PM4BC :
Improving the Security of Financial DApps through Process Model Exploration

Mourad RABAH (L3i), Ronan CHAMPAGNAT (L3i), Amine BOUCHIHA (L3i), Mounia HADJEBAR (L3i),
Emmanuel CONCHON (XLIM), Cristina ONETE (XLIM)

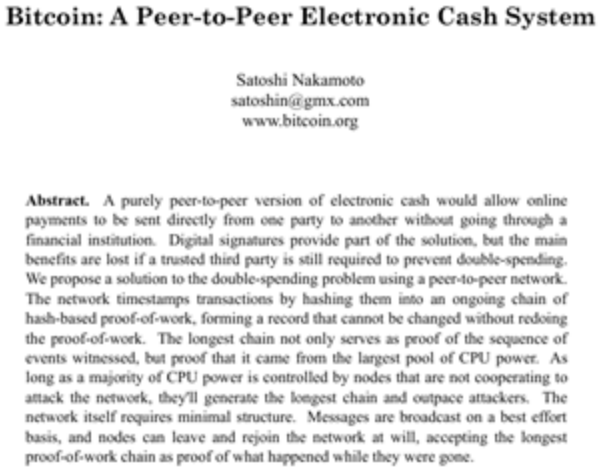
AG Mirès 7-8 juillet 2025

Contexte

- Collaboration L3i équipe e-Adapt et XLIM équipe Cryptis
- Travail exploratoire transversal entre les thématiques
  - Sécurité des systèmes et des réseaux (Cryptis – XLIM)
  - Transparence et gestion de la vie privé dans les systèmes à base de BlockChain (e-Adapt – L3i, Cryptis – XLIM)
  - Fouille de processus (e-Adapt – L3i)
- Question de recherche
  - Peut-on améliorer la sécurité des applications distribuées utilisant les Blockchain à l'aide de la fouille de processus ?

Decentralized finance

- DeFi leverages distributed ledger technologies to deliver financial services without traditional intermediaries, enabling direct peer-to-peer lending, investing, and trading through decentralized protocols.
- Blockchain 1.0 established the foundation for decentralized digital cryptocurrency transfers.
- Blockchain 2.0 platforms with smart contract execution capabilities enabled sophisticated financial operations, leading to the proliferation of financial DApps across multiple blockchain, ex: Ethereum, Tron, and Solana.



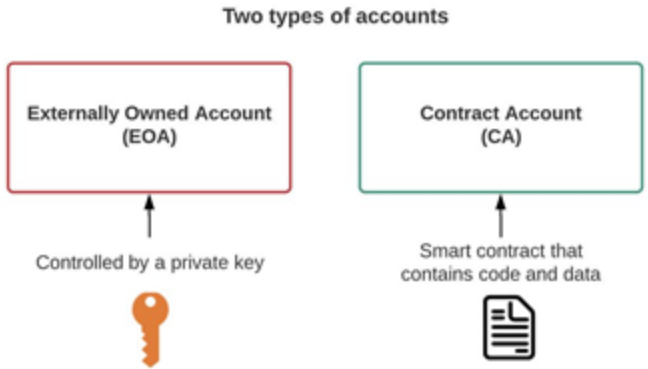
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bots on Ethereum

- Bots re often implemented as Externally Owned Accounts (EOAs) interact with smart contracts and execute transactions autonomously, without any human intervention
- Bots help by performing tasks like providing liquidity, executing trades, balancing prices across platforms.
- But some bots are designed to exploit the system for profit often at the expense of regular users.



Wallet behaviour and Bot detection

There has been multiple studies to identify bots and classify wallets :

Bot detection	[1] Niedermayer, Thomas, Pietro Saggese, and Bernhard Haslhofer. "Detecting Financial Bots on the Ethereum Blockchain." Companion Proceedings of the ACM on Web Conference 2024. 2024.
Bot detection	[2] Morit Zwang, Shahar Somin, Alex 'Sandy' Pentland, and Yaniv Altshuler. 2018.Detecting Bot Activity in the Ethereum Blockchain Network.
Wallet behaviour	[3] Gianluca Bonifazi, Enrico Corradini, Domenico Ursino, and Luca Virgili. 2022.Defining user spectra to classify Ethereum users based on their behavior. Journalof Big Data 9, 1 (April 2022), 37.
Anomaly detection	[4] S. SAYADI, S. BEN REJEB and Z. CHOUKAIR, "Anomaly Detection Model Over Blockchain Electronic Transactions," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco, 2019, pp. 895-900, doi: 10.1109/IWCMC.2019.8766765.
Wallet behaviour	[5] H. Baek, J. Oh, C. Y. Kim and K. Lee, "A Model for Detecting Cryptocurrency Transactions with Discernible Purpose," *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, Zagreb, Croatia, 2019, pp. 713-717, doi: 10.1109/ICUFN.2019.8806126.

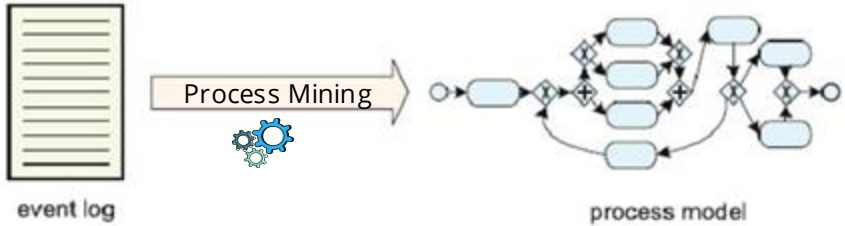
- Existing approaches primarily rely on statistical features for classification, overlooking the sequential nature of actions.
- Moreover, they do not offer a behavioral model that characterizes bot behavior or distinguishes it from that of human-managed EOAs.

Process mining

- Process mining is a data-driven technique that analyzes event logs to discover, monitor, and improve processes by extracting insights about how activities are actually executed over time.

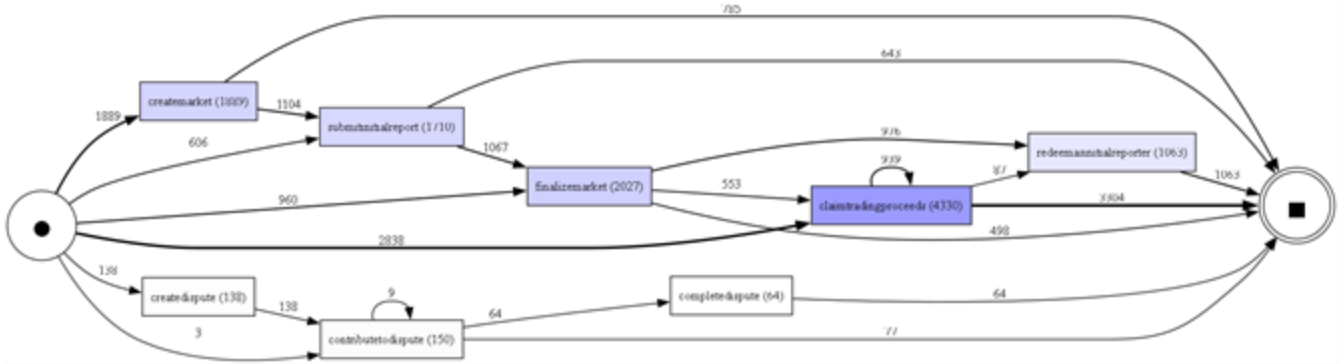
- An event log records real process executions as traces, each made up of a sequence of events from a single case.
    - each event logs an activity with key attributes: case ID, activity, timestamp.

- Process mining, especially process discovery, uses these logs to automatically reconstruct and analyze actual process flows.



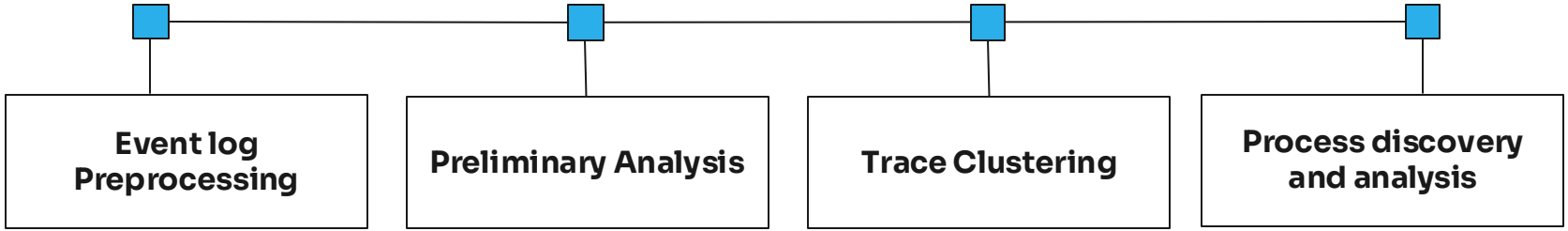
Starting point: *Augur Case Study [6]*:

- Augur is a prediction and betting marketplace, where users can create bets and trade on predictions.
- In a recent paper[6] , the authors succeed using process mining techniques to get valuable insights about process workflow of markets in this Dapp.
- We tried to use the same eventlog considering the EOAs as cases, however on resulted models and confirming on the ethrescan website some events related to EOA were not included in the event log .

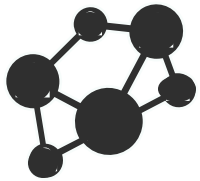


[6] Hobeck, Richard, et al. "Process mining on blockchain data: A case study of augur." Business Process Management: 19th International Conference, BPM 2021, Rome, Italy, September 06–10, 2021, Proceedings 19. Springer International Publishing, 2021.

Methodology



Event Log



Ethereum Blockchain

Etherscan Api

Raw Transactions

Filter Transactions by Annotated EOAs List

Annotated EOAs [1]

hash	block_number	transaction_index	from_address	to_address	input_data	nonce	gas

	case_id	method_category	block_datetime
0	0xa4e5961b58dbe4876399296430cb1dc3048daf5e	transferETH	2022-09-09 01:39:42

Event Log

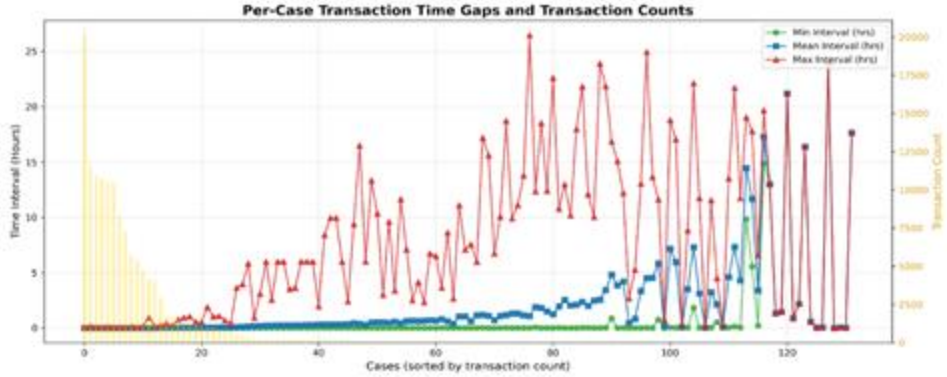
Get Function Signature for each input

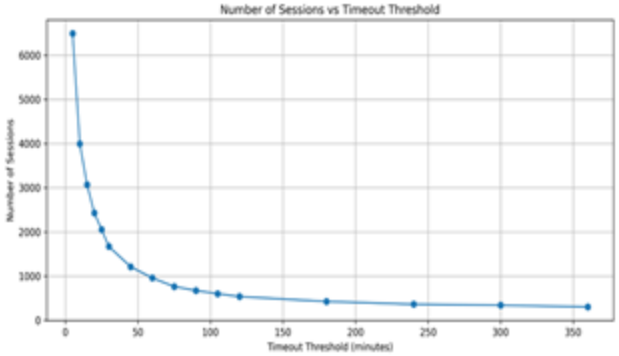
ABI decoders / 4byte directory / Smart Contracts

[1] Niedermayer, Thomas, Pietro Saggese, and Bernhard Haslhofer. "Detecting Financial Bots on the Ethereum Blockchain". Companion Proceedings of the ACM on Web Conference 2024.

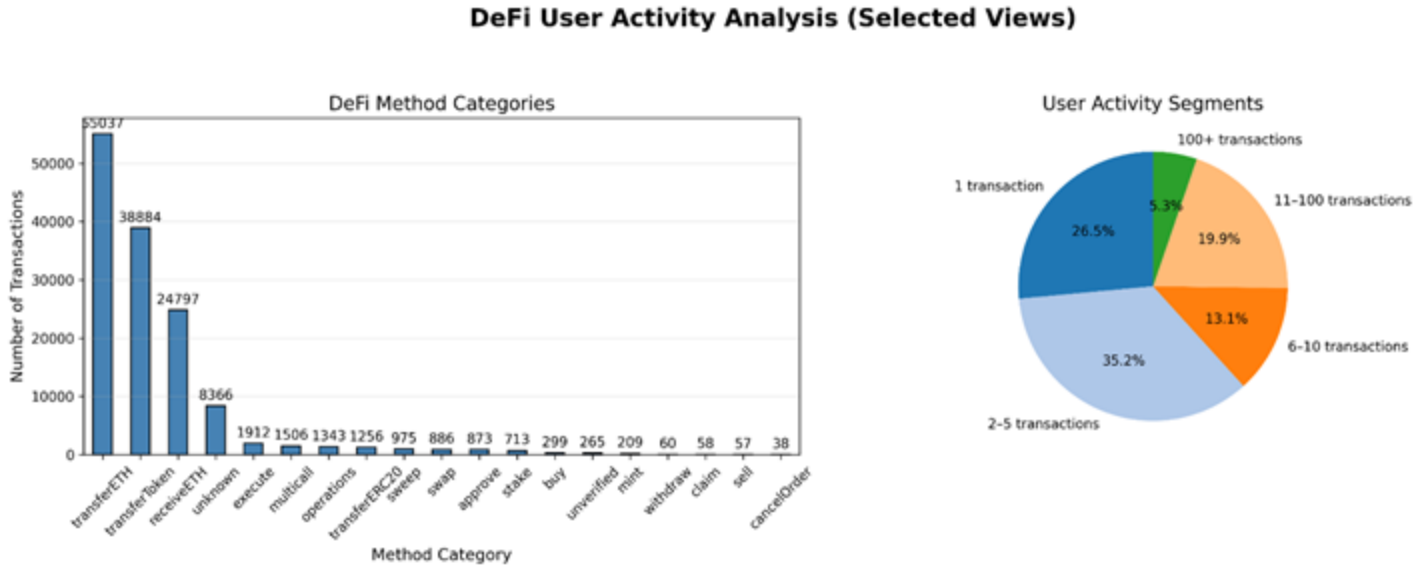
Preliminary Analysis

- Sample taken from Ethereum transactions in block range 15,500,000 to 15,511,999.
- Total of 143 EOAs (Externally Owned Accounts):
  68 bots, 57 humans, 18 unclear
- Event log contains 137,534 events.
- Identified 19 categories of activities based on transaction intent.
- After sessionization, extracted 627 traces with 402 variants.





Eventlog Overview



Trace Clustering

Data Representation

Trace based clustering
Feature based clustering (FFS encoding)

Distance Measure

Levenshtein distance
Cosine Distance

Clustering algorithm

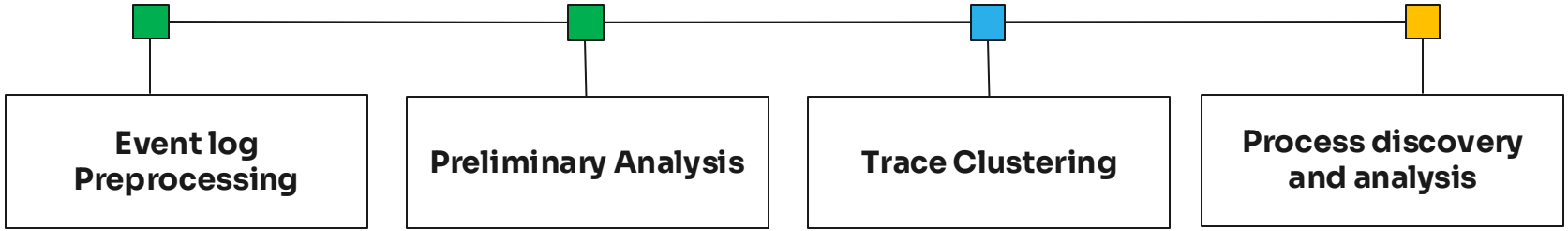
Hierarchical clustering : agglomerative
Density based clustering : dbscan

Clustering evaluation

Silhouette score and Davies–Bouldin Index
labeled EOAs list

Agreement Type ↓ / Cluster →	C1	C2	C3	C4	C5
Bot	3	8	23	16	59
Human	0	10	0	1	1
Unclear	4	7	3	0	11

PM4BC Level of Progress




Informatique
Image
Interaction
Univ. La Rochelle


La Rochelle
Université


Fédération
mires
Mathématiques et Interactions
Images, Information numérique
& systèmes
Réseaux et Sécurité

Thanks!

Table of contents