Blockchain Interoperability
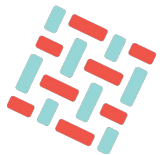
Rafael Belchior

PhD Researcher & TA @ Técnico Lisboa

Mentor @ Hyperledger Foundation

2019 - Distributed Access Control

2020 - Blockchain Interoperability

Mentor @ Hyperledger Foundation

2019 - Distributed Access Control
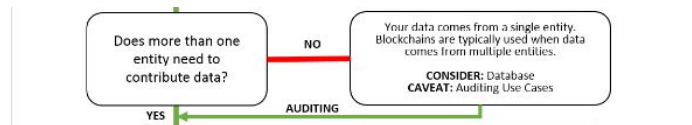
2020 - Blockchain Interoperability
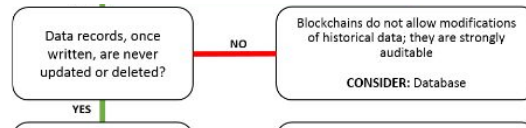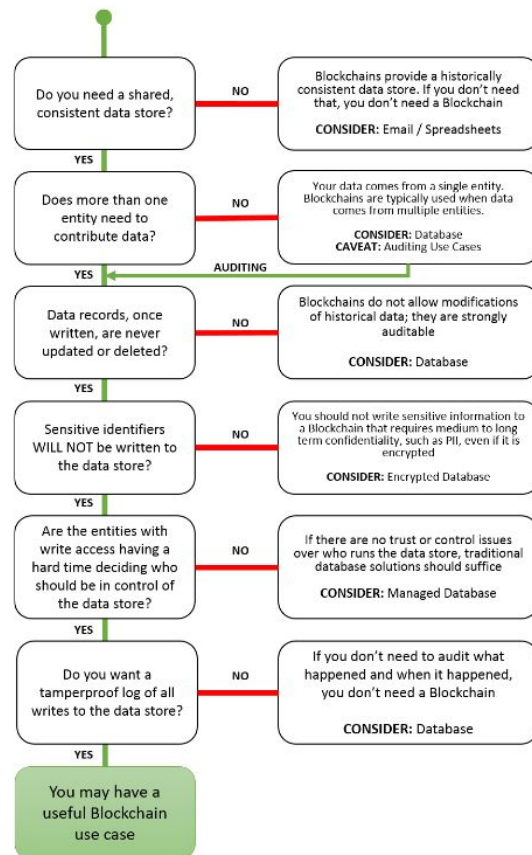
JusticeChain

What are blockchain's main problems?

Figure 6 - DHS Science & Technology Directorate Flowchart

❏ Market cap: $260 billion spread across hundreds of blockchains.

❏ However, enterprises are reluctant to invest in blockchain technology: vendor lock-in, risk of obsolescence, lack of standards

The DAO Attack

We take a look at the most significant event in cryptoeconomics since the birth of Bitcoin and it's impact on the Ethereum Blockchain

The DAO (Decentralised Autonomous Organisation) - a programme built on the Ethereum Blockchain platform was breached earlier this year in a case that resulted in $50 million worth of Ether being stolen.

Only weeks after one of the largest crowd funding projects ever, the DAO seemed a promising application that contributed to bringing hype to the Blockchain space. One hacker spotted a flaw in the DAO's code and managed to drain 3.6 million Ether into a personal account which sent the Ethereum community into panic mode, causing the price to plummit and created a reluctance amongst the community to invest. The price of Ether has since recovered somewhat and the trust has been regained to a certain extent, but the attack proved that Blockchain technology is not flawless.

Download the full infographic

The DAO Attack

This repository has been archived by the owner. It is now read-only.

hyperledger / composer Archived

forked from hyperledger-archives/composer

👁 Watch ▾ 1   ★ Star 1

<> Code   ⏸ Pull requests 0   ▶ Actions   🛡 Security 0   📊 Insights

⚠ ⚠ ⚠ Hyperledger Composer has been deprecated ⚠ ⚠ ⚠   https://wiki.hyperledger.org/display/...

⟲ 5,043 commits   ⑂ 9 branches   📦 0 packages   🏷 106 releases   👥 78 contributors
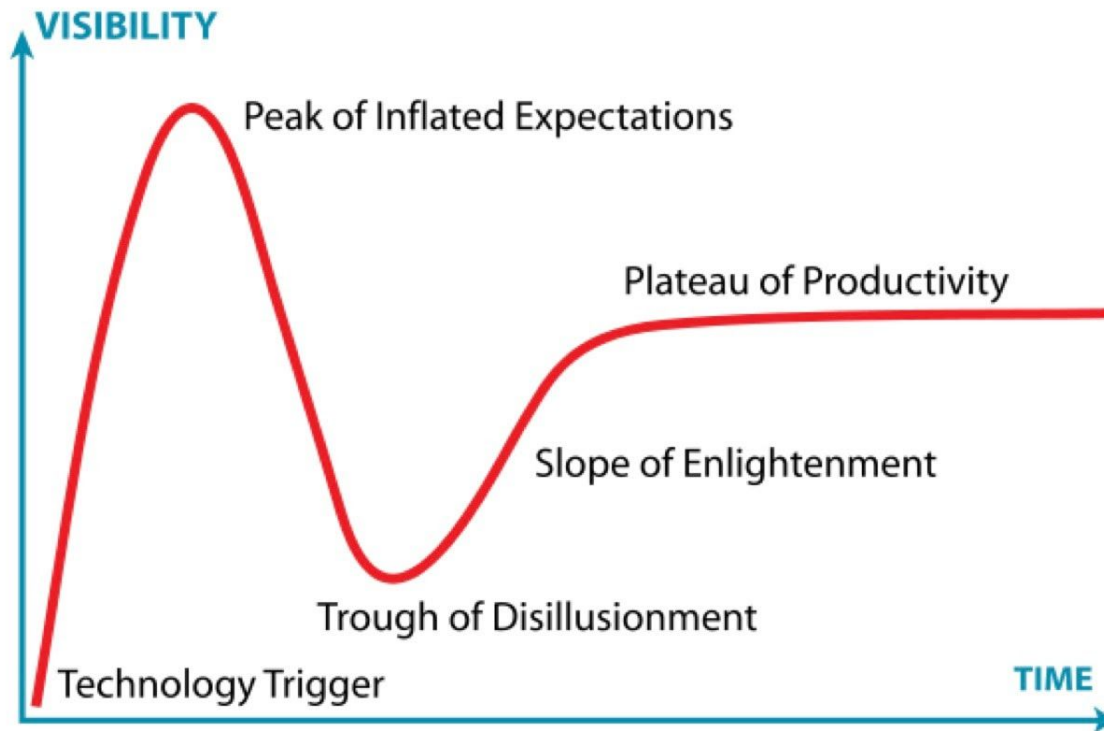
Branch: master ▾   Create new file   Upload files   Find file   Clone

This branch is even with hyperledger-archives:master.   ⏸ Pull request

Gartner Hype Cycle

Blockchain life-cycle stage by market size

Life-cycle stages

At today's tipping point, many prototypes have been built but blockchain technology has not yet seen widespread application at scale, and the future remains uncertain.
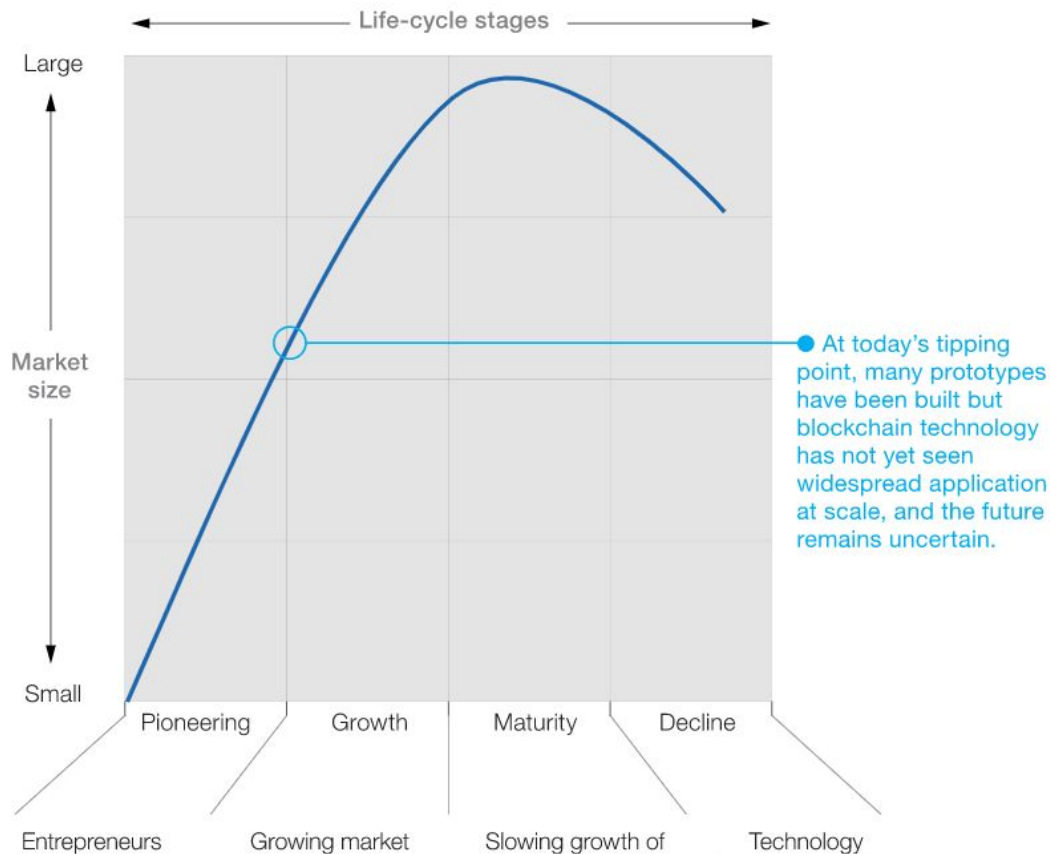
- ❏ Niche applications
- ❏ Modernization value
- ❏ Reputational value

Source: McKinsey
February 2019 report

❏ Study December 2019 - August 2020

❏ 300+ documents analysed, 80 papers included in the review

A Survey on Blockchain Interoperability: Past, Present, and Future Trends

RAFAEL BELCHIOR, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal
ANDRÉ VASCONCELOS, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal
SÉRGIO GUERREIRO, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal
MIGUEL CORREIA, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal

Blockchain interoperability is emerging as one of the crucial features of blockchain technology, but the knowledge necessary for achieving it is fragmented. This fact makes it challenging for academics and the industry to seamlessly achieve interoperability among blockchains.

Given the novelty and potential of this new domain, we conduct a literature review on blockchain interoperability, by collecting 262 papers, and 70 grey literature documents, constituting a corpus of 332 documents. From those 332 documents, we systematically analyzed and discussed 80 documents, including both peer-reviewed papers and grey literature.

Our review classifies studies in three categories: Cryptocurrency-directed interoperability approaches, Blockchain Engines, and Blockchain Connectors. Each category is further divided into sub-categories based on defined criteria. We discuss not only studies within each category and subcategory but also across categories, providing a holistic overview of blockchain interoperability, paving the way for systematic research in this domain. Our findings show that blockchain interoperability has a much broader spectrum than cryptocurrencies.

The present survey leverages an interesting approach: we systematically contacted the authors of grey literature papers and industry solutions to obtain an updated view of their work.

Finally, this paper discusses supporting technologies, standards, use cases, open challenges, and provides several future research directions.
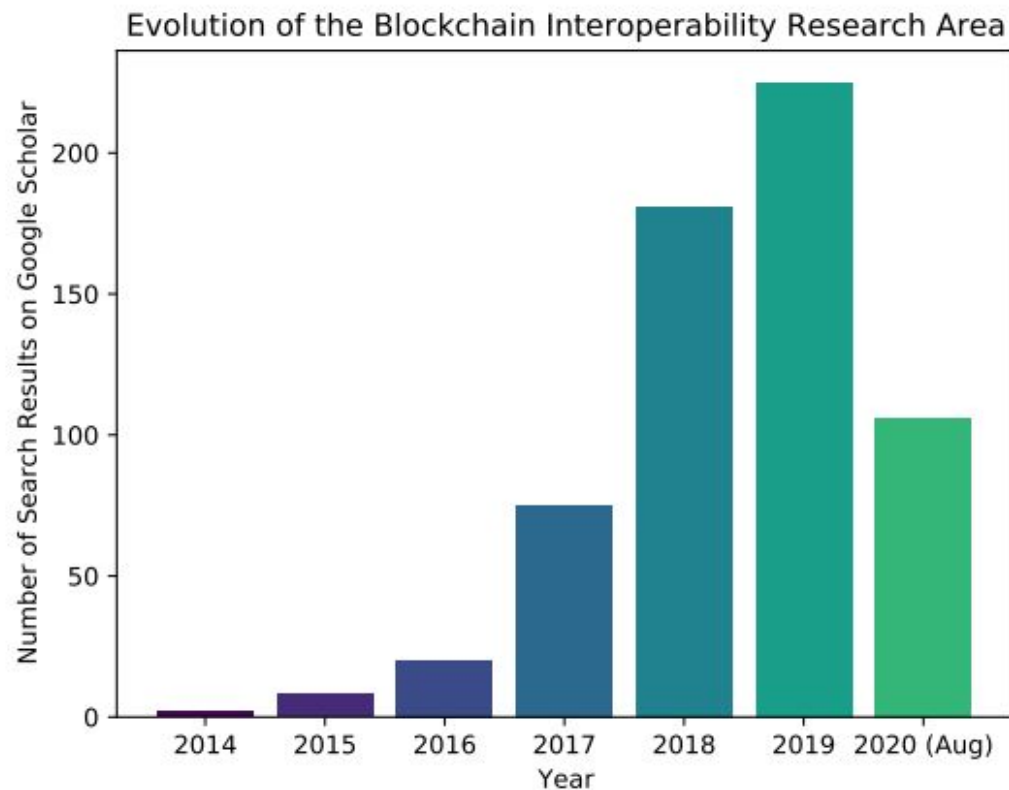
https://arxiv.org/pdf/2005.14282.pdf

Fig. 1. Academic research trends on blockchain interoperability

Table 2. Categorization of blockchain interoperability solutions. Crytocurrency-directed approaches and Blockchain Engine solutions are primarily studied and developed by the industry, with Crytocurrency-directed approaches gaining tracking in the academia. Blockchain Connectors are studied both by the industry and academia.

Category	Subcategory	Main use case
Cryptocurrency-directed Approaches	Sidechains	Scalability, asset exchange
	Notary Schemes	Cryptocurrency exchanges
	Hashed timelocks	Cryptocurrency trading
	Hybrid	Enabling cross-chain assets

| **Blockchain Engines** | - | Creation of customized blockchains |

		customized blockchains
Blockchain Connectors	Trusted Relays	Efficient interoperation
	Blockchain-Agnostic	General protocols
	Blockchain of Blockchains	Cross-blockchain dApps
	Blockchain Migrators	Risk reduction

Table 2. Categorization of blockchain interoperability solutions. Crytocurrency-directed approaches and Blockchain Engine solutions are primarily studied and developed by the industry, with Crytocurrency-directed approaches gaining tracking in the academia. Blockchain Connectors are studied both by the industry and academia.

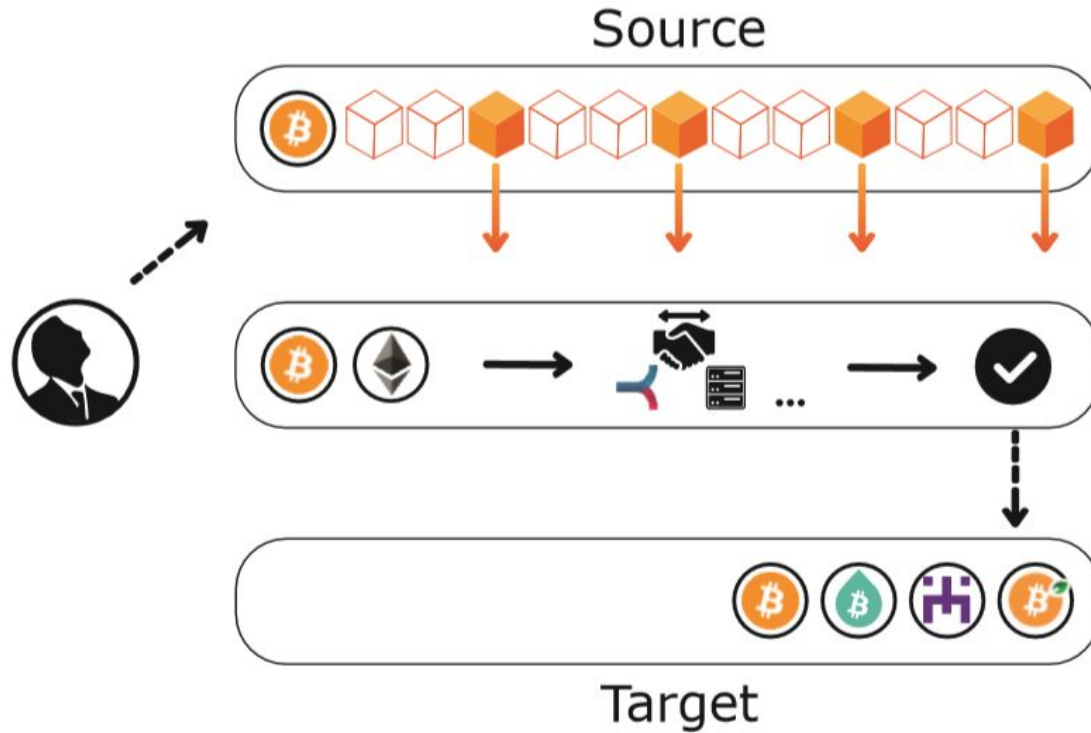| Category	Subcategory	Main use case
Cryptocurrency-directed Approaches	Sidechains	Scalability, asset exchange
	Notary Schemes	Cryptocurrency exchanges
	Hashed timelocks	Cryptocurrency trading
	Hybrid	Enabling cross-chain assets
Blockchain Engines	-	Creation of customized blockchains
Blockchain Connectors	Trusted Relays	Efficient interoperation
	Blockchain-Agnostic	General protocols
	Blockchain of Blockchains	Cross-blockchain dApps
	Blockchain Migrators	Risk reduction

Fig. 5. A general sidechain system [57]

Table 3. Comparison of *Sidechains* solutions

| Reference	Mainchain	Sidechain consensus	Summary	Strong points	Weak points	Roadmap
BTC Relay [57] ✓	Ethereum	×	Ethereum smart contract reading Bitcoin's blockchain	Simple solution relying on saving block headers	Limited functionality	None
POA Network [22] ✓	Ethereum	Proof of Authority	Applicational interoperability to Ethereum-based dApps	Inexpensive consensus	Validators confined to one country (geographic concentration)	POA-based stable token
Liquid [24, 117] ✓	Bitcoin	Strong Federations	Strong federation-based settlement network	Strong federation of functionaries maintain the network	Consensus secured by specialized hardware	Wallet and mining services
Loom Network [7] ✓	Ethereum	Delegated proof of stake	dApp platform with interoperability capabilities	Support for a high number of tokens	Closed source solution	Integrations with major blockchains
Zendoo [67]	Bitcoin	zk-Snark*	Sidechain creation platform	zk-Snark solution allows the mainchain to verify the sidechain without disclosing sensitive information	zk-Snarks are computationally expensive	Further specification of the protocol
RSK [96] ✓	Bitcoin	DECOR+	Federated sidechain, in which RBTC is tethered to BTC	Merge mining allows reutilization of work	Relies on PoW, energetically inneficient	Decentralized bridge with Ethereum
Blocknet [49] ✓	Ethereum	Proof of stake	Ethereum-based blockchain with interoperability capabilities	Blocknet protocol allows trustless blockchain interoperability	Currently limited to digital assets	EOS/NEO/other integrations

✓ Our description was endorsed

× Not specified

∗ Although zk-Snarks are not a consensus algorithm, consensus on which operations were performed at each sidechain is obtained through a process that uses zk-Snarks to generate proofs of sidechain state that, on its turn, generate certificate proofs for the mainchain
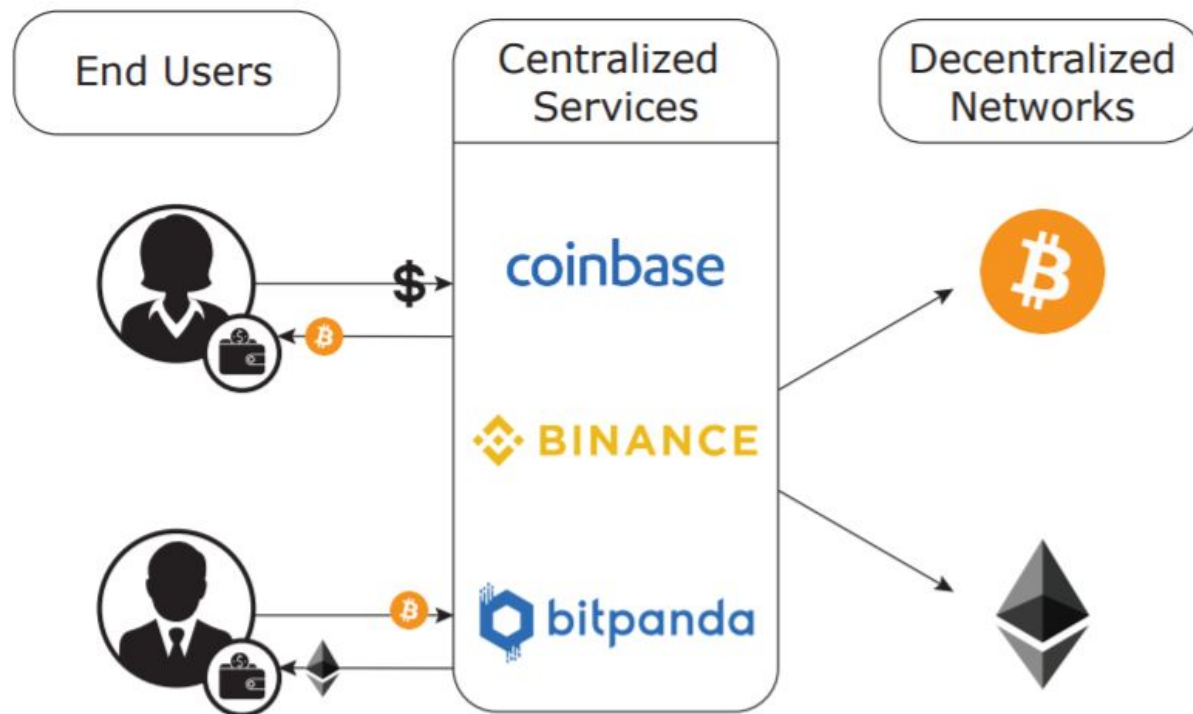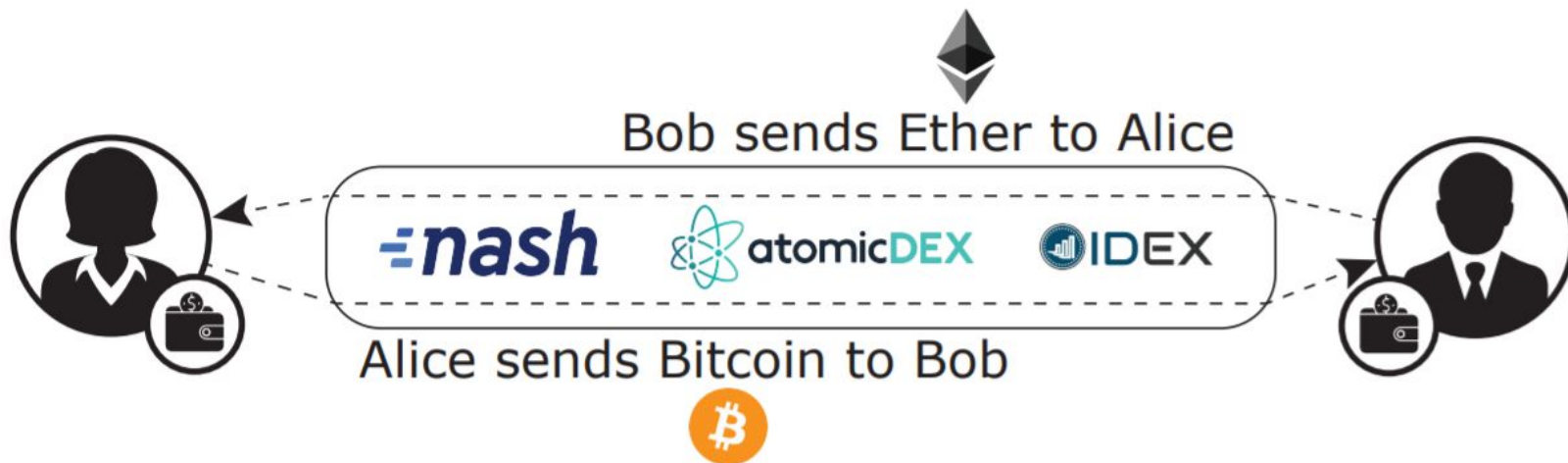
Source: XClaim presentation
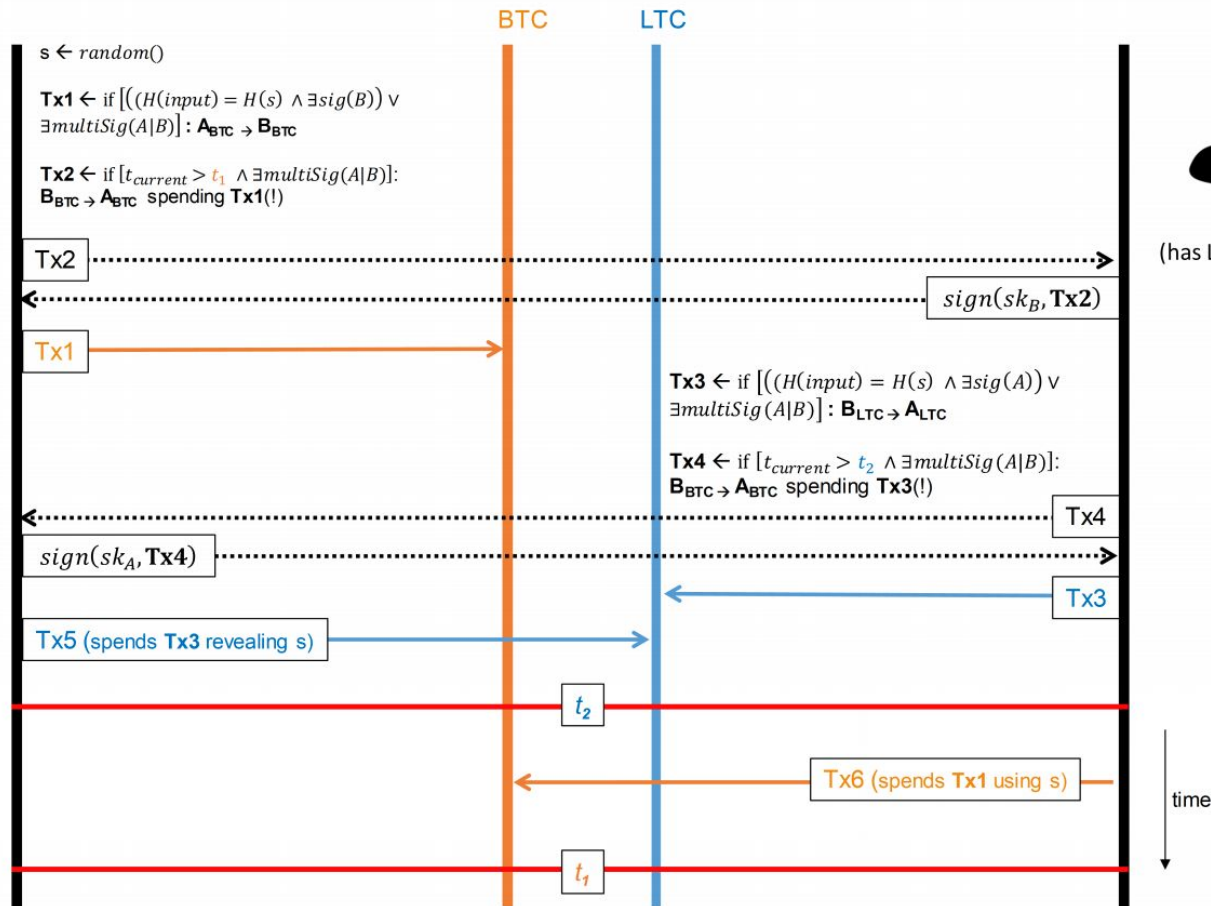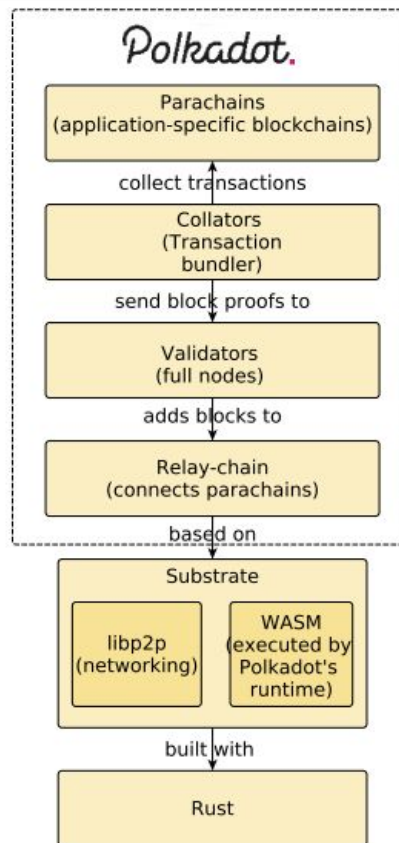
❏ *Blockchain Engines are frameworks that provide reusable data, network, consensus, incentive, and contract layers for the creation of customized blockchains, to power decentralized applications, that interoperable between each other.*

Fig. 10. Polkadot's stack [181, 187]

Connecting the dots

Relay Chain

The heart of Polkadot, responsible for the network's shared security, consensus and cross-chain interoperability.

Parachains

Sovereign blockchains that can have their own tokens and optimize their functionality for specific use cases.

Parathreads

Similar to parachains but with a pay-as-you-go model. More economical for blockchains that don't need continuous connectivity to the network.

Bridges

Allow parachains and parathreads to connect and communicate with external networks like Ethereum and Bitcoin.

Consensus Roles

Nominators

Secure the Relay Chain by selecting trustworty validators and staking dots.

Validators

Secure the relay chain by staking dots, validating proofs from collators and participating in consensus with other validators.

Collators

Maintain shards by collecting shard transactions from users and producing proofs for validator.

Fishermen

Monitor the network and report bad behavior to validators. Collators and any parachain full node can perform the fisherman role.

Table 8. Comparison of *Blockchain Connector* solutions

|	Reference	Cross blockchain transaction validation	Protocol	Supported Blockchains	Public PoC
Blockchain Connecting Protocols	Wang et al., [150]	Validators, nominators, surveillants, and connectors	PBFT	×	!
	Jin & Dai, [84]	×	×	×	!
	Ding et al., [55]	Validators Gateways	3-Way handshake	×	!
	Hardjono et al. [72, 73]	Blockchain Gateways (analogous to ISP networks)	×	×	!
	Montgomery et al., [111]* ✓	Interoperability validators	Direct transfer between requestors	Private	✓
	Borkowski et al., [37]	Observers	PBTs, claim-first transactions, deterministic witnesses	Public	✓
	Amiri et al., [19]	Blockchain views, internal and external transactions	Ordering: separate set of orderers, hierarchical consensus, and one-level consensus)	Private	!
	Abebe et al., [16]	Relay Service and Verifiable Proofs	System contracts, communication protocol. protocol buffers	Private	!
	Vo et al., [139]	×	×	×	!
	Kan et al., [87]	Router blockchain	3-phase-commit Protocol	×	!

README.md

HYPERLEDGER CACTUS

Hyperledger Cactus

`license Apache-2.0` `cii best practices in progress 89%` `issues 57 open` `build failing`

This project is an *Incubation* Hyperledger project. For more information on the history of this project see the Cactus wiki page. Information on what *Active* entails can be found in the Hyperledger Project Lifecycle document.

Hyperledger Cactus aims to provide Decentralized, Secure and Adaptable Integration between Blockchain Networks. Hyperledger Cactus is currently undergoing a major refactoring effort to enable the desired to-be architecture which will enable plug-in based collaborative development to increase the breadth of use cases & Ledgers supported.
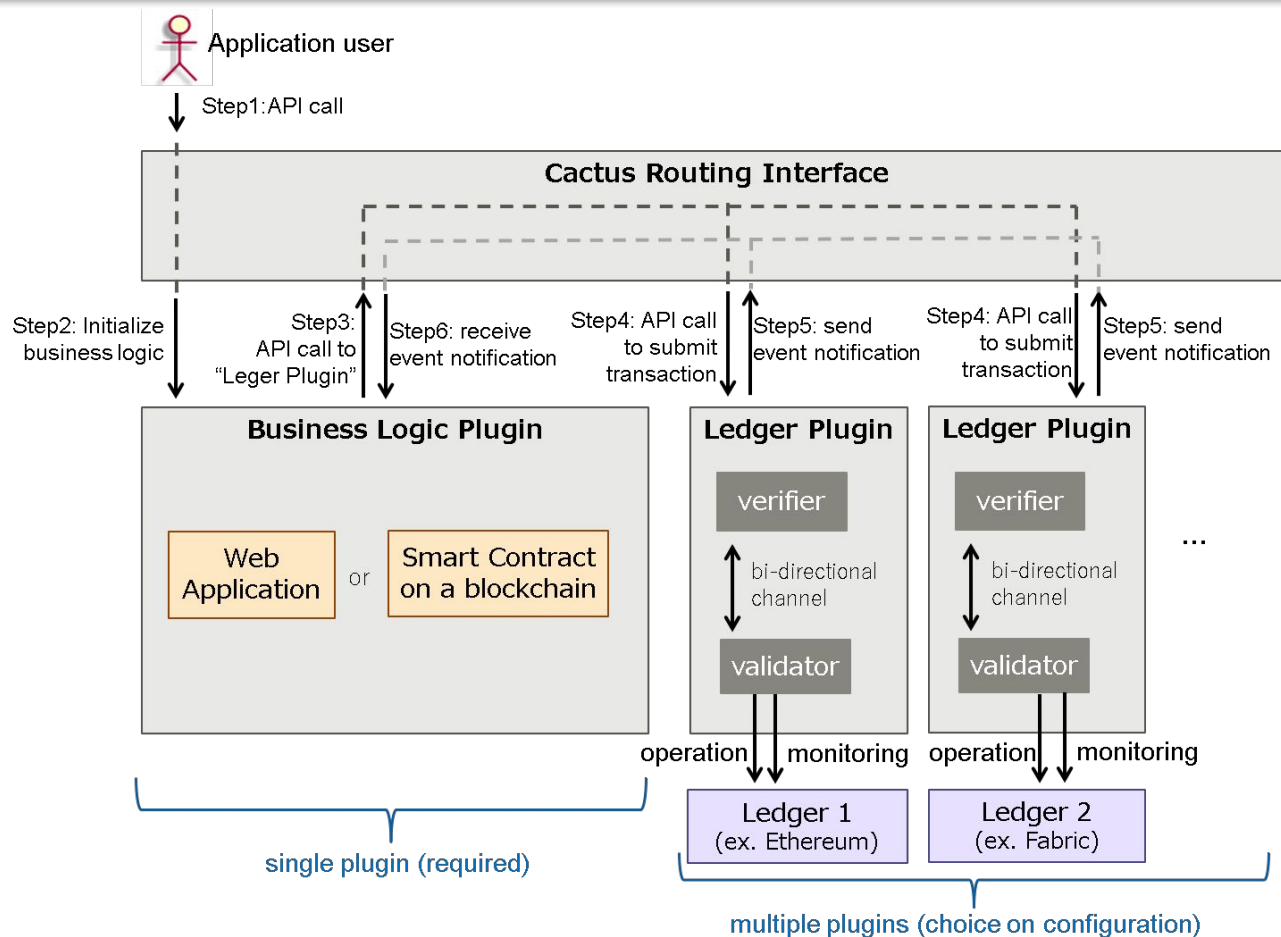
Blockchain of Blockchains	Verdian et al, [145]* ✓	BPI, Messaging, Filetering and Ordering layers	Posets and order theory	Public	!
	Liu et al., [102]	USM, NSL, UIP	NSB, ISC, HTE, PROT(BC) protocols	Public	✓
	Block Collider [83]* ✓	Base tuples, FIX	Proof of Distance	Public	✓
Blockchain Migrators	Frauenthaler et al., [62]	Notary Scheme	Adapters	Public	✓
	Scheid et al., [128]	Notary Scheme	Adapters	×	!

✓ Our description was endorsed
∗ Considered grey literature
! Lacks implementation or implementation is not public
× Not defined or not applicable

TABLE II
WEIGHTS USED BY THE FRAMEWORK.

Weight	Meaning
0	No importance
1	Very low importance
2	Low importance
3	Medium importance
4	High importance
5	Very high importance

TABLE III
SCORE DEFINITIONS USED BY THE FRAMEWORK.

Score	Meaning
0	Does not satisfy
1	Partly satisfies
2	Substantially satisfies
3	Almost satisfies
4	Fully satisfies

TABLE IV
AN EXAMPLE OF A WEIGHTED RANKING WITH TWO BLOCKCHAINS.

Metric	Weight	Blockchain A		Blockchain B	
		Score	W. Score	Score	W. Score
M1	5	4	20	3	15
M2	3	4	12	4	12
M3	4	4	16	2	8
M4	5	2	10	4	20
M5	3	3	9	3	9
M6	3	3	9	3	9
M7	5	3	15	4	20
M8	4	3	12	2	8
Total	**32**	**26**	**103**	**25**	**101**

❏   Emerging standards:

❏   ISO Technical Committee 307 - (ISO/TC/SG7)

❏   IEEE 2418.2-2020 standard

❏   EU Blockchain Observatory & Forum

❏   IETF

❏   Supporting Technologies:

❏   Decentralized Identifiers & Verifiable Credentials

❏   Cross-chain programming languages (DAML/HSL)

❏   Interoperability public-private blockchains

❏ Interoperability public-private blockchains

❏ Blockchain Migration

❏   Interoperability public-private blockchains

❏   Blockchain Migration

❏   Decentralized identity for blockchain participants (identity portability)

- ❏ Interoperability public-private blockchains

- ❏ Blockchain Migration

- ❏ Decentralized identity for blockchain participants (identity portability)

- ❏ Blockchain interoperability standards

- ❏ Interoperability public-private blockchains

- ❏ Blockchain Migration

- ❏ Decentralized identity for blockchain participants (identity portability)

- ❏ Blockchain interoperability standards

- ❏ Blockchain of blockchains approach

❏ Blockchain interoperability is a research area in expansion, with practical applications

❑ Blockchain interoperability is a research area in expansion, with practical applications

❑ Blockchain interoperability can promote flexibility, portability of solutions, and risk reduction, enabling enterprises to invest in this technology, with extra safety guarantees

❏ Blockchain interoperability is a research area in expansion, with practical applications

❏ Blockchain interoperability can promote flexibility, portability of solutions, and risk reduction, enabling enterprises to invest in this technology, with extra safety guarantees

❏ Blockchain interoperability can ultimately promote mass adoption of blockchain, as data and value silos can be eliminated

master ⌄ | 2 branches | 1 tag

Go to file | Add file ⌄ | ⬇ Code ⌄

RafaelAPB docs: update README | a3a29b2 9 days ago | 🕐 30 commits

📁 .github	Create PULL_REQUEST_TEMPLATE.md	last month
📁 source	chore: Review Lab06 guide	23 days ago
📁 support	chore: move labs	9 days ago
📄 CONTRIBUTING.md	docs: add contributing.md	3 months ago
📄 LICENSE	Initial commit	4 months ago
📄 README.md	docs: update README	9 days ago
📄 ebt.png	docs: add course logo	3 months ago

About

A Hyperledger Lab focused developing materials for a university course.

📖 Readme

⚖ Apache-2.0 License

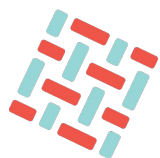**Releases**

🏷 1 tags

Create a new release

Packages

No packages published
Publish your first package

README.md

Enterprise Blockchain Technologies

##A Hyperledger Fabric's v2.x University Course 🎓

Blockchain Interoperability

[Rafael Belchior](https://rafaelapb.github.io/)

rafael.belchior@tecnico.ulisboa.pt
https://rafaelapb.github.io/