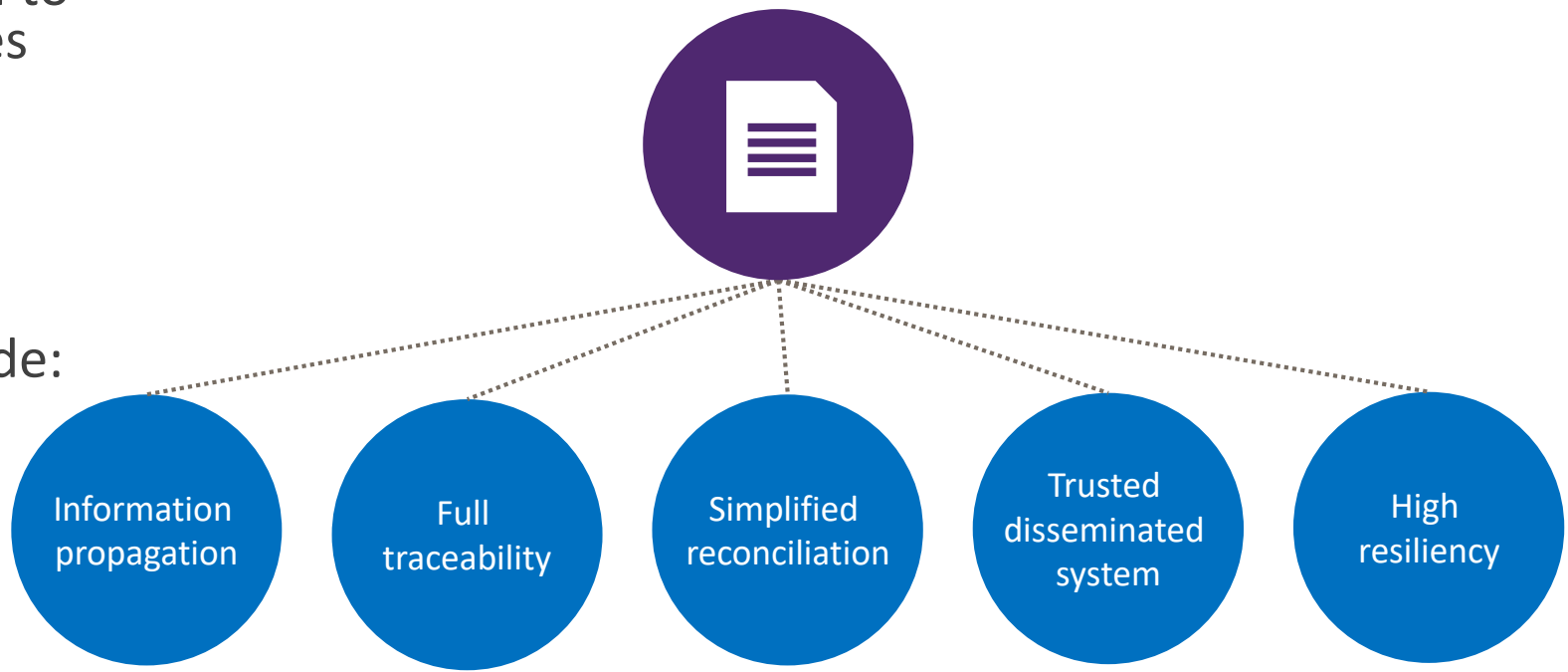
Opportunities and Challenges for Financial Services

Opportunities in Financial Services

SLTs have the potential to bring new opportunities and efficiencies to the financial industry.

The strengths of the technology for the financial industry include:

- Information propagation
- Full traceability
- Simplified reconciliation
- Trusted disseminated system
- High resiliency

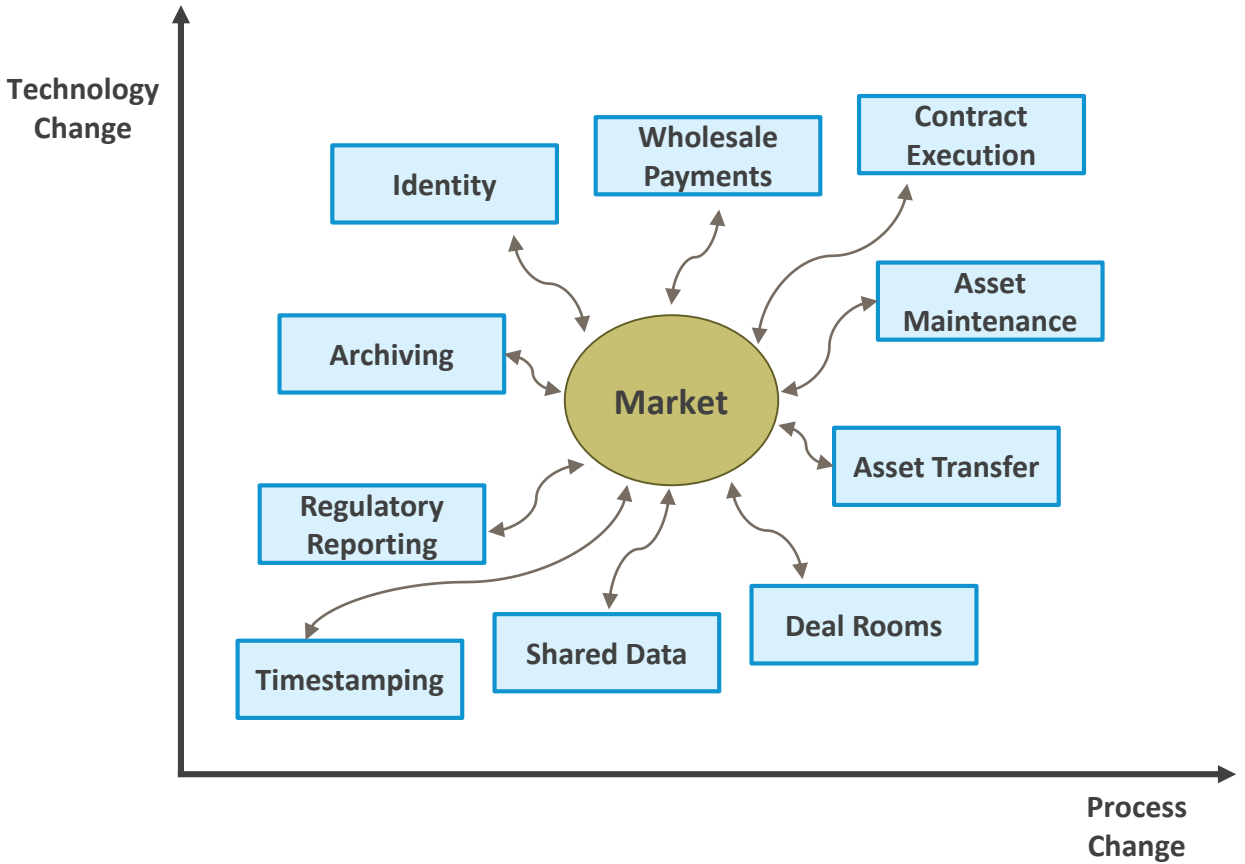


Opportunities in Financial Services

The applicability of SLT in financial services goes far beyond cryptocurrencies.

SLT could transform the way we exchange identity information, documentation, and agreement confirmation.

As the technology evolves, we will be able to progress from timestamping, a relatively simple process crucial in proving event succession, to the more complicated processes of wholesale payments, asset transfer, and contract execution.

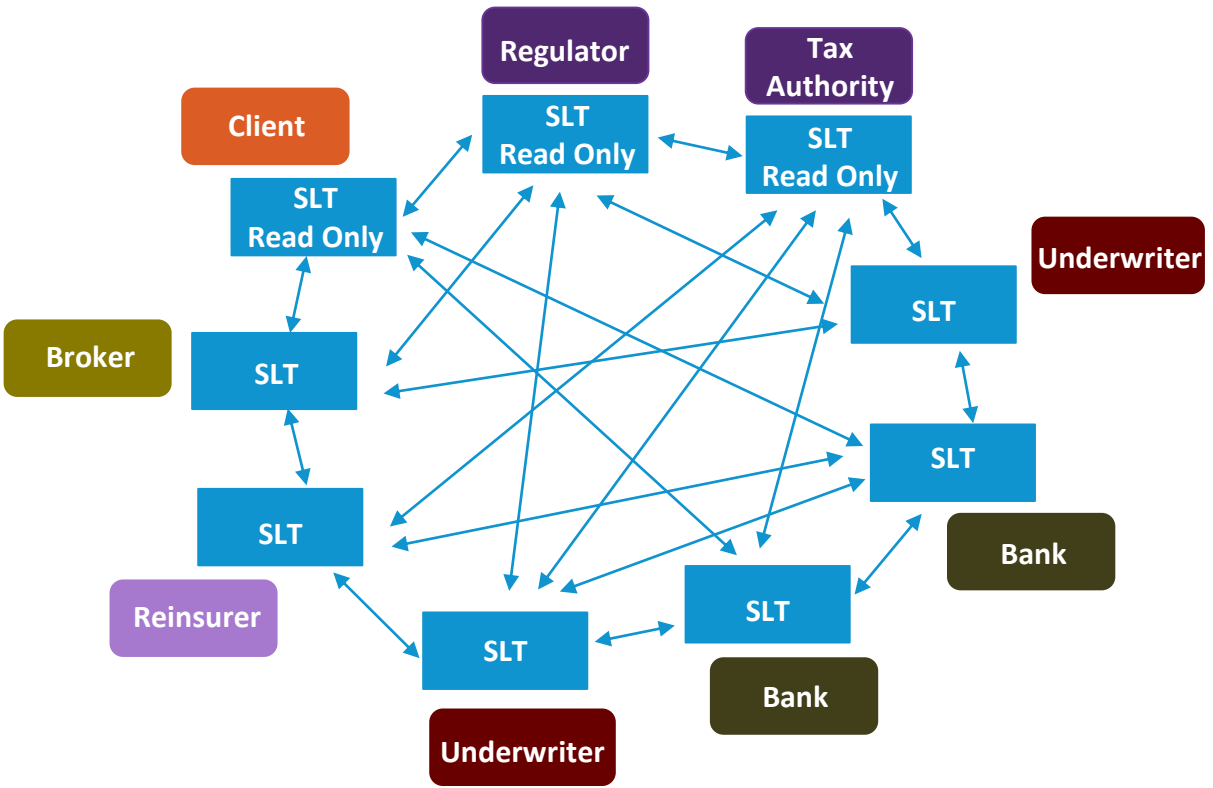


Challenges: Economics Matters

SLTs must overcome a number of challenges in order to be widely adopted by the financial industry.

In terms of economics:

- The cost per SLT transaction is significantly higher than through a central database.
- Due to the consensus mechanism, SLT is not well suited for real time, high-frequency, low-latency, applications.
- A super-audit trail entails an increasingly large mutual ledger, making storage a serious issue.



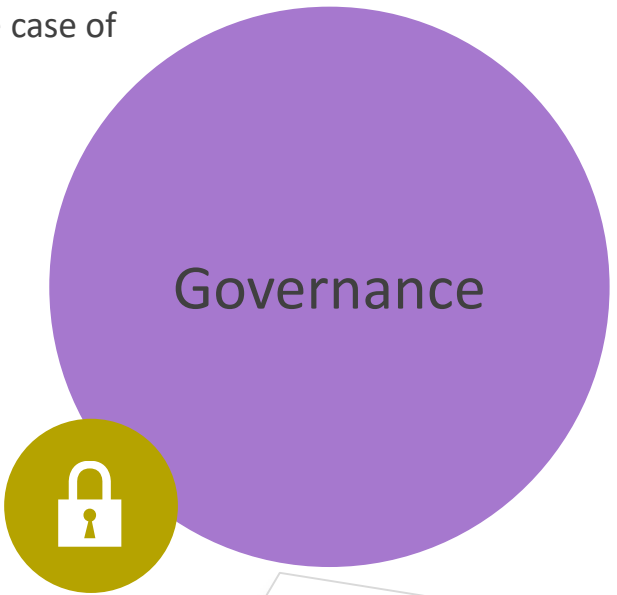
Challenges: Governance and Regulatory Compliance

How are rules created and enforced?

What happens in the case of dispute?

Who is allowed to make changes?

How to standardise?



The services used by the financial industry need to rely on strong governance models to ensure the delivery of effective, predictable and sustainable financial services. SLTs emerged through cryptocurrencies and use a community self-governing model, and, while it may be seen as fairly effective in that context, it does not yet provide the level of trust, transparency and accountability required by the global financial industry.

.

Who is the regulator?
(especially in SLTs that transcend national borders)

Can external regulation be enforced?

How are SLTs audited?

The financial industry is heavily regulated and regulatory pressure is only increasing. SLT compliance with regulatory requirements remains, to a great extent, unexplored and considerable work is still required. Key questions such as who should be regulated, and by whom, are yet to be answered with the answer far from straightforward due to the decentralised and cross-border nature of distributed ledgers.

41 Lothbury, London EC2R 7HG, United Kingdom
+44 (0) 20 7562-9562 hub@zyen.com
www.zyen.com