Laura Emilia Maria Ricci

Blockchain under the lens: insights from the Pisa DLT Lab

DeFI & Crypto Workshop

Scuola Normale Superiore

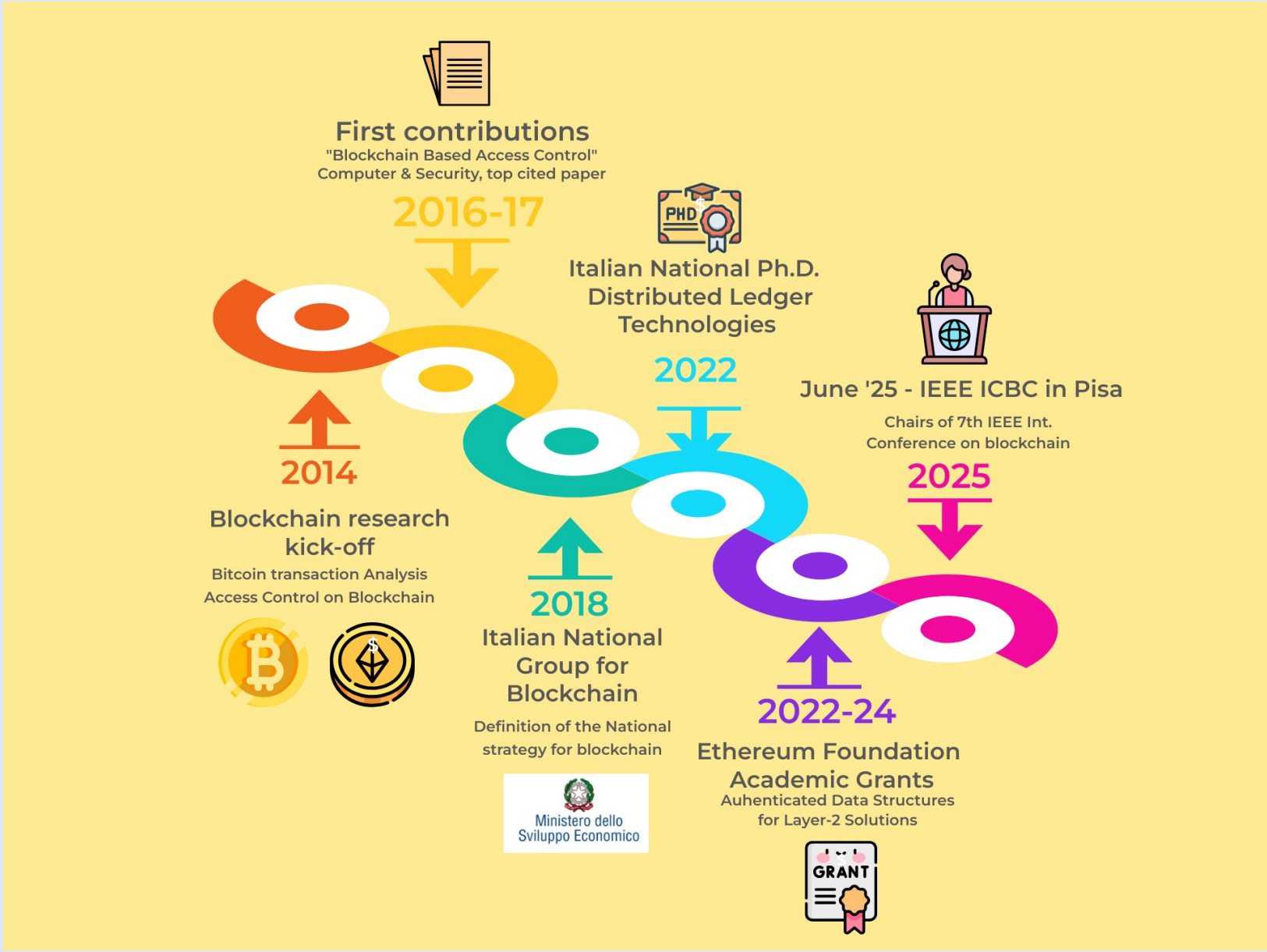
January 28th 2025

DLT LAB'S TEAM

- 2 full professors
- 1 associate professor
- 1 RTT (tenure track)
- 1 research associate
- 1 post-doc
- 7 Ph.D. students
- several collaborations
  - Italian National Research Council, CNR
  - University of Florence
  - Bank of Italy
  - University of Cambridge, UK
  - University of Surrey, UK
  - KAUST, South Arabia

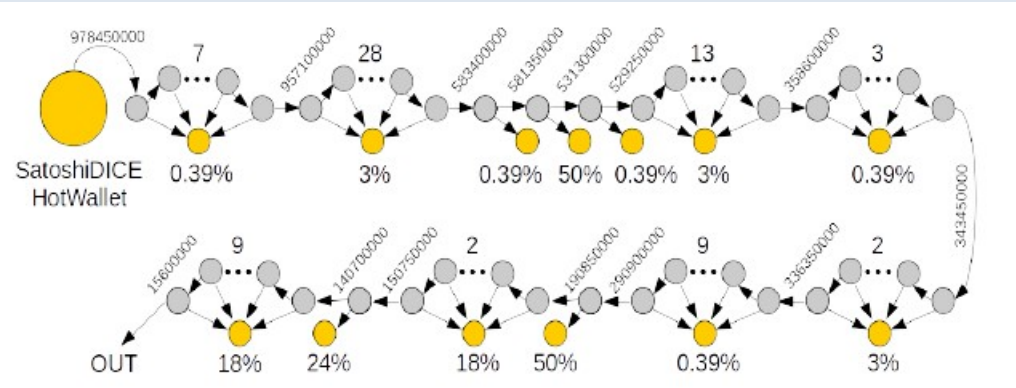
https://sites.google.com/unipi.it/pisadltlaboratory

DLT LAB MILESTONES



LAB'S ACTIVITIES AT A GLANCE

On-chain data analysis



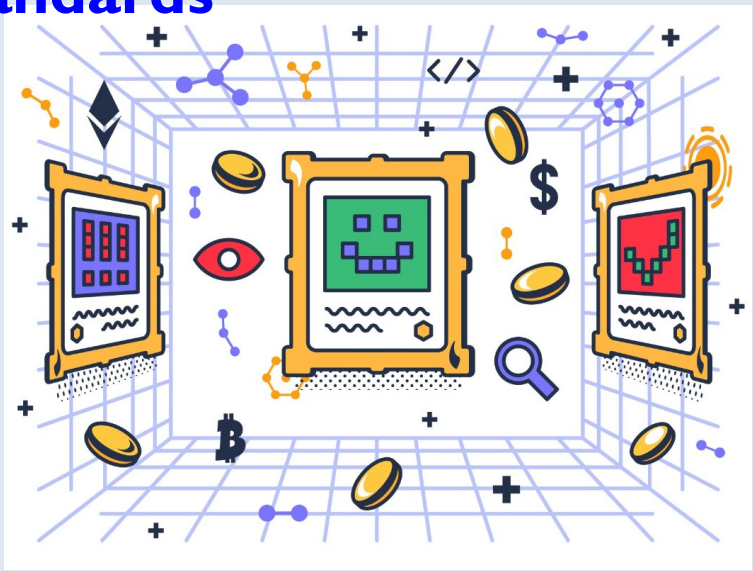
- Bitcoin, analysis of
  - the whole transaction network
  - gambler behaviour and betting strategies
  - deanonymization
  - taint analysis for ramsomware
- Ethereum, analysis of
  - token network (ERC-20, ERC-721, ER-1155)
  - DeFi Protocols: UNISWAP

Off-chain data analysis: Crypto Exchangers artificial behavious

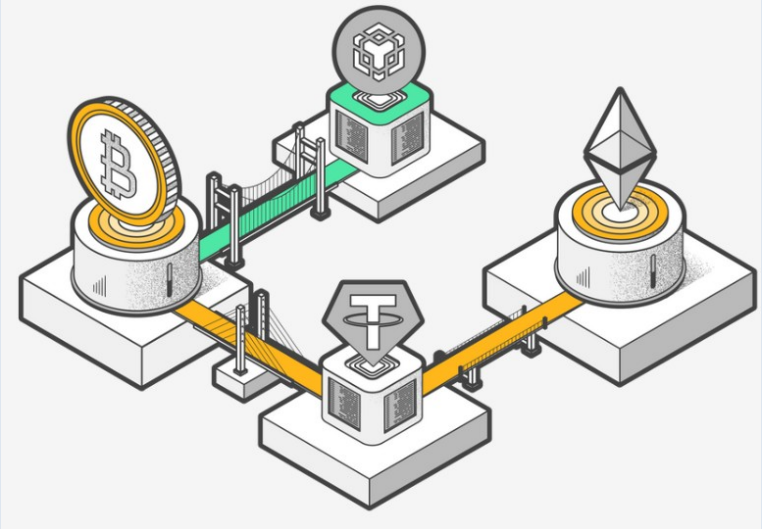
LAB'S ACTIVITIES AT A GLANCE

new token Standards

- NMT (Non Fungble Mutable Token): mutable assets protected with access control policies
- integration with
  - Self Sovereign Identity
  - privacy preserving mechanisms



Cross Chain Solutions

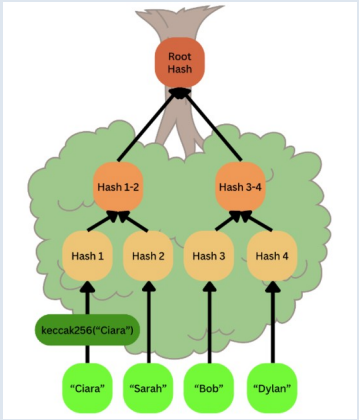


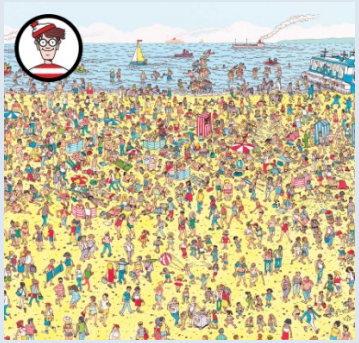
- exchanging data between different blockchain through IBC of COSMOS
- enhancing the COSMOS inter-chain protocol with access control for inter-chain transactions ontrol

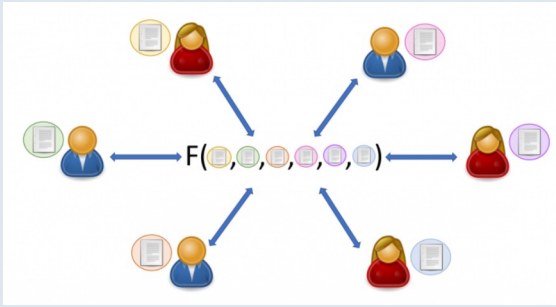
LAB'S ACTIVITIES AT A GLANCE

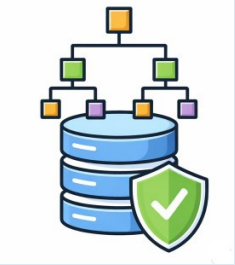
Advanced Cryptograpy Tools

- evaluating cryptographic libraries
  - Merkle Trees and their alternatives
  - Zero Knowledge Proofs (ZKP)
  - Fully Homorphic encryption (FHE)
  - Multiparty computations (MPC)
  - Authenticated Data Structures (ADS)
- goal: testing performances, usability, integration with the blockchain





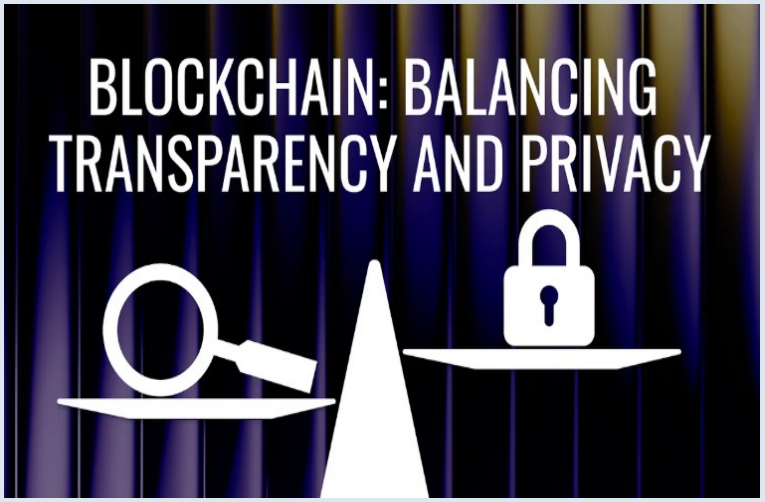




LAB'S ACTIVITIES AT A GLANCE

Applying Advanced Cryptography

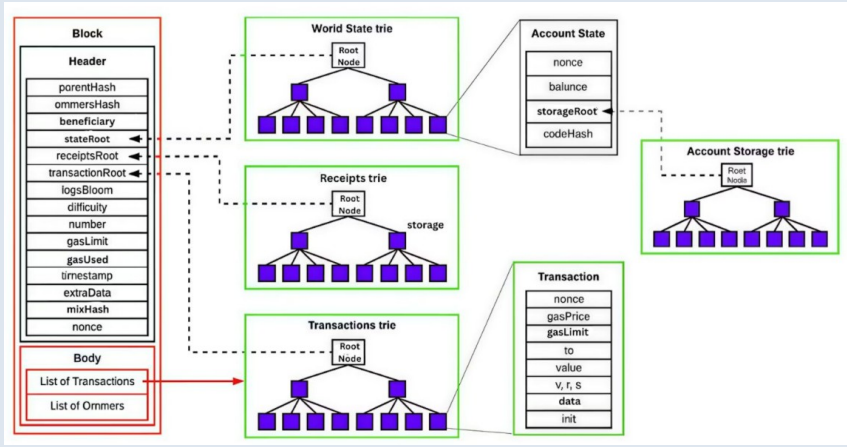
- ZKP-based and FHE-based access control systems
- applications exploiting ZKP roll-ups
  - verifiability without disclosure
  - scalability: heavy computation off-chain and verification on chain
  - verifible data structures
- we plan to investigate
  - privacy in financial transactions: hidden balances and trades
  - secure computation on encrypted data applied to `DeFi` protocols



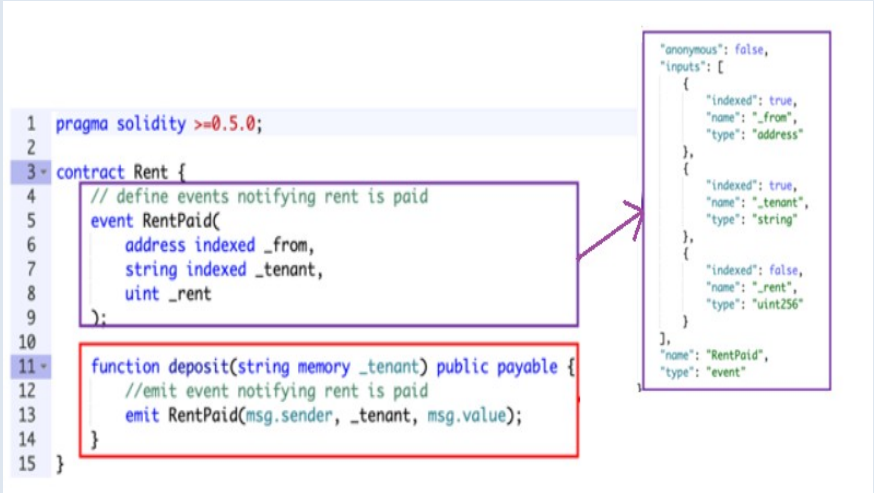
ON-CHAIN DATA ANALYSIS

ETHEREUM STATE

- Ethereum state
  - full contract storage must be read and interpreted
  - complex computations may be required to reconstruct history
  - requires access to full blockchain



- Ethereum events
  - contracts emit events when actions occur
  - act as a log for off-chain consumption
  - indexed and queryable
  - enable not only notifications and monitoring, but also analytics



OUR METHODOLOGY

- exploiting events emitted by the contracts to analyse token protocols
  - easier than rebuilding the whole `Ethereum` state

```
event Transfer(address indexed _from, address indexed _to,
    uint256 _value)

event Approval(address indexed _owner, address indexed _spender,
    uint256 _value)
```

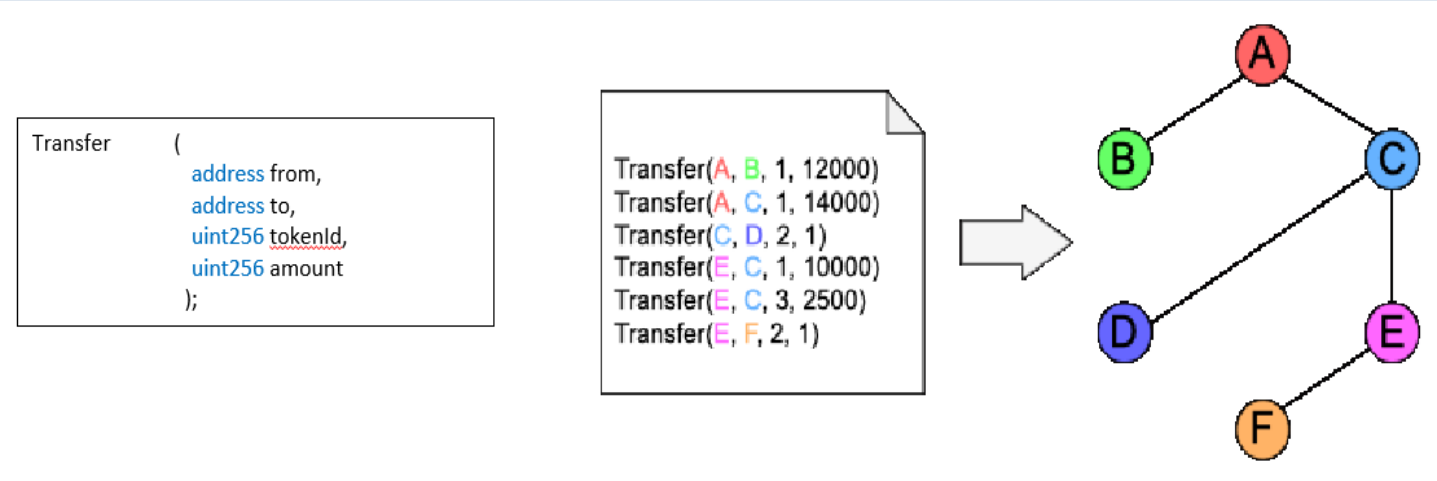
- each event is recorded on the blockchain as transaction receipts


```
{
  ...
  "logs": [{
    "address": "0xdac17f958d2ee523a2206206994597c13d831ec7",
    "topics": [
      "0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef",
      "0x000000000000000000000000a9e6cf4e3157670a3b991c25d6f4fcbd9419c03",
      "0x000000000000000000000000e5c78023c283dde16b6feab95d7d8d8ba1f785e"
    ],
    "data": "0x0000000000000000000000000000000000000000000000000000000241b02f00",
    "blockNumber": "0x8c4731",
    "transactionHash": "0
     xb213c5e15ba8c8d86c482fc11ad8e0521f11f2eb464f75ac72a5dc4520f33b53",
    ...
  }],
  ...
}
```


- loss of accuracy: not all information is available in the event

OUR METHODOLOGY: GRAPH ANALYSIS

- build a graph from events: transfers of tokens signaled by transfer events publicly recorded on chain: represent users (addresses) by nodes of the graph, transfers by edges
- perform graph analysis on the resulting graph
- graph properties: diameter, clustering coefficient, density, connected components, communities,..



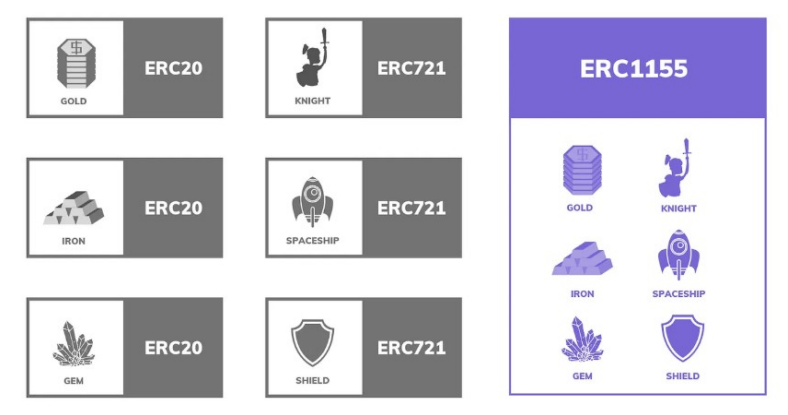
ANALYSING ERC-20 AND ERC-721

- analysis of the topological properties of the top 100 ERC-20 and ERC-721 token contracts by number of transfers
- using the numerical features associated with each network to perform a clustering-based analysis with two main objectives
  - identify groups of networks with similar topological features
  - determine whether networks with similar topological characteristics correspond to contracts with the same application domain

- Comparing Ethereum fungible and non-fungible tokens: an analysis of transfer networks, M. Loporchio, D Di Francesco Maesa, A Bernasconi, L Ricci, Applied Network Science 9 (1), 72

- Analysis and Characterization of ERC-20 Token Network Topologies,M. Loporchio, D Di Francesco Maesa, A Bernasconi, L. Ricci, International Conference on Complex Networks and Their Applications, 344-355

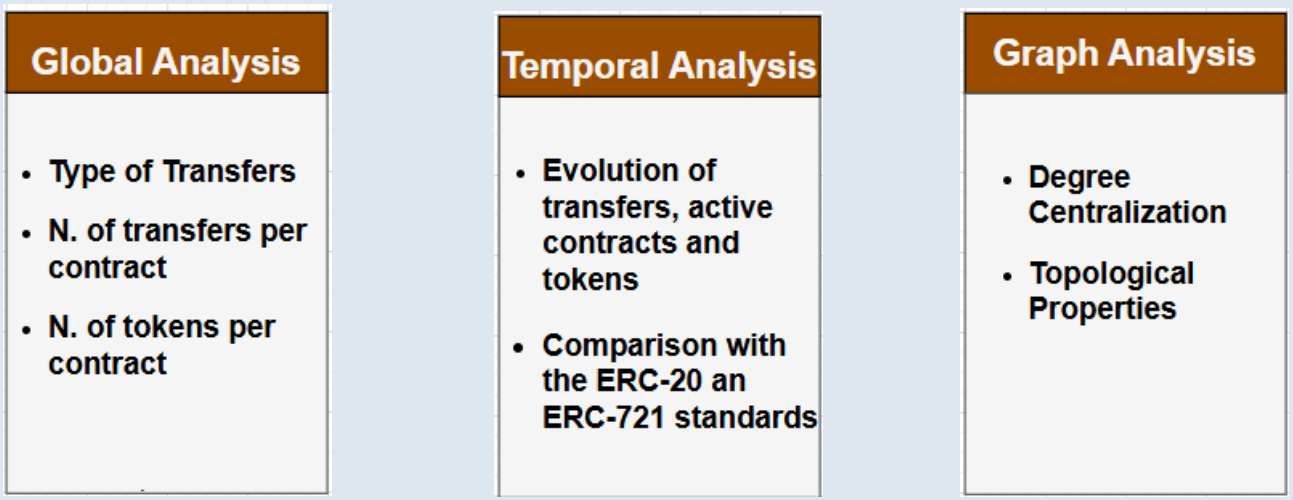
ANALYSING ERC-1155 TOKENS



- manage multiple fungible and non-fungible tokens within the same contract
  - supports single and batch transfer mode
- benefits:
  - reduce transaction costs and more efficient use of blockchain resources
  - simplify DApp development
- research question
  - how does the introduction of the new standard affect the behaviour of the Ethereum users?
  - which functionalities of the new standard are more used by the users?

ANALYSING ERC-1155 TOKENS

- dataset: all Ethereum blocks from height 0 to 21 525 890 included
- time period between July 30th, 2015 and December 31st, 2024

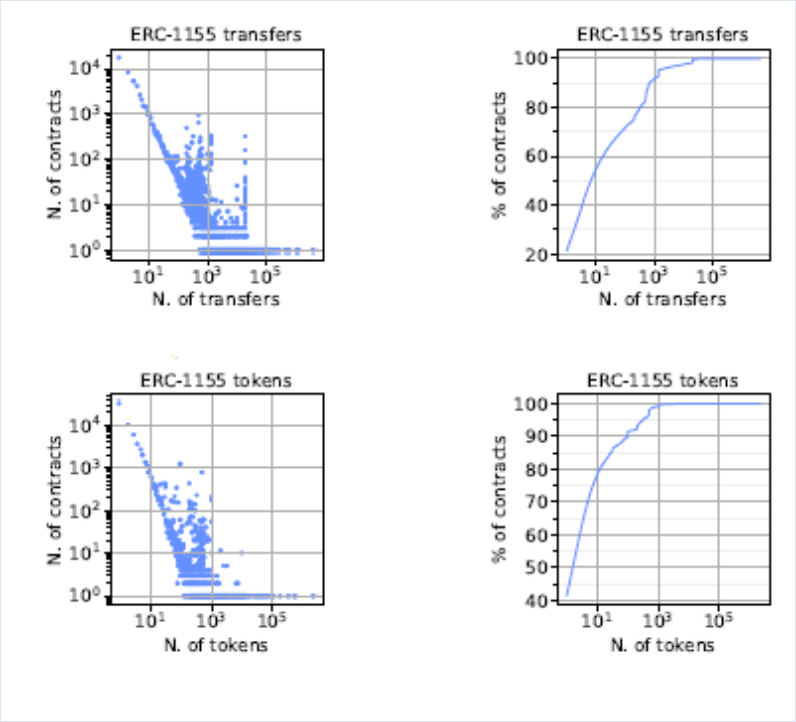


- ERC-1155 under the lens: a graph-based analysis of the Ethereum multi-token standardM Loporchio, D Di Francesco Maesa, A Bernasconi, L Ricci, Accepted for pubblication Applied Network Science

- Analyzing ERC-1155 Adoption: A Study of the Multi-token Ecosystem, M. Loporchio, A Bernasconi, D Di Francesco Maesa, L Ricci, Complex Networks & Their Applications XIII, 2024

ERC-1155 : GLOBAL ANALYSIS

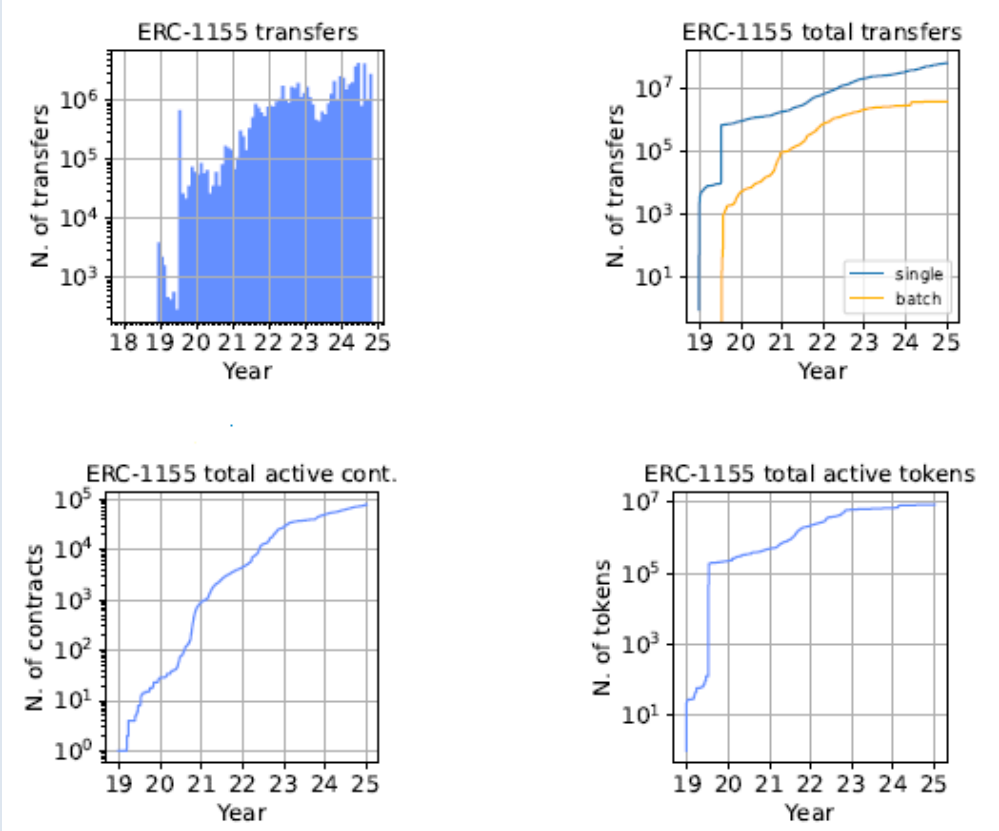
- 91% of all transfer events are of type `TransferSingle`
  - the batch functionality is less frequently used
- a big amount of contracts produce a single transfer
  - minimal activity for many activated contracts
  - only a 10% of the accounts produce more than 1000 transfers
- 80% of the contracts manage a single token



ERC-1155 : TEMPORAL ANALYSIS

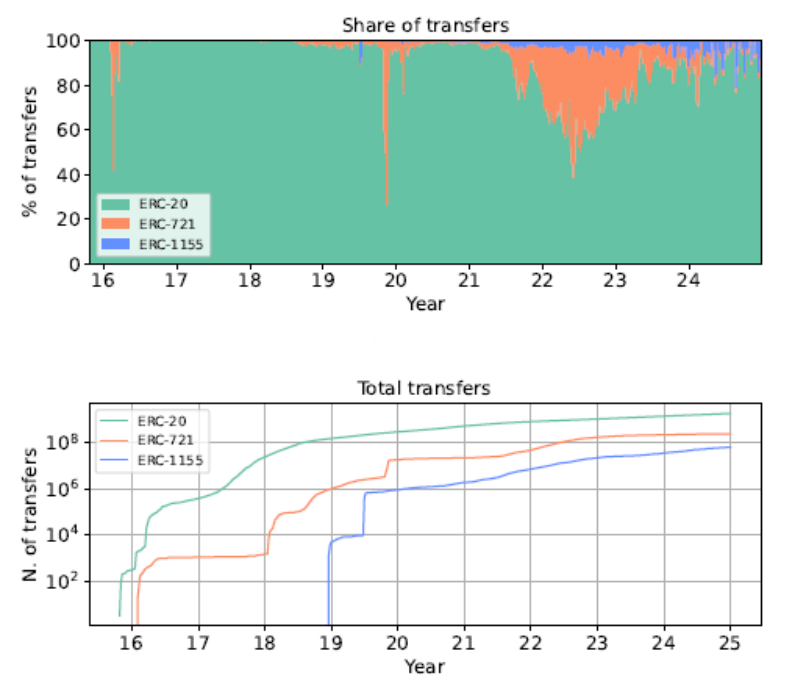
- the launch of the Enjin platform (July 2019) caused a sharp increase in transfers and active tokens

- batch transfers have consistently been less utilized w.r.t. single transfers

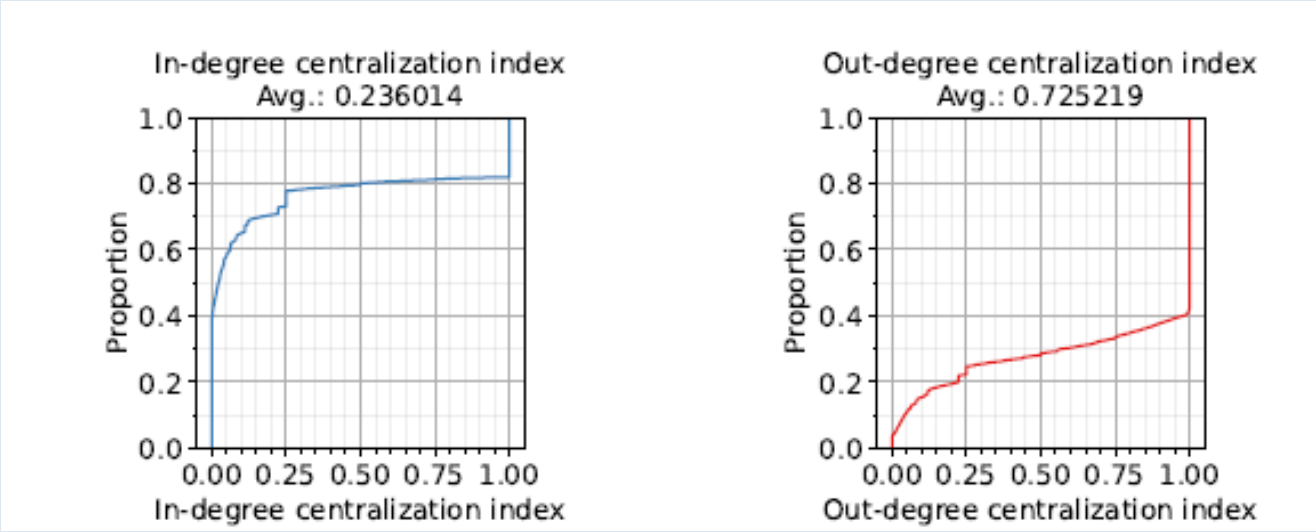


ERC-1155: TEMPORAL ANALYSIS

- ERC-20 transfers are predominant for most of the time
- the launch of the Enjin platform in July 2019 provided a significant initial boost to ERC-1155 adoption
- ERC-1155 adoption is increasing and is slightly below the ERC-721 transfers at the end of 2024



ERC-1155: DEGREE CENTRALIZATION

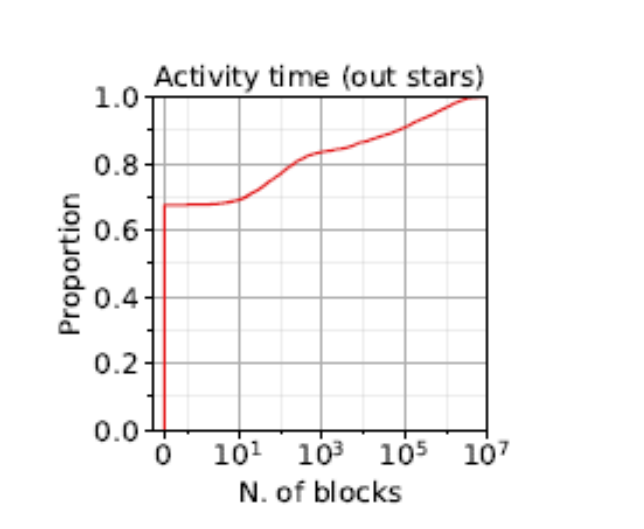


- build a graph for each ERC-1155 contract, after a filtering step
- computation of the normalized degree centralization index
  - sum of the deviations from maximum degree
  - normalized by dividing the score by that of a star graph with the same number of vertices
- about 20% of the graph have an in degree index equal to 1, while 60% have an out degree equal to 1

ERC-1155: OUT DEGREE STARS

- airdrop campaigns: a single central entity (either an honest promoter or a spammer) massively distributes tokens "in one go" to arbitrarily selected recipients
  - marketing strategies where users receive free tokens from a single central entity to promotea new project or reward current community members
  - pishing purposes
- degree centralization appears consistent with these behaviours
- `Alchemy`'s service returns that about 80% of the out-degree star contracts are classified "spam" (suspect behaviour)

ERC-1155: OUT DEGREE STARS

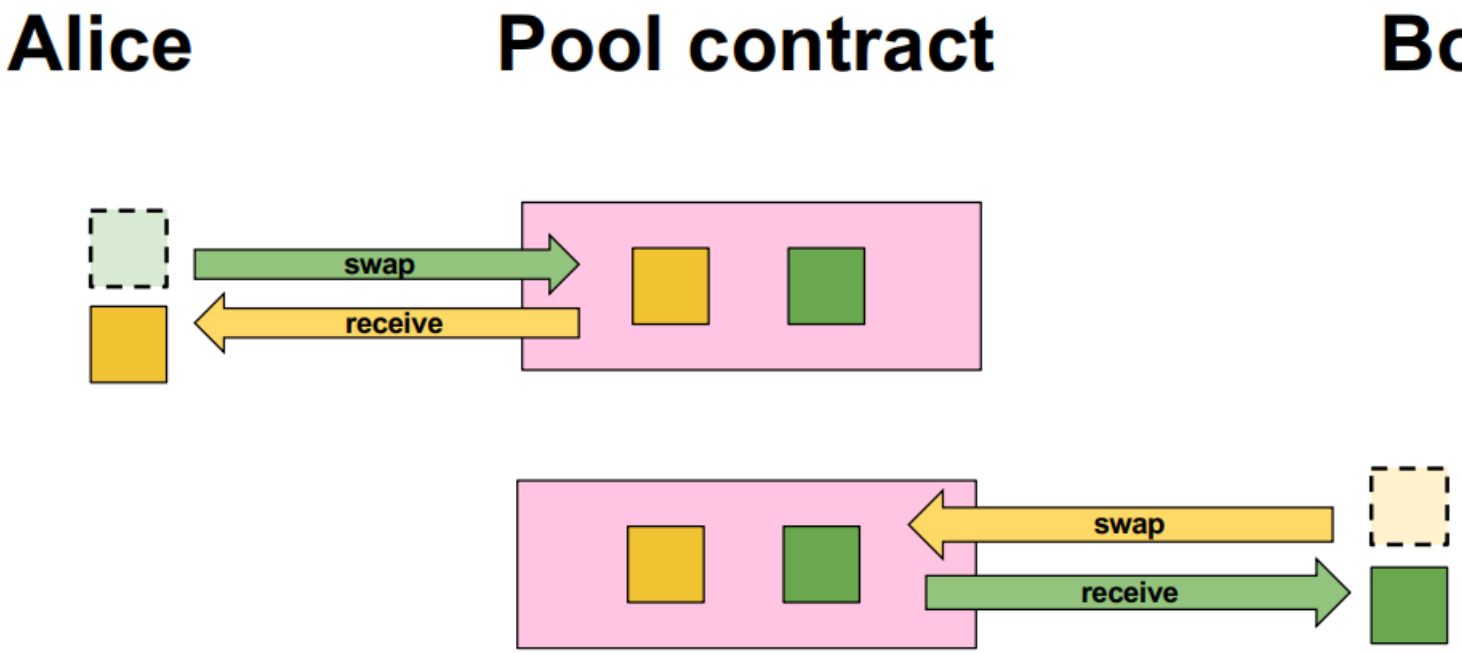


- contract activity: number of blocks between the first and the last transfer recorded in the dataset
- cumulative distribution for contract activity times for out degree star networks
- typical behaviour for "in one go" distribution of tokens, consistent with airdrop campaigns

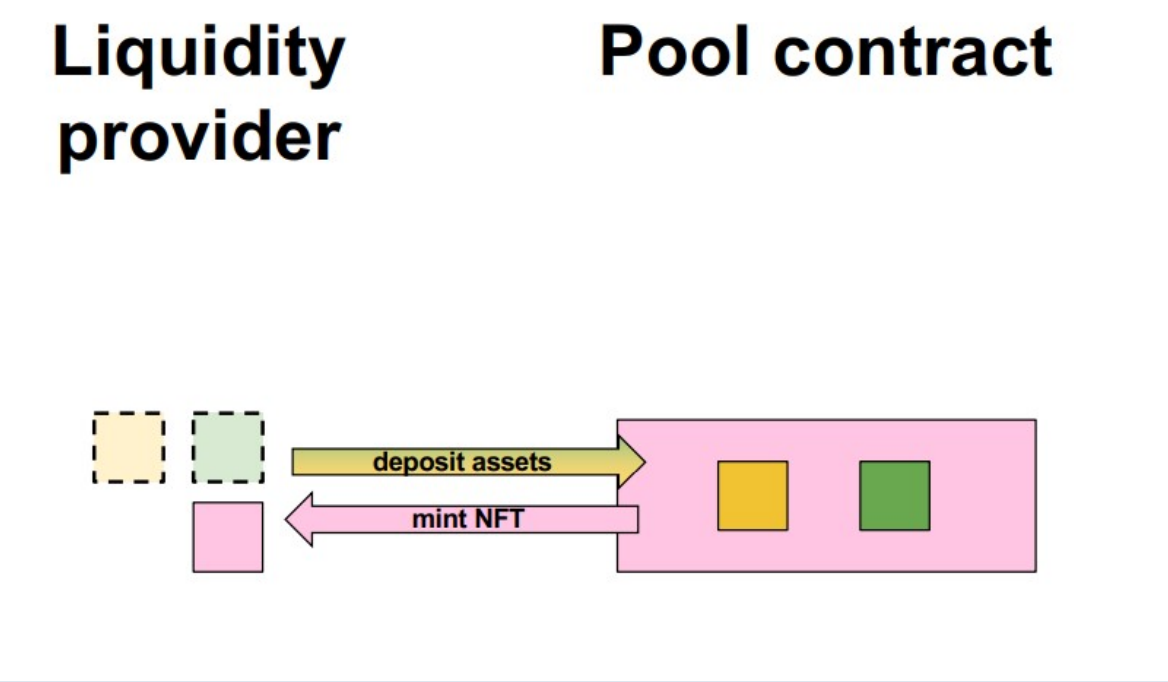
UNISWAP AT A GLANCE

- `Decentralized Exchange (DEX)` : enables peer-to-peer trading directly on the blockchain
- `built on Ethereum`: operates through smart contracts, ensuring transparency and trustless execustion
- `Automated Market Making`: uses liquidity pools instead of traditional order books to facilitate trades
- `Permissionless Access`: anyone can trade or provide liquidity without approval
- `Core DeFi Infrastructure`: widely used as a foundational protocol in the decentralized finance ecosystem

UNISWAP V3: TRADING

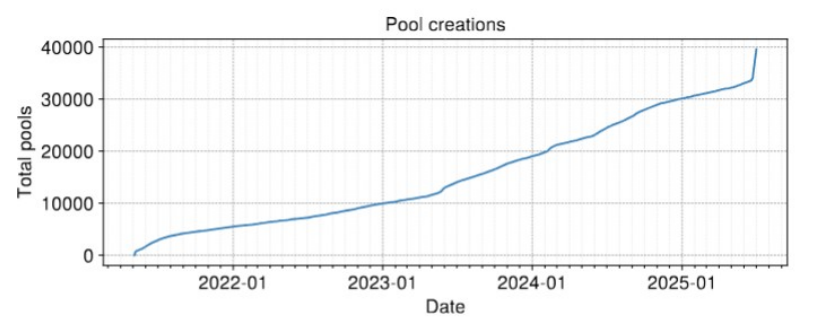


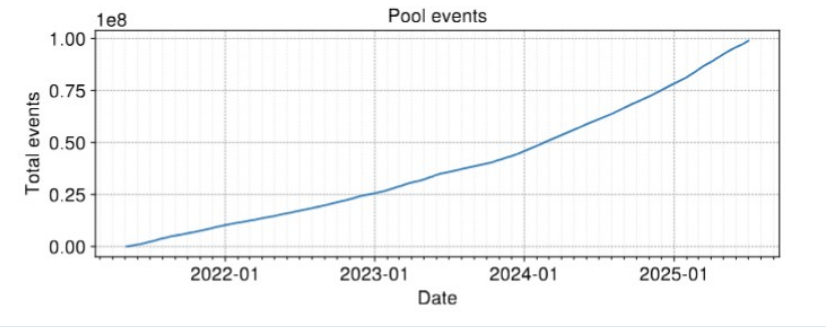
UNISWAP V3 : ADDING LIQUIDITY



- Uniswap V3 liquidity positions are represented as LP NFTs
- each position (NFTs) is subject to a distinct and customizable set of parameters that determines its value and rewards.

UNISWAP ANALYSIS: PRELIMINARY RESULTS





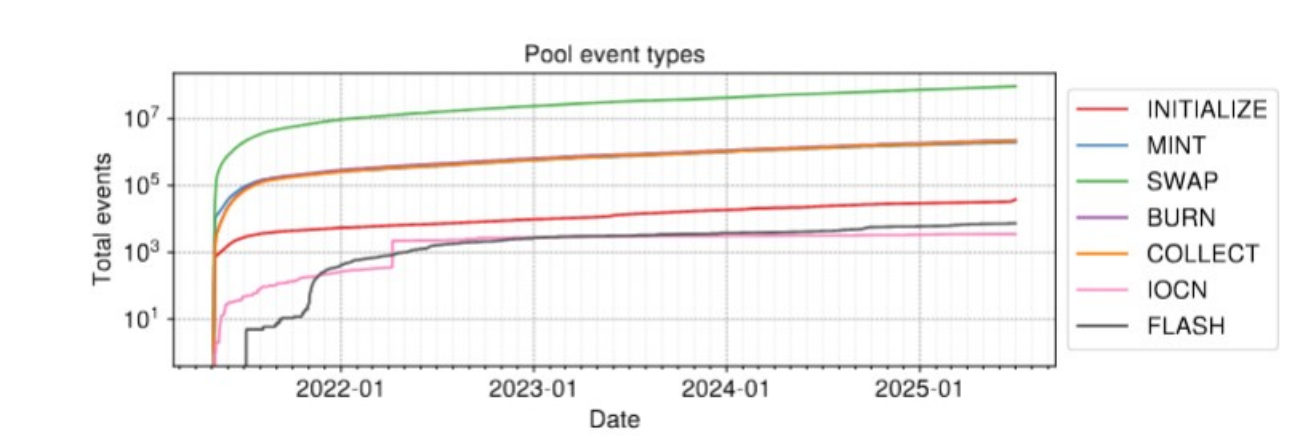
Token	Symbol	Frequency	Percentage
0xc02aaa39...6cc2	WETH	29,213	75.925
0xa0b86991...eb48	USDC	2,589	6.729
0xdac17f95...1ec7	USDT	2,560	6,653
0x6b175474...1d0f	DAI	486	1.263
0x2260fac5...c599	WBTC	310	0.806
0x69825081...1933	PEPE	114	0.296
0x1f9840a8...f984	UNI	97	0.252
0x7f39c581...2ca0	WSTETH	81	0.211
0x33ba0f96...6202	nsurance	79	0.205
0xf19308f9...65b1	TitanX	79	0.205

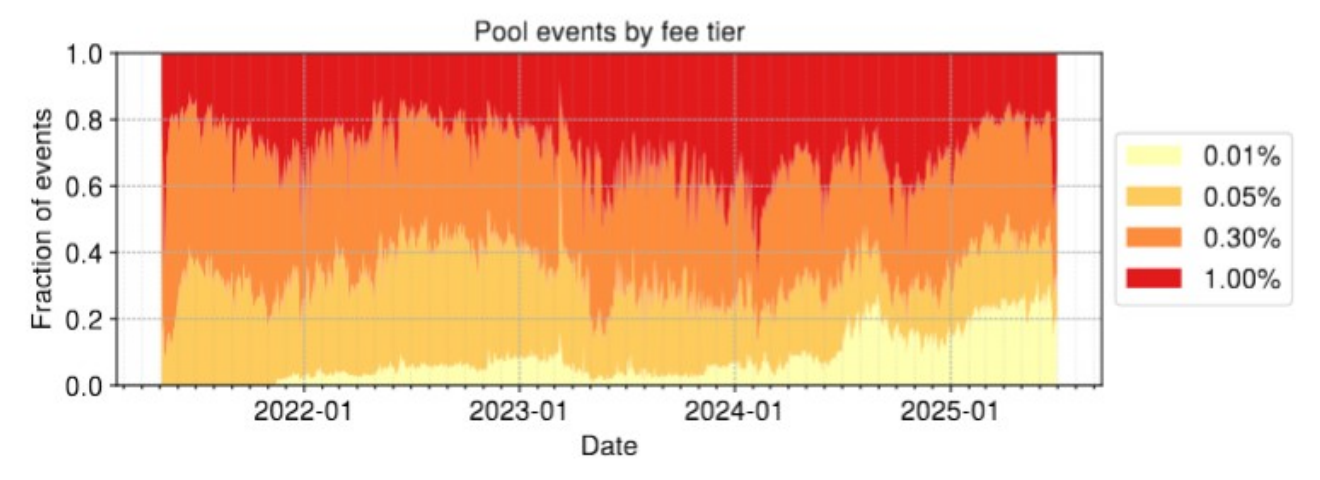
top 10 most frequent tokens among liquidity pools.

the dataset used includes all events generated by `Uniswap` pools on the `Ethereum mainnet` from

- `May 4th, 2021 19:52:36 UTC` (i.e., the launch date of `version 3`)
- `to June 30th, 2025 23:59:59`

UNISWAP ANALYSIS: PRELIMINARY RESULTS



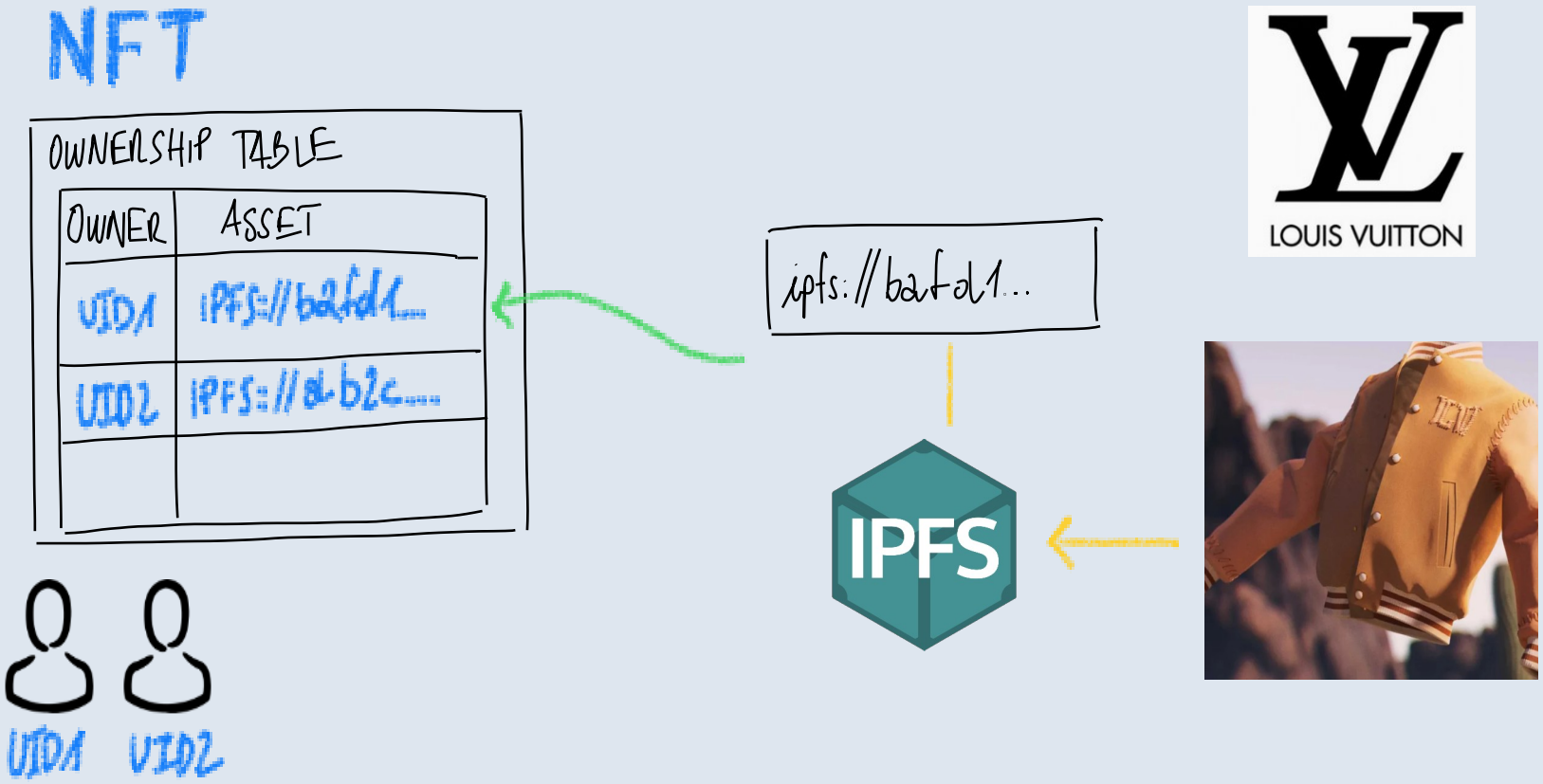


UNISWAP V3:
FUTURE ANALISIS AND EXPLORATION

- a huge amount of on-chain data is generated by the UNISWAP V3 ecosysem, and we plan to perform several further analysis
- liquidity provision and removal (Mint and Burn events)
  - track the total liquidity per pool or token pair
  - analyse liquidity providers (LP) behaviour: how often liquidity is added or removed
  - identify whale LP vs retail LP
  - measure average LP holding period
- fees
  - see which fee tier are most used
  - compare trading volume per fee tier
  - compute accumulated fees based on liquidity ranges

NEW NFT MODELS

ERC-725 IS NOT ENOUGH



ERC-725 IS NOT ENOUGH

NFT

OWNERSHIP TABLE

OWNER	ASSET
UID1	IPFS://b2fd1...
UID2	IPFS://a-b2c...

ipfs://b2fd1...

IPFS

LOUIS VUITTON

UID1 UID2

MUTATE THE ASSET

CHANGE SLEEVES COLOR

ERC-725 IS NOT ENOUGH

NFT

OWNERSHIP TABLE

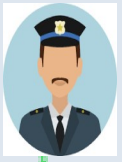
OWNER	ASSET
UID1	IPFS://b2fd1...
UID2	IPFS://a-b2c...

UID1 UID2

ipfs://b2fd1...

IPFS

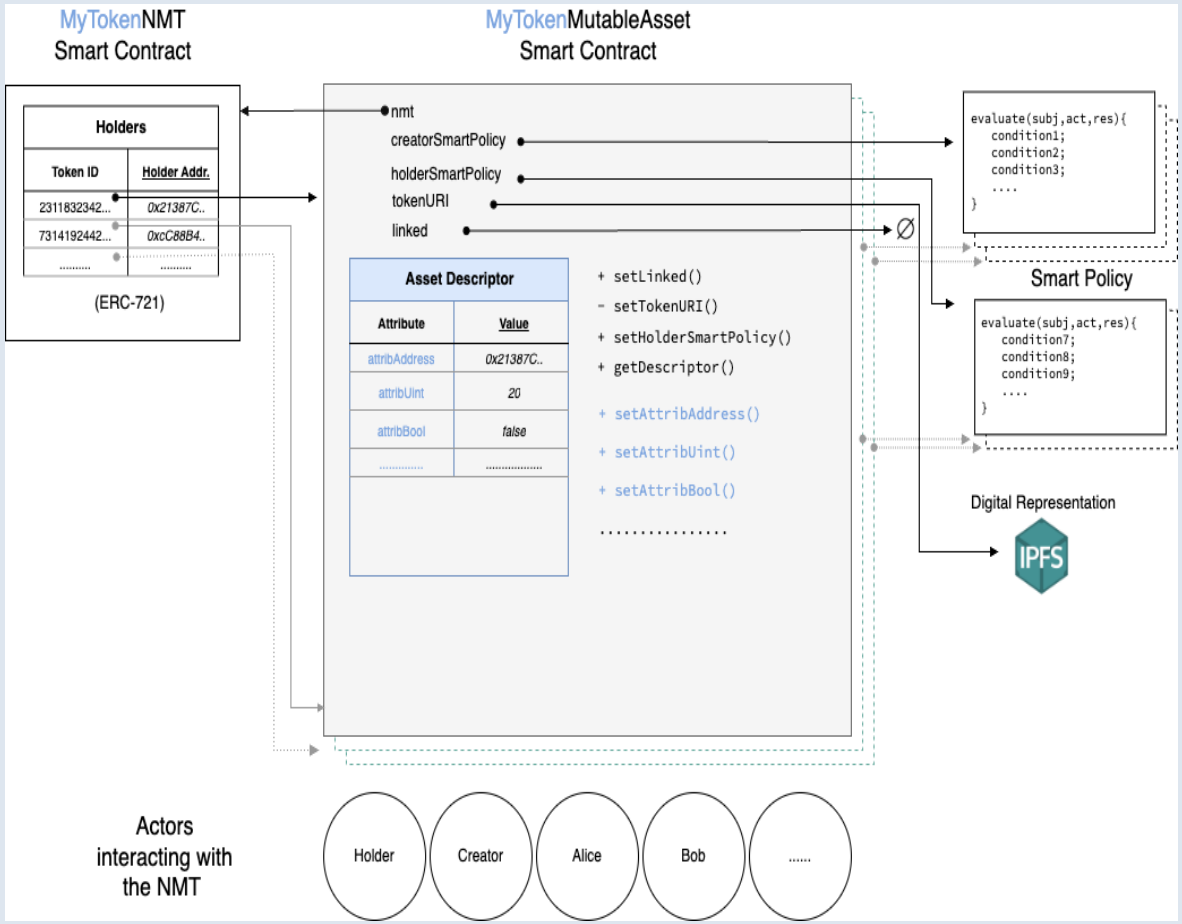
CONTROL OVER MUTATION



CONTROL

CHANGE SLEEVES COLOR

NMT ARCHITECTURE



- Protecting non fungible mutable tokens: an application in the metaverseDDF Maesa, F Donini, P Mori, L Ricci, 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2024)

NFT IN DeFi


Governance & Access
DAO Voting, Admin Keys
Collateral & Lending
NFT-Based Loans
Gamification
Achievement NFTs
Insurance & Risk
NFT Coverage
NFT
Yield & Staking
Reward Programs
Synthetic Assets
NFT Derivatives
Real-World Assets
Tokenized RWAs
Identity & Reputation
On-Chain Profiles
Real-World Assets
Tokenized RWAs

ERC-721 IS NOT ENOUGH FOR DeFi

- NFT ERC-721 are not mutable (dynamic), while financial positions (staked tokens, rewards, privileges,…) are mutable
  - can add more tokens to your stake
  - can earn rewards
- NFT ERC-721 do not offer proper mechanism to define complex access policies
  - to update the state of a financial position
  - example: a lending or swap protocol may require a quorum of users with the following characteristics
    - owns a UNISWAP V3 LP NFT
    - with a minimum liquidity threashold
    - within a certain tick range
    - staked at least for 7 days
  - to adjust the lending or swap fees

PRIVACY VS. AUDITABILITY: CRYPTOGRAPHIC TOOLS

PRIVACY VS. AUDITABILITY

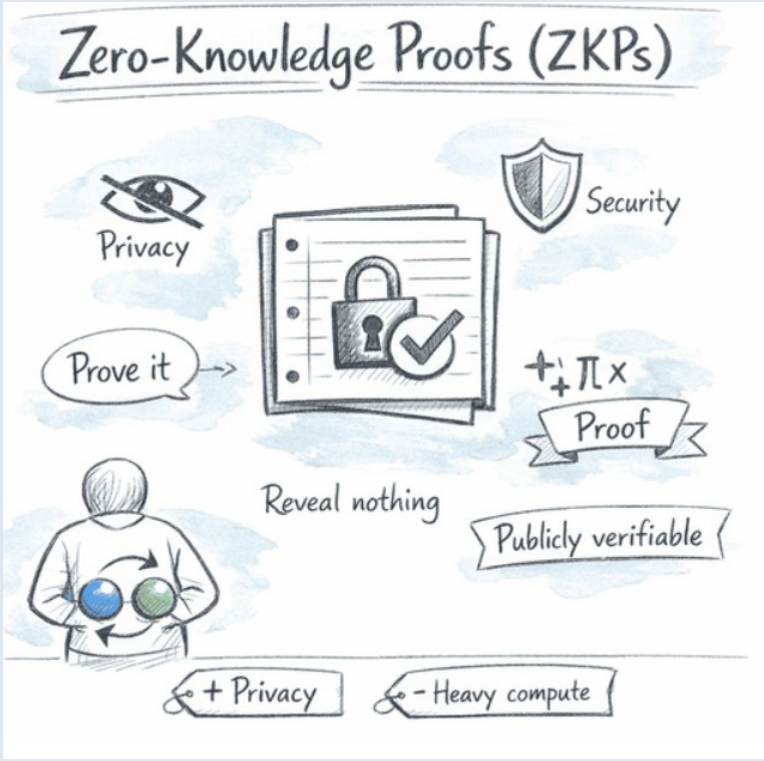
- balancing privacy and auditability in blockchain may be challenging
  - enhancing privacy often obscures transaction details
  - full auditability requires transparency, forcing protocols to carefully trade off confidentiality against verifiability
- confidentiality
  - `DeFi` protocols may need confidentiality
    - confidential transactions, deposit, swaps, and borrow assets without revealing amount or addresses on chain
    - users do not want to expose borrowed amounts, `Uniswap` liquidity pool contributions
  - access control may require confidentiality for attributes which are sensitive

PRIVACY VS. AUDITABILITY

- auditability
  - DeFi protocols may also need auditability
    - even though some data are private, the protocol must verify correctness
    - check double-spending, confirm collateralisation
  - access control system decision must be checked to verify they are correct

ZERO KNOWLEDGE PROOFS

- a cryptographic method to prove that a statement is true without revealing the underlying information.
- key Idea: "*I can prove I know a secret without showing the secret itself.*"
- why it matters
  - in `DeFi`, prove you have enough collateral to borrow without revealing the exact amount.
  - in `DeFi`, verify an `NFT` meets eligibility requirements without disclosing stake size.
  - in access control system prove you have some attributes without revealing them on-chain



OUR RESULTS

- a systematic study of the main libraries for "*programmable cryptography*"

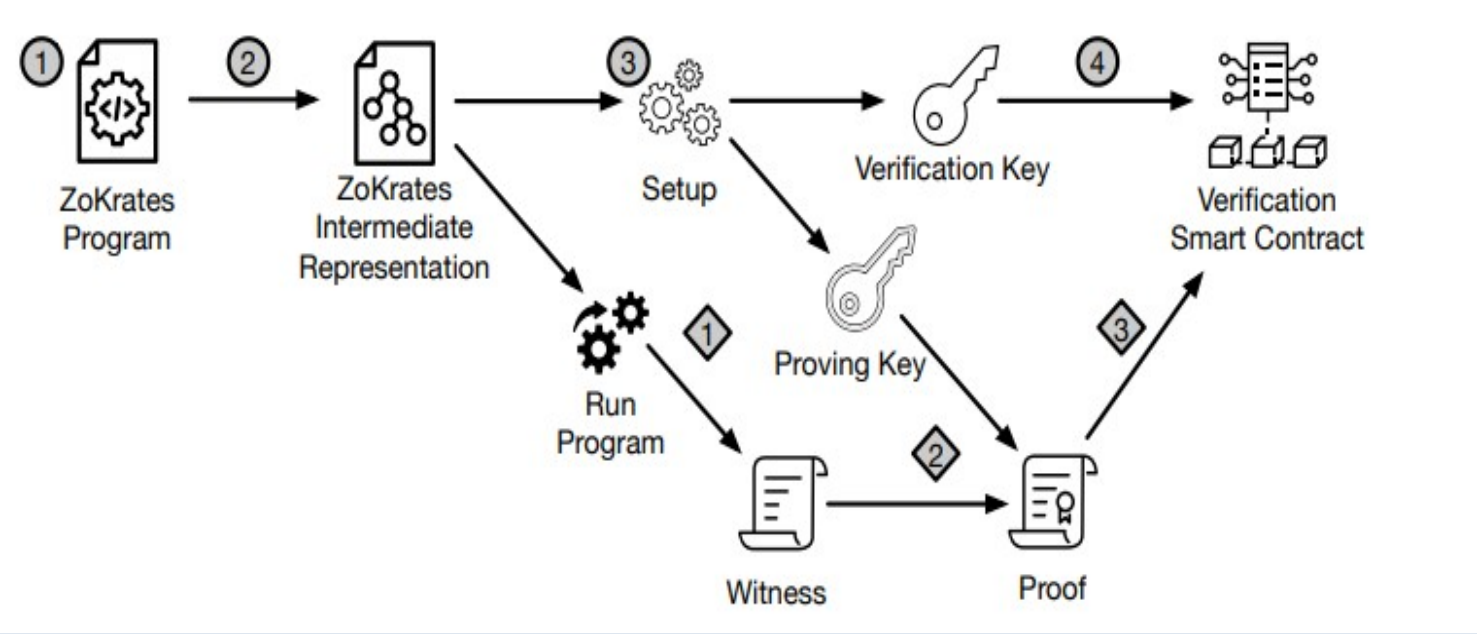
Library	Language	Description
Circom	DSL (custom)	Write arithmetic circuits; used with SnarkJS
SnarkJS	JavaScript	Trusted setup, proof generation & verification for Circom circuits
Noir	Rust-based DSL	Modern, developer-friendly zkDSL by Aztec for writing ZK programs
Halo2	Rust	zkSNARK framework developed by the Zcash Foundation
Arkworks	Rust	Modular zkSNARK library (Groth16, Marlin, Poseidon, etc.)
Zokrates	DSL + Solidity	High-level language for ZK circuits + Solidity verifier contract generation
Bulletproofs	Rust	Range proofs and confidential transactions without trusted setup
gnark	Go	zkSNARK framework in Go; good for enterprise & backend apps
libsnark	C++	One of the first general-purpose zkSNARK libraries (outdated but educational)

OUR RESULTS: PRIVACY-BASED ACS VIA ZKP

- the key idea
  - implement an ABAC system on top of a blockchain
  - execute on-chain the logic of `ABAC` policies through `Smart Policies` implemented by smart contracts
- advantages
  - outsource the access control decision process
  - no need of a trusted third party to perform the access control decision
  - auditability, decentralization
- in our first proposal values are provided in clear on-chain from `Attribute Managers` smart contracts to `Smart Policies`
- the original proposal was improved to support private attributes that still contribute to the policy evaluation, but are not disclosed on-chain
  - use `Zero Knowledge` proof implementation of `Zokrates`

OUR RESULTS: ABAC ACS ON ETHEREUM

- our solution exploits the ZoKrates toolbox implementation of zkSNARK



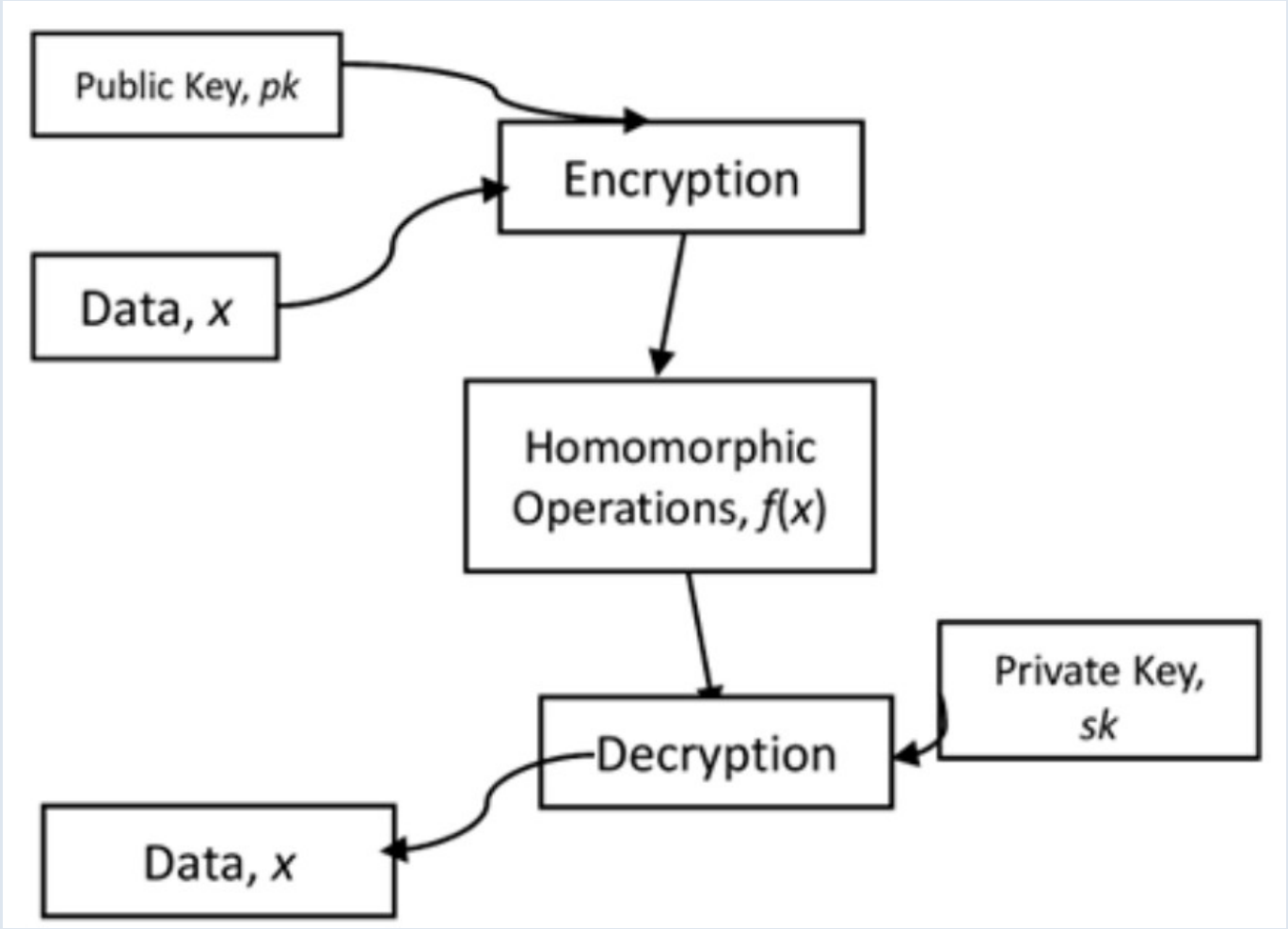
- A blockchain based approach for the definition of auditable access control systems, DDF Maesa, . Mori, L. Ricci Computers & Security 84, 93-119

- Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge, DDF Maesa, A Lisi, P. Mori, L Ricci, G Boschi, Journal of Network and Computer Applications 212, 103577

FULLY HOMOMORPHIC ENCRYTION (FHE)

- a type of encryption that allows computations on encrypted data without decrypting it
- the results of computations, once decrypted, match what would have been obtained from the plaintext
- key idea:
  - "*I can compute on your secret data without ever seeing the secret itself*"
- why it matters in `DeFi / Blockchain`:
  - privacy-preserving computations: Perform lending, staking, or yield calculations without revealing user balances
  - protocols can prove correctness of operations while protecting user secrets
- example:
  - a lending protocol computes loan eligibility or interest rates on encrypted balances
  - users' exact balances remain private, but the system still produces correct results

FHE: THE ZAMA LIBRARY



- ZAMA provides an easy integration of FHE with any blockchain protocol following an Ethereum Virtual Machine (EVM) model

OUR RESULT: PRIVACY-BASED ACS BY ZAMA

- another approach to define privacy preserving privacy preserving `Access Control System`
- definition of a protocol that
  - relies on `ZAMA FHE`
  - exploit `MPC (Multi Party Computation)` to ensure the security of a sensitive global private key for decryption
  - exploit `ZKP` to attest the validity of encryption performed off-chain in untrusted environments
  - supports the concept of privacy with accountability
    - decisions are kept private
    - but can be disclosed in a trustworthy manner by the interested parties in case of disputes

LAB's RECENT COMPLETED PROJECTS

- *Advanced and Quantum-safe Solutions for Digital Identity and Digital Tracing"(AQuSDIT)*, PNRR Project, Spoke 5-Cryptography and Distributed Systems Security, 2024-2025, Unipi, Local Coordinator, (≈ €450k)

- *Cross chain authenticated queries Ethereum* Ethereum Foundation Academic Grant , 2022, (≈ €20k)

- *Authenticated and Efficient Inter Block Event Queries on Ethereum* Ethereum Foundation Academic Grant, 2024, (≈€20k)

LAB'S CURRENT PROJECTS

- *AWESOME: Analysis framework for WEb3 SOcial Media,* Italian National Project, PRIN, 2023-25 (€240k)
- *DLT-FRUIT: A user centered framework for facilitating DLTs FRUITion,* Italian National Project, PRIN, 2023-25 (€233k)
- *POESIA, Proof Of Environmental and Social Impact of Authority,* Bando Ministero per lo Sviluppo Economico, fondo per lo sviluppo di tecnologie e applicazioni di intelligenza artificiale, blockchain e internet of things, 2025-2027 (€130k)
- *TRAENT*, Bando Ministero per lo Sviluppo Economico, Fondo per lo sviluppo di tecnologie e applicazioni di intelligenza artificiale, blockchain e internet of things, 2026-2028, (€80k)
- *A Fair and Trustworthy Remuneration Framework for AI Model Training using Ethereum*, Ethereum Foundation Academic Grant, 2025 (≈ €20k)

SELECTED RESULTS

Skip index: supportig efficient inter-block queries and query authentication on the blockchain, FGCS, DOI: 10.1016/j.future.2024.107556
M. Loporchio, A. Bernasconi, D. Di Francesco Maesa, L. Ricci

Tethering Layer 2 solutions to the blockchain: a survey on proving schemes,
D. Tortola, A.Lisi, P.Mori, L. Ricci, Computer Communications,
Volume 225, September 2024,

L2DART: a trust management system integrating blockchain and off-chain computation , ACM TOIT; DOI: /10.1145/3561386
A. De Salve, L. Franceschi, A. Lisi, P. Mori, L. Ricci,

Self Sovereign and Blockchain-based Access Control: Supporting Attribute Privacy with Zero-Knowledge, JCNA, DOI: 10.1016/j.jnca.2022.103577
D. Di Francesco Maesa, A. Lisi. P. Mori, L. Ricci, G. Boschi,