

An Overview of Blockchain Interoperability

...

May 24, 2018

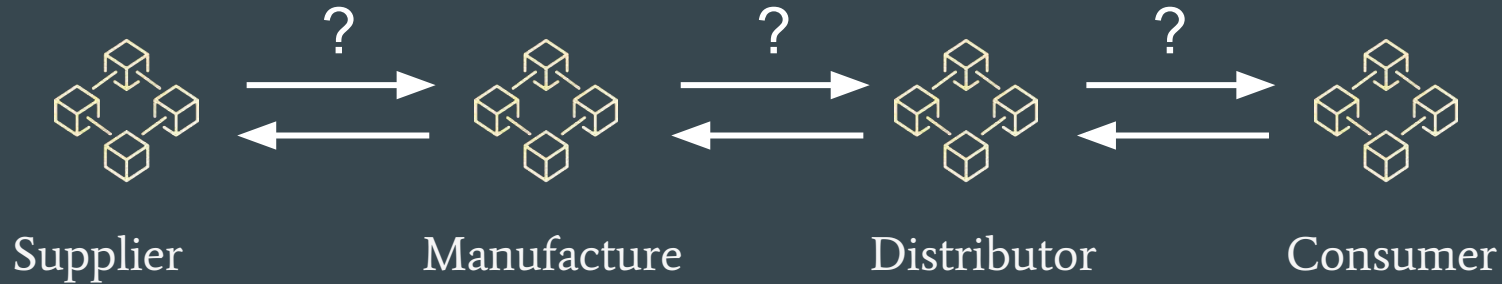
Te Tan, Vasileios Koukoutsas

Index

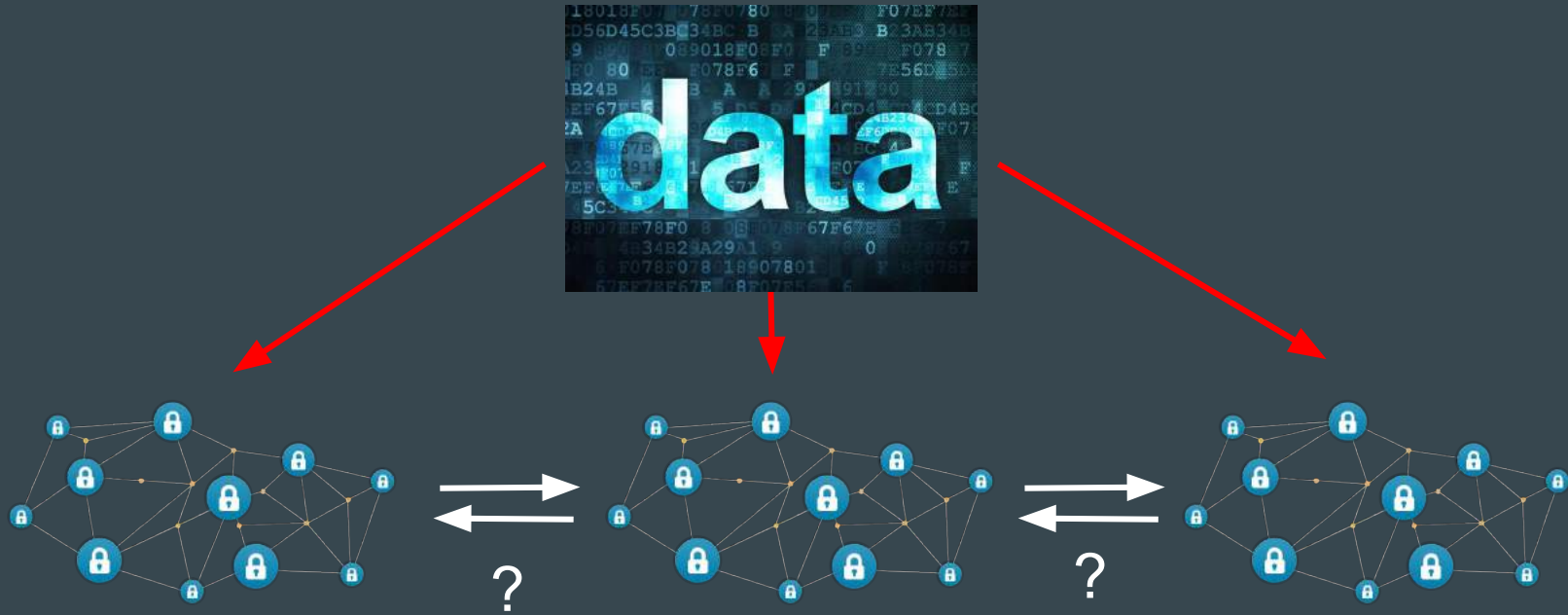
1. Introduction
2. Approaches to Interoperability
3. Use cases of Interoperability
4. Challenges
5. Conclusion
6. Discussion & QA

1. Introduction

Why is there a need for blockchain interoperability ?



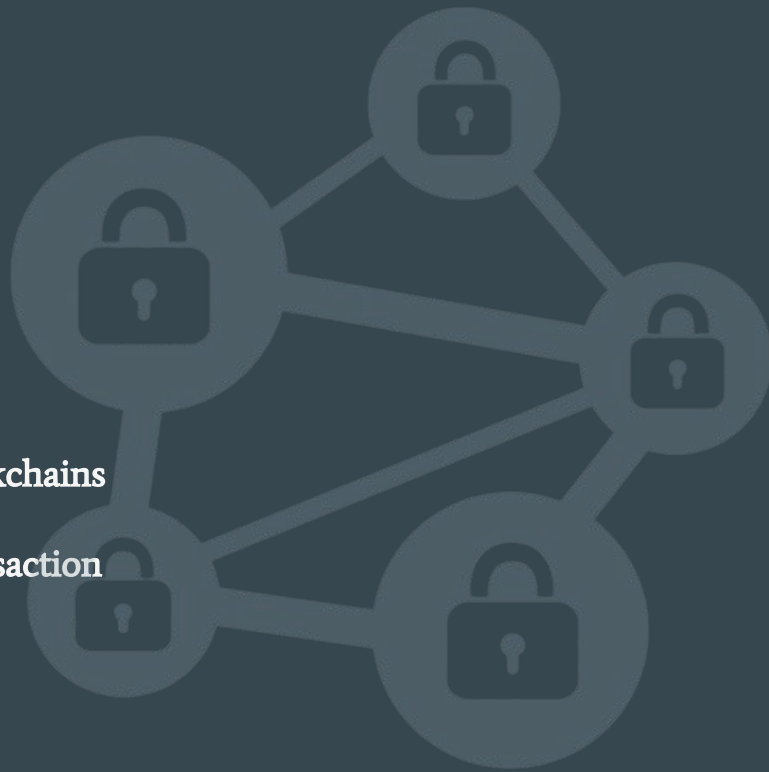
Why is there a need for blockchain interoperability ?



2. Approaches

1. Notary

- Simplest approach
- Use a (set of) trusted entities - Notaries
 - Notaries have accounts on (at least) two blockchains
 - Notaries coordinate and synchronize the transaction



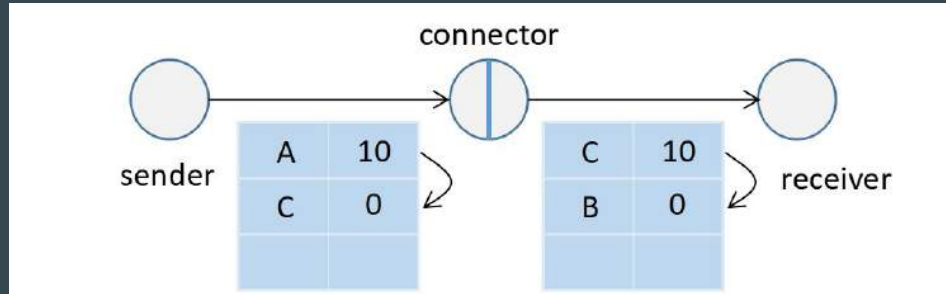
1. Notary

An example:



A protocol which enables inter-blockchain transactions.

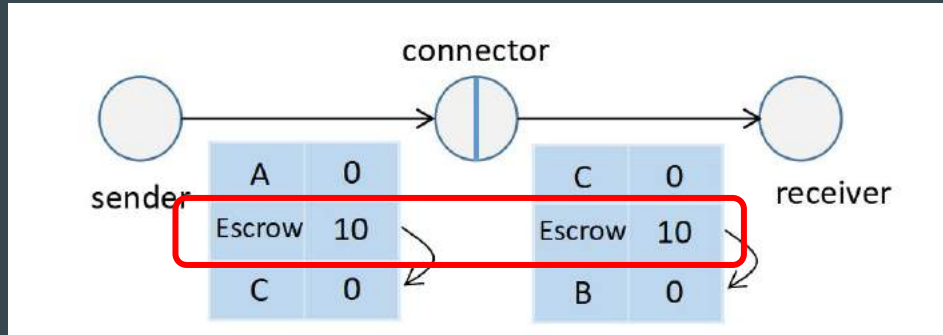
1. Notary



- 3 Roles:
sender, receiver, connector
- Connector has accounts on both ledgers

What if C steals some money ?

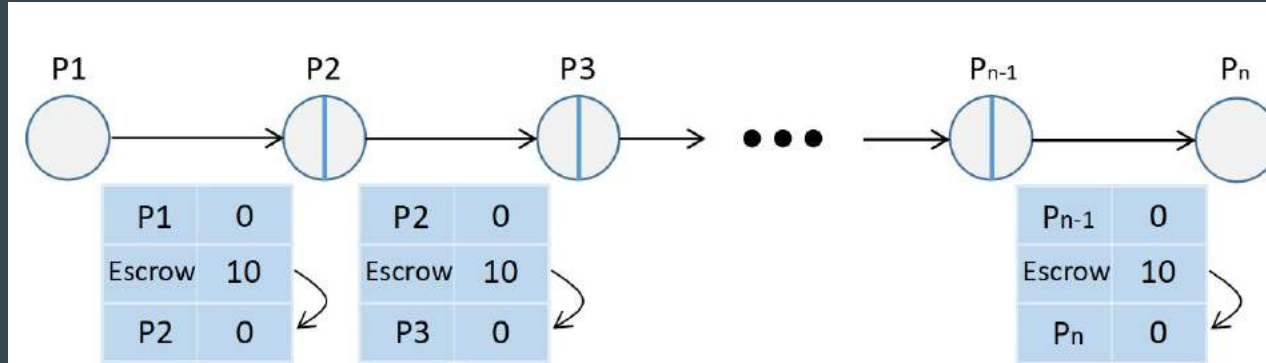
1. Notary



- Escrow:
an intermediate between participants
- A connector is a notary

All the participants only transfer their assets to their respective escrows

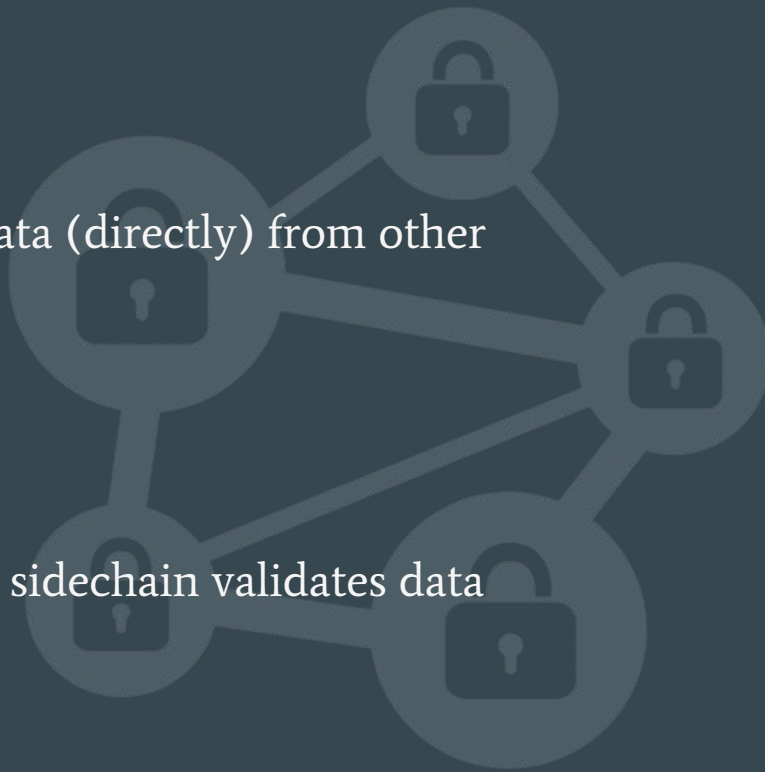
1. Notary



1. P_1 select a set of trusted notaries,
2. All participants transfer assets to escrows,
3. P_n sign a message and send to all notaries,
4. Notaries verify message and execute the transaction

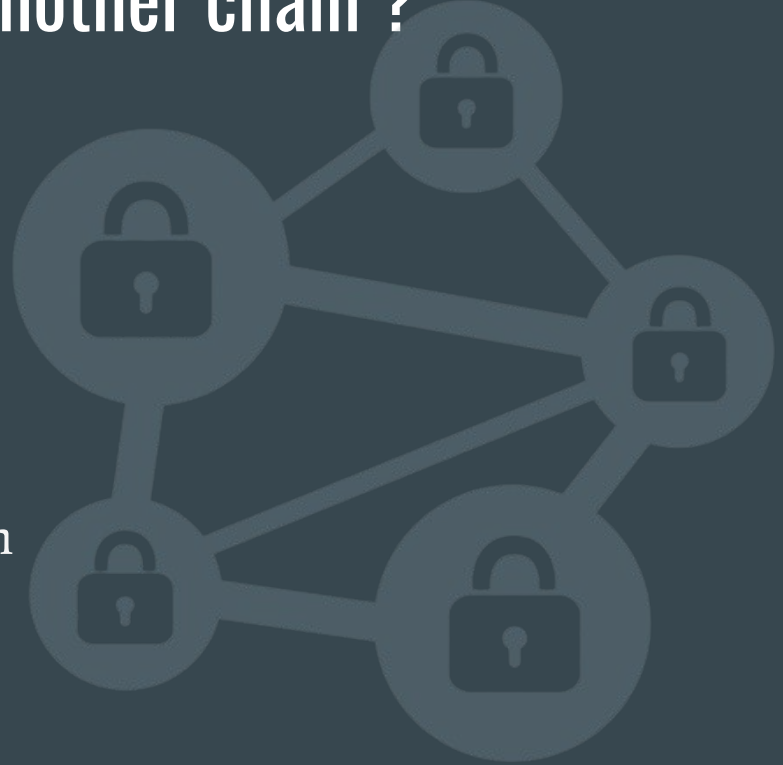
2. Sidechain

- Sidechain:
 - a blockchain which validates data (directly) from other blockchains
- Main chain:
 - the blockchain from which the sidechain validates data



How to verify a transaction in another chain ?

- 1. Validate the block header
 - Verify the proof-of-work
 - Wait until the block is finalized
- 2. Verify the target transaction



How to verify a transaction in another chain ?

- 1. Validate the block header
 - Verify the proof-of-work
 - Wait until the block is finalized

Table 1.1: Information contained in the block header

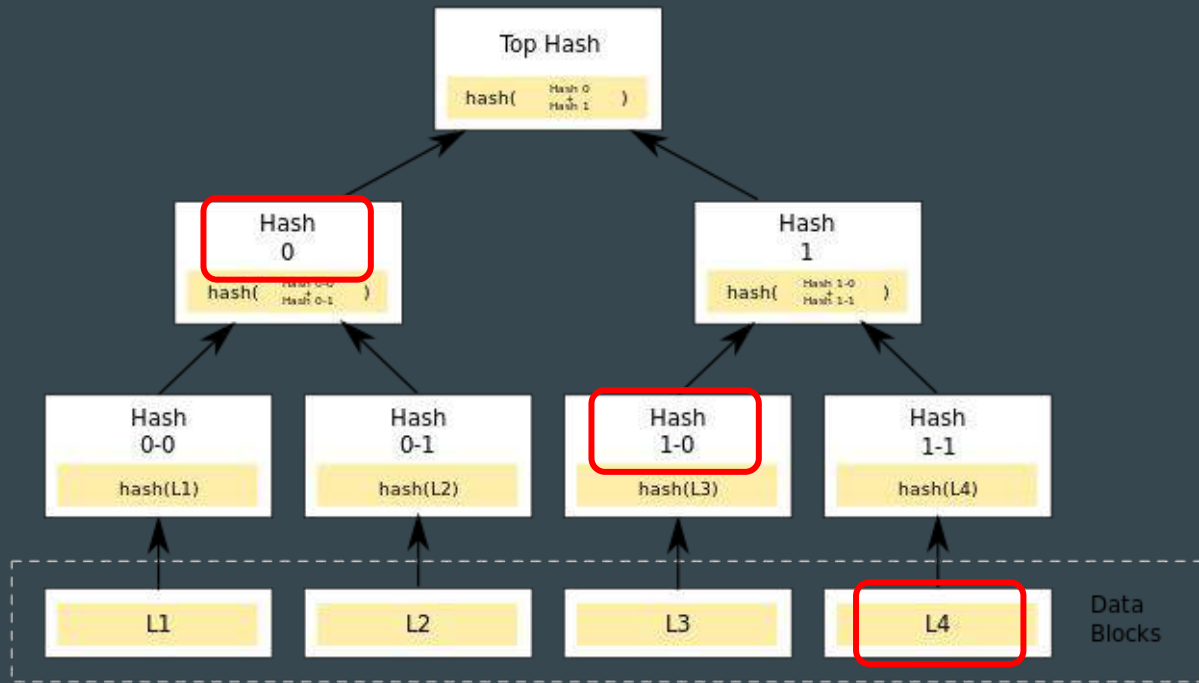
Field	Description
Version	The version number of blockchain
Previous block hash	the hash code of previous block
Merkle root	the hash code of the root of the Merkle tree
Timestamp	the timestamp of the block
Difficulty target	the difficulty target for the formation of the block
Nonce	the counter used by validators to generate a block

How to verify a transaction in another chain ?

- 2. Verify the target transaction

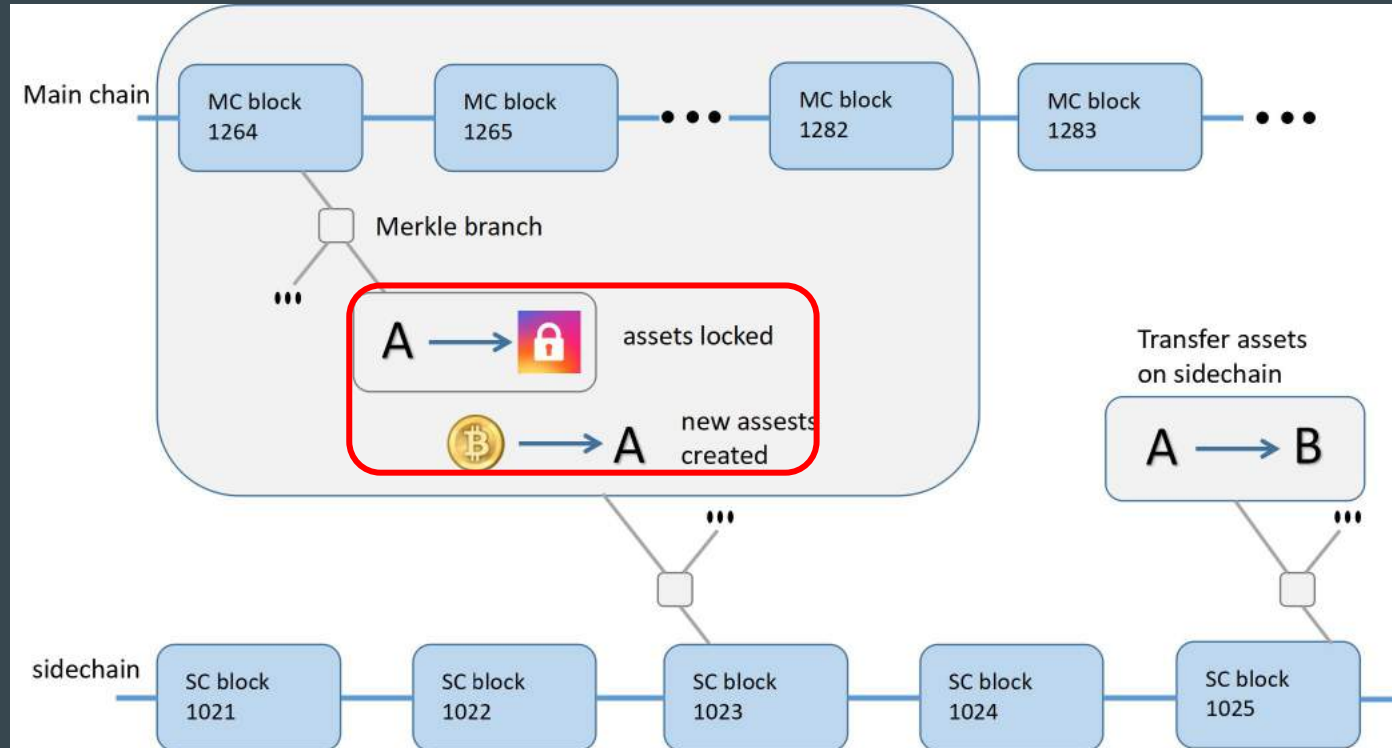
Table 1.1: Information contained in the block header

Field	Description
Version	The version number of blockchain
Previous block hash	the hash code of previous block
Merkle root	the hash code of the root of the Merkle tree
Timestamp	the timestamp of the block
Difficulty target	the difficulty target for the formation of the block
Nonce	the counter used by validators to generate a block



An example of Merkle tree structure

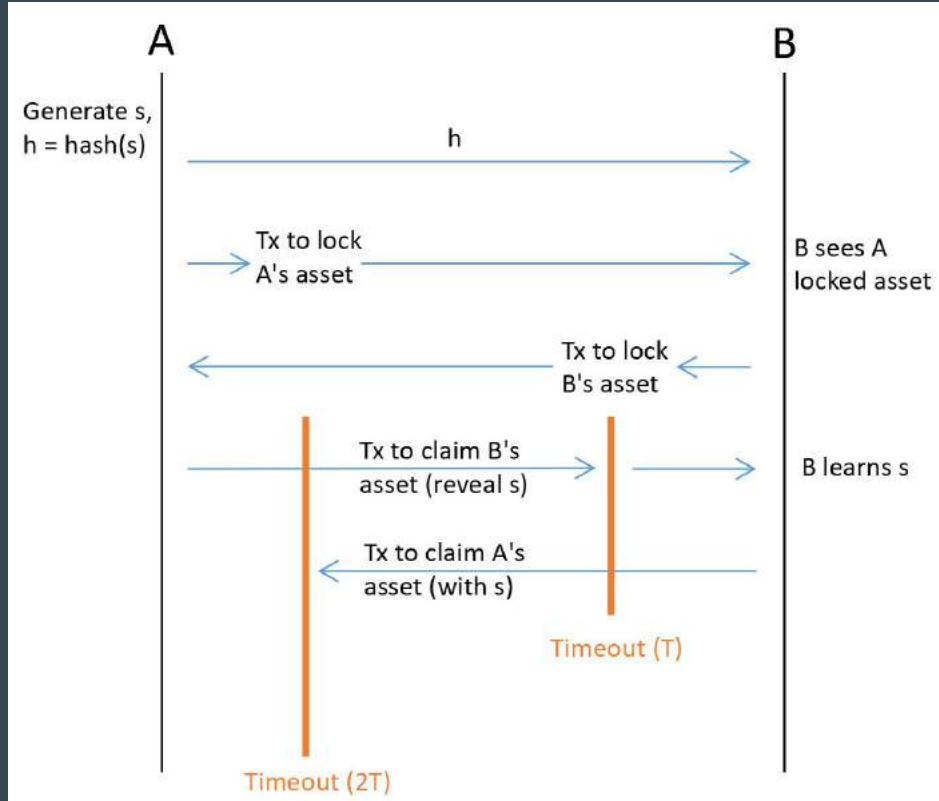
Sidechain enables asset portability



3. Hash-locking

- No notary or sidechain needed
- Can only be used for atomic operations(assets exchange)
- Based on smart contract

3. Hash-locking



3. Interoperability

Use cases

Interoperability of Cryptocurrencies

- 1597 cryptocurrencies in total

- ❑ Coins: 869

- ❑ Tokens: 728

- Total Market Cap: ~440B \$

- 24h Vol: ~23B \$

- BTC Dominance: 36%

(As of May 5th 2018)

Cryptocurrencies: 1597 • Markets: 10649 • Market Cap: \$439,885,359,721 • 24h Vol: \$23,425,364,967 • BTC Dominance: 36.1%

CoinMarketCap

Market Cap • Trade Volume • Trending • Tools •

Search

Top 100 Cryptocurrencies by Market Capitalization

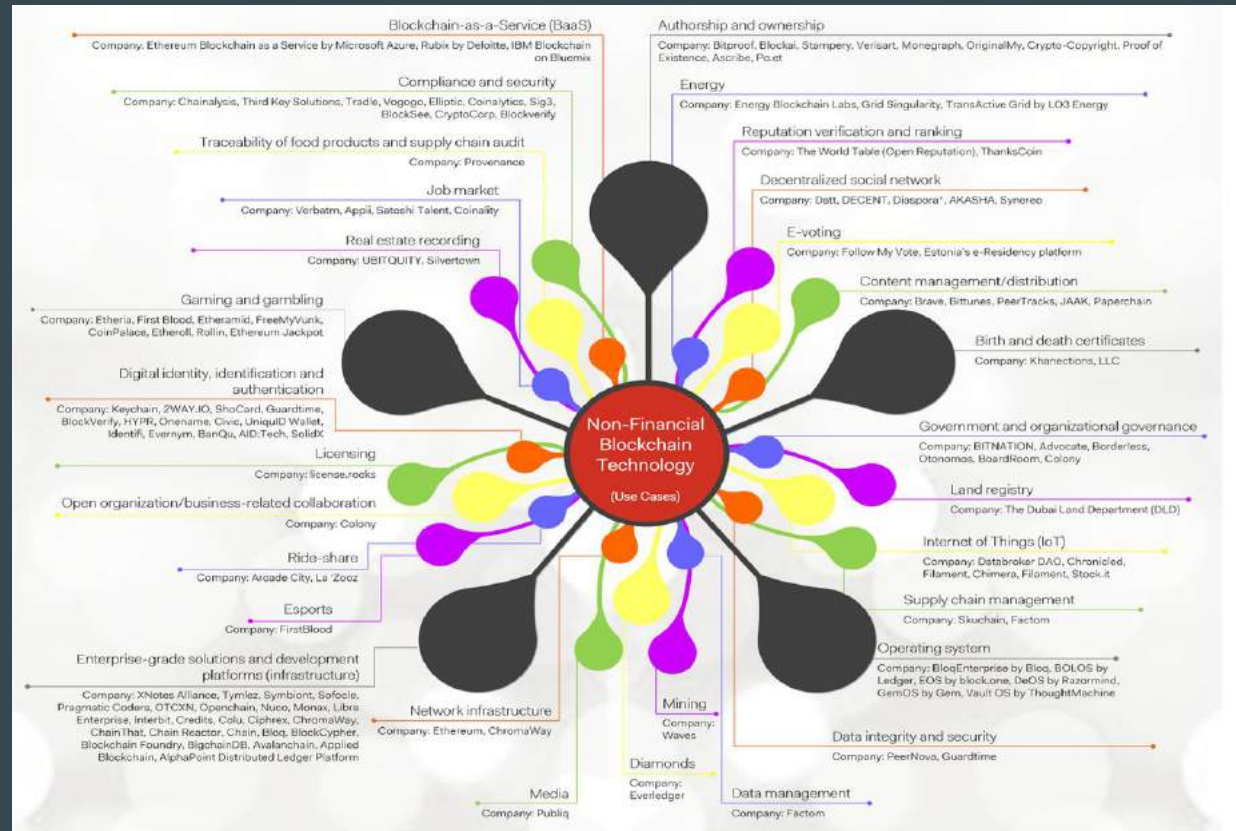
Cryptocurrencies • Watchlist

USD • Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	\$158,743,897,958	\$9,325.94	\$6,997,740,000	17,021,737 BTC	-0.04%	
2	Ethereum	\$74,247,269,096	\$747.67	\$3,542,040,000	99,304,733 ETH	3.15%	
3	Ripple	\$32,258,477,746	\$0.823377	\$467,108,000	39,178,259,468 XRP *	-0.09%	
4	Bitcoin Cash	\$27,674,268,591	\$1,616.83	\$1,119,030,000	17,116,375 BCH	0.07%	
5	EOS	\$15,488,978,843	\$18.38	\$1,707,370,000	842,836,713 EOS *	-3.11%	
6	Litecoin	\$9,179,388,054	\$162.65	\$499,561,000	56,437,488 LTC	0.41%	
7	Cardano	\$8,650,411,523	\$0.333644	\$142,560,000	25,927,070,538 ADA *	1.47%	
8	Stellar	\$7,371,600,723	\$0.396911	\$50,413,700	18,572,427,379 XLM *	1.28%	
9	IOTA	\$7,017,674,673	\$2.52	\$212,918,000	2,779,530,283 MIOTA *	17.55%	
10	TRON	\$5,442,306,516	\$0.082775	\$395,426,000	65,748,111,645 TRX *	1.20%	

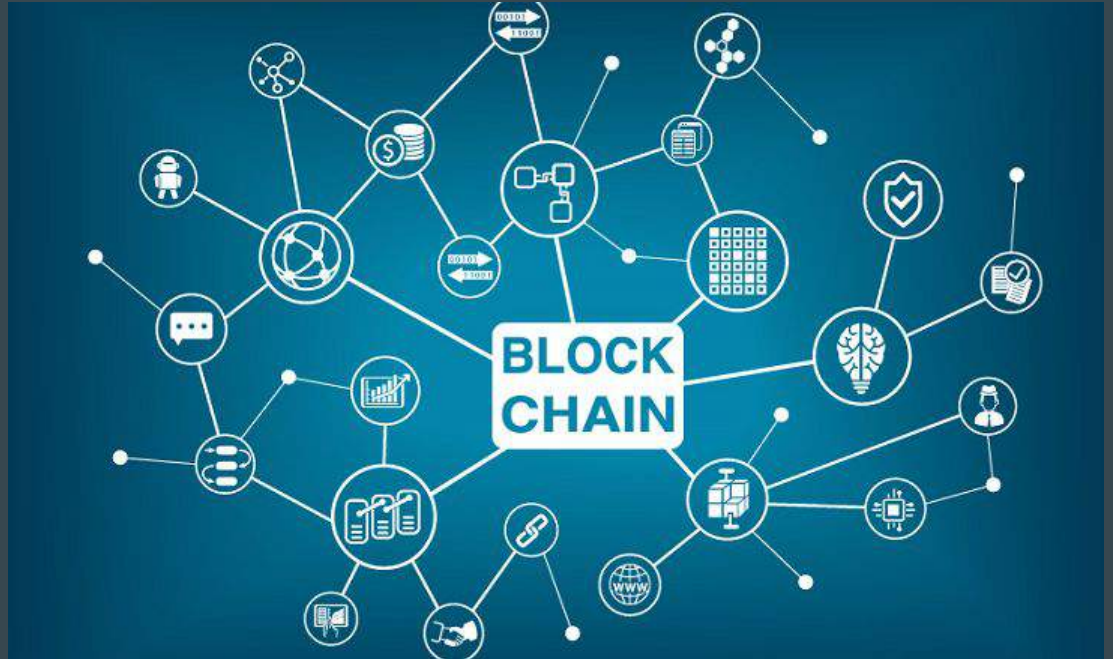
Interoperability of Blockchain Projects

- Supply Chain
- Healthcare
- Insurance
- Internet of Things
- Digital Identity
- E-Voting



Interoperability of the Ecosystem

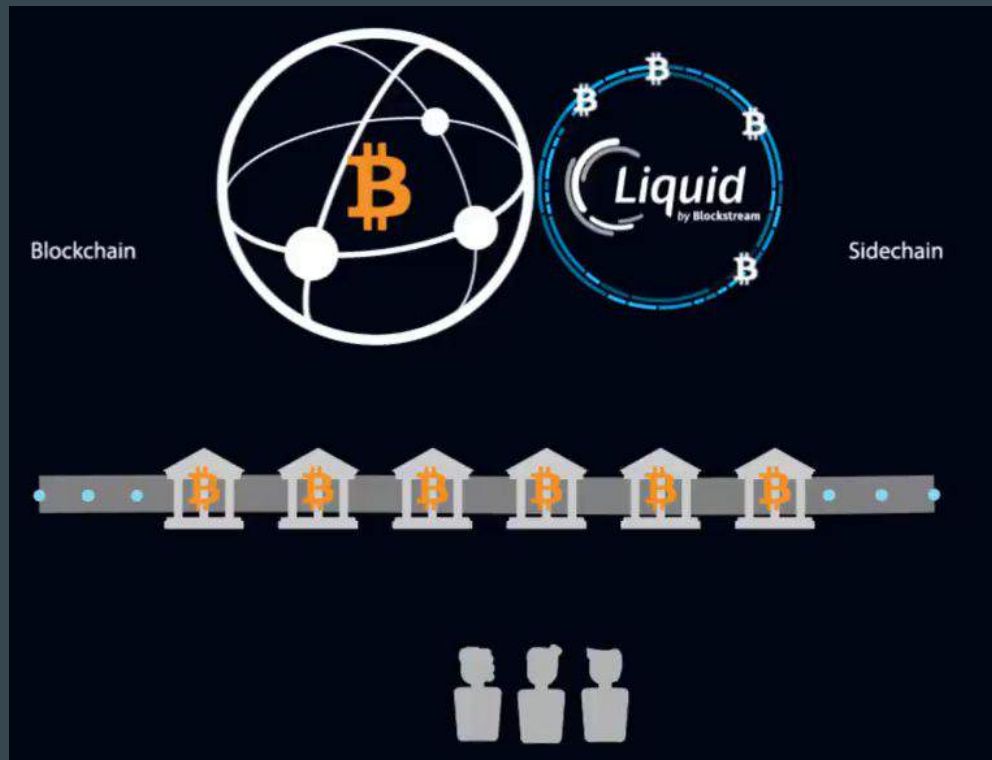
- **Financial Markets & Asset Portability**
- **Cross-chain Contracts**
- **Supply Chain**



3.1 Financial Markets & Asset Portability

Liquid

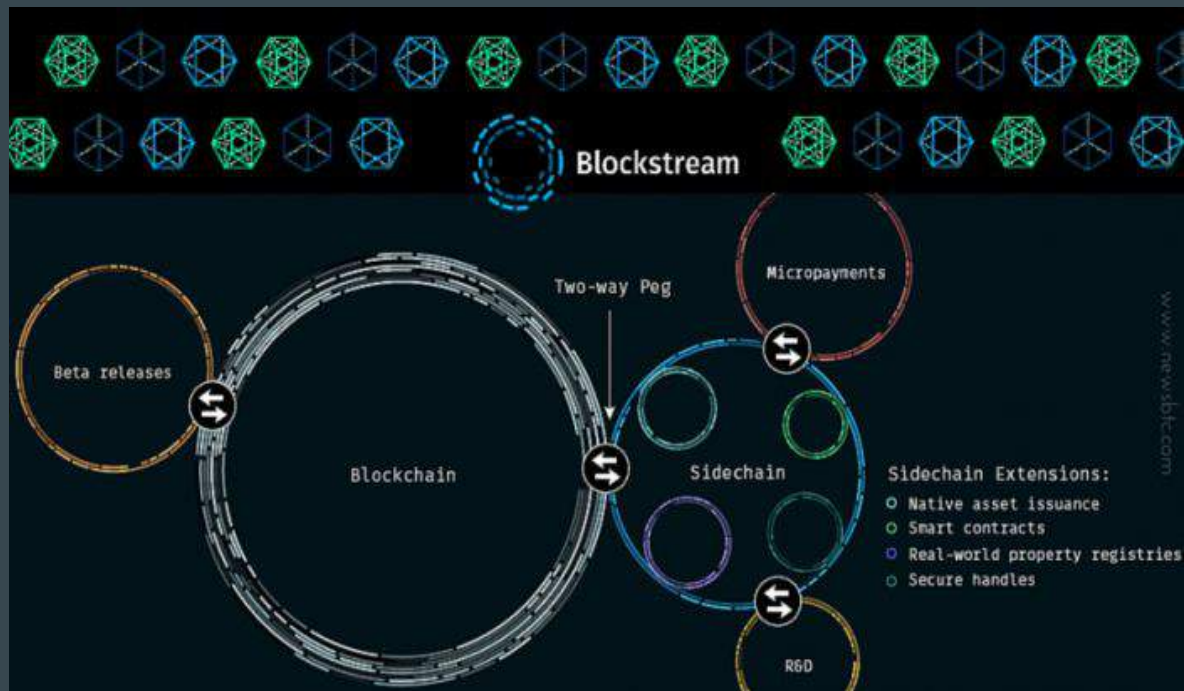
- Provides liquidity for exchanges
- First Commercial Sidechain
- Uses Strong Federations
- Uses Bitcoin's network for security



Source: <https://www.youtube.com/watch?v=FOo7Q4om0Fg>

Liquid Advantages

- Faster Trading
- Enhanced Efficiency
- Better Privacy
- Superb Reliability



Source: <https://blockstream.com>

Liquid Mechanics

- Custom addresses
- 1 min blocks
- Confidential Transactions
- Exchanges Peg In/Out

Liquid Functionary

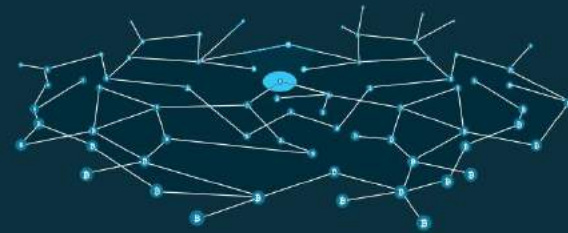
Using special, tamper-resistant hardware, a Liquid functionary signs each new block after validating that it conforms to the rules of the system. Each company maintains one such node, but cannot change the rules of the system without agreement by a supermajority of their peers.

Liquid Grid

As a group, the Liquid nodes agree that the latest block is in fact valid, and so it is added to the chain. If any one actor changes the rules, the other nodes immediately catch the change and prevent malicious activity.

Bitcoin

The security offered by the Bitcoin network is the final say in the Liquid system. Bitcoin can be sent to the Liquid sidechain, moved freely within it, and then withdrawn back to the Bitcoin network when desired.



Source: <https://blockstream.com>

3.2 Cross-chain Contracts

Aelf

- Decentralized Cloud Computing Blockchain Network
- Cross-chain Communication Protocol
- Multi-chain Parallel-processing System
- Self-evolving Governance



Aelf Innovations

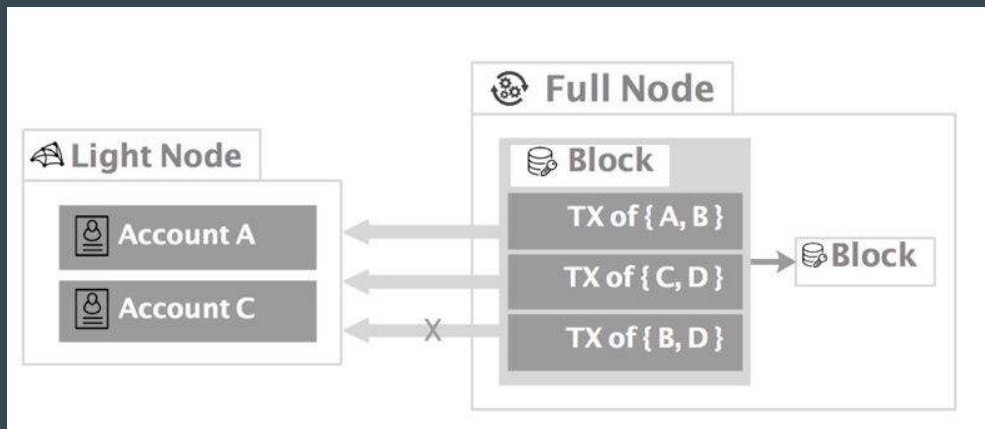
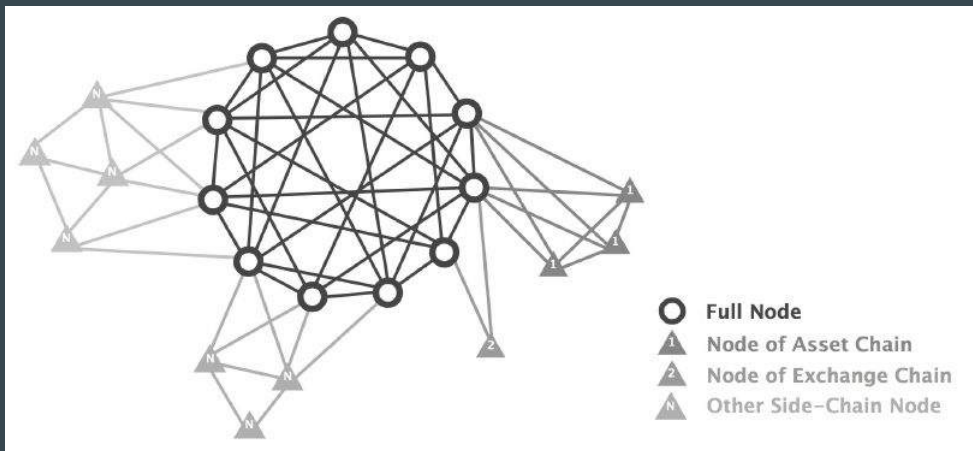
- Scalable nodes on cluster of computers
- Resource isolation for smart contracts via “one chain to one smart contract”
- Side chain dynamic indexing



Aelf Nodes

Main Chain Full Nodes

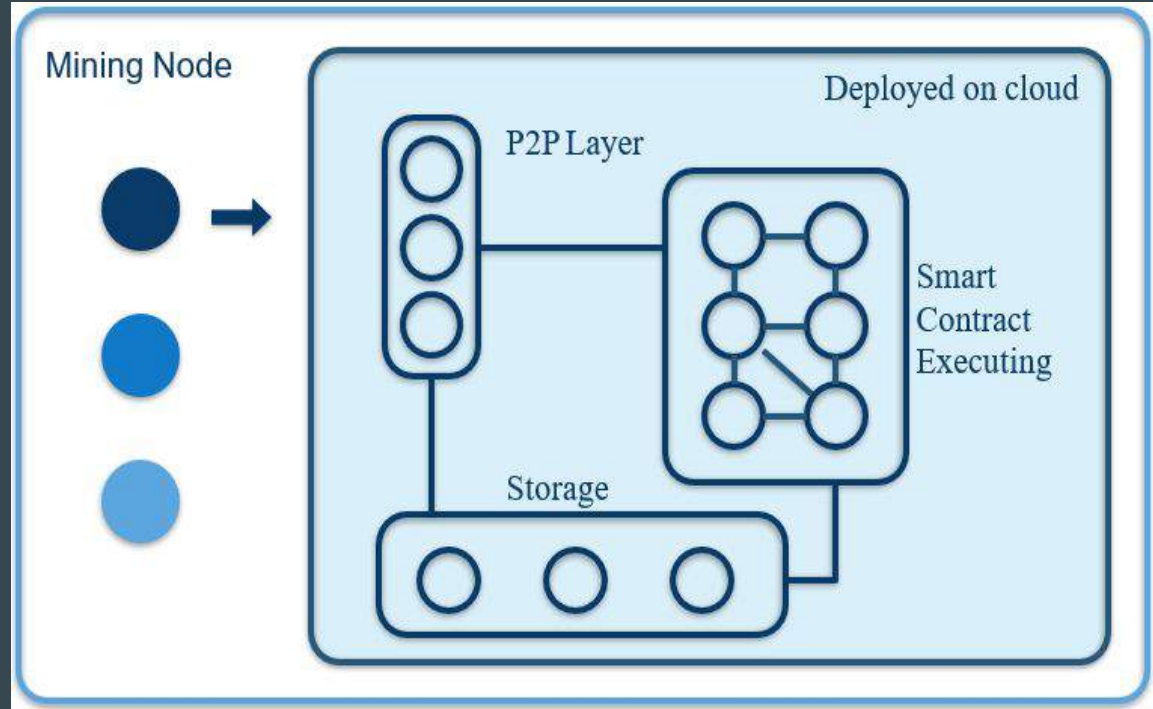
Side Chain Nodes



Light Nodes

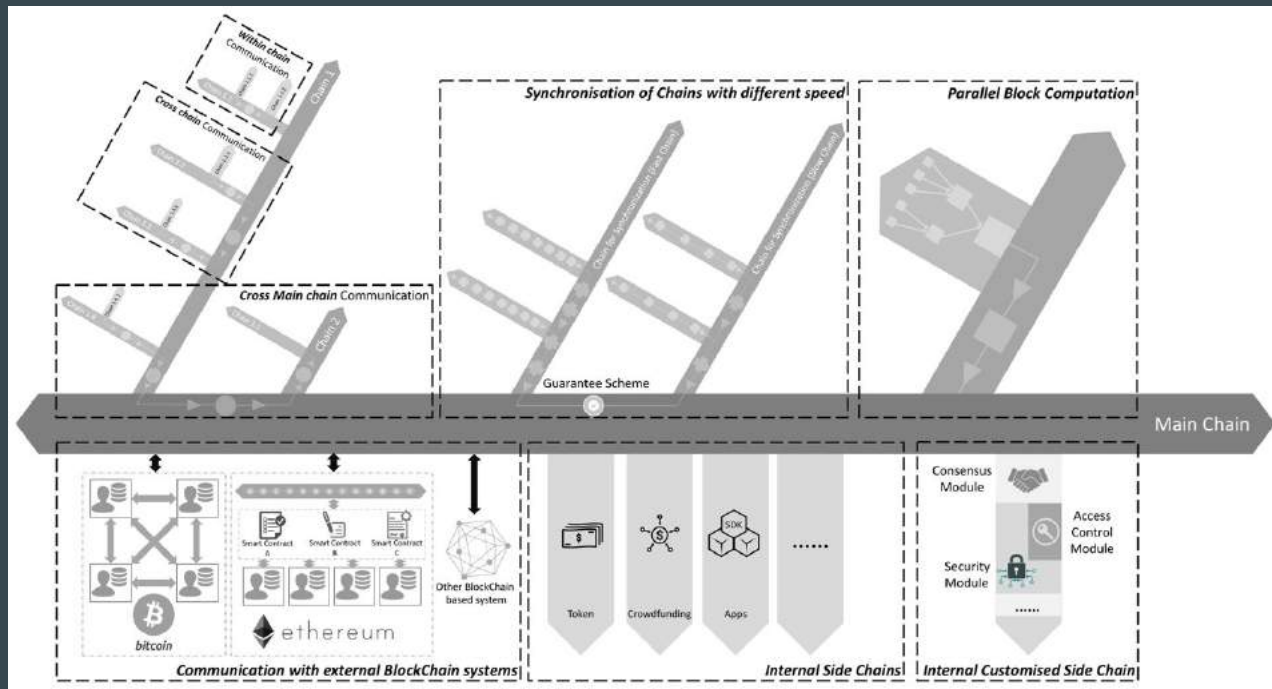
Aelf Node Types

- **Full Nodes:**
 - Mining
 - Ledger
- **Light Nodes (non-mining)**
- **Side chain Nodes:**
 - Full or Light (custom)



Aelf Architecture

- Abstract
- Modular
- Scalable
- Customizable
- Upgradeable



Aelf Governance

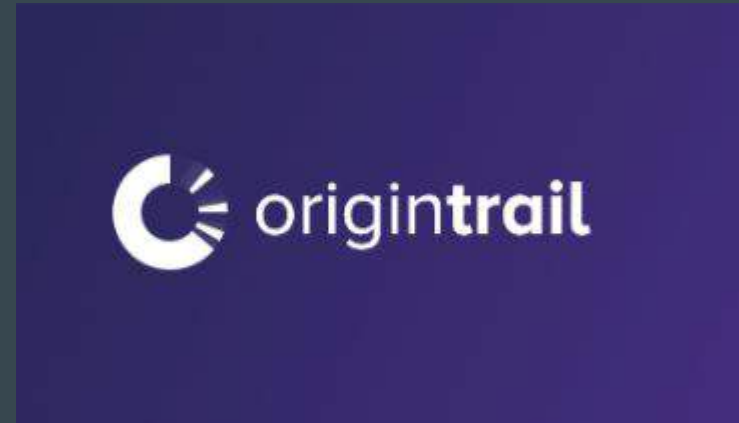
- Grid Foundation (SG)
- Representative Democracy (DPoS)



3.3 Supply Chain

OriginTrail

- **Supply Chain efficiency**
- **Automated compliance**
- **Quality assurance**
- **Secure Storage**
- **Fully compatible with existing ERP systems**



Current Challenges in Supply Chain

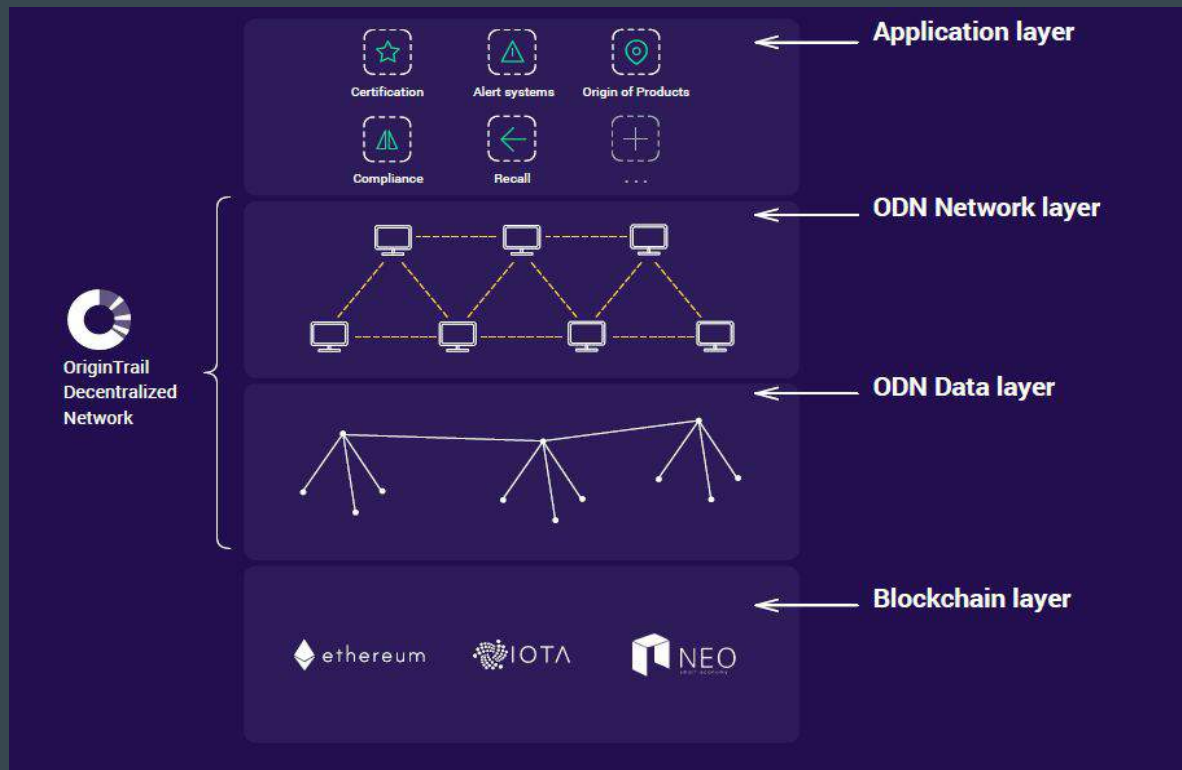
- Data Fragmentation
- Supply Chain Data Centralization



Solution stack

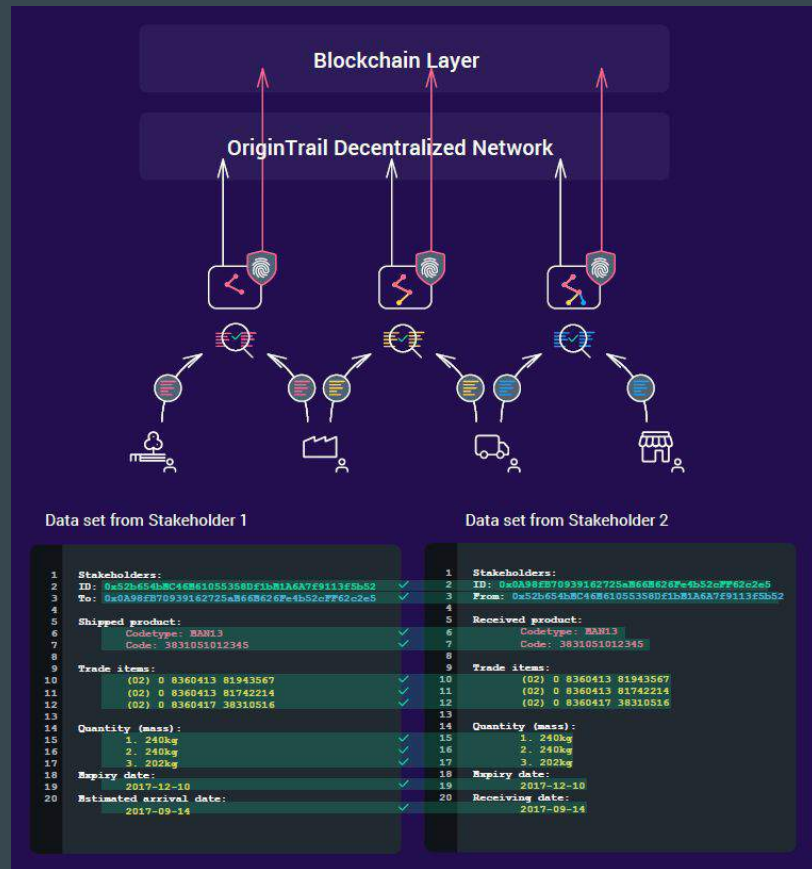
→ Origin Decentralized Network (ODN)

- Asset/Goods tracking
- Defragmentation of complex Data Sets
- Scalability & Seamless Transactions
- Cost-effective governance of business ecosystems



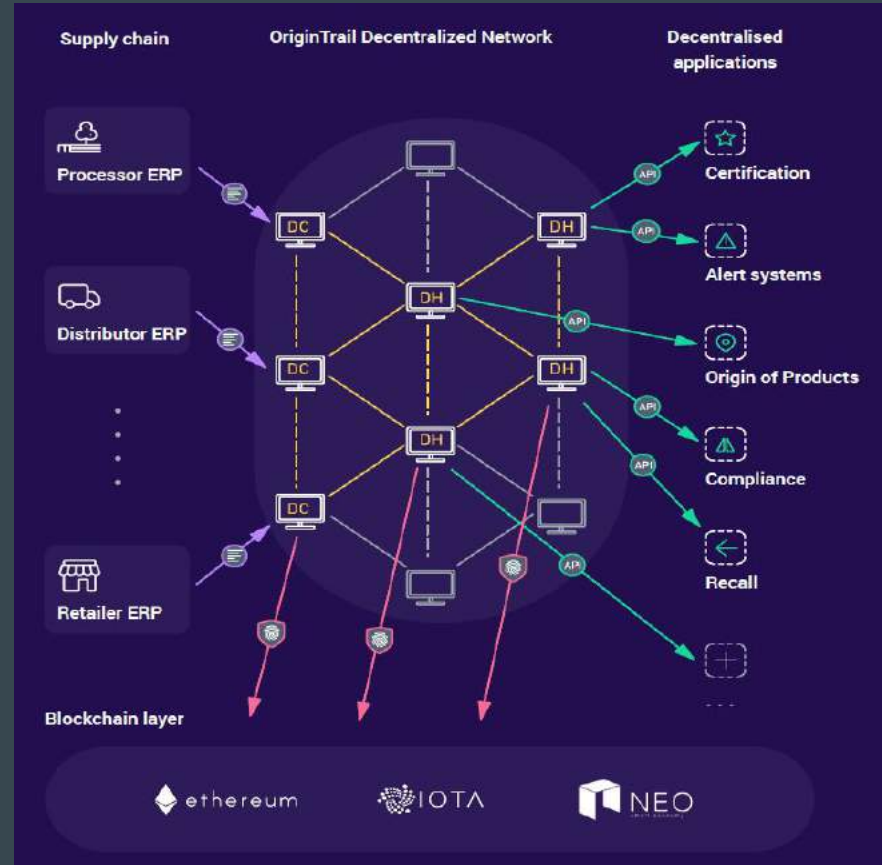
Interoperability and data integrity

- Interoperability (GS1 standard)
 - Master Data
 - Transaction Data
 - Visibility Data
- Consensus
 - Chain of accountability
 - Information Verification
(zk-SNARKs for sensitive data)
 - Data confirmation by auditing and compliance organizations



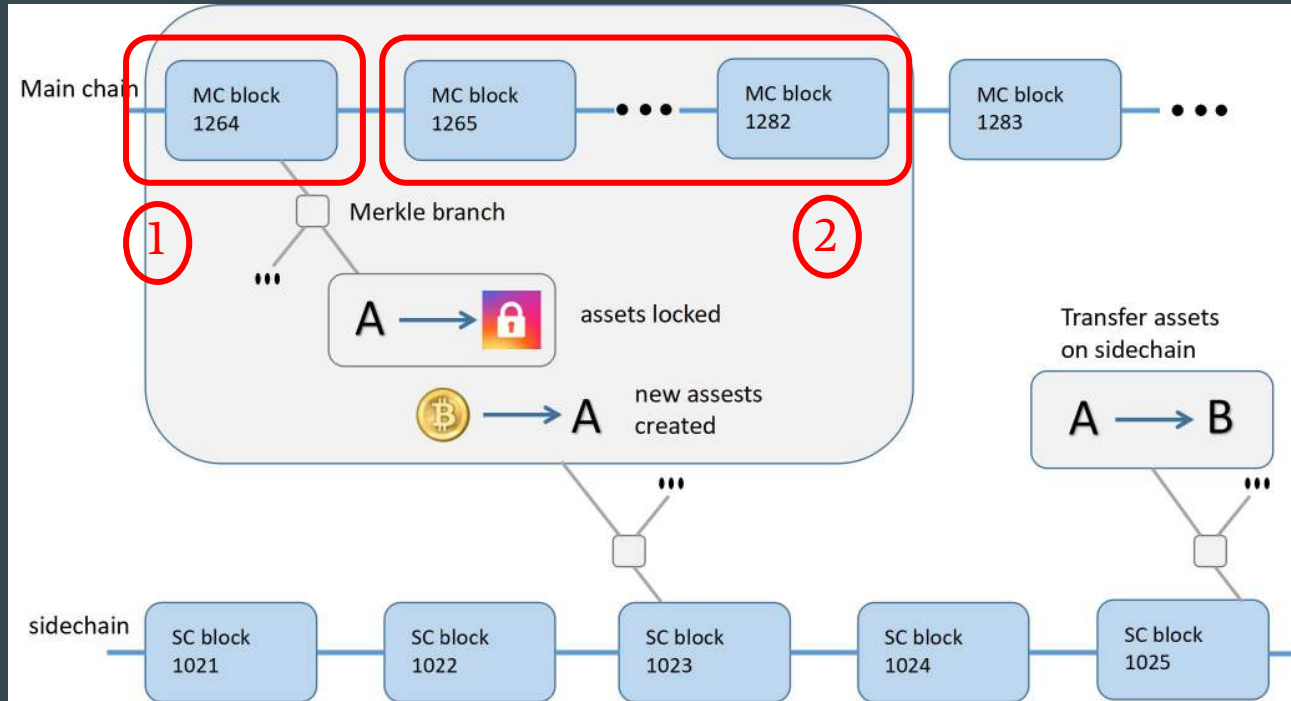
System Overview

- **Data Creator (DC)**
 - Disseminates data to the network
- **Data Holder (DH)**
 - Safekeeping
 - Fingerprinting
 - Data standardization checks
 - Consensus checks



4. Challenges

1. Scalability

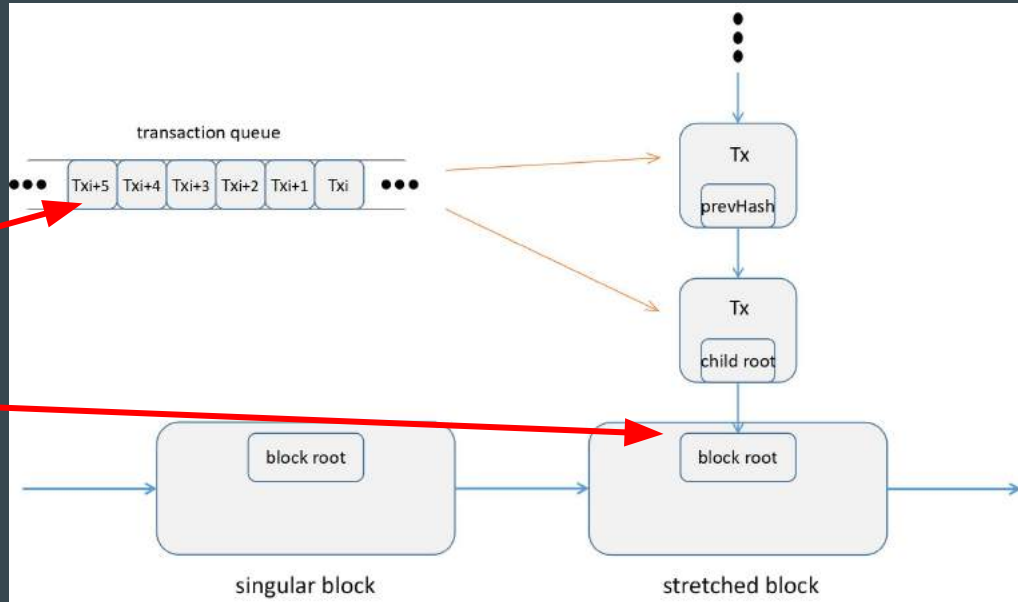


① Block generation

② More blocks generated

1. Scalability

- Proof-of-state
- Transaction queue
- 'Stretched' block



HERDIUS

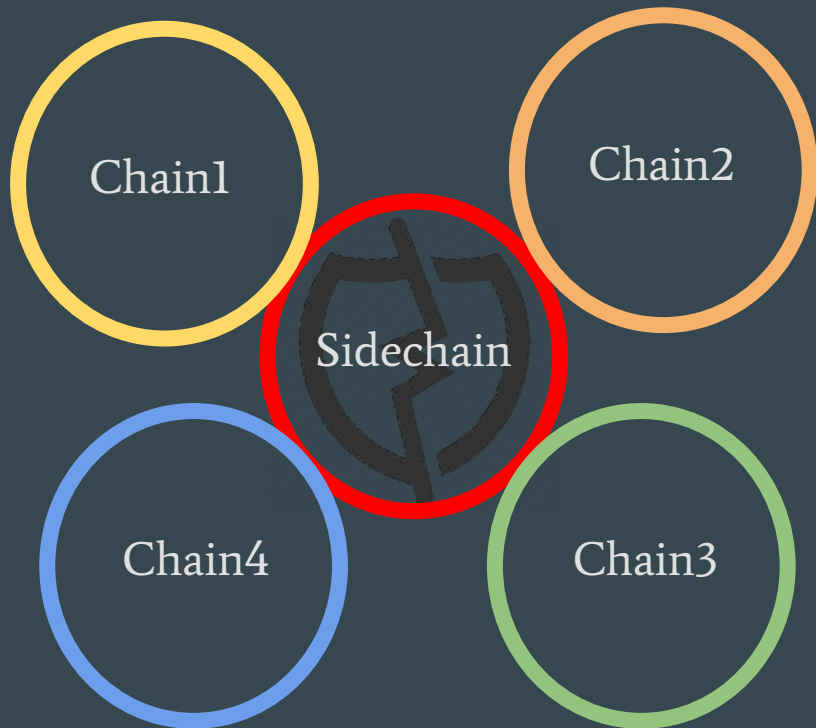
2. Security

New security models needed:

- Multi-chain context
- Information transmission across chains
- Risk re-evaluation



2. Security



3. Practice

- Resource-consuming no matter which solution adopted
- Still in research or 'whitepaper' stage



5. Conclusion

Blockchain Interoperability Overview

- **3 approaches:**
 - **Notary:** a set of trusted entities
 - **Sidechain:** verify another chain directly
 - **Hash-locking:** only for atomic operations
- **Challenges:**
 - Scalability
 - New security model
 - Lack of practice



Current state of Blockchain Interoperability

- **Few commercial Blockchain apps deployed**
 - Only wide usage so far in cryptocurrencies
 - First real-world blockchain applications entered the market Q4 2017
- **Blockchain interoperability**
 - In practice not required yet
 - If achieved it could boost global economy



Questions ??

6. Discussion

Q1: Do you think that BC interoperability is needed?

**Q2: What are the main security concerns for
blockchain interoperability?**

Q3: Can Blockchain Interoperability enable applications in different regulatory environments to interact seamlessly?

Q4: What do you think about having a dominant sidechain as the central exchange platform ?

Q5: Will IoT systems benefit from the data-sharing enabled by Chain Interoperability?

Thank you !