UNIVERSITY of NICOSIA

Session 2

DeFi Infrastructure – L1 Networks

BLOC 611: Decentralized Finance

Agenda

- Layer 1 protocols
- Consensus Algorithms
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Delegated Proof of Stake (DPoS)
  - Proof of Authority (PoA)
- Notable Layer 1 Protocols
  - Ethereum
  - Tezos
  - Cardano
  - Avalanche
  - Binance Smart Chain
- Scaling
  - Layer 1
  - Layer 2
- Bridges
  - Types
  - Evaluation
  - Spectrum
- Conclusion

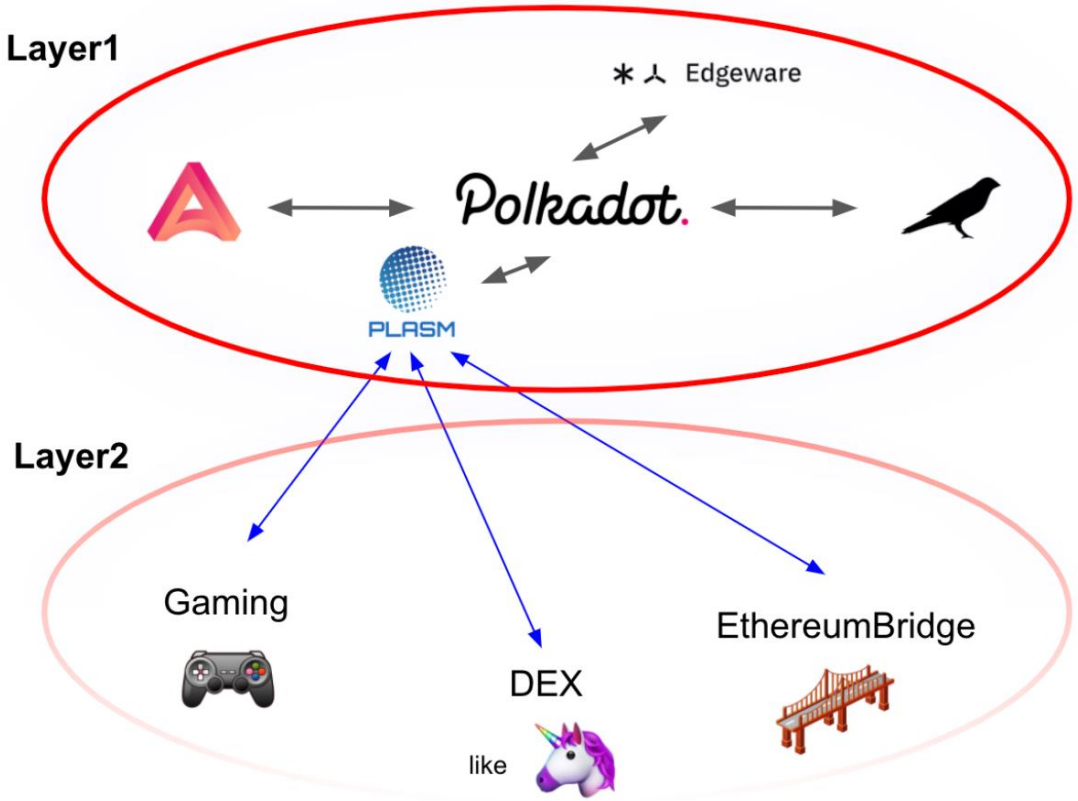
Disclaimer: As usual, the inclusion of any particular blockchain project or organisation is for educational purposes only. This should not be construed as an endorsement or investment advice.

Session 1: DeFi Infrastructure L1 Networks.

1. Layer 1 Protocols

What is Layer 1?

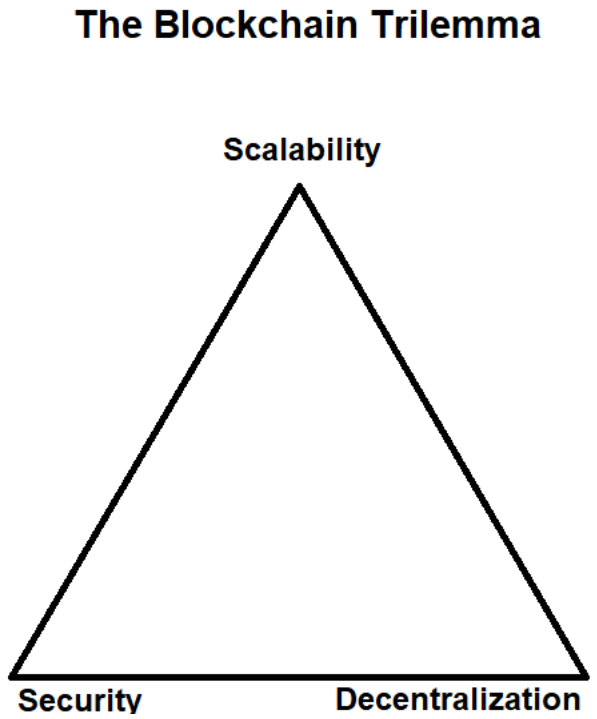
- **Layer 1 (L1)** refers to the main underlying blockchain architecture (or the Settlement Layer from the previous session).
- According to blockchaincomparisons, there are more than 100 blockchain solutions in the ecosystem.
- Each protocol is built with different utility, speed, security, smart contract capabilities and level of decentralization.
- This part aims to study the main characteristic between the L1 protocols, the consensus algorithms.



Source: https://blockchain-comparison.com/blockchain-protocols/ , https://zephyrnet.com/plasm-network-a-layer-2-parachain/

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**



Session 1: DeFi Infrastructure L1 Networks.

2. Consensus Algorithms

What is a consensus algorithm?

- Layer 1 protocols **have no central authority** validating transactions and state transitions. Yet networks must reach a consensus (agreement) on its correct state, in a secure manner.
- A **consensus algorithm** is a mechanism through which all the participants (nodes) of a blockchain reach a joint agreement about the ledger's state. In this way, consensus algorithms create reliability and trust between unknown peers in a distributed computing environment.

The goal of the consensus algorithm is to solve the **Byzantine Fault Tolerance**.

- Byzantine Fault Tolerance is a property of systems that can withstand the types of failures derived from the **Byzantine General Problem**.

Source: Papangelou, Stamatis. "Chaotic pattern assessment and exploitation in Blockchain Technology." (2021).

Proof of Work (PoW)

- This consensus algorithm is used for selecting a node, called **miner**, that will validate the newly generated block in the network. In this method, all the available miners compete with each other in a complex mathematical puzzle, which is difficult to solve but easy to validate.
- Validating a block is **expensive**, and it requires that a miner (the node that is creating the block) uses their own resources (processing power) to earn the privilege of mining and the price that comes with it in the form of tokens (coins) of the corresponding digital currency.
- The computing power that the miner offers is used to hash (**SHA256** in Bitcoin) the candidate block's data while a solution to the cryptographic math puzzle is being found. The *"hash"* is a cryptographic method called *"hash function",* which takes an arbitrary number of bits as input and produces a cryptographic fixed bit output.
- Although **PoW** can be considered one of the most secure consensus protocols, this protocols have issues such as:
  - Low transaction throughput
  - Centralization due to hard-coded nodes and mining pools
  - Wasted of computing and power

Source: Papangelou, Stamatis. "Chaotic pattern assessment and exploitation in Blockchain Technology." (2021).

Proof of Work (PoW) (Cont.)

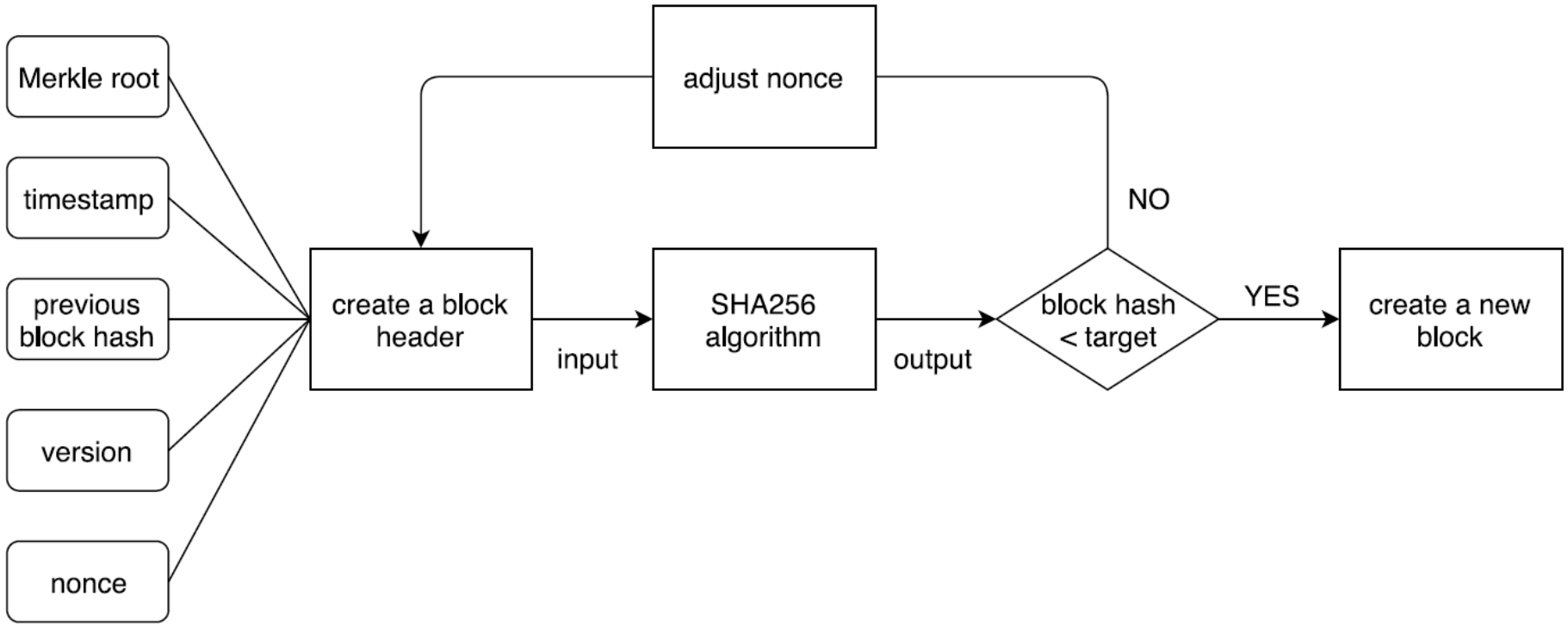


Fig. 1. Flow of PoW.

Source: Zhang, Shijie, and Jong-Hyouk Lee. "Analysis of the main consensus protocols of blockchain." ICT express 6.2 (2020)

Proof of Stake (PoS)

- In 2011, a Bitcoin forum user, ”QuantumMechanic (quantum power)” proposed a new technology he called ***”Proof of Stake”*** (PoS). The author believes that it would be wasteful behavior to let everyone compete with each other for mining as an alternative. The PoS mechanism uses an **election mechanism**.
- An individual node in the network is **randomly selected**. This node will be responsible for verifying the next block. It seems that there is an indirect difference in terminology. In the PoS algorithm, miners no longer exist. Instead, there is a ***”verifier”*** and this algorithm does not allow everyone to ***”mine”***, but ***”create”*** Blocks. Of course, the selection of ***”validators”*** is not a completely random process.
- In order to become a validator, a node must first mortgage a certain number of Tokens as ***”Stake (property)”***. You can think of this deposit just like a bank deposit. The number determines the probability of you being selected as a *”validator”* in the next election.
- Overall, the main pros and cons of PoS are as follows

Pros:

- Energy efficient
- Fast and inexpensive processing
- Special equipment is not required

Cons:

- Not proven in terms of security
- Validators with large holdings can have a big influence
- Some PoS require the lock up of tokens for a minimum amount of time

Source: Papangelou, Stamatis. "Chaotic pattern assessment and exploitation in Blockchain Technology." (2021).

Proof of Stake (PoS) (Cont.)

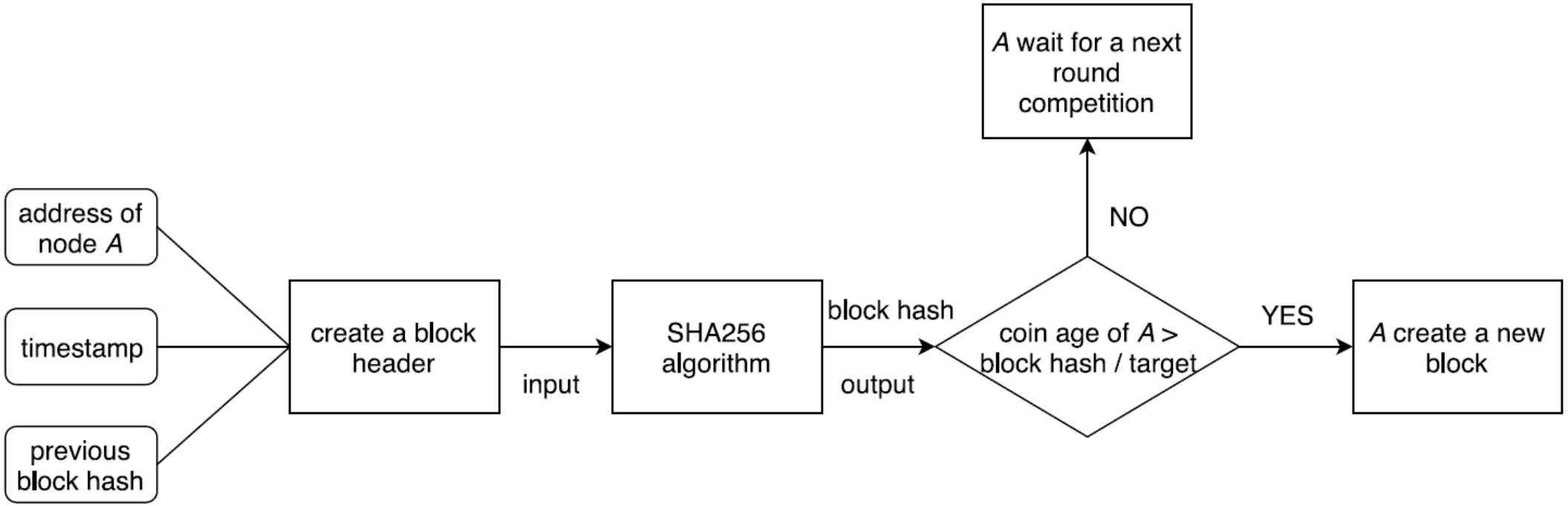


Fig. 2. Flow of PoS.

Source: Zhang, Shijie, and Jong-Hyouk Lee. "Analysis of the main consensus protocols of blockchain." ICT express 6.2 (2020)

Delegated Proof of Stake (DPoS)

- **Delegated Proof of Stake** is in some ways similar to PoS, with the major difference that lets the nodes who hold stake to participate in a voting mechanism that elects the block verifiers.
- With this method stake holders are giving the right of creating blocks to the delegated nodes instead of doing them themselves.
- This results to **zero power and computing consumption** of the staked holders.=
- Overall, the main pros and cons of DPoS are as follows :

Pros:

- Energy efficient
- Fast and scalable
- Real time voting security
- Special equipment is not required

Cons:

- More centralized compared to PoS or PoW
- More vulnerable to 51% attacks

Source: Zhang, Shijie, and Jong-Hyouk Lee. "Analysis of the main consensus protocols of blockchain." ICT express 6.2 (2020)

Delegated Proof of Stake (DPoS) (Cont.)

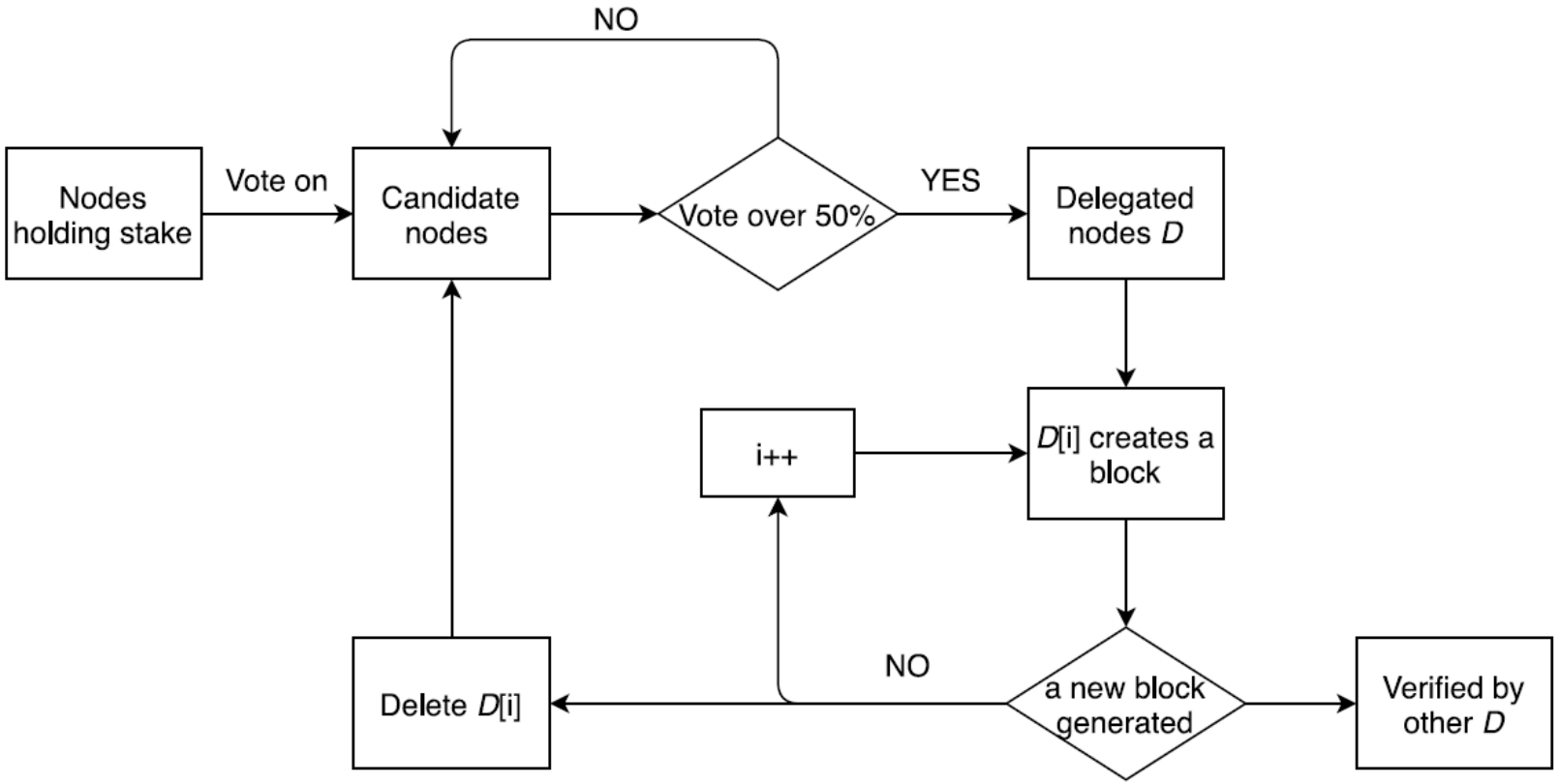


Fig. 3. Flow of DPoS.

Source: Zhang, Shijie, and Jong-Hyouk Lee. "Analysis of the main consensus protocols of blockchain." ICT express 6.2 (2020)

Proof of Authority (PoA)

- **Proof of Authority** is a federated system where people trust a central authority, like government agencies, and give licenses to a couple of nodes that get to operate in the blockchain and take turns signing blocks.
- The critical limitation of proof of Authority is that the **trust** to the authorizing signatory; so whatever this government agency is who is giving out the stamps for which nodes are allowed in the blockchain.
- That entity itself could be corrupt and could give stamps to agencies that do not deserve them, or it could make sure that most of the stamps that it gives out to the majority of the likely malicious nodes, which can corrupt the blockchain in its favor.
- Overall, the main pros and cons of PoA are as follows:

Pros:

- Very secure, because validators are pre-checked
- Energy efficient
- Fast transaction processing
- Quick block generation & low transaction costs.

Cons:

- Centralized and thus susceptible to all the perils of centralization (exclusion, censorship, etc.)

Source: Zhang, Shijie, and Jong-Hyouk Lee. "Analysis of the main consensus protocols of blockchain." ICT express 6.2 (2020)

Do you see the Trilemma?

Other Consensus Protocols

- Leased Proof of Stake (LPoS)
- Proof of Elapsed Time (PoET)
- Practical Byzantine Fault Tolerance (PBFT)
- Simplified Byzantine Fault Tolerance (SBFT)
- Delegated Byzantine Fault Tolerance (DBFT)
- Directed Acyclic Graphs (DAG)
- Proof of Activity (PoA)
- Proof of Importance (PoI)
- Proof of Capacity (PoC)
- Proof of Burn (PoB)
- Proof of Weight (PoW)

Session 1: DeFi Infrastructure L1 Networks.

3. Notable Layer 1 Protocols

Ethereum

As it was extensively investigated on last week's lecture, Ethereum is a Layer one solution with many applications, large community and and vivid ecosystem of decentralized applications.

It currently relies on **PoW** but will transition to **PoS**.

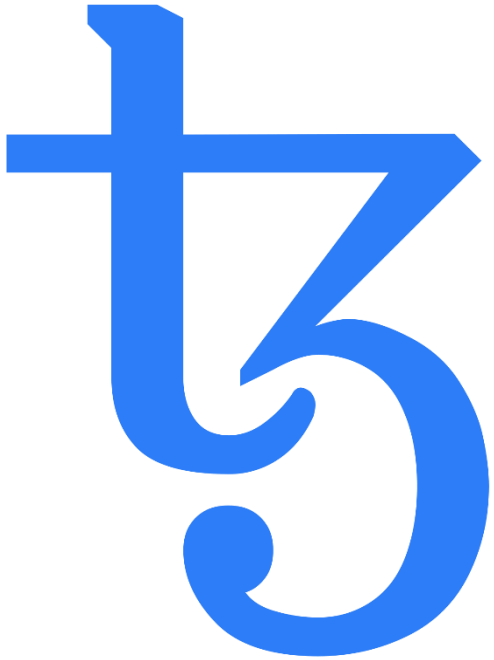
According to the Defiprime, Ethereum is home to approximately **85%** of all DeFi applications

- You can see the list of these platforms here: https://defiprime.com/ethereum

ethereum

Source: https://defiprime.com/ethereum

Tezos



- **Tezos** was firs proposed in 2014 and launched in 2018.
- Similarly, to Ethereum, Tezos also supports **smart contracts** which allow its developers to create decentralized applications, such as DeFi protocols.
- Tezos uses a special form of PoS. Its consensus protocol is **Liquid Proof of Stake** (LPoS)
- Some of the key metrics of Tezos include:
  - 40 transactions per second
  - 30 seconds block time (Granada update)
  - Circulating supply ~ 750,000,000 XTZ
  - Self-amendment gives decentralization benefits

DeFi in Tezos

- According to Tezos projects, Tezos is currently home to **24** operational or upcoming DeFi projects.
- This includes:
  - StableCoins, CBDCs:
    - Lugh – a stabelcoin that has 1-to-1 ratio with the Euro
    - StableTez – deploying stablecoins such as USDtez and ETHtez
    - Societe General – CBDC for the digital Euro
  - DEXs
    - Quipswap
    - Dexter
    - SEXP
  - Lending
    - Tezfin
  - You can explore the full list here: https://tezosprojects.com/?page=defi

Cardano

- **Cardano** was founded in 2015 and launched in 2017 by Charles Hoskinson
- This protocol has **Proof of Stake** consensus algorithm that is called Ouroboros.
- In October 2021 Cardano's native token ADA had more than 70 billion of market capitalization.
- Cardano is currently the top PoS network by marketcap.
- In September of 2021 also supports **smart contracts**, so now it gives the opportunity to the developers to create decentralized applications and DeFi platforms.

DeFi on Cardano

- Cardano only recently implemented changes to facilitate smart contracts. As a result, its DeFi ecosystem is dormain.
- Some DeFi protocols on Cardano include:
  - Meld – Lending protocol very similar to *"Aave"* protocol which is build on Ethereum.
  - Coti – A stablecoin
  - Liqwid – A lending and borrowing platform

Source: https://medium.com/coinmonks/cardano-100x-defi-projects-will-make-you-fortune-79a2ece75933

Cardano Ecosystem

Avalanche

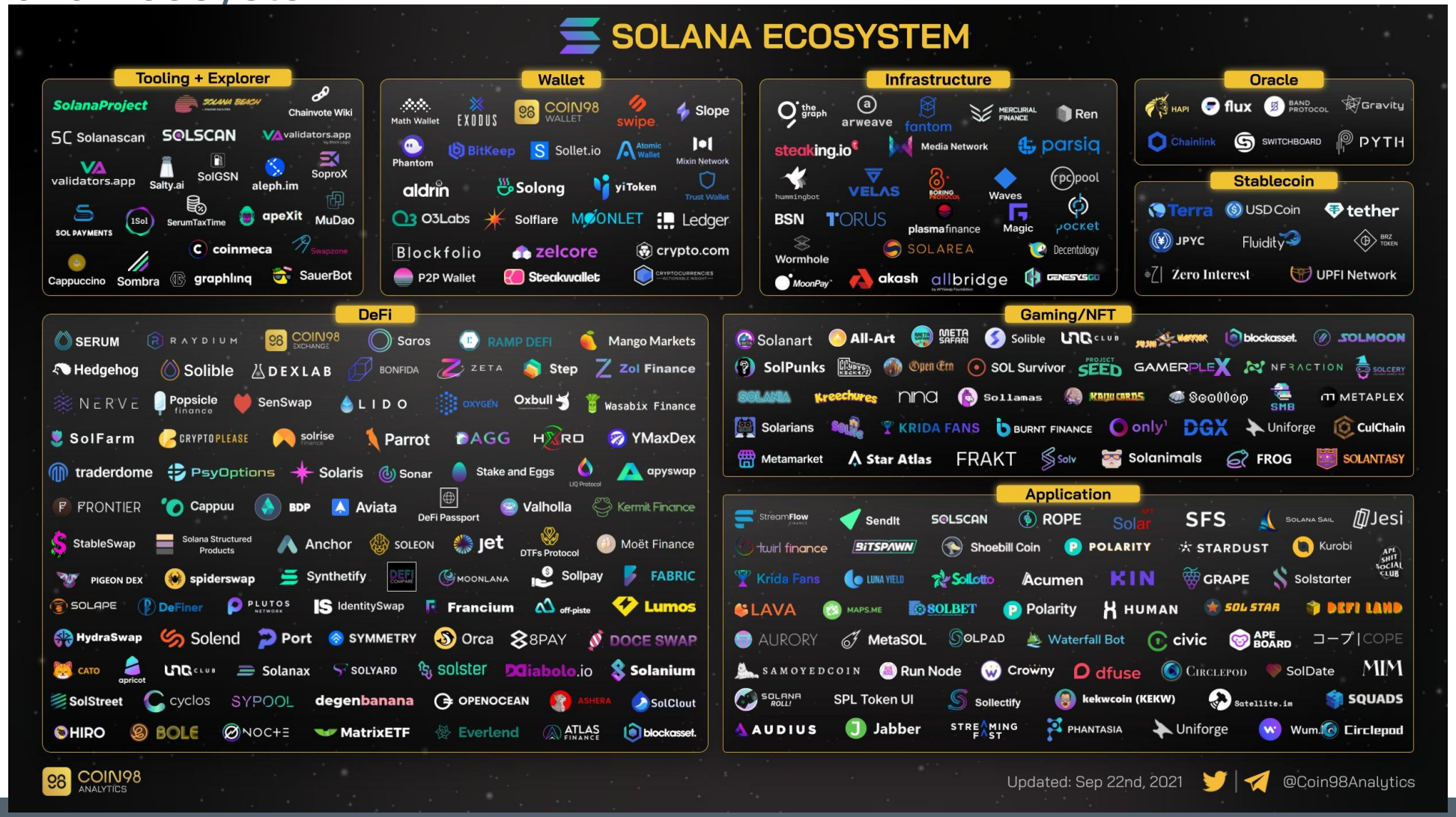
- **Avalanche** provides with a protocol aims on solving consensus of unreliable machines.
- This protocol was introduced on **InterPlanetary File System** on May 16, 2018, and it was then formalized extensively by researchers in Cornell University in 2019.
- Avalanche relies on its own consensus mechanism called **Avalanche Consensus**.
- Every node in the Avalanche network has a **vote.**

Avalanche Ecosystem

Solana

- Was introduced in April 2019.
- **Solana** is an open-source decentralized blockchain platform and it uses both Proof of Stake and Proof of History consensus protocols and supports smart contracts.
- With **570** global validators Solana has block creation time lower than **1000** microseconds.

Solana Ecosystem



Binance Smart Chain (BSC)

- Binance introduced the Binance Smart Chain in September of 2020.
- **Binance Smart Chain** (BSC) is a smart contract blockchain, operating in parallel to the Binance Chain
- This protocol uses **Proof of Staked Authority** (PoSA) as a consensus algorithm.
- In order to become validators nodes must stake BNB, the native asset of Binance Chain.

Session 1: DeFi Infrastructure L1 Networks.

4. Scaling Solutions

Back to the Trilemma

- Let's now discuss the yet another corner 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 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

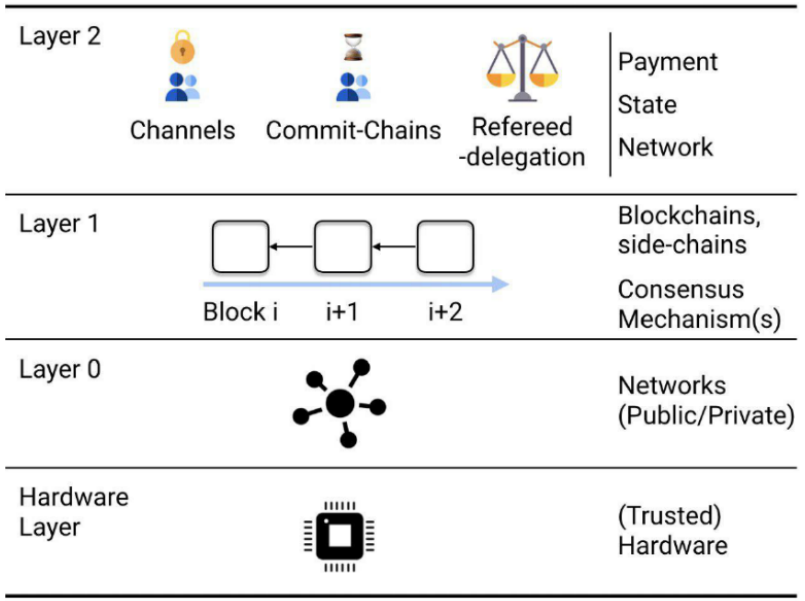
Source: Scaling Blockchains: A Comprehensive Survey, Abdelatif H. et. al. (2020)

Layer 1 Solutions

- Most of the Layer 1 scalability solutions focus on the rules of the protocol itself so the increased transaction **speed** and **capacity** is achieved while more data and users are accumulated.
- The solutions are categorized in two main improvements:
- Consensus Algorithm Improvement
  - As shown in previous slides, 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 just hold its assigned shard.
  - Example of protocols that practice this method are : Tezos, Zilliqa and Qtum.
- Direct Acyclic Graphs (DAGs)
  - Moving away from the hierarchical structure of blockchains (e.g., IOTA).

Layer 2 Solutions

- **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**.



- This solutions perform ***"off-chain"*** operations through authenticated and private communication networks.
- Such optimizationσ **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.

Popular Layer 2 protocols

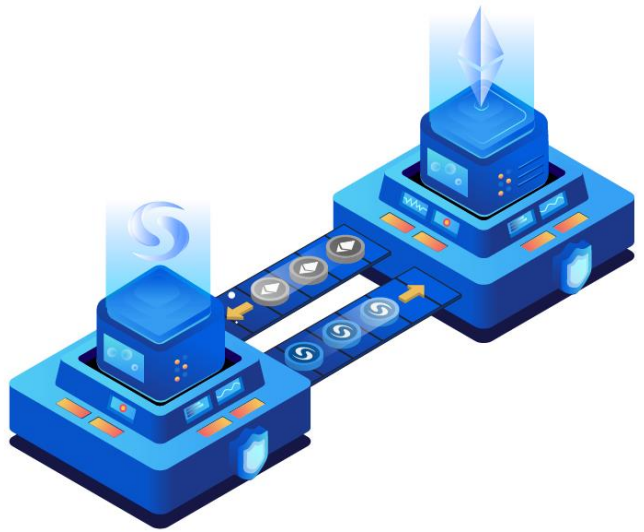
- **Bitcoin Lightning Network**
  - Build on top of Bitcoin's layer 1 protocol.
  - Improve transaction speeds form 10 minutes in the traditional network, to milliseconds.
  - Capable on handling billions of transactions per second.
  - Very low cost compered to Bitcoin's blockchain.
- **Arbitrum**
  - Main focus is the interoperability with Ethereum, and not speed or throughput.
  - Enables Solidity developers to make easier cross-compilations of their developed smart contacts.
  - Arbitrus also supports for sidechain aggregation of transactions (rollup technology).
- Further Reading:
  - https://www.block123.com/en/feature/awesome-layer-2-list/
  - https://101blockchains.com/ethereum-layer-2-solutions/

Session 1: DeFi Infrastructure L1 Networks.

5. Bridges

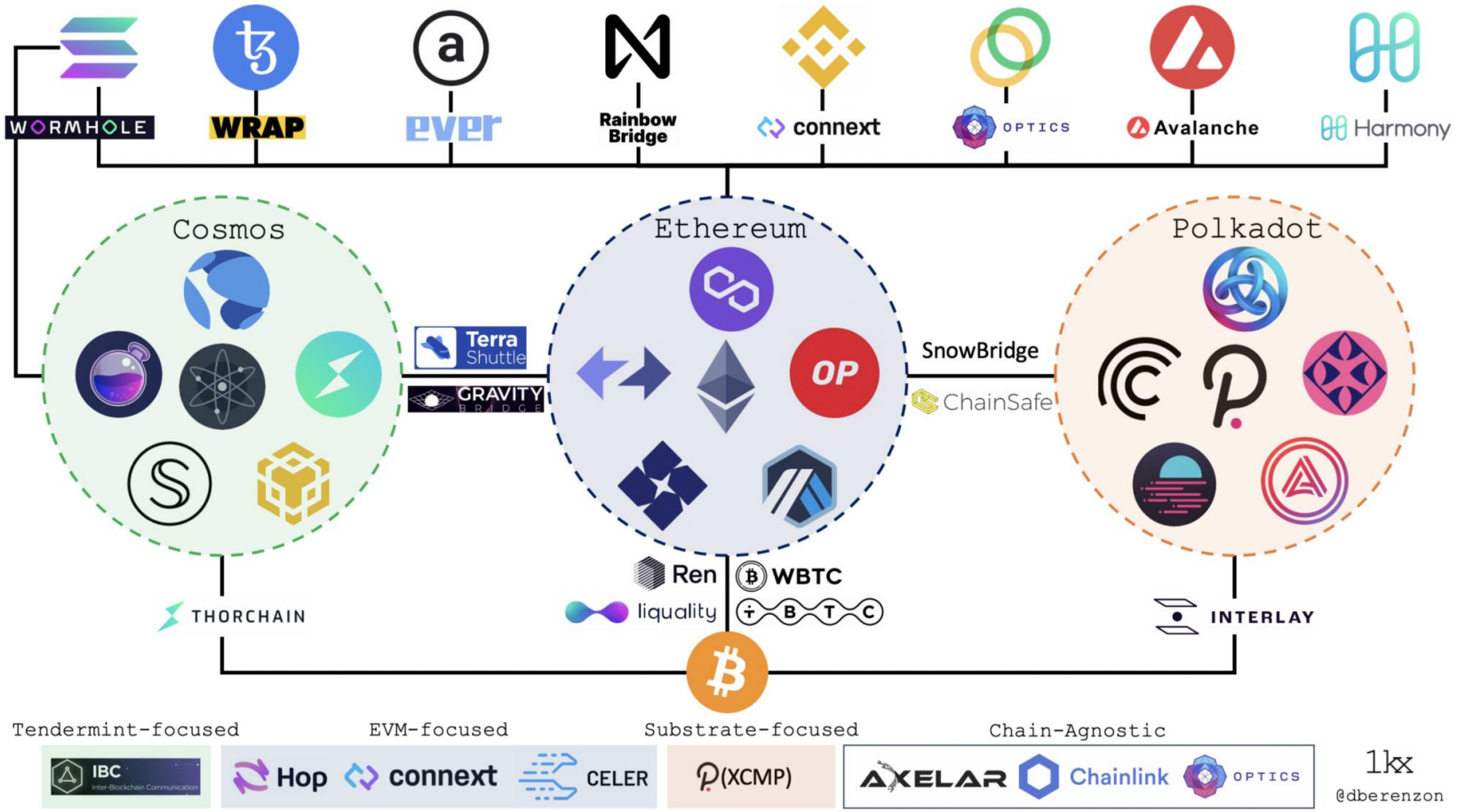
What is Blockchain Bridge?

- The main utility of bridge system is **transferring** information from one Layer 1 to one or more blockchain protocols.
- Bridges are an important part of the DeFi *"lego"* as they facilitate interactivity, throuhg 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

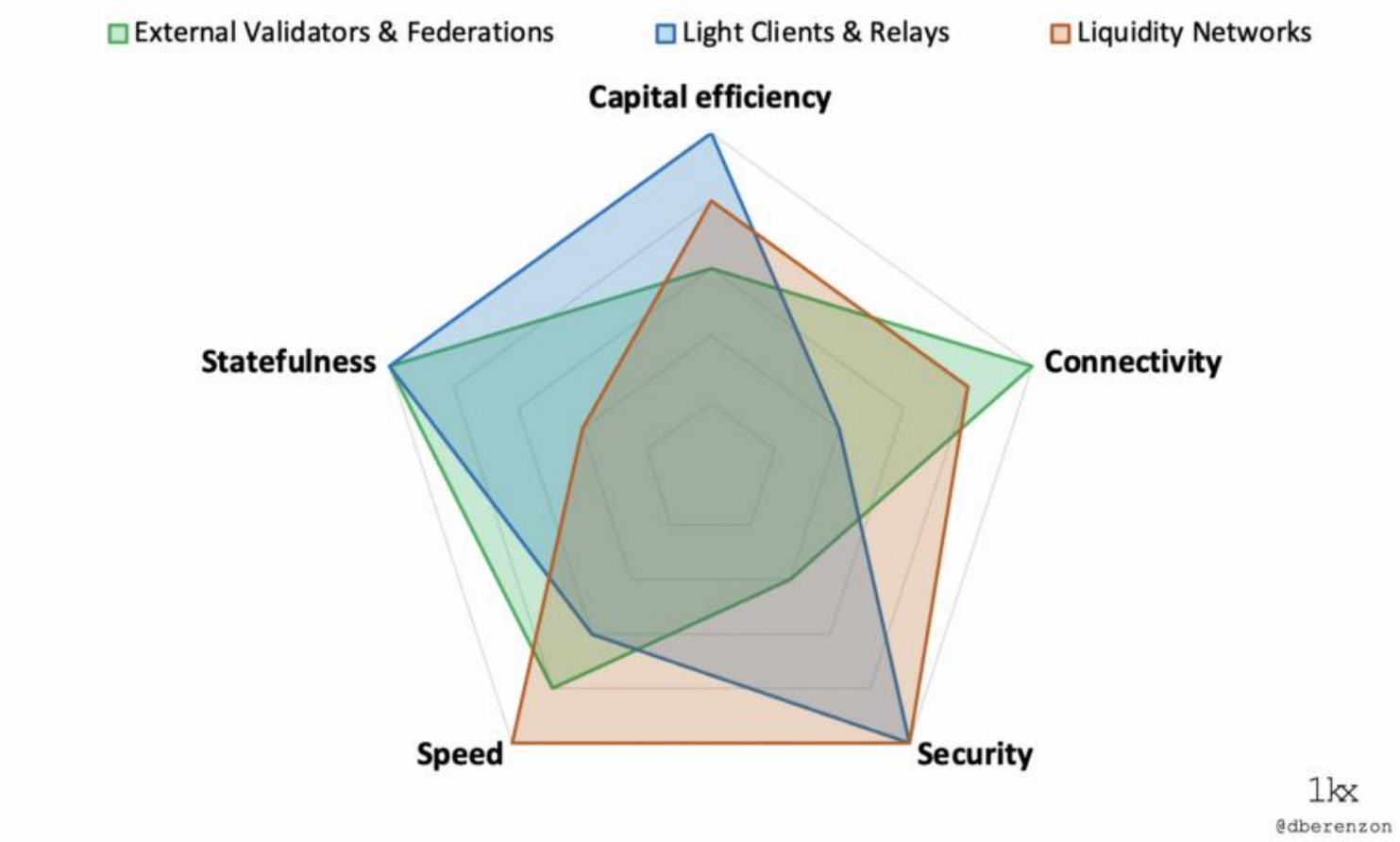
- Asset specific bridges are protocols that provide access to specific **asset** or assets that exist in other protocols. *"Wrapped"* assets are usually created which are fully collateralized by the underlining ones. More on that in week 4!
- Chain specific is a bridge that connects two **blockchains** 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 (Cont.)

Asset-specific	Chain-specific	Application-specific	Generalized
everRise (AR) INTERLAY (BTC) BTC WBTC WRAPPED 1kx @dberenzon	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 LayerZero. Movr OPTICS Polymer PolyNetwork orbit router

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

Bridge evaluating factors

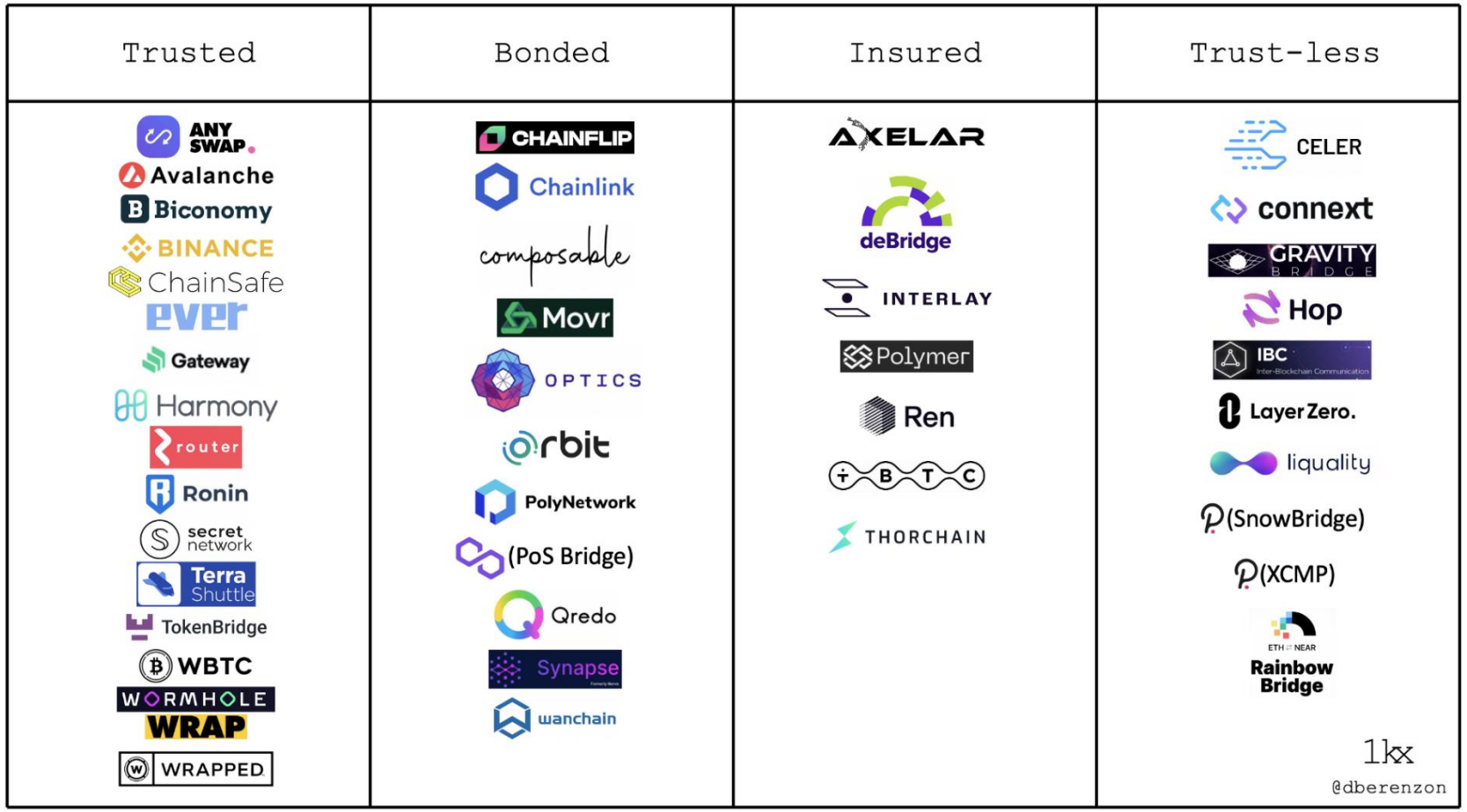


Source: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8

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 (Cont.)



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

Session 1: DeFi Infrastructure L1 Networks.

6. Conclusion

Conclusion

- The brief description of what Layer 1 protocols are was given
- Investigation of the Blockchain Trilemma which includes:
  - Security
  - Scalability
  - Decentralization
- Then the consensus protocols were investigated and how they affect the blockchain trilemma
- Major Layer 1 protocols were discussed:
  - Ethereum
  - Tezos
  - Cardano
  - Etc.
- Scalability solutions on both Layer 1 and Layer 2
- The importance of Bridges was shown alongside the types and characteristics

Further Reading

- Blockchain Layer 1 protocols:
  - https://blockchain-comparison.com/blockchain-protocols/
- Consensus Protocols:
  - https://www.sciencedirect.com/science/article/pii/S240595951930164X
- Scaling
  - Gudgeon, Lewis, et al. "Sok: Layer-two blockchain protocols." International Conference on Financial Cryptography and Data Security. Springer, Cham, 2020.
  - Hafid, Abdelatif, Abdelhakim Senhaji Hafid, and Mustapha Samih. "Scaling blockchains: A comprehensive survey." IEEE Access 8 (2020): 125244-125262.
  - https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network#section-layer-2-scaling-solutions
  - https://medium.com/the-capital/layer-1-vs-layer-2-what-you-need-to-know-about-different-blockchain-layer-solutions-69f91904ce40
  - https://learn.bybit.com/blockchain/blockchain-layer-1-vs-layer-2/
- Bridges
  - https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **defi@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**