Monnaies numériques

ESILV 2018/2019

Agenda

Buidling on Ethereum
It's not a typo

Ethereum today: Issues
Scaling & decentralization

Ethereum tommorow: Solutions
PoS, Sharding, Plasma

Buidling on Ethereum

Node clients

GETH

- **GETH is a GO implementation of the Ethereum protocol**
- https://github.com/ethereum/go-ethereum/wiki/Geth
- **It is generally seen as the reference implementation**
- **Advantages include:**
  - **Clique algorithm for testnets/private nets, amongst them the Rinkeby test network**
  - **Easier to get into the code**
  - **Present in a variety of other projects, such as Quorum**
- **Disadvantages:**
  - **Can be resource intensive**

Parity

- Parity is a RUST implementation of the Ethereum protocol
- https://wiki.parity.io/
- Developed by Parity, a german start up led by Gavin Wod, one of Ethereum's founding member
- Advantages include:
  - Better management of server ressources
  - Cleaner and more user friendly interface
  - Faster synch when setting up a node
- Disadvantages:
  - More user focused than developer focused

Full node vs Light nodes

- A full node downloads, verifies and keeps an updated copy of the Blockchain
- Advantages:
  - Faster access to the Blockchain
  - Enhanced privacy
  - No censorship
- Disadvantages:
  - Severe hardware requirement
  - Important bandwidth requirement
  - Requires maintenance
  - Long initial synch time

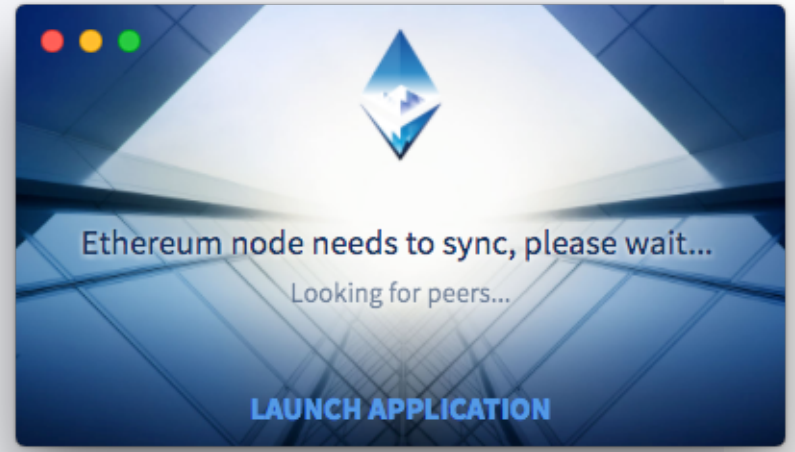
Full node vs Light nodes

- A light node downloads only the parts of the Blockchain its needs to verifiy transactions
- Advantages:
  - Much lighter to run
  - Faster to synch initially
  - More user friendly, easier to maintain
- Disadvantages:
  - Relying on a wallet provider
  - Possible cost in the future
  - No privacy
  - Not censorship resistant

Buidling on Ethereum

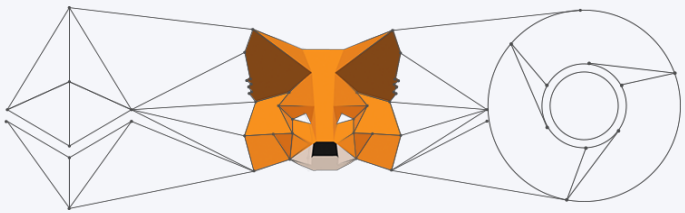
Wallets

Mist



- **MIST is a user interface to access to the Ethereum Blockchain and Daps**
- https://github.com/ethereum/mist/releases
- **Based on GETH**
- **Requires to use your own node**
- **Useful to access private chains and Dapps**

Metamask



- Portable browser wallet
- https://github.com/MetaMask
- Developped by Infura, a Consensys Start Up
- Relies on an architecture of hosted nodes, provided by Infura
- UX is great!
- UX sucks!
- The easiest tool to build your Dapp on

Buidling on Ethereum

Developping languages

Solidity

- TD#3 debriefing
- https://github.com/l-henri/solidity-101
- Important points:
  - Pragma compiler version
  - Contract declaration
  - Contract constructor
  - Contract inheritance
  - Public/private/internal/external functions
  - Structures
  - Types
  - Msg object
  - Payment management
  - Payment fallback functions
  - Importing contracts
  - Using contracts
  - Events

Buidling on Ethereum

Useful tools

Truffle

- Integrated environment to write, test and deploy smart contracts
- Node package
- Folder architecture
- Functions:
  - Compiling
  - Testing
  - Migrating

Ganache

- Easy to use local blockchain
- Easy account management
- Usable with Metamask
- Fast bootup
- Fast transactions
- Easy to test on
- NOT useful to record transactions

Testnets

- Rinkeby testnet
  - Used with GETH
  - Faucet linked with social media
  - Relatively fast to use
  - Easy access through Infura
  - Clique consensus algorythm
- Kovan testnet
  - Used with Parity
  - Faucet requires a Github account
  - Test ETH is called KETH
  - Slightly more permissioned
  - Proof of Authority consensus
- Ropsten testnet
  - Geth and Parity
  - POW based
  - Was DDOSED, which led to creating the 2 other nets

Buidling on Ethereum

Deploying new networks

Consensus algorythms

- Proof of Work
  - High carbon footprint
  - Vulnerable if not the leading network using this algorythm
- Proof of Authority
  - Multiple rounds required
  - Dependant on validator failure
  - Has variants, such as Clique and IBFT
- Raft
  - Used in distributed systems
  - Very fast
  - Highly vulnerable to validator modificiation
  - Only available in private nets

Private blockchains

- Both Parity and Geth offer the possibility to instantiate private networks
- Initiating the network, one needs to take in account various parameters:
  - Consensus algorithms
  - Initial supply
  - Network connectivity
  - Predeployed contracts
- Securing such networks is a challenge

Buidling on Ethereum

Converging towards standards: ERC

ERCs vs EIPs

- EIPs: Ethereum Improvement proposals
  - Similar to Bitcoin's BIPs
  - Related to network infrastructure and consensus
  - Usually proposed on Ethereum Github and associated channels
- ERCs: Ethereum Request for Comment
  - A proposed standard for Smart contracts
  - Related to deployed code, on chain
  - A way to standardize best practices in Smart Contract programmation

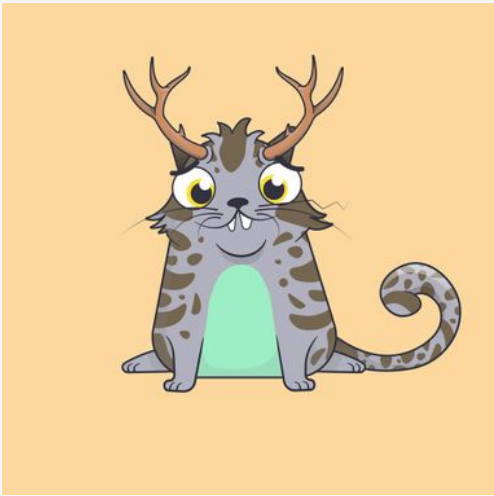
ERC20: Make money money

- A standard for token creation
- https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md
- A simple interfacer to create, exchange and manipulate tokens
- Adopted by most ICOs
- Widely used to list tokens on exchanges

ERC223: Better money

- A new token standard, to mitigate drawbacks of ERC20
- Can you identify ERC 20 drawbacks?
- https://github.com/ethereum/EIPs/issues/223

ERC721: In the beginning were the Kitties



- A standard for non fungible assets token (NFT)
- https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md
- Started by AxiomD, the company behind Crypto Kitties

ERC1400:
Security tokens

- A standard for Security Tokens
- https://github.com/ethereum/EIPs/issues/1410
- After playing cat and mouse with regulation authorities for a while, the Ethereum community is embracing security tokens

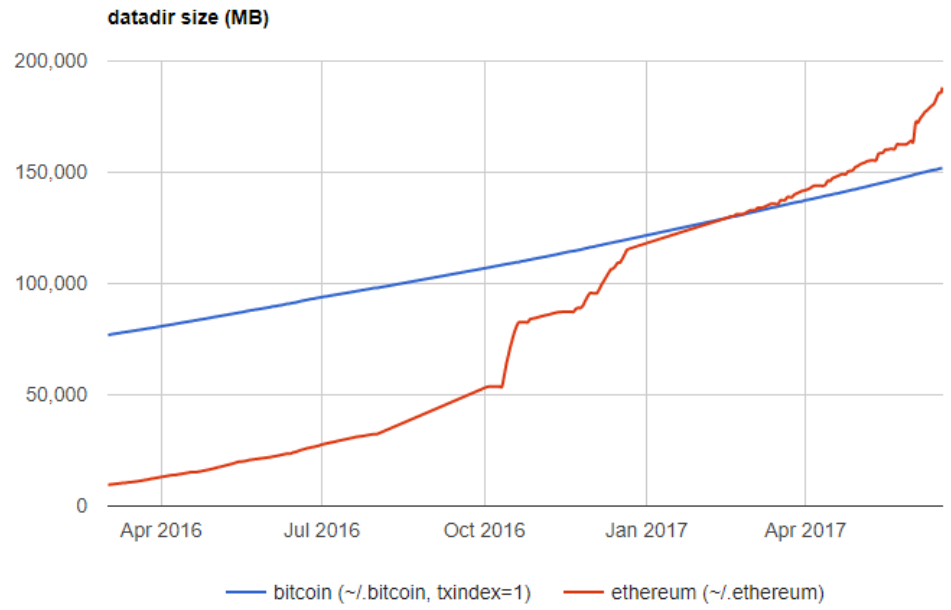
ERCs in practice

- **Presentation by your colleague of his work during last week's TD**
- https://github.com/YOHANMAURIN/Project/tree/master/Ubisoft_Hackathon

Issues with Ethereum today

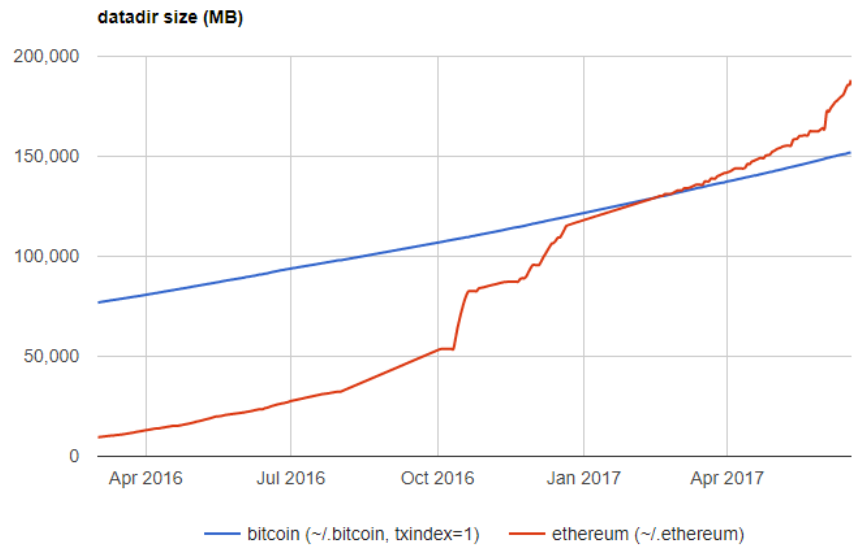
Storage usage

- The Ethereum Blockchain is using more storage each year
- Storage is getting cheaper every year, though
- But something else is not. What is it?



Storage usage

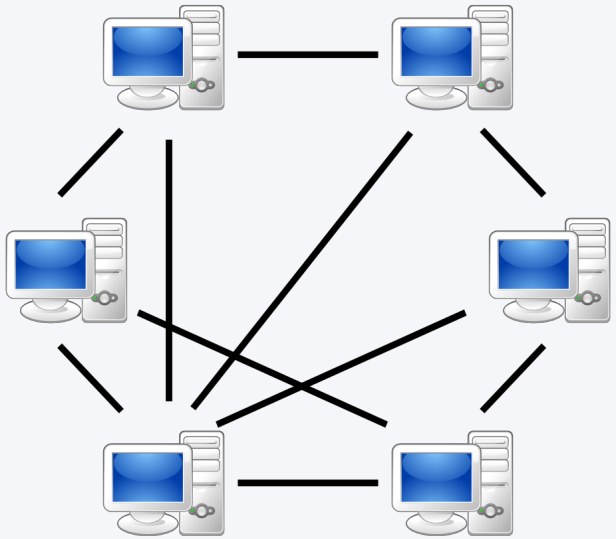
- The memory size (RAM) required to run a full node is growing
  - More powerful computers are now required
  - What will be the impact on the network decentralization?
- New concepts such as contract rent are being introduced; but they will require massive updates on the network.



Bandwidth

- Associated with bigger data sets is bandwidth usage
- Exchanging more information requires bigger pipes
- How to design mobile apps?
  - Based on full nodes?
  - Based on hosted nodes?
  - Based on existing wallets?
- This also leads to synchronization problems: Some nodes are never able to catch up

Network connectivity



- If consumer node can serve the Blockchain to a total of 25 peers (GETH), and requires to be connected to 4 other full nodes to be operationnal and stay in synch with the chain (arbitrary value), and there are 100 000 (common evaluation), what is the maximum user number the network can serve?
- How do you give access to the next X billion humans?
- This problem is present for Bitcoin also. The rationale on Bitcoin seems to be that each user should have its own full node

Network centralization

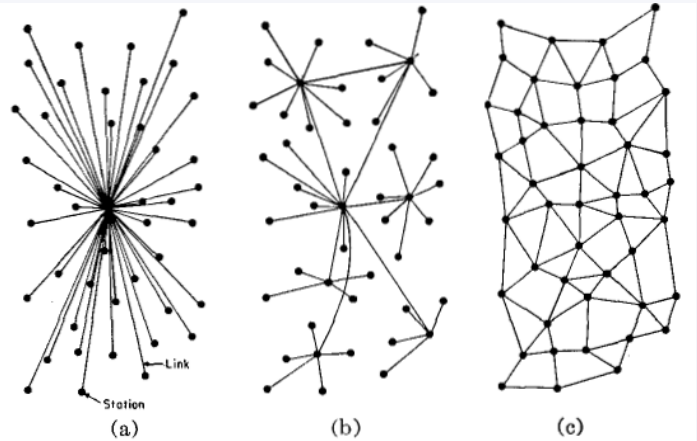
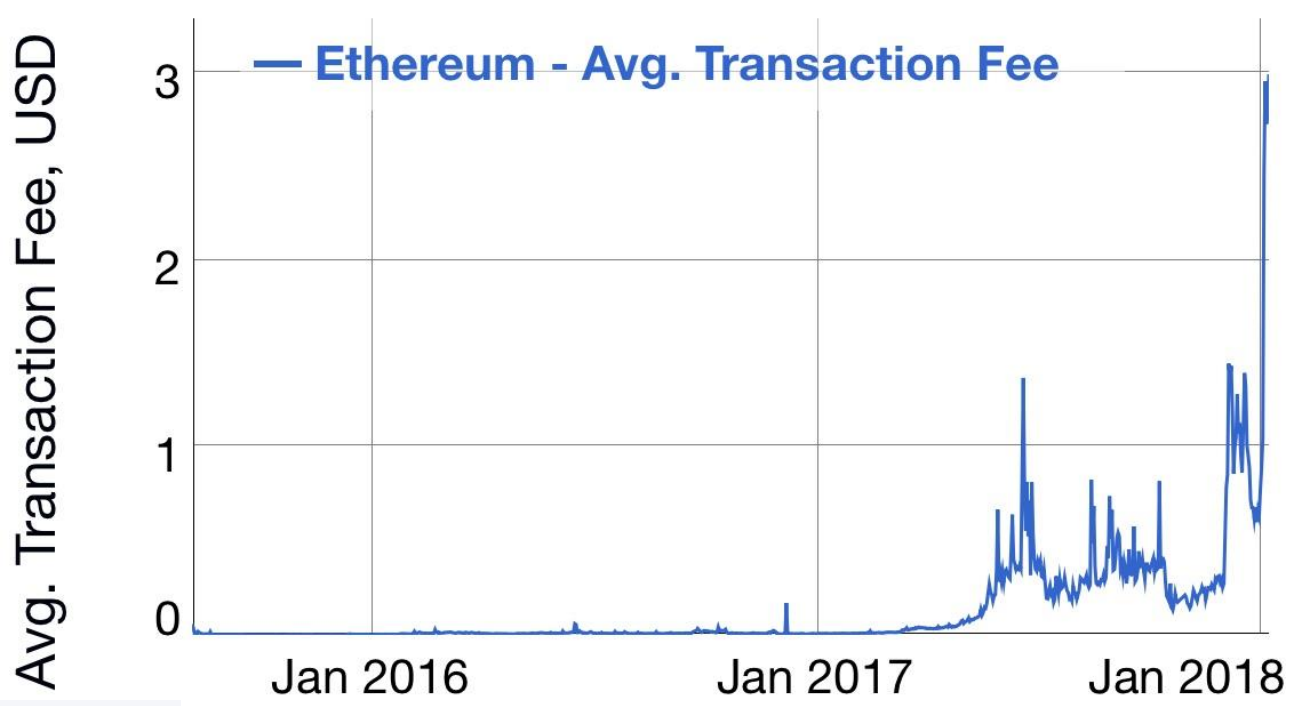


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

- If running a node is more cumbersome than going through a provider, how many end user will end up running nodes in the longterm?
- What will be the political power of architecture providers such as Metamask? Infura?
- Here Ethereum has a specification: Running a node should be doable on dedicated consumer grade hardware, so as not to be dependant on data centers
- But how doable is this, given the current growth of the network?
- https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Rising transaction fees: Come back of kitties



Proof of work: a growing carbon footprint

- The carbon footprint of the POW mechanism is seen as a negative externality by most of the Ethereum community
- If hash power follows price; is the total hashpower/power consumption meant to rise also?
- Does this mean more power generation? Higher energy prices?

Money supply

- Contrary to Bitcoin, the money supply is not fixed in Ethereum
- This decision has been postponed until the introduction of POS
- The delay of POS introduced a bigger inflation than initially expected by the investors
- Currently one of the nastiest debates in the space

Solutions for Ethereum tommorow

Layer 1

Staking

- Staking refers to the act of commiting resources to a system in order to prove one's involvement
- EG: Qt the entrance of ESILV, if you are not a student, you can « stake » your id card in exchange for a visitor's pass. That way, the front desk knows for sure that you will be back
- In a decentralized application, a user can stake resources and in exchange get a specific role assigned. If he cheats, his stake can be taken. If he behaves correctly, he can get a reward
- Proof of work is a form of staking electricity and capital

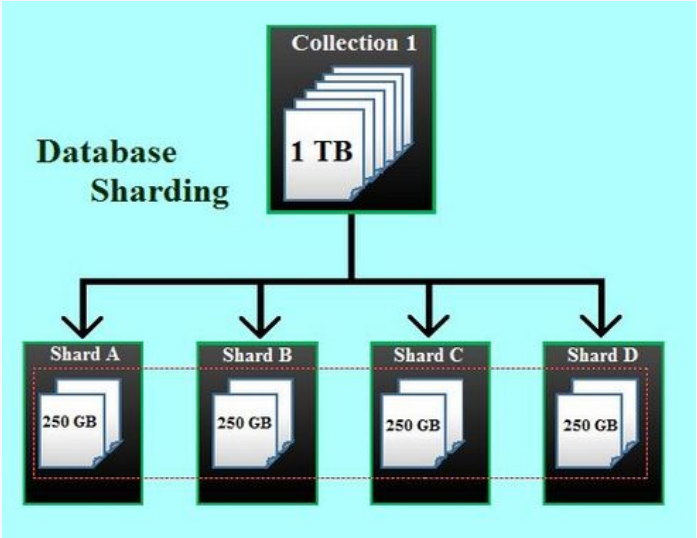
Proof of stake

- Proof of stake (PoS) is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In PoS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e., the stake)In a decentralized application, a user can stake resources and in exchange get a specific role assigned. If he cheats, his stake can be taken. If he behaves correctly, he can get a reward
- This has been an objective of Ethereum since its inception
- Two main branches: Casper FFG and Casper
- Recently, efforts where gathered around Casper and its lead architect, Vlad Zamfir

Proof of stake

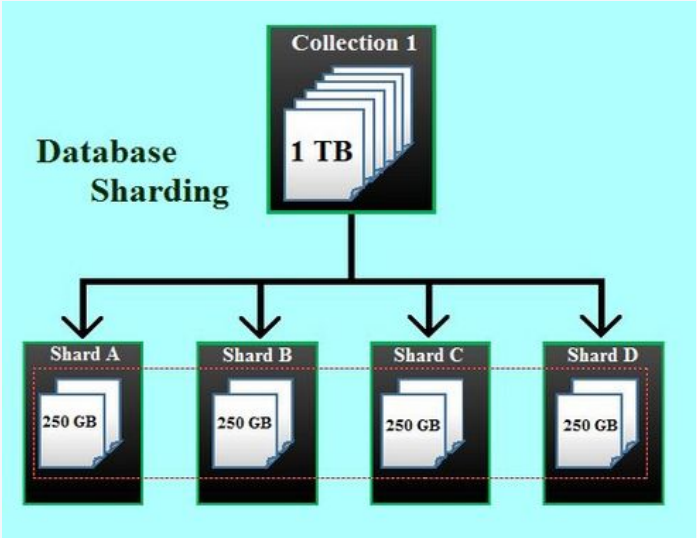
- The minimum requirement for staking is aimed for 32 ETH
- Along with Staking comes Slashing: whats happens to bad stakers
- Design issues are different than Proof of Work
  - Nothing at stake
  - Long range attacks
- Scheduled upgrade « before 2020 »; but a moving goalpost
- It is being considered to keep POW and POS alongside as a first step

Sharding



- A database management technique: split the data between servers
- In the Ethereum Blockchain, the objective would be to have shards which are all tethered to a main Blockchain
- The main chain should be able to check the integrity of the shards
- Users can keep track of a handfull of shards, which they are interested in
- Transfer between shards should be possible

Sharding



- As with POS, it has been an objective for a long time
- It was considered to do both upgrade separately
- Since 2018, it has been decided to perform an upgrade together: POS + sharding

Solutions for Ethereum tommorow

Layer 2

Truebit

- Truebit uses the Ethereum Blockchain as a contract execution repository
- Each contract contains all the logic required to execute it
- User can provide execution results, without executing the contract onchain
- The contract is executed off chain
- Other users can act as auditors
- If they see an incorrect code execution, they can challenge it
- This protocol allows for large code executions to be done offchain

Plasma

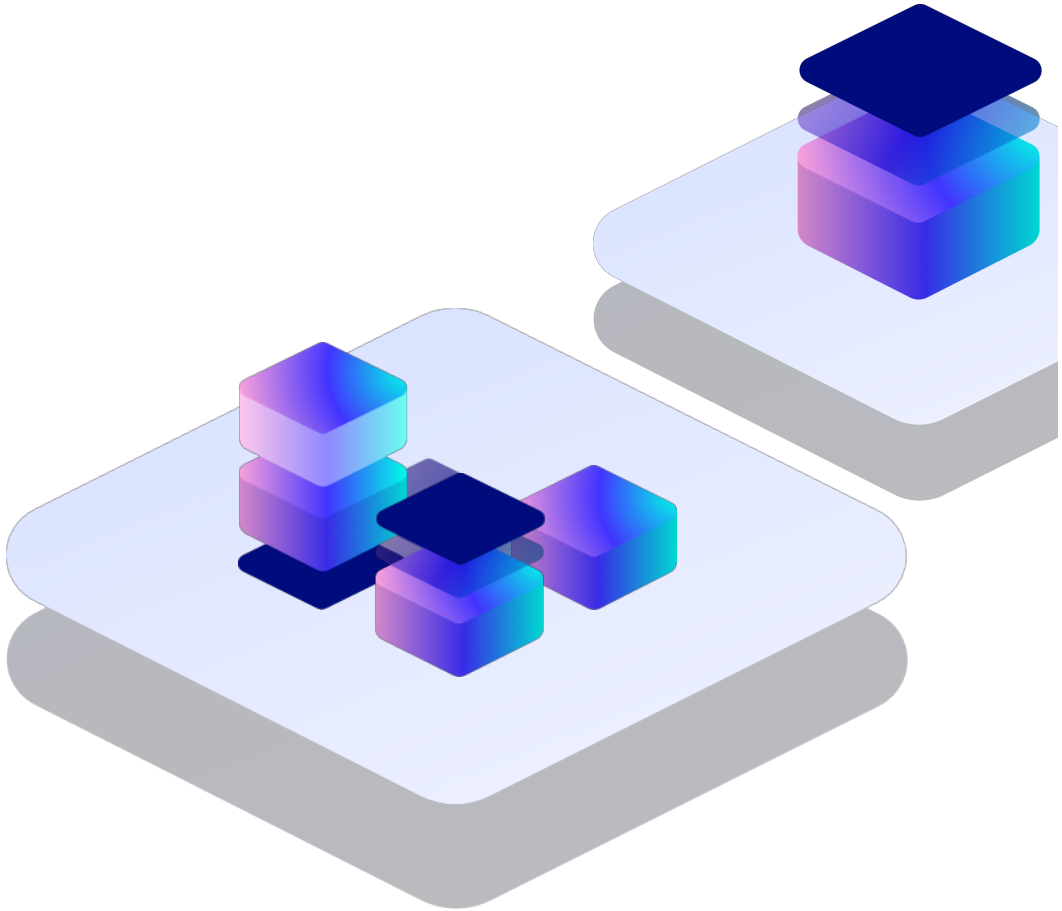
- Plasma is considered as one of the most promising and readily solution to scaling
- Loom networks is currently focusing on this topic, among other groups
- As in Lightning network, users transact outside the main chain, on a secondary chain
- Users get receipts and proofs of ownership on the secondary chain
- In case they want to leave the chain, they can redeem their tokens/assets with these receipts

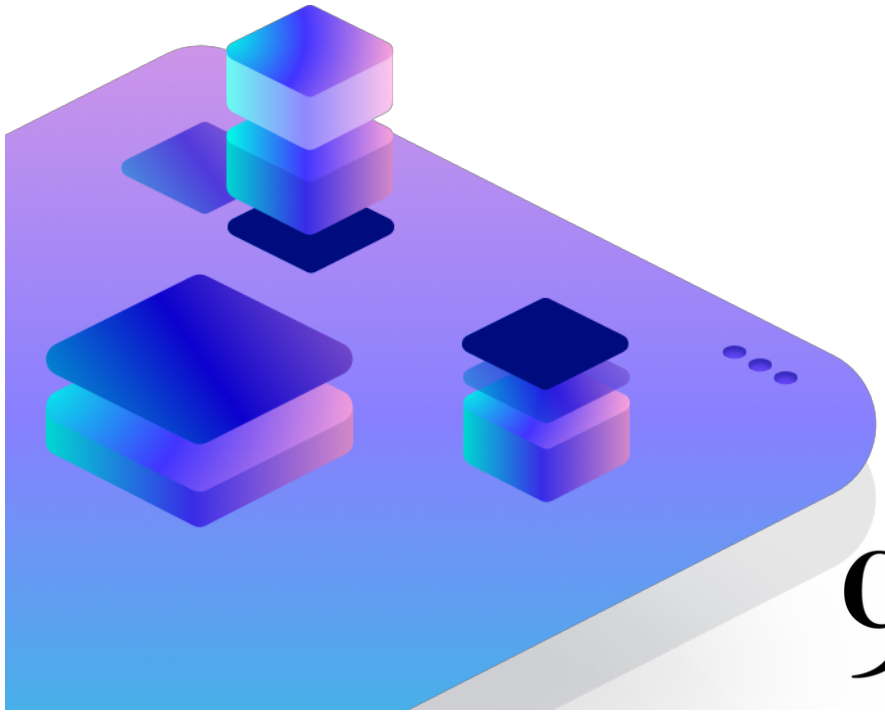
Plasma

- The main disadvantage of Plasma is that it does not come in a single shape
- Each plasma chain will have its specificities
- Each plasma chain needs to deploy its own architecture
- Plasma chains might not be able to comunicate with one another
- However, for application specific networks such as games, it can make sense

Merci

pour votre attention !





klsn.io

Twitter: @97network
Hello@97.network
Station F, 5 parvis Alan Turing, 75013 Paris
Github.com/97network