UNIVERSITY *of* NICOSIA

Week 5 – Session 10

Interoperability and Scalability in Blockchains

BLOC 512: Blockchain Systems and Architectures

Session Objectives

- To discuss data sharing and interoperability in blockchains, where two or more separate blockchain networks or applications enable cross-chain data sharing.
- To discuss blockchain scalability techniques for Layer 1 and Layer 2 networks, as well as, between different blockchain networks.

Agenda

1. Blockchain interoperability
2. Sidechains
3. Bridges
4. Blockchain scalability

Blockchain interoperability

Do you agree with the below statement?

“The challenge of interoperability is not only a technology problem, but even more so a problem in terms of governance, data ownerships and commercial business models.”

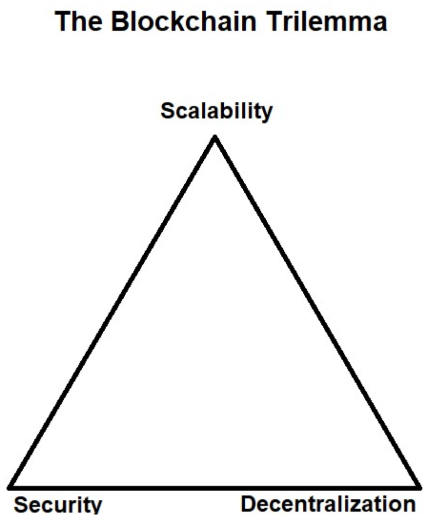
Nadia Hewett, Blockchain and Digital Currency Project Lead at the World Economic Forum

Blockchain adoption – key challenges

- Interoperability
- Scalability
- Regulation
- Adoption
- Lack of standardization

The Blockchain Trilemma

- The disadvantages (limitations) of decentralised blockchain systems are summarized by the **blockchain trilemma**, proposed (in this form) by Vitalik Buterin.
- It states that blockchains **by desing** can **only** be:
  - Scalable and Secure, **but not Decentralized**
  - Secure and Decentralized, **but not Scalable**
  - Scalable and Decentralized, **but not Secure**
- The blockchain trilemma is an oversimplification of the **mutually exclusive choices** made by developers, users, speculators etc
- It explains why so many different blockchain protocols exist
  - **Different priorities**, result in **different design tradeoffs**



Blockchain archipelago and its challenges

- World Economic Forum - *"Balkanised in Silos"*
- Scattered collection of siloed blockchain ecosystems
- Many with weak network of nodes
- How can we enable:
    - Data-sharing?
    - Cross-chain interactions?
    - State transfers?

Bitcoin
Ethereum
EOS
Ripple
Tezos
CARDANO

Blockchain interoperability definition

Interoperability definition

“The ability to exchange data with other platforms, including those running different types of blockchains, as well as with the off-chain world” (EU Blockchain Observatory and Forum, 2019).

Interoperability:

- Allows disparate blockchains to communicate with each other.
- Ability to share, see, and access information across different blockchains without the need for an intermediary

Blockchain interoperability – key features

- Facilitates the integration with existing systems,
- Initiates transactions on other networks,
- Conducts transactions with other chains,
- Transacts between deployments on the same chain by integrating apps and making it easy to switch one underlying platform for another.
- Enables smooth information sharing,
- Supports easier execution of smart contracts,
- Offers a more user-friendly experience,
- Provides the opportunity to develop partnerships, and the sharing of solutions

Blockchain interoperability – Mashup APIs approach

Two approaches for Blockchain interoperability: (a) Mashup APIs, (b) network of networks

Mashup APIs

- Blockchains interact through a consistent API
- Think of this API like a USB or an adapter for electrical devices
- API purpose: to serve as a glue to bridge multiple blockchains
- Multiple capabilities defined in smart contracts and data models
- Lack of a governance structure
  - → flexible and practical
  - → poor choice for organizing interoperability in the long run.

Blockchain interoperability – network of networks approach

Two approaches for Blockchain interoperability: (a) Mashup APIs, (b) network of networks

Network of networks

- Efficient and scalable approach
- Joint effort to identify standards
- **Network of networks (NoN) = web of interconnected networks**
- NoN architecture allows organizations to
  - connect and transact with multiple blockchains
  - Create channels to connect with various chains
  - Open up market for new solutions
  - Reduce complexity
- Now gains momentum and blockchain hubs emerge

Blockchain interoperability – network of networks approach

Existing practice

- “1st wave” - public blockchains interoperability
- Practices used include:
  - sidechains (or relay chains),
  - notary schemes
  - timed hash-locks.

- “2nd wave” interoperability
- Private to Private
- Private to public blockchains

Ways to solve interoperability

- Hub and spoke (bridge approach)
- Example:
  - Blockchain A and Blockchain B are connected through Blockchain C.
  - C maintains the ledger for the transactions and messaging between A and B

- Off-chain (so called non-blockchain interoperability)
  - Oracles
  - Atomic swaps
  - State channels

Blockchain interoperability – Interesting projects

- Cosmos
- Polkadot
- Chainlink
- Hybrix
- Wachain
- Aion
- Ark
- ICON
- Transledger
- Overledger
- Loom
- Proof of Authority Network
- Liquid
- Rootstock (RSK)

How blockchain interoperability is achieved?

Sidechains: sidechains are separate blockchain networks that are compatible with some other chain (aka the parent chain). Each sidechain has its own consensus mechanism, protocol rules, tokens and security parameters. These sidechains generally have their own specific use cases that are distributed accordingly in order to improve the overall ecosystem's processing efficiency and self-sovereignty.

Oracles: oracles bridge the information gap between on-chain and off-chain environments. The main role of Oracles is to feed off-chain data to blockchain-enabled smart contracts and contribute to blockchain interoperability by ensuring that different ecosystems are referring to a common source of truth.

Bridges and swaps: Cross-chain bridges enable a digital asset owned by a party to be locked on one chain while an identical asset is "minted" on another chain and sent to an address owned by the original owner. In contrast, atomic swaps enable users to exchange tokens from different blockchain networks in a decentralized manner. Both are automatically enabled through the use of smart contracts and play a central role in facilitating seamless cross-chain value transfers.

Source: https://www.gemini.com/cryptopedia/why-is-interoperability-important-for-blockchain#section-how-is-blockchain-interoperability-achieved

Sidechains

Sidechains – definitions and key features

- **Sidechains:** secondary blockchains connected to some main blockchain without affecting the main chain.
- We can use sidechains for enabling interaction between the multiple chains and to make blockchains more scalable.

1. **Pegged Sidechains:**
    - Pegged Sidechains are used to transfer assets between multiple blockchains. Pegged sidechains is nothing but a blockchain that is attached to the parent chain (blockchain) through a pegging mechanism:
        - **One-way peg (1WP):** this mechanism enables the transfer of assets when one blockchain destroys its assets publicly and upon deletion of these assets a new blockchain will create new assets.
        - **Two-way peg (2WP):** enables a bidirectional transfer of assets between the parent chain and the sidechain at a fixed deterministic exchange rate by simply reusing the existing bitcoin currency. Despite this bidirectional transfer of assets between multiple blockchains they are isolated i.e., any cryptographic break in one blockchain will not be reflected in the other blockchain.

Sidechains – definitions and key features

2. **Pegged Sidechains:**
   - **Federated Peg (or Multi-signature):** A cluster of notary nodes are controlling the lockboxes (i.e., a special address (lockbox) where assets are locked). The lockbox needs to have n of m signatures from the group of nodes in order to make the exchange. In this option trust is placed on a group of nodes.
   - **SPV (Simple Payment Verification) proofs**: is a way to cryptographically prove to a sidechain that a transaction has been initiated on mainchain that locks funds for an address on a sidechain.

- **Other key features**
  - Sidechain consensus may be different from the mainchain's consensus
  - Isolated from the main chain
  - Sidechains can
    - add new functionalities
    - Improve privacy
    - Enhance security
  - Relatively new and immature

2WP – scenario (1/2)

Scenario: A sidechain is attached to a public and permissionless primary blockchain with a 2WP.

Primary blockchain:

- operates a cryptocurrency called MainCoin
- Cannot execute non-trivial smart contracts due to the absence of a Turing complete Virtual Machine.

The sidechain:

- operates its own cryptocurrency of named SideCoin,
- has the capability of executing non-trivial smart contracts
- offers significantly higher transaction rate (i.e., higher TPS) than the mainchain.

Singh et al 2020

- 2WP: allows transfers of MainCoins to the sidechain and vice versa
- Fixed rate: 1 MainCoin = 1 SideCoin.
- Suppose a user wishes to transfer 5 MainCoins to the sidechain to play a rock, paper and scissor game with another random user based on a smart contract implemented on the sidechain
- The winner takes all
- Draw results in no exchange of coins), then this system

2WP – scenario (2/2)

- **Step 1:** The user sends 5 MainCoins to a special address (lockbox) where the coins are locked and can only be unlocked once funds on sidechain are locked and transferred back to the mainchain.
- **Step 2:** Once the funds locked on the mainchain, 5 SideCoins are created on the sidechain.
- **Step 3:** The user can now use these SideCoins to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of SideCoins.
- **Step 4:** Depending on the outcome of the game, 10 SideCoins are transferred to the winner or 5 SideCoins are transferred back to their respective owners (draw).
- **Step 5:** The user(s) can then transfer their funds back to the mainchain, which essentially means that the SideCoins will be locked/destroyed on the sidechain and an equivalent number of MainCoins will be unlocked on the mainchain from the lock-box (in step 1) after SideCoins are destroyed on the sidechain.

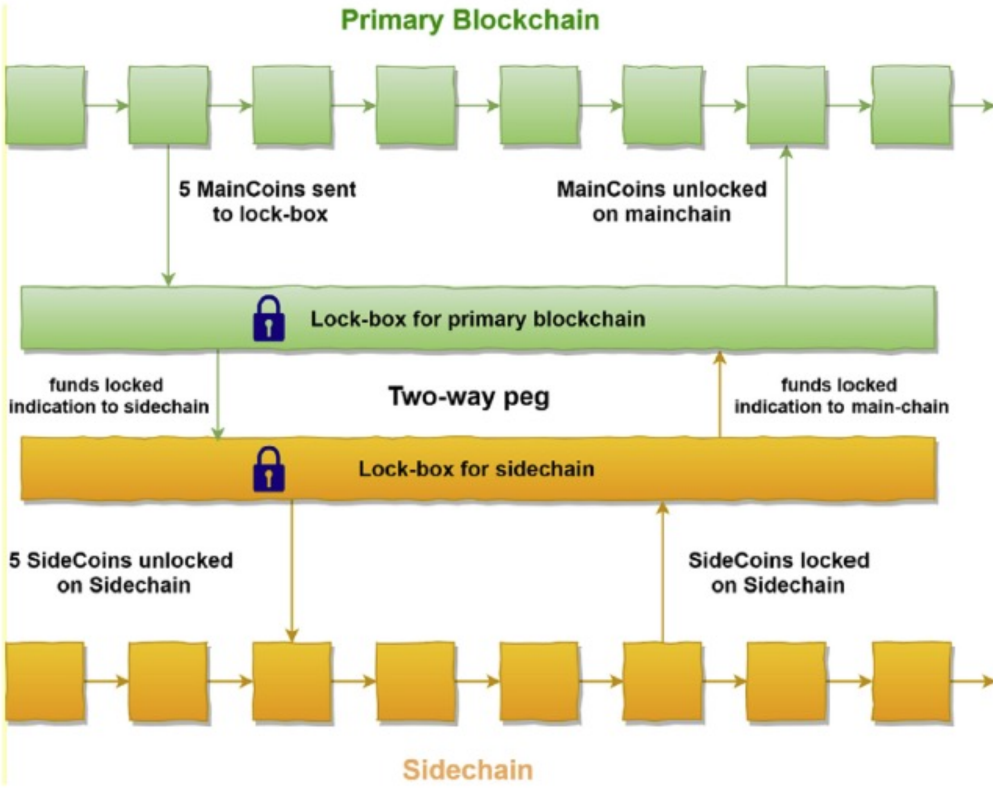

Primary Blockchain
5 MainCoins sent to lock-box
MainCoins unlocked on mainchain
Lock-box for primary blockchain
funds locked indication to sidechain
Two-way peg
funds locked indication to main-chain
Lock-box for sidechain
5 SideCoins unlocked on Sidechain
SideCoins locked on Sidechain
Sidechain

Fig. 1. Transfer of funds between mainchain and sidechain with a two-way peg.

Singh et al 2020

Sidechains – observations for the above scenario

- Total number of MainCoins in the mainchain ecosystem remains the same
- Adding new functionality to the above scenario (e.g., execution of non-trivial smart contracts and faster transaction rates) will not impact the number of MainCoins
- The implementation of these new features with sidechains do not require any major change in the core features or consensus protocol of the mainchain itself.

Singh et al 2020

Sidechains - centralized 2WP

- A trusted 3rd entity holds custody of the locked funds
- The trusted 3rd party is responsible for the locking and unlocking of funds on both the mainchain and its sidechain. This causes changes to the steps reported in the main scenario
- **Step 1:** The user sends 5 MainCoins to a lock-box address maintained by a *trusted centralized entity* meant for regulating fund transfer between the two blockchains.
- **Step 2.** The trusted entity then generates 5 SideCoins on the sidechain and sends these funds to the user's requested address.
- **Step 3.** The user can now use these SideCoins to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of SideCoins.
- **Step 4.** Depending on the outcome of the game, 10 SideCoins are transferred to the winner or 5 SideCoins are transferred back to their respective owners (in case of a draw).
- **Step 5.** The user(s) can then transfer their funds back to the mainchain, by sending their SideCoins to the lock-box address on the sidechain which is also maintained by the same trusted central entity. The user(s) also specify the address where the funds need to be sent on the mainchain.
- **Step 6.** The trusted central entity destroys the SideCoins on the sidechain and sends the equivalent number of MainCoins to address specified by the user(s).

Singh et al 2020

Sidechains - centralized 2WP - pros and cons

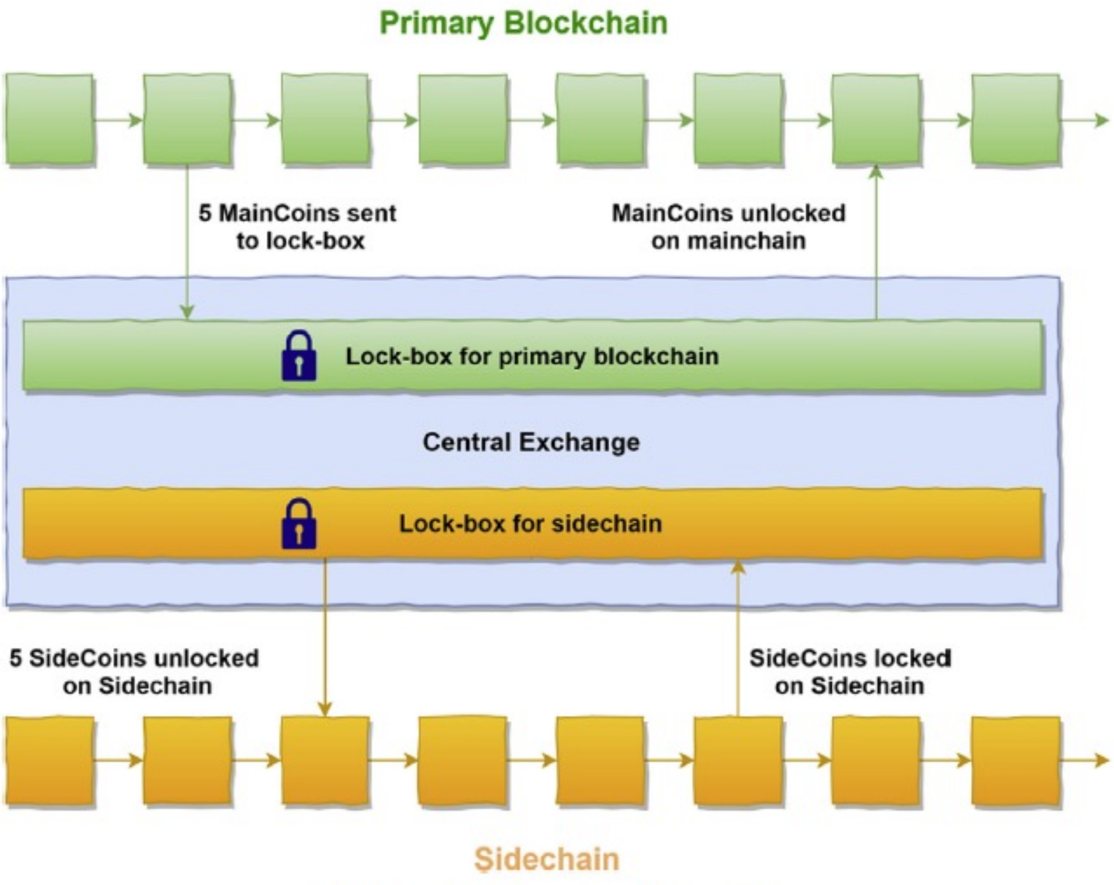

Primary Blockchain
5 MainCoins sent to lock-box
MainCoins unlocked on mainchain
Lock-box for primary blockchain
Central Exchange
Lock-box for sidechain
5 SideCoins unlocked on Sidechain
SideCoins locked on Sidechain
Sidechain

Fig. 2. Centralized two-way peg implementation.

- **Advantages**
  - easy to visualize and implement
  - Fast transfer of funds among chains

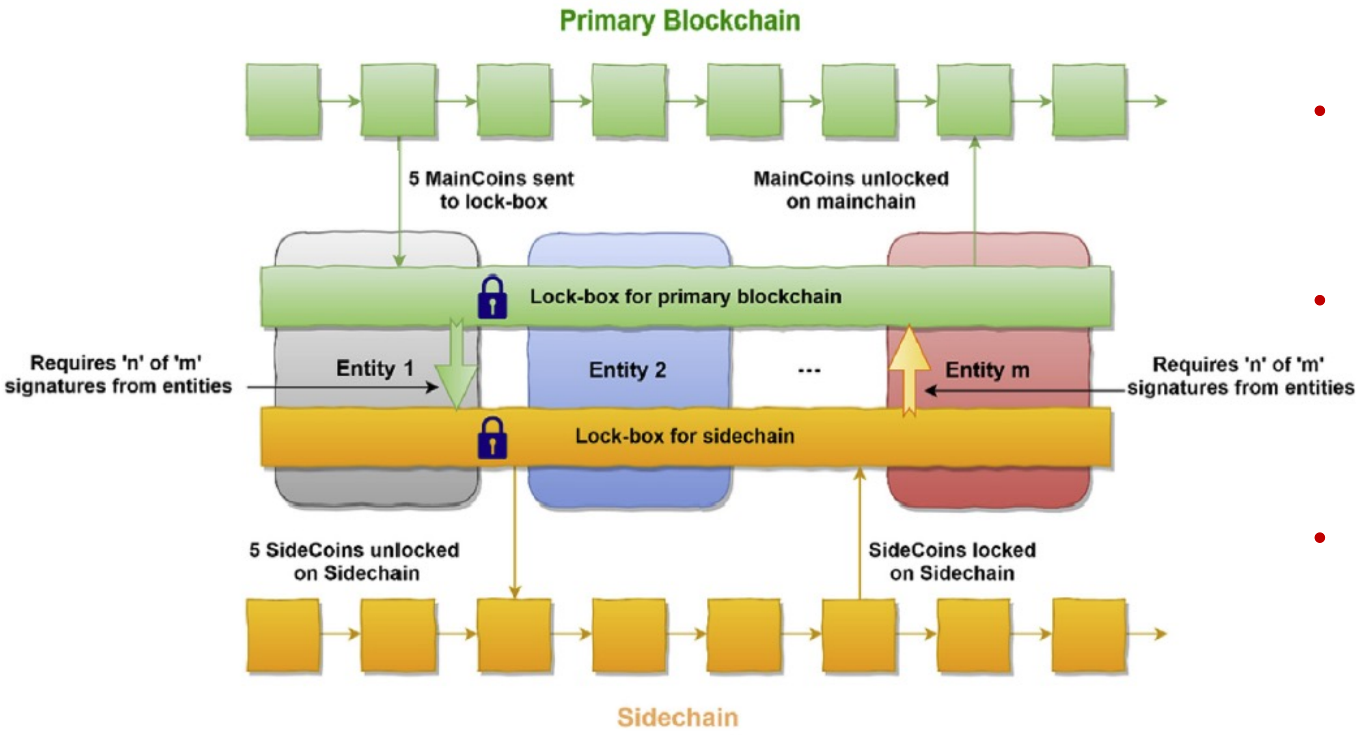
- **Disadvantages**
  - Bitcoin, Ethereum and other public blockchains were designed to improve political decentralization
  - Single point of failure
  - If the trusted entity is malicious, it can result to loss of locked funds

Singh et al 2020

Sidechains - multi-signature or federated 2WP

- **Step 1:** The user sends 5 MainCoins to a lock-box address maintained by a federation of entities. The entities then sign this transaction after verifying that the funds have been received in the lockbox.
- **Step 2**: If the majority sign the transaction, then the federation generates 5 SideCoins on the sidechain and sends these funds to the user's requested address.
- **Step 3:** The user can use these SideCoins to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of SideCoins.
- **Step 4:** Depending on the outcome of the game, 10 SideCoins are transferred to the winner or 5 SideCoins are transferred back to their respective owners (in case of a draw).
- **Step 5:** The user(s) can then transfer their funds back to the mainchain, by sending their SideCoins to the lock-box address on the sidechain which is also maintained by the same federation of entities. The user(s) also specify the address where the funds need to be sent on the mainchain.
- **Step 6:** The entities of the federation again sign the transaction after verifying that the funds have been received in the lock-box on the sidechain.
- **Step 7:** If the majority of the entities sign the transaction, then the federation destroys the SideCoins on the sidechain and sends the equivalent number of MainCoins to address specified by the user(s).
- **Step 8:** In the case when the majority of the entities within the federation do not reach an agreement regarding a transaction, then the funds are sent back to their respective owners on either chain.

Sidechains - multi-signature or federated 2WP – pros and cons



Primary Blockchain
5 MainCoins sent to lock-box
MainCoins unlocked on mainchain
Lock-box for primary blockchain
Requires 'n' of 'm' signatures from entities
Entity 1
Entity 2
...
Entity m
Requires 'n' of 'm' signatures from entities
Lock-box for sidechain
5 SideCoins unlocked on Sidechain
SideCoins locked on Sidechain
Sidechain

Fig. 3. Federated two-way peg implementation.

- A group of entities or notaries control the lock-box.
- The group holds custody of the locked funds and regulates fund transfer chains
- The fund transfer takes place only when most of the entities sign the transaction

- **Advantages**
  - Improves decentralization
  - Could be implemented with specialized federation protocols for fast transfer of funds
- **Disadvantages**
  - Not fully decentralized (it relies on a small group of entities)
  - Security issues: lock-box funds could be stolen if the majority lose their private keys (e.g., a malicious internet attack)

Sidechains - Simplified Payment Verification (SPV)

- Simplified Payment Verification allows a lightweight client to prove that a given transaction was included in a legitimate block of the longest Proof-of-Work (PoW) blockchain
- Lightweight client:
  - No need to download the entire chain from the genesis block itself.
  - Only required to download the block headers of the entire blockchain, (much smaller in size than the actual block itself)
  - To verify if a given transaction was included in a legitimate block, an SPV client requests a proof of inclusion, in the form of a Merkle branch of that transaction.

Singh et al 2020

Sidechains - Simplified Payment Verification (SPV) - process

1. After a transaction is submitted for the transfer of funds from the mainchain to the sidechain or vice versa (i.e., the funds are locked in the lockbox), there is a confirmation period, which is strategically in place to allow miners to mine on top of the last block which consequently, allows the generation and submission of SPV proof.
2. The SPV proof is then submitted by the user and the block in which the his/her transaction is recorded is located.
3. The user then provides the hashes along the Merkle tree branch on which his/her transaction lies. This is done in the following manner:
   a. Suppose a user is looking to validate Transaction 2 (Fig. 5), he/she can obtain the hash of Transaction 1 and a combined hash of Transaction 3 and 4 i.e., Transaction (3, 4) from a number of other full nodes.
   b. With this information the user can compute the root hash of the Merkle tree in the block.
4. If these hashes all collectively hash to the original Merkle root of the transaction hash tree in that block, then the transaction is valid.
5. After an SPV proof is submitted there is a reorganization period in which other users may submit their own SPV proofs to contradict the user's transaction. The SPV proof in which more blocks have been mined is considered to be the correct proof and decides the fate of the transaction.

Singh et al 2020

Sidechains - Simplified Payment Verification (SPV) - scenario

- **Step 1**: The user sends 5 MainCoins to a lock-box address which is usually maintained by the miners of the network. Once the coins are locked on the mainchain, the user has to wait for a predetermined confirmation period to allow the mines to create new blocks to create SPV proofs
- **Step 2:** Once sufficient blocks are created by the miners, the user can submit an SPV proof verifying that the coins were locked on the mainchain.
- **Step 3:** After the SPV proof is submitted, the user has to wait for the reorg period where other users can submit their SPV proofs to nullify a fraudulent transactions, in case one has taken place.
- **Step 4:** After the SPV proof is verified 5 SideCoins are unlocked on the sidechain.
- **Step 5:** The user can now use these SideCoins to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of SideCoins.
- **Step 6:** Depending on the outcome of the game, 10 SideCoins are transferred to the winner or 5 SideCoins are transferred back to their respective owners (in case of a draw).
- **Step 7:** The user(s) can then transfer their funds back to the mainchain, by sending their SideCoins to the lock-box address on the sidechain and repeating the same process mentioned in steps 1–4 on the sidechain side.

Singh et al 2020

Sidechains - Simplified Payment Verification (SPV) – pros and cons

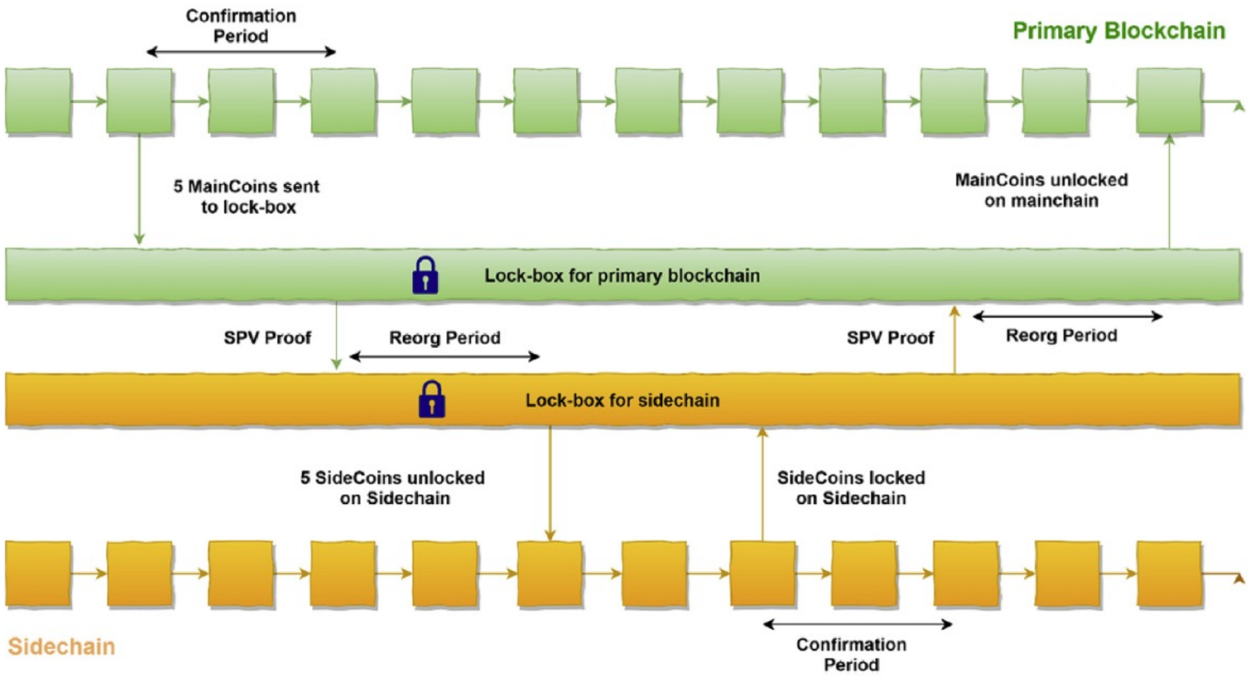

Confirmation Period
Primary Blockchain
5 MainCoins sent to lock-box
MainCoins unlocked on mainchain
Lock-box for primary blockchain
SPV Proof
Reorg Period
SPV Proof
Reorg Period
Lock-box for sidechain
5 SideCoins unlocked on Sidechain
SideCoins locked on Sidechain
Sidechain
Confirmation Period

Fig. 4. Two-way peg based on SPV proofs.

- **Advantages**
  - Decentralised solution
  - 3rd trusted party is eliminated
- **Disadvantages**
  - Slow (user needs to wait for confirmation and reorg periods before having access to his/her funds on either mainchain or sidechain.)

Singh et al 2020

Sidechains – Comparison of the 2WP designs

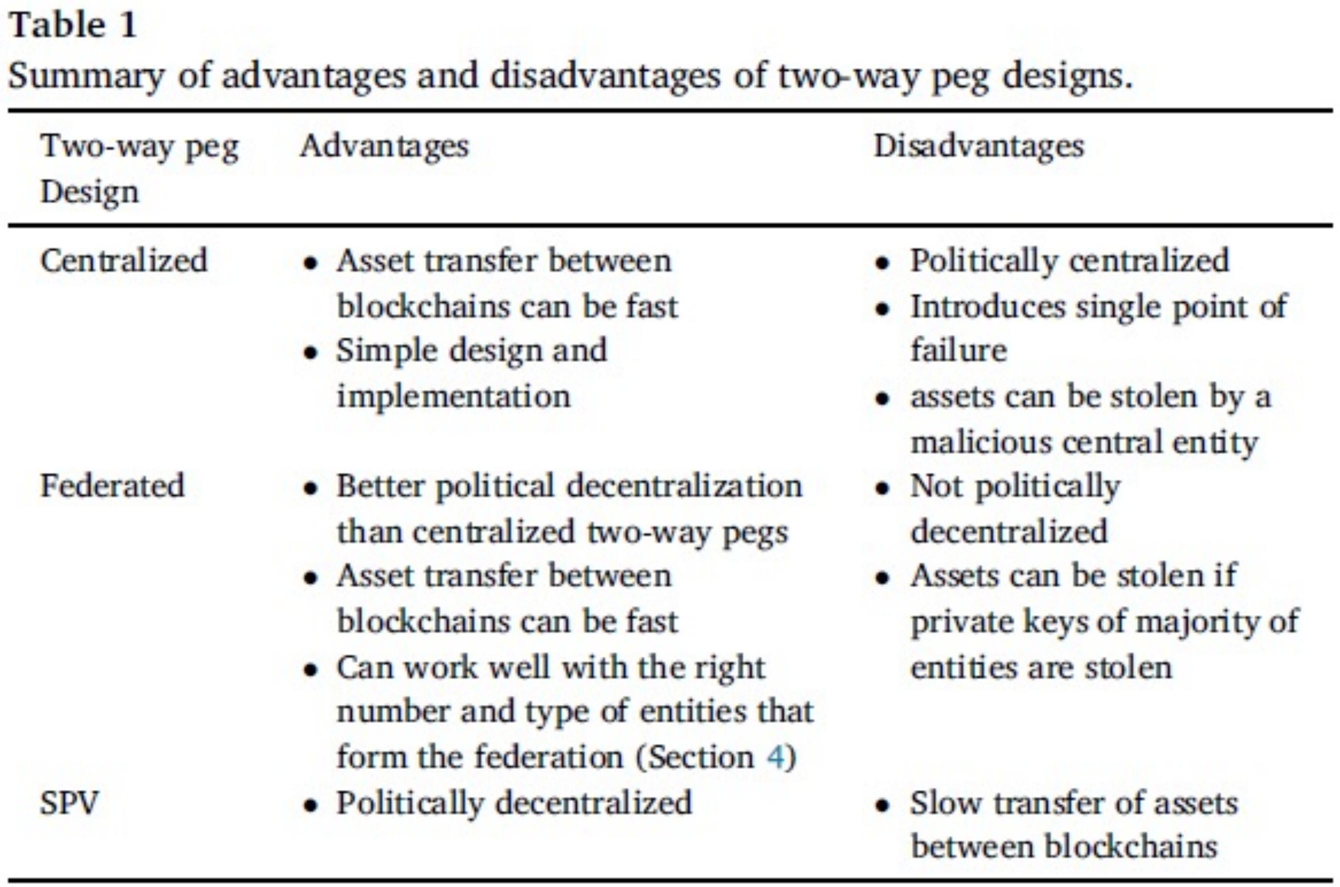


Table 1

Summary of advantages and disadvantages of two-way peg designs.

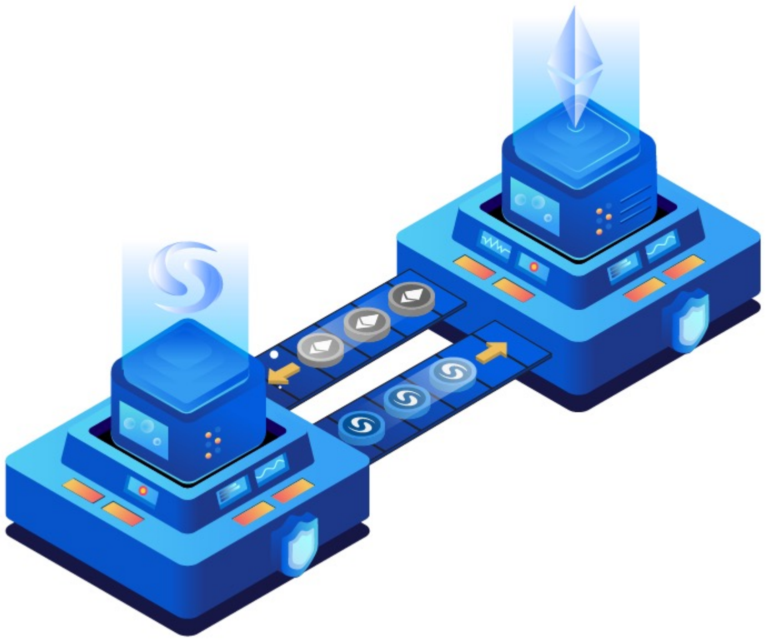
Two-way peg Design	Advantages	Disadvantages
Centralized	• Asset transfer between blockchains can be fast • Simple design and implementation	• Politically centralized • Introduces single point of failure • assets can be stolen by a malicious central entity
Federated	• Better political decentralization than centralized two-way pegs • Asset transfer between blockchains can be fast • Can work well with the right number and type of entities that form the federation (Section 4)	• Not politically decentralized • Assets can be stolen if private keys of majority of entities are stolen
SPV	• Politically decentralized	• Slow transfer of assets between blockchains

Singh et al 2020

Bridges

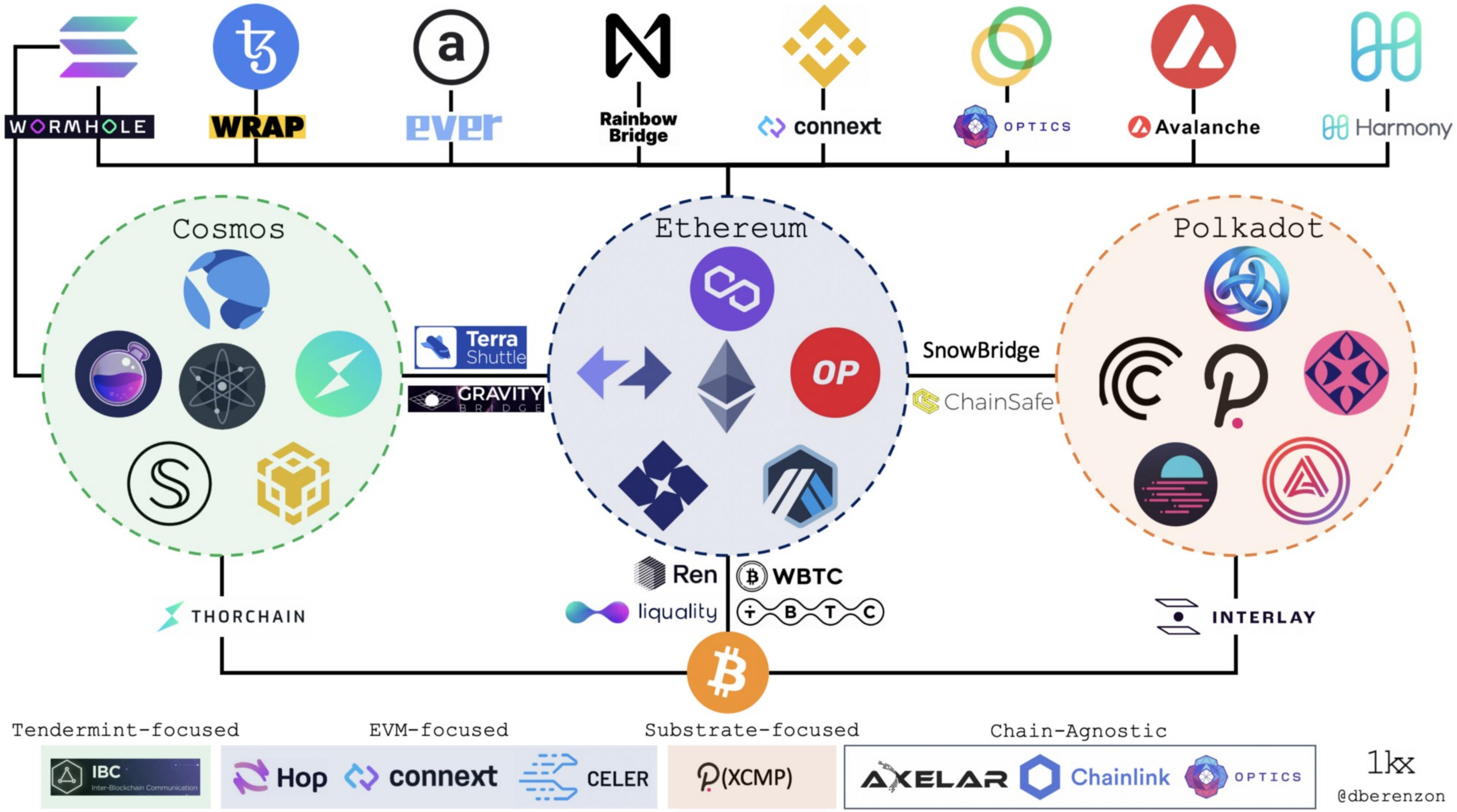
What is Blockchain Bridge?

- The main utility of bridge system is **transferring** information from one Layer 1 to one or more blockchain protocols (to enable cross-chain data sharing).
- Bridges are an important part of the blockchain ecosystem as they facilitate interactivity, through the transfer of information between L1 protocols.
- The "*transferred*" information can include:
  - Assets
  - Proofs
  - Contract calls
  - States



Source: https://chinadefi.com/866.html

Bridges visualized

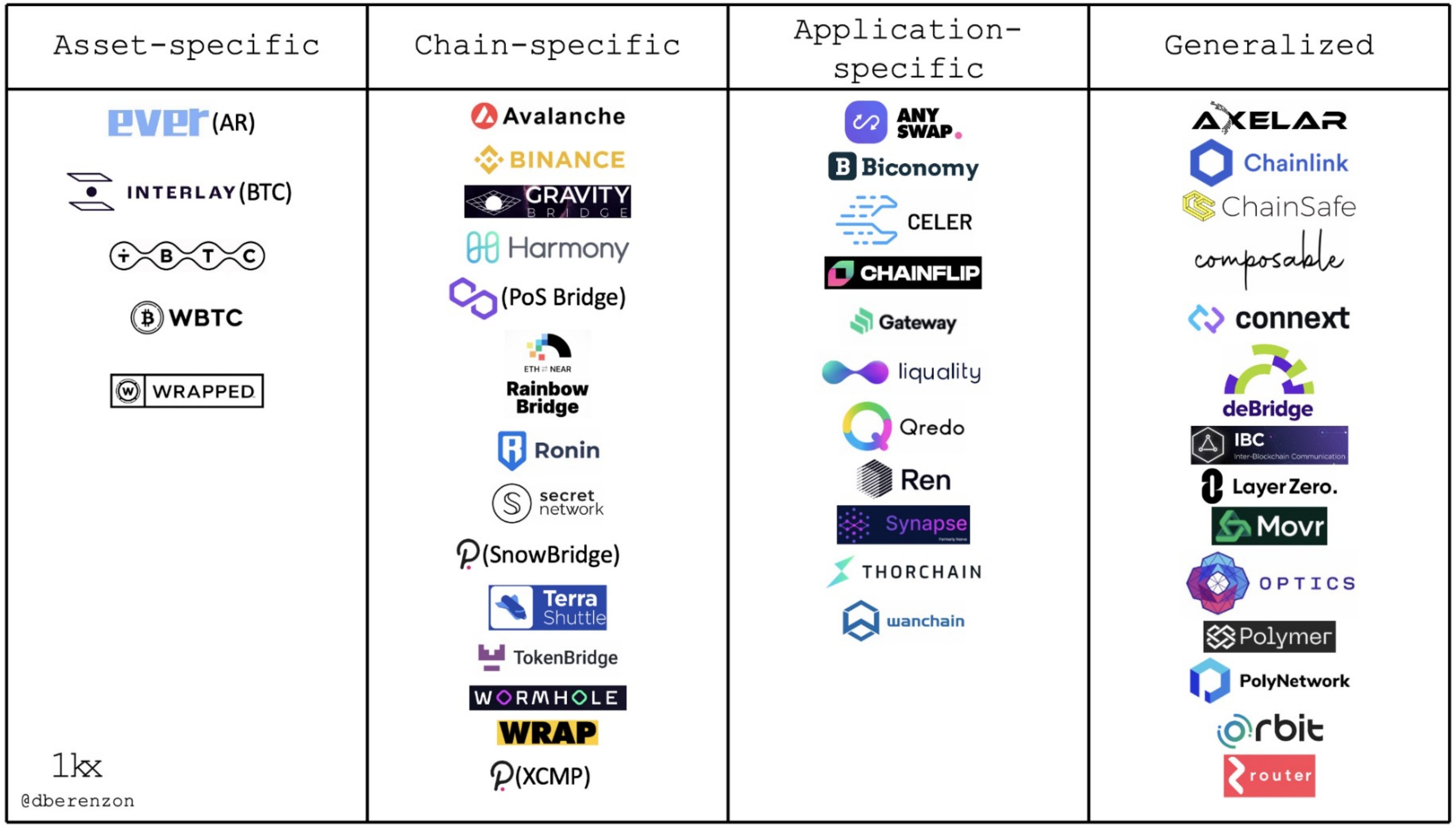


Source: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8

Bridge types

- Asset specific bridges are protocols that provide access to specific **asset** or assets that exist in other protocols. *“Wrapped”* assets are usually created which are fully collateralized by the underlining ones.
- Chain specific is a bridge that connects two **blockchains** with similar properties by locking or unlocking tokens, and subsequently minting or burning tokens.
- Application specific bridges are bridges that operate within certain specific dApps, for interoperability purposes.
- Generalized bridges are as the name suggests, transfer all kinds of information across various blockchains.

Bridge types

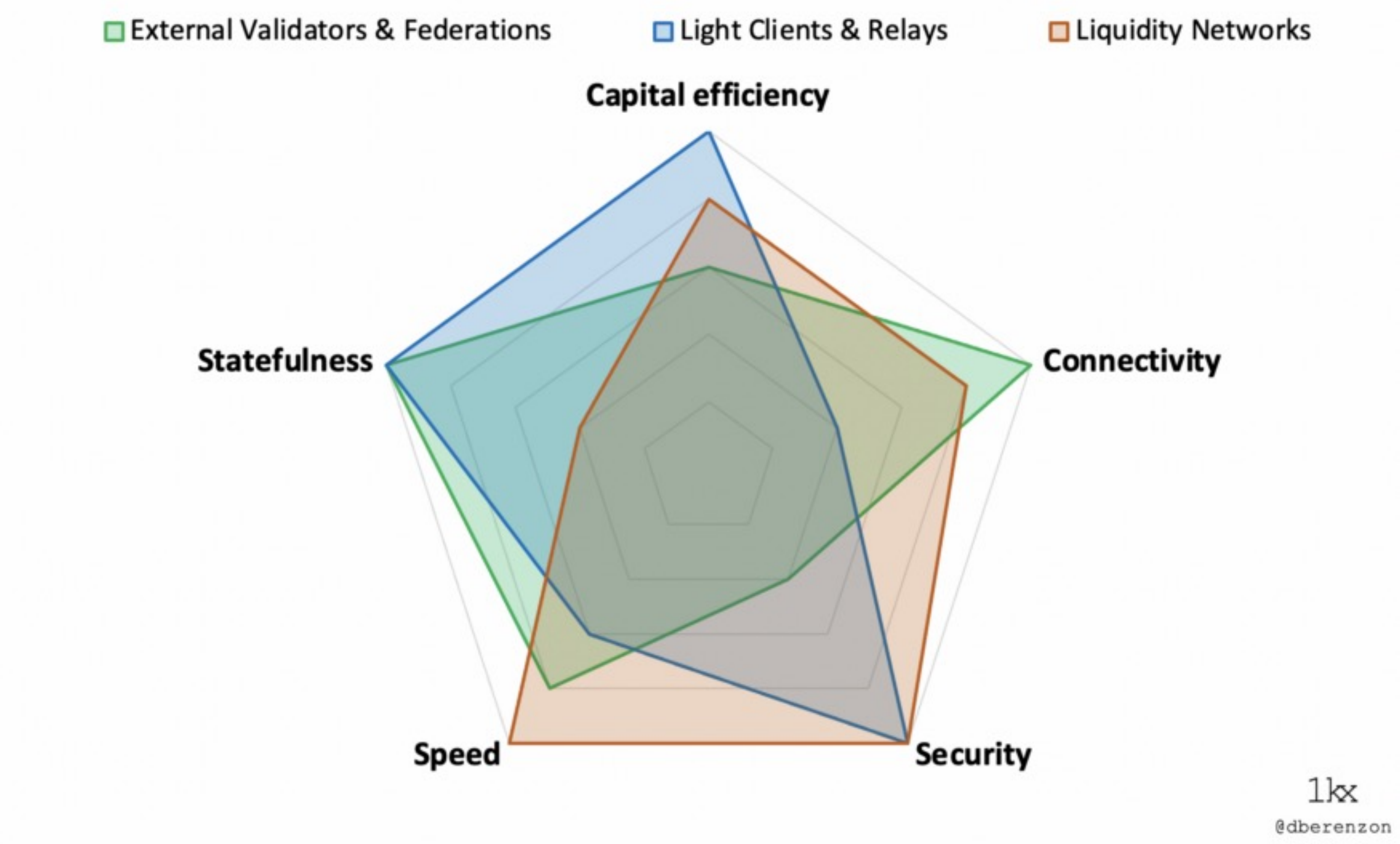


Asset-specific	Chain-specific	Application-specific	Generalized
ever (AR) INTERLAY (BTC) TBTC WBTC WRAPPED	Avalanche BINANCE GRAVITY BRIDGE Harmony (PoS Bridge) ETH NEAR Rainbow Bridge Ronin secret network (SnowBridge) Terra Shuttle TokenBridge WORMHOLE WRAP (XCMP)	ANY SWAP Biconomy CELER CHAINFLIP Gateway liquality Qredo Ren Synapse THORCHAIN wanchain	AXELAR Chainlink ChainSafe composable connext deBridge IBC Inter-Blockchain Communication LayerZero. Movr OPTICS Polymer PolyNetwork orbit router

1kx
@dberenzon

Source: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8

Bridge evaluating factors

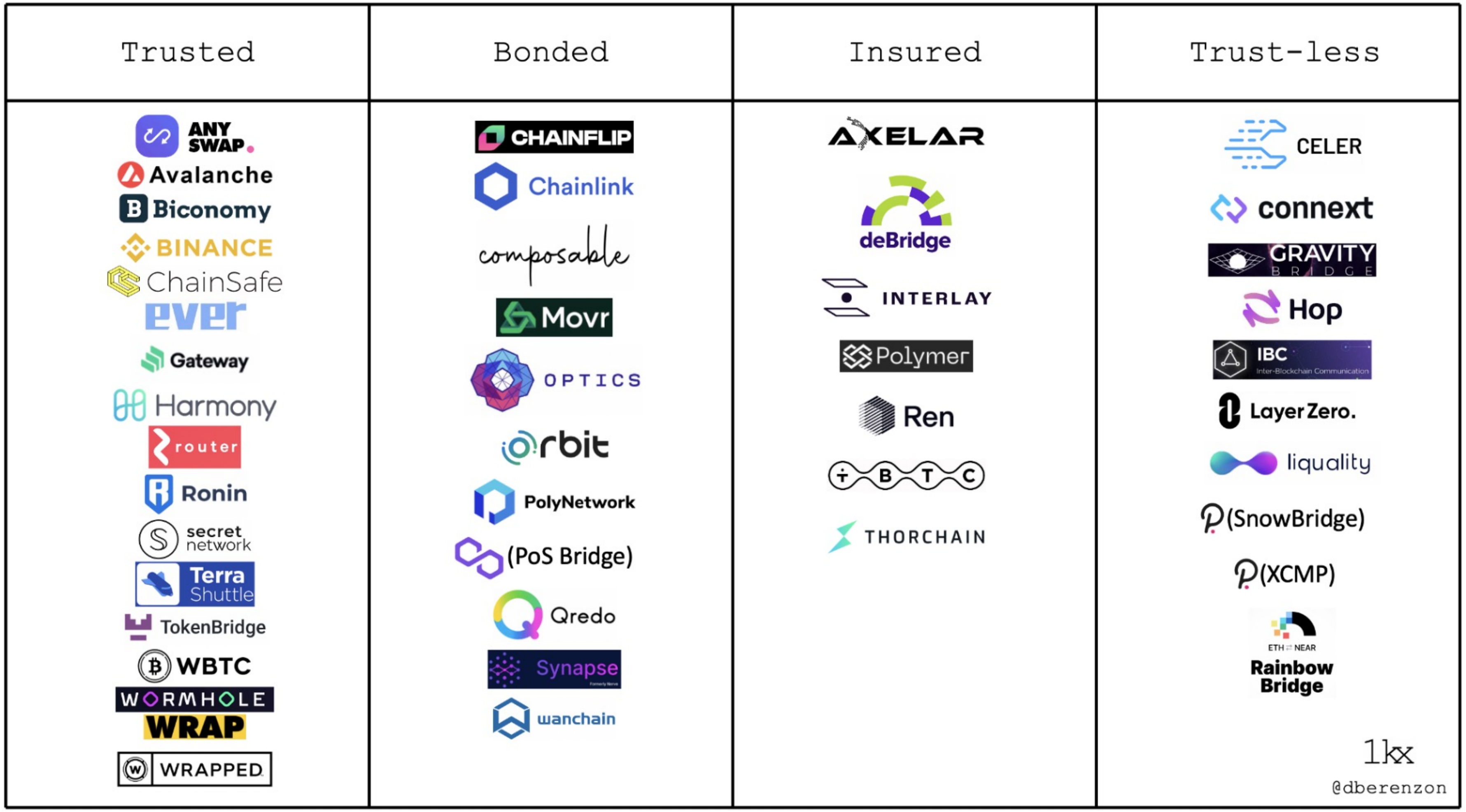


Source: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8

Bridge spectrum

- Trustless is a bridge that shares the **same security** and **trust** with the underlying Layer 1 protocol. The users' funds cannot be stolen or lost outside of a consensus-level attack.
- Insured is a bridge that requires users to post **collateral** so that possible malicious activity is likely to be unprofitable. In any case if a user lose their founds, then their assets will be reimbursed through slashed collateral.
- Bonded bridges have similar malicious economic incentives, with the difference that users do not always get their assets back after an attack. Such bridges uses an **endogenous collateral** (the protocol token is the collateral) which is a riskier choice.
- Trusted is a bridge that doesn't post a collateral at all and in the case of system failure or in an attack users can not recover their funds. The trust is held completely into the **platform**.

Bridge spectrum



Trusted	Bonded	Insured	Trust-less
ANY SWAP.	CHAINFLIP	AXELAR	CELER
Avalanche	Chainlink	deBridge	connext
Biconomy	composable	INTERLAY	GRAVITY BRIDGE
BINANCE	Movr	Polymer	Hop
ChainSafe	OPTICS	Ren	IBC Inter-Blockchain Communication
ever	orbit	tBTC	LayerZero.
Gateway	PolyNetwork	THORCHAIN	liquality
Harmony	(PoS Bridge)		(SnowBridge)
router	Qredo		(XCMP)
Ronin	Synapse		ETH ⇄ NEAR Rainbow Bridge
secret network	wanchain		
Terra Shuttle			
TokenBridge			
WBTC			
WORMHOLE			
WRAP			
WRAPPED			

1kx
@dberenzon

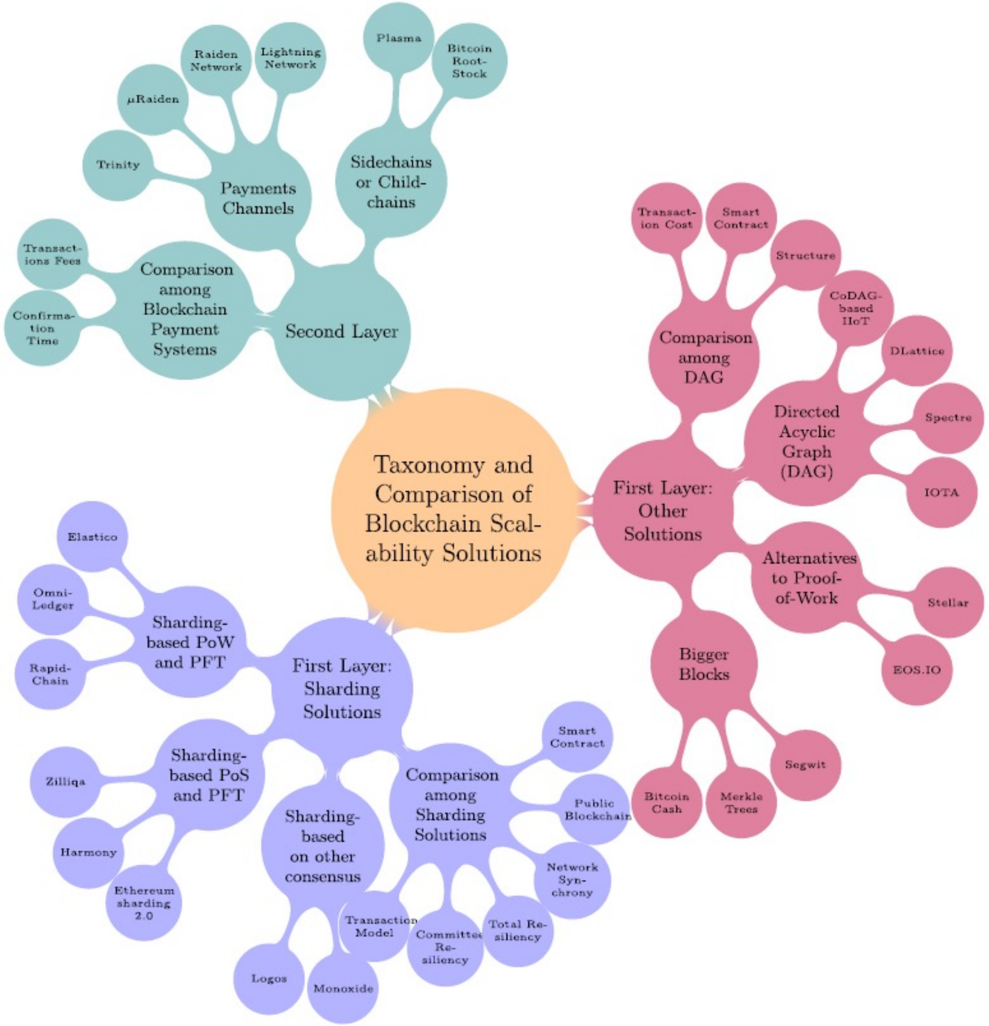
Source: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8

Scaling Solutions

Back to the Trilemma

- Let's now discuss the yet another dimension of the blockchain **trilemma**, Scalability.
- **Blockchains** offer an immutable, decentralized, distributed peer-to-peer ledger for transactions and state transitions.
- But in a world of thousands of transactions per second, the 7 or 15 TPS of Bitcoin and Ethereum are simply not enough. (Remember the Trilemma?)
- Achieving scalability while remaining secure and decentralized is problem with no easy solutions.
- Many solutions have been proposed and implemented.
- Some focus on the so-called **“Layer 1”** and more specifically on improving consensus algorithms.
- Others are **Layer 2** solutions, or separate networks abutting to Layer 1.

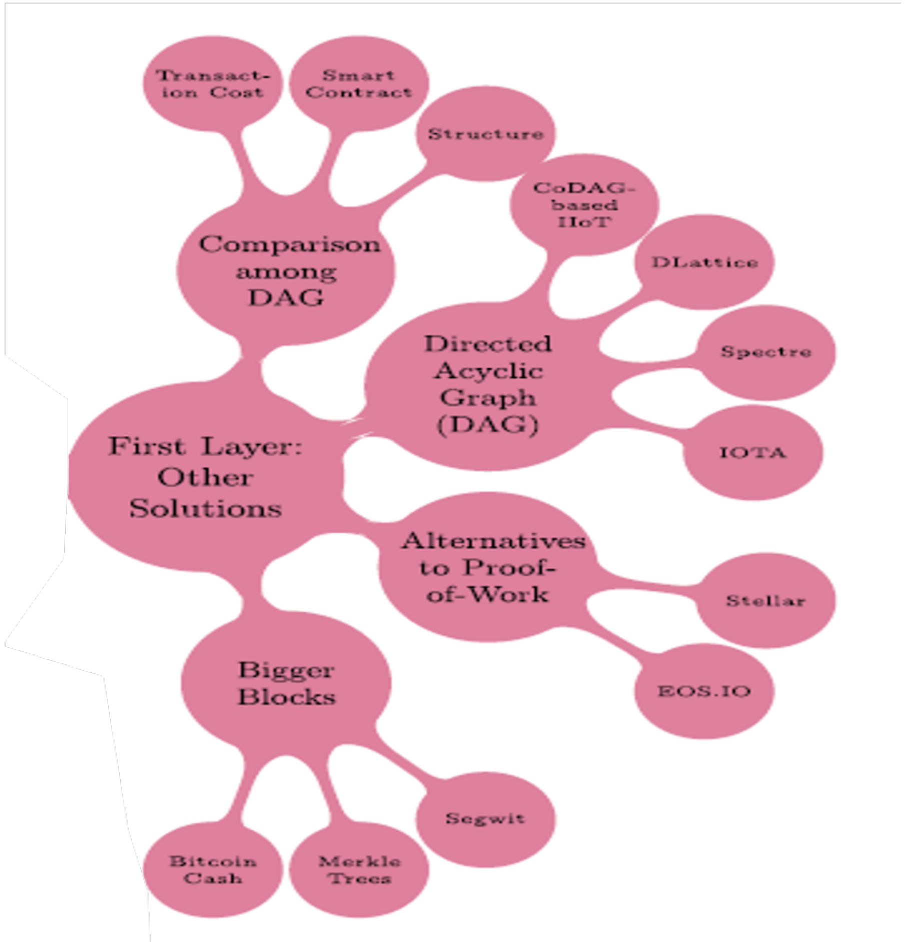
Taxonomy of Blockchain Scalability Solutions



Source: Hafid, Abdelatif, Abdelhakim Senhaji Hafid, and Mustapha Samih. "Scaling blockchains: A comprehensive survey." IEEE Access 8 (2020):

Layer 1 Solutions

- Layer 1 scalability solutions focus on the rules of the protocol itself. These solutions are mainly focus on the following protocol improvements:
- **Consensus Algorithm Improvement**
  - As we have already discussed, different consensus algorithms, have different trade-offs.
  - A good example is the transition from Proof of Work to a Proof of Stake consensus algorithm for Ethereum.
- **Sharding**
  - This method separates the state of the entire chain into smaller distinct datasets that are called ***"shards"***.
  - This shards are processed parallelly by the network simultaneously, increasing network throughput.
  - Each node is not maintaining a copy of the entire blockchain but focuses only to its assigned shard.
  - Example of protocols that practice this method are: Ethereum 2.0, Tezos, Zilliqa and Qtum.
- **Alternative Data Structures**
  - Moving away from the hierarchical structure of blockchains (e.g., Direct Acyclic Graphs (DAGs).



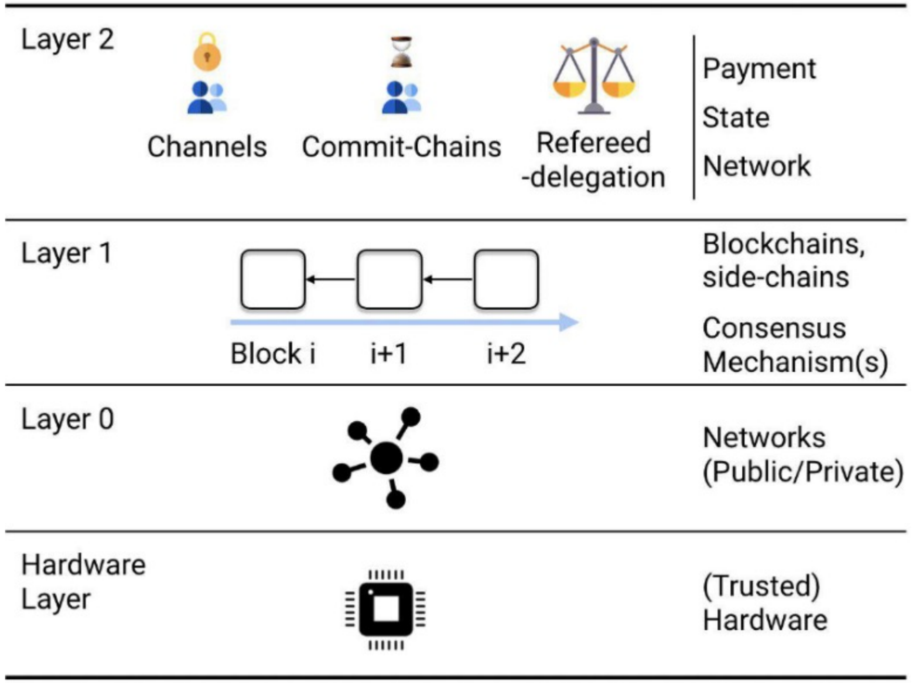
Layer 2 Protocols

- **Layer 2** protocols, built on top of Layer 1 (L1) blockchains. The main principle is to avoid disseminating every transaction to the L1 network by exchanging authenticated transactions off-chain. **Layer 2** solutions process portions of L1 transactions.
- Such protocols handle the brunt of the network's processing and **reports back** only a subsequent statement to the main blockchain in order to **finalize its results**.
- These solutions perform ***"off-chain"*** operations through authenticated and private communication networks.
- Such optimizations **reduce** the transaction load of L1 protocols or offer provided utility beyond what is possible in L1.

Source: Gudgeon, Lewis, et al. "Sok: Layer-two blockchain protocols." International Conference on Financial Cryptography and Data Security. Springer, Cham, 2020.

Layer 2 Protocols

- **Hardware Layer:** Trusted Execution Environments (TEE) enable efficient protocols at other layers such as off-chain payments.
- **Layer 0** (Network layer): is typically a peer-to-peer layer on which blockchain nodes exchange information asynchronously.
- **Layer 1** (Blockchain Layer): hosts an immutable append-only chain of blocks that accumulates transactions from parties in a network for public verifiability. Each transaction encodes an update of the state of the blockchain.
- **Layer 2** (off-chain): such protocols enable transactions between users through the exchange of authenticated messages via a medium which is outside of a layer-one blockchain. Authenticated assertions are submitted to the parent-chain only in cases of a dispute.
  - The parent-chain is deciding the outcome of the dispute.

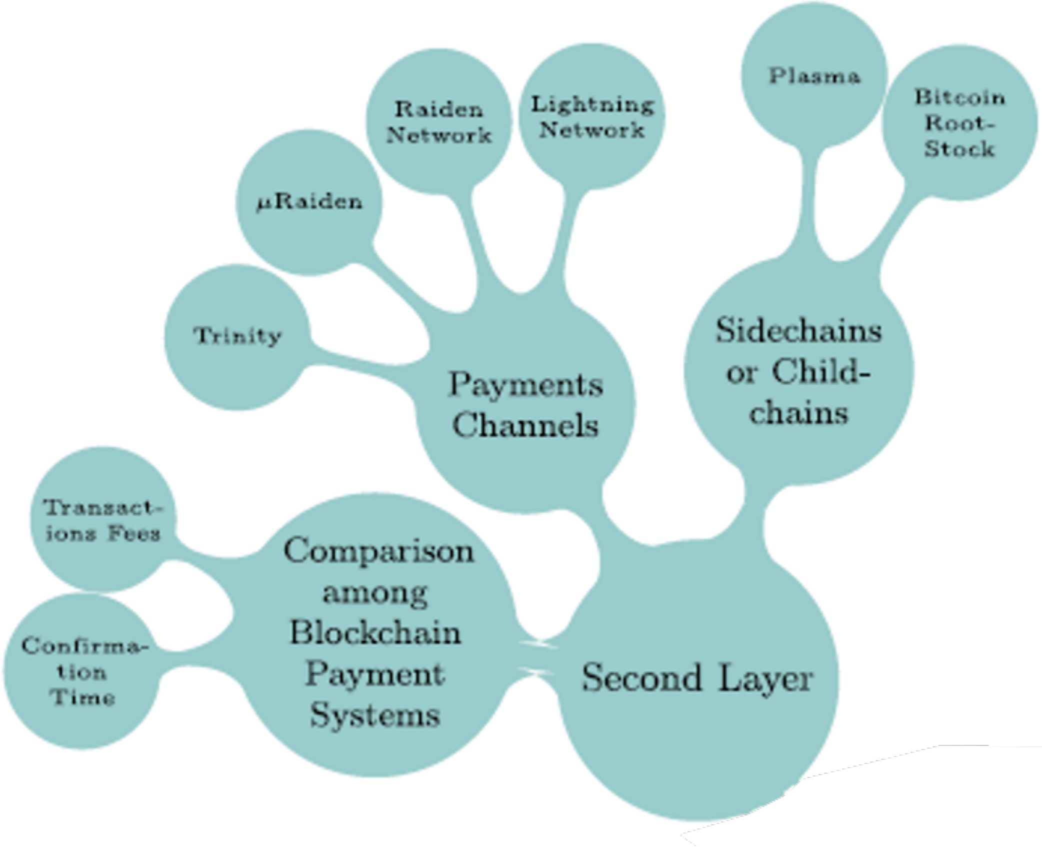


Overview of blockchain layers [1]

Source: [1] Gudgeon, Lewis, et al. "Sok: Layer-two blockchain protocols." International Conference on Financial Cryptography and Data Security. Springer, Cham, 2020.

Layer 2 Protocols

- From the literature, different off-chain protocols focus on:
  - state and virtual channels
  - payment channel networks (PCNs)
  - routing protocols, channel rebalancing
  - commit-chains
  - channel hubs

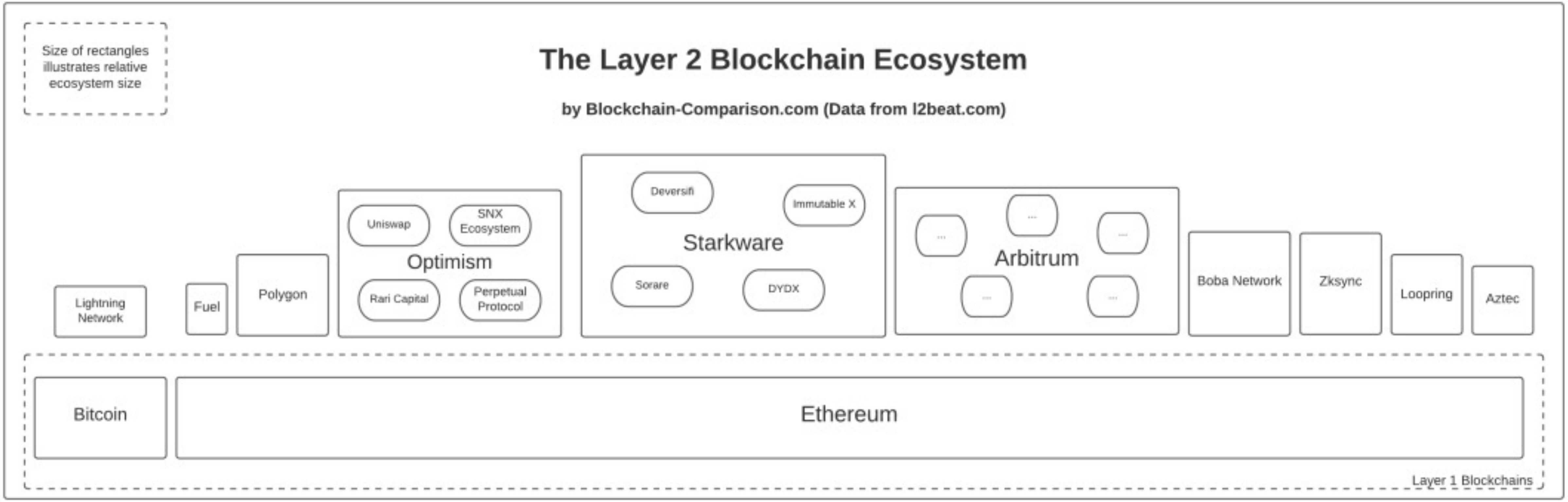


Layer 2 Protocols: Security

- The theoretical transaction throughput is only bounded by the communication bandwidth and latency of the involved parties.
- Off-chain transaction security can be guaranteed via allocated collateral, e.g., in payment channel designs or by offering delayed transaction finality in commit- chain proposals.
- Security and non-custodial properties of a layer-two protocol rely on the consensus algorithm of the parent-chain.

Source: Gudgeon, Lewis, et al. "Sok: Layer-two blockchain protocols." International Conference on Financial Cryptography and Data Security. Springer, Cham, 2020.

Layer 2 Protocols: Examples



Source: blockchain-comparison.com (data from i2beat.com)

https://blockchain-comparison.com/layer-2-blockchain-protocols/

Layer 2 Protocols: Examples

- **Bitcoin Lightning Network**
  - Build on top of Bitcoin's layer 1 protocol.
  - Improve transaction speeds form 10 minutes in the traditional network, to milliseconds.
  - Capable on handling billions of transactions per second.
  - Very low cost compered to Bitcoin's blockchain.
- **Ethereum Layer 2: e.g., Polygon, Arbitrum**
  - Main focus is the interoperability with Ethereum, improved speed and/or throughput.
  - Enables Solidity developers to make easier cross-compilations of their developed smart contacts.
  - Sidechain aggregation of transactions (zk-proofs, rollups etc).
- Further Reading:
  - https://www.block123.com/en/feature/awesome-layer-2-list/
  - https://101blockchains.com/ethereum-layer-2-solutions/

Conclusions

Conclusions

- Blockchain interoperability and scalability are important challenges that impact blockchain widespread and adoption
- Two approaches for Blockchain interoperability: (a) Mashup APIs, (b) network of networks
  - Mashup APIs serve as a glue to bridge multiple blockchains
  - Network of networks (NoN) is a web of interconnected blockchain networks
- Sidechains are secondary blockchains connected or pegged to the main blockchain a well-known technique is using a two-way peg (2WP). There are 3 design options for 2WP:
  - (a) Centralized 2WP, (b) Multi-signature or federated 2WP and (c) Simplified Payment Verification
- Bridges are an important part of the blockchain ecosystem as they facilitate interactivity, through the transfer of information between L1 protocols. In the literature we distinguish the following types of bridges:
  - Asset specific bridges; protocols that provide access to specific asset or assets that exist in other protocols
  - Chain specific bridges; a bridge that connects two blockchains with similar properties
  - Application specific bridges; bridges that operate within certain specific dApps, for interoperability purposes.

Glossary

Glossary

Sidechains: are blockchains that allow for digital assets from one blockchain to be used securely in a separate blockchain and subsequently returned to the original chain

Blockchain Interoperability: two or more blockchain systems can interact with other communicate and share value.

Multi-chain Frameworks: Blockchains can plug into a framework to become a part of the standardized ecosystem and transfer data and value between each other.

Merged Consensus: allow for two-way interoperability between chains through the use of a relay chain. Merged consensus can be quite powerful, but generally must be built into the chain from the ground up. Projects like Cosmos and ETH2.0 use merged consensus.

Glossary

Atomic Swaps: Atomic swaps are smart contracts that give you the ability to exchange digital assets on-chain or off-chain seamlessly and securely without the involvement of a third-part. It allows users to trade one cryptocurrency for another directly in a peer-to-peer transaction.

Layer-two protocols: A layer-two protocol allows transactions between users through the exchange of authenticated messages via a medium which is outside of a layer-one blockchain. Authenticated assertions are submitted to the parent-chain only in cases of a dispute. In such cases the parent-chain is determining the outcome of the dispute. Security and non-custodial properties of a layer-two protocol rely on the consensus algorithm of the parent-chain.

Further Readings

Further Reading

[1] Jin, H., Dai, X., & Xiao, J. (2018). Towards a novel architecture for enabling interoperability amongst multiple blockchains. Proceedings - International Conference on Distributed Computing Systems, 2018-July, 1203–1211. https://doi.org/10.1109/ICDCS.2018.00120

[2] Hardjono, T., Lipton, A., & Pentland, A. (2018). Towards a Design Philosophy for Interoperable Blockchain Systems, 1–27. Retrieved from http://arxiv.org/abs/1805.05934

[3] Kan, L., Wei, Y., Hafiz Muhammad, A., Siyuan, W., Linchao, G., & Kai, H. (2018). A Multiple Blockchains Architecture on Inter-Blockchain Communication. Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security Companion, QRS-C 2018, 139–145. https://doi.org/10.1109/QRS-C.2018.00037

[4] Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. IEEE Access, 8(July), 125244–125262. https://doi.org/10.1109/ACCESS.2020.3007251

[5] Gudgeon, L., Moreno-sanchez, P., Roos, S., Mccorry, P., & Gervais, A. (2020). SoK : Off The Chain Transactions. Financial Cryptography and Data Security, Layer 2.

[6] Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). SoK: Layer-Two Blockchain Protocols. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12059 LNCS(i), 201–226. https://doi.org/10.1007/978-3-030-51280-4_12

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: @mscdigital
Instructor's Email: christodoulou.kl@unic.ac.cy

Course Support:
Mark Wigmans - wigmans.m@unic.ac.cy
Marios Touloupos - touloupos.m@unic.ac.cy

IT & live session support: dl.it@unic.ac.cy