The Hidden Layers of Blockchains: Technical Nuances & their Unforeseen Consequences

PhD Thesis Defence

Shayan Eskandari

15 May 2024

Université Concordia University

Agenda

- **Motivation**
- **Methodology**

- **Cryptojacking:** from Replacing Ads to Invisible Abuse
- **Front-running:** from Transparency to Extracting Value
- **Oracles:** from Ground Truth to Market Manipulation
- **Blockchain Audits:** from Existence to Internal Controls

- **Conclusion**
- **Questions**

Motivation

- ➔ Influenced by my professional experiences
  - Blockchain Engineer at a Bitcoin ATM company
    - Friction with the current financial system and the limitations
  - Security Engineer at a Smart Contract Auditing firm
    - Comprehensive perspective into the tech and common false (technical) assumptions
  - Chief Technology Officer at a Publicly-traded company holding Cryptoassets
    - Experiencing with the disconnect between traditional (financial) auditing methods and the nuanced requirements of cryptoassets custody, ownership, etc

- ➔ Aim to shed some light on the knowledge gaps and discuss potential ethical issues & technical solutions to narrow these gaps

from

new economical models

decentralized and open networks

real-time financial reporting

to

Invisibile theft

Manipulation and value extraction

complex financial fraud

Methodology

- Most chapters were initially written as a paper, which were accepted in a peer-reviewed conferences or journals
  - Many of these papers fall under *“Systemization of Knowledge”, or SoK*, with addition of measurement studies of the introduced framework

- Critically read, gather data and research
- Looks for themes and behaviours → taxonomy
- Fit the findings into the taxonomy → comparative analysis
- Support with measurements when appropriate

SoK + Measurement

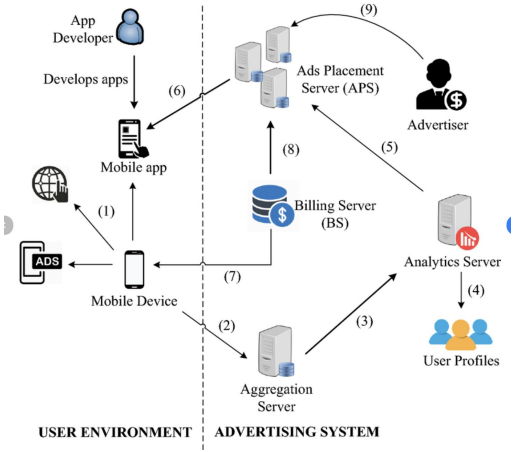
Cryptojacking: from Replacing Ads to Invisible Abuse

Based on the paper published at:

- 2018 *IEEE Security & Privacy on the Blockchain*
  co-located with the *IEEE European Symposium on Security and Privacy (EuroS&P)*
- First paper on the topic
- 211 academic citations, so far

New online economy

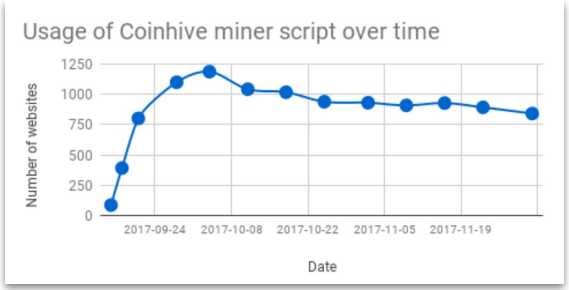
- ➔ Current online advertisements money flow is broken
  - ◆ Many intermediaries
  - ◆ malvertisement
- ➔ A new system to have direct economical model between the user and the website owner
  - ◆ User sees no ads → pays the website using their computer resources (CPU mining)
  - ◆ UNICEF “The HopePage”
    - Donate a CPU to a charity
  - ◆ Streaming websites, premium content, etc



Ullah, I., Boreli, R., & Kanhere, S. S. (2023). Privacy in targeted advertising on mobile devices: a survey. International Journal of Information Security, 22(3), 647-678.

Cryptojacking: Invisible Abuse?

- Anyone with access to the website code could have an income
  - Website (Webmaster, third-party services such as web plugins)
  - Browser Extensions
  - Breaches
  - Man-in-the-middle



Website	Results	Query Parameter
Coinhive	30611	‘coinhive.min.js‘
JSEcoin	1131	‘load.jsecoin.com‘
Crypto-Loot	695	‘CryptoLoot.Anonymous‘
Minr	324	‘minr.pw‘,‘st.kjli.fi‘, ‘abc.pema.cl‘,‘metrika.ron.si‘, ‘cdn.rove.cl‘,‘host.d-ns.ga‘, ‘static.hk.rs‘,‘hallaert.online‘, ‘cnt.statistic.date‘,‘cdn.static-cnt.bid‘
CoinImp	317	‘www.coinimp.com/scripts/min.js‘, ‘www.hashing.win‘
ProjectPoi (PPoi)	116	‘projectpoi.min‘
AFMiner	46	‘afminer.com/code/miner.php‘
Papoto	42	‘papoto.com/lib/papoto.js‘

Invisible Abuse is defined as **“the intentional use of the invisible operations of a computer to engage in unethical conduct”**
- Moor, James H. "What is computer ethics?." The Ethics of Information Technologies. Routledge, 2020.

Cryptojacking: Discussion

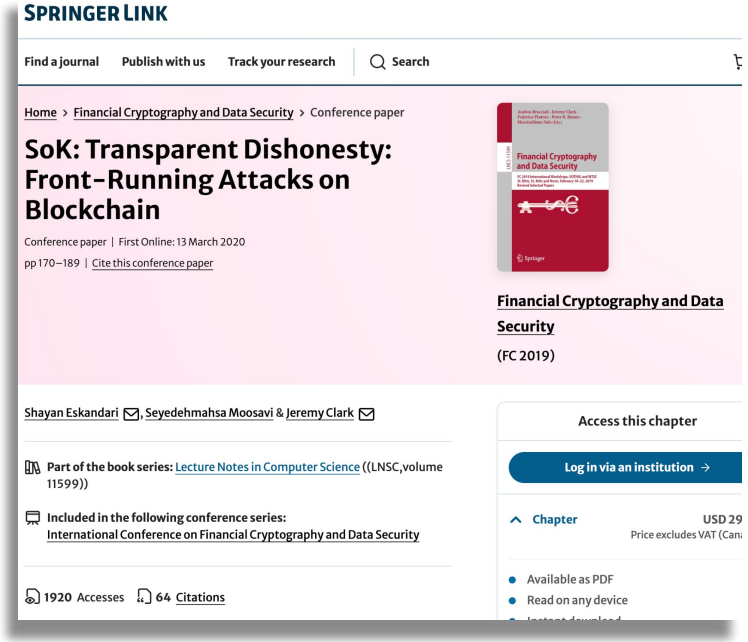
- The use of cryptojacking
  - **(1) On a breached website** **⟵ Unethical**
  - **By the website owner**
    - **(2) Without user's consent** **⟵ Unethical**
    - **(3) With user's consent**

- Ambiguity in:
  - Obtaining user's consent <> Effectiveness of the current EU cookie banners
  - Policy Void in ethical use of user's resources as form of payment
    - Regulations on capped usage of resources (with consent) to replace Ads

Blockchain Front-running: from Transparency to Extracting Value

Based on the paper published at:

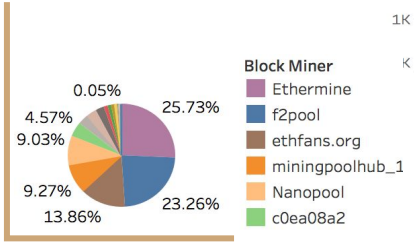
- *3rd Workshop on Trusted Smart Contracts*
  In Association with *Financial Cryptography (FC)*
  February 2019.
- First paper on the topic
- 236 academic citations, so far
- Presented at:
  - *Stanford Blockchain Conference SBC 2020*
  - *DevCon V, Osaka, Japan*

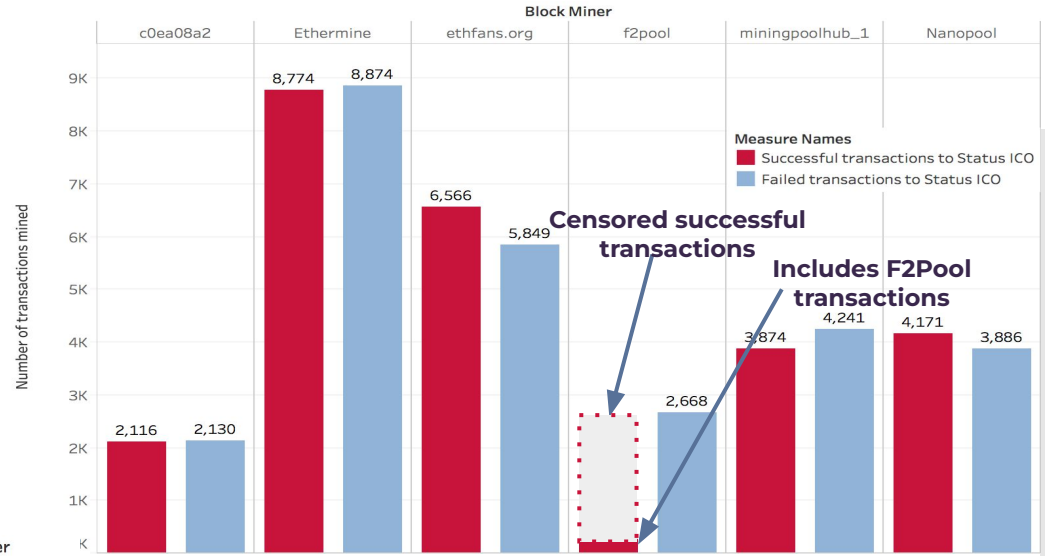


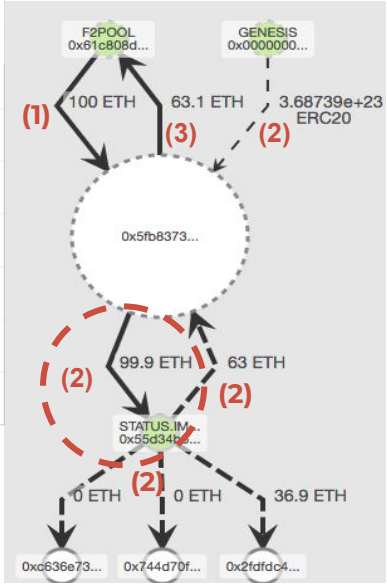
Blockchain: “Open Finance”

- **Permissionless**
  - Pseudonymous
- **Public**
  - Peer to Peer
- **Transparent**
  - Everyone (Full Nodes) in the network have access to all information
    - Unconfirmed Transactions → “Privilege Information” in TradFi
- **Irreversible**
  - Programmable

Blockchain Front-running







Blockchain Front-running Attacks Taxonomy

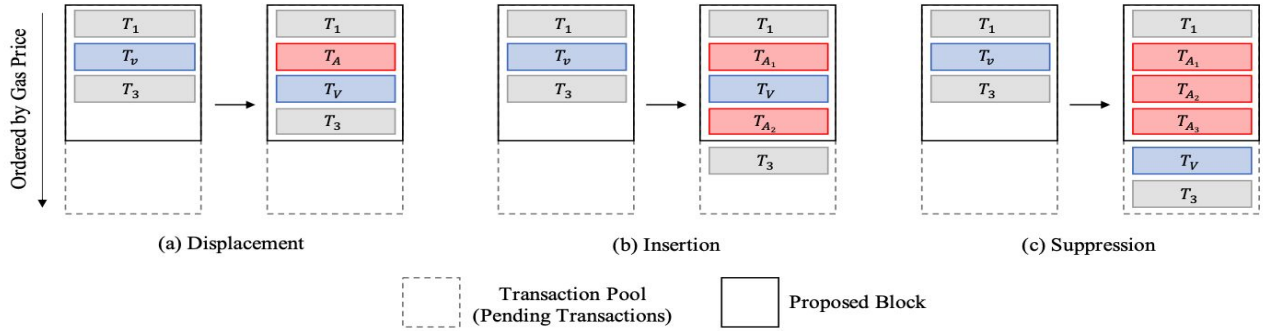


Figure 1: Illustrative examples of the three frontrunning attack types.

*Torres, Christof Ferreira, and Ramiro Camino. "Frontrunner jones and the raiders of the dark forest: An empirical study of frontrunning on the ethereum blockchain." 30th USENIX Security Symposium (**USENIX Security 21**). 2021.*

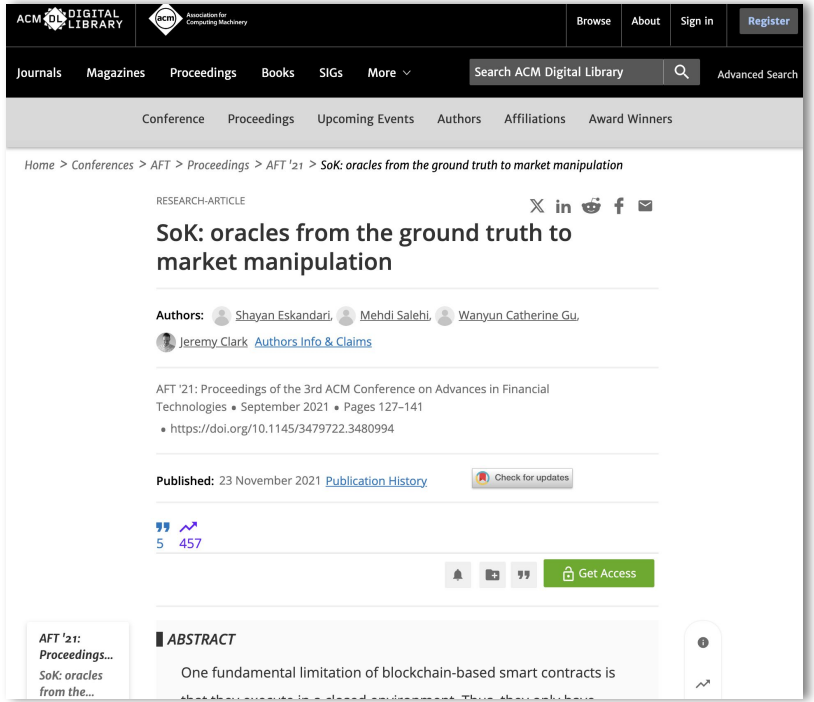
Key Mitigations

- **Transaction Sequencing**
  - not trivial to order transactions on a distributed network
  - might introduce centralization
- **Confidentiality**
  - limit the visibility of transactions
  - side-channels leak information and signal intention
- **Design Practices**
  - assume front-running is unpreventable —> remove any benefit from it
- **Embracing Front-running**
  - “Democratizing MEV”: sharing the profit of the front-running opportunities

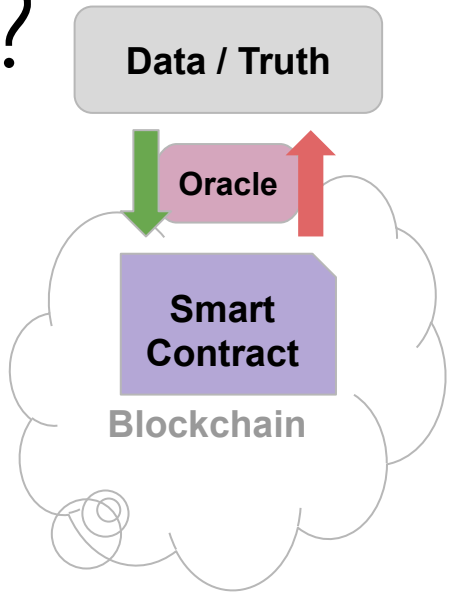
Oracles: from Ground Truth to Market Manipulation

Based on the paper published at:

- AFT 2021 - *3rd ACM Conference on Advances in Financial Technologies*
- 45 academic citations, so far
- Follow up work presented at:
  - *ethCC[4]*



What is special about Oracles?

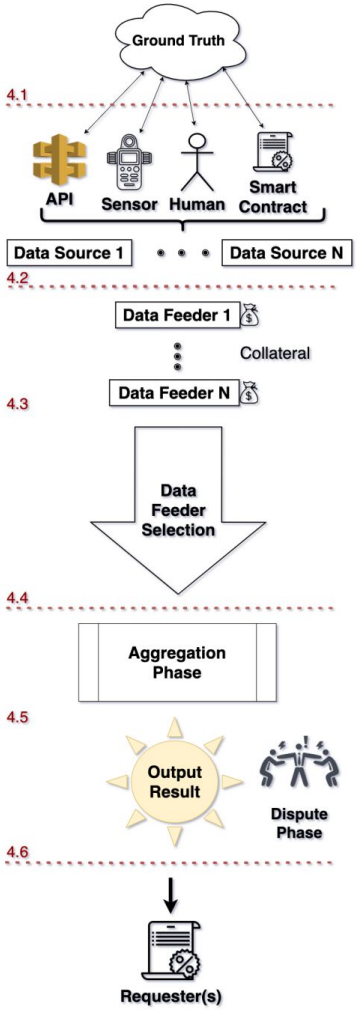


- Blockchain are closed systems, that value decentralization of trust
  - *Smart Contracts → “Code is Law”*
- There are different approaches to get data in & out of a blockchain → “Oracles”
  - *Who can bend the truth and how?*
- We break down the design of blockchain oracle systems into modules
  - Modular lens provides better methodology to find the weak/trusted points

Oracles: Modular Workflow

- Ground Truth
- Data Sources
- Data Feeders
- Selection of Data Feeders
- Aggregation
- Dispute Phase

- Off-chain Infrastructure
- Blockchain Infrastructure
- Smart Contracts
  - Oracle
  - Data Consumer



Oracles Classification

Oracle	Data Source	Selection Mechanism	Staking	Aggregation Mechanism	Provider/Data Vetting	Determining the Truth	Consequences (Slash, Ban, Loss)
		Data Feeder			Dispute		
ChainLink [41]	API	Reputation, Staking	•	Statistical Measure	P	Statistical Measure	S
UMA [104]	Human, API	FCFS†	•	×	D	Staking	S
Augur [87]	Human	Single Source★	•	×	D	Voting	S
Uniswap [105]	Smart Contract	×	×	TWAP	×	×	×
MakerDAO V1 [74]	Human, API	Centralized Allowlist	×	Median	×	×	×
MakerDAO V2 [74]	Human, API	Decentralized Allowlist	×	Median	P	Voting	B
NEST [81]	Human	×	•	×★★	D	Arbitrage	L
Band protocol [89]	API	Random Selection	•	Statistical Measure	P	Staking	S
Tellor [31]	Human, API	PoW	•	Median	P	Staking	S B
ASTRAEA [3] TruthCoin [99]	Human	Staking	•	Mode	D	Voting	S
Provable [10] PriceGeth [44]	API	×	×	×	×	×	×
DIA Oracle [38]	API, Smart Contract	×	×	×	D	Staking	B
DECO [116] TownCrier [115]	HTTPS	×	×	×	×	×	×
API3 [9] \w Kleros [68]	Oracles	Decentralized Allowlist	•	Statistical Measure	P	Voting	S B

Table 2: A classification of the existing oracle implementations using the modular framework described in Section 4.
• indicates the properties (columns) are implemented in the corresponding oracle (rows), and × indicates the property is not applicable.
† First Come First Serve ★*The Market Creator assigns the designated reporter* ★★ *The series of reported prices will be sent to requester without aggregation (See 4.6.1)*

Blockchain Audits: from Existence to Internal Controls

Building upon the paper published in:

- JIS 2021 - *American Accounting Association Journal of Information Systems*
- 59 academic citations, so far
- Follow up work presented at:
  - *ETHDenver 2023*

American Accounting Association | Journal of Information Systems

ARTICLES | INFORMATION FOR AUTHORS | PUBLICATION POLICIES & PROCEDURES | HELP

Volume 35, Issue 2
Summer 2021

RESEARCH ARTICLE | JUNE 01 2021

Systemizing the Challenges of Auditing Blockchain-Based Assets

Erica Pimentel; Emilio Boulianne; Shayan Eskandari; Jeremy Clark

+ Author & Article Information

Journal of Information Systems (2021) 35 (2): 61–75.

https://doi.org/10.2308/ISYS-19-007

Share | Tools | Cite

ABSTRACT

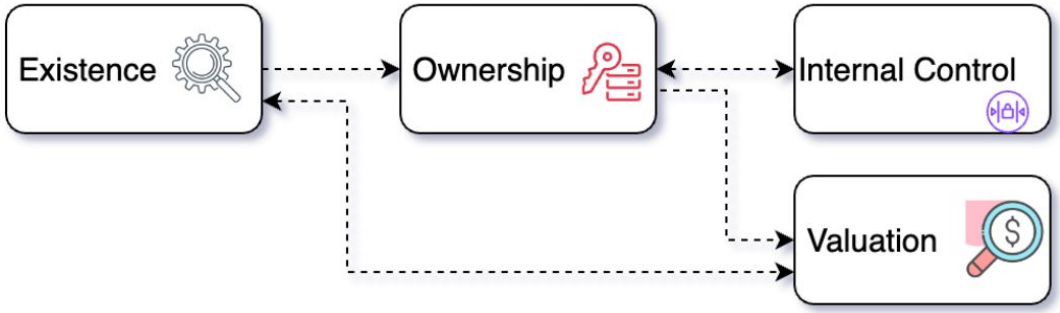
Presently, auditing firms are hesitant to accept mandates from companies that hold a significant amount of cryptoassets, primarily because the blockchain sector introduces novel, technically sophisticated, and risky propositions that auditors are unequipped to handle. Abrupt recusals by auditors operating in this sector have led to several enterprises being placed on cease trade by securities regulators for failure to produce audited financial statements on time, thus impeding these companies from raising capital and bringing new investments to fund innovation in this space. Through an iterative process of interviews with senior accounting professionals, structured brainstorming among a multidisciplinary team of accountants and blockchain experts, and a focus group with experienced auditors, we critically analyze the purported roadblocks to auditing blockchain firms and map them to traditional auditing practices. We urge auditors to reconsider their resistance to the blockchain sector by demonstrating that providing an audit opinion is challenging but not insurmountable.

financial audit of the crypto-assets

⟨⟩

technical audit of the smart contracts

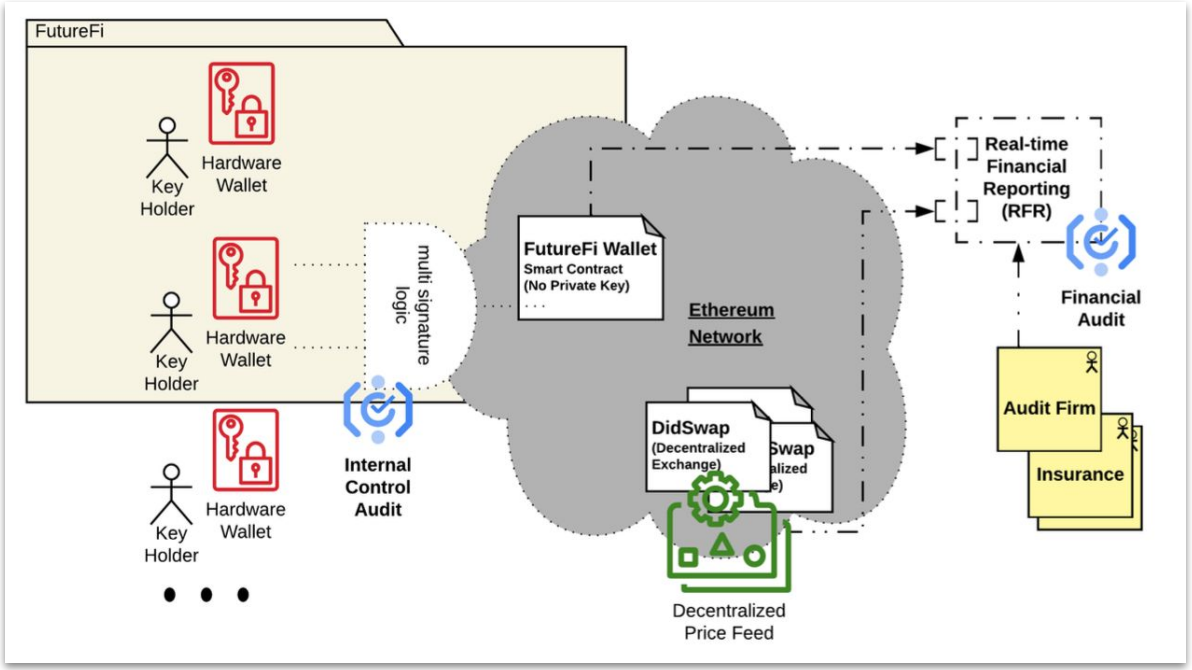
Blockchain Audits Framework



- **Existence**: verify the reported cryptoassets actually exist and how to verify
- **Ownership:** verify the custody of the cryptoassets
- **Valuation:** verify values reported in the financial statements are accurate and represent the underlying economic reality
- **Internal Control:** key management, access control, IT security, etc

Blockchain Audits: Real-time Financial Reporting (RFR)

- 4 Case Studies



Blockchain Audits: Paths Forward

Paths Forward
Reject Cryptoassets Audits
Collaborate with Experts
Develop In-house Expertise
Maturity of Cryptoassets (Test of Time)
Precedence of Previous Audits

Concluding Remarks

- Blockchain technology can enable really novel approaches to remove trust in the intermediaries and significantly change the information flow in different businesses.
- Also brings forth some unforeseen consequences that were not possible before the existence of this technology

  - Cryptojacking: from Replacing Ads to Invisible Abuse
  - Blockchain Front-running: from Transparency to Extracting Value
  - Oracles: from Ground Truth to Market Manipulation
  - Blockchain Audits: from Existence to Internal Controls

from

new economical models

decentralized and open networks

real-time financial reporting

to

Invisibile theft

Manipulation and value extraction

complex financial fraud

Publications

- **Eskandari, S**., Leoutsarakos, A., Mursch, T., & Clark, J. (2018, April). **A first look at browser-based cryptojacking**. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 58-66). IEEE.

- Gaggioli, A., **Eskandari, S.**, Cipresso, P., & Lozza, E. (2019). **The middleman is dead, long live the middleman: the "trust factor" and the psycho-social implications of blockchain.** *Frontiers in Blockchain,* 2, 20.

- Rahimian, R., **Eskandari, S.**, & Clark, J. (2019, June). **Resolving the multiple withdrawal attack on erc20 tokens**. In *2019 IEEE European symposium on security and privacy workshops (EuroS&PW)* (pp. 320-329). IEEE.

- **Eskandari, S.**, Moosavi, S., & Clark, J. (2020). **Sok: Transparent dishonesty: front-running attacks on blockchain**. In *Financial Cryptography and Data Security: FC 2019 International Workshops*, Springer International Publishing.

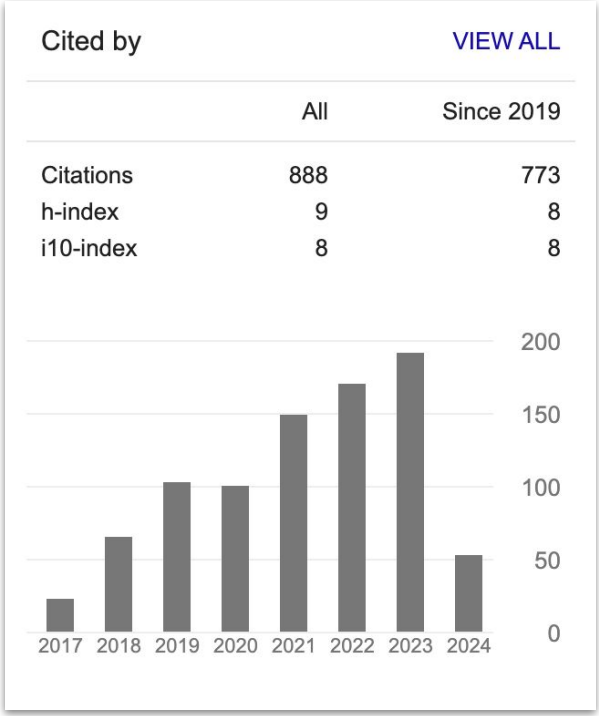
- Pimentel, E., Boulianne, E., **Eskandari, S.**, & Clark, J. (2021). **Systemizing the challenges of auditing blockchain-based assets**. *Journal of Information Systems*, 35(2), 61-75.

- **Eskandari, S.**, Salehi, M., Gu, W. C., & Clark, J. (2021, September). **SoK: oracles from the ground truth to market manipulation**. In Proceedings of the *3rd ACM Conference on Advances in Financial Technologies* (pp. 127-141).

Thank you

For being part of this journey with me

Shayan Eskandari
May 2024



UNIVERSITÉ Concordia UNIVERSITY

Timetable

Term	Academic Progress	Work Experience
Fall 2017	INSE 6110 - Foundation of Cryptography (A+) INSE 6630 - Recent Development in Information Systems Security (A+) Research: Cryptojacking and browser-based mining	Blockchain Engineer Bitaccess
Winter 2018	Published: *A first look at browser-based cryptojacking* [121] Research: Ethereum & Smart Contracts Security	
Summer 2018	Research: front-running attacks on blockchain	
Fall 2018	Research: front-running attacks on blockchain	
Winter 2019	Published: *SoK: Transparent Dishonesty: front-running attacks on Blockchain* [122] INSE 6421 - Systems Integration and Testing (A+)	Security Auditor ConsenSys Diligence
Summer 2019	Research: blockchain oracles and security frameworks Co-authored: *Resolving the multiple withdrawal attack on erc20 tokens* [276]	
Fall 2019	Co-authored: *the "trust factor" & the psycho-social implications of blockchain* [144]	
Winter 2020	Research: challenges of auditing crypto-assets in finance ENCS 8501 - Comprehensive Exam	
Winter 2021	Co-authored: *Systemizing the challenges of auditing blockchain-based assets* [264]	
Summer 2021	Research: modular framework design for Blockchain Oracles	
Fall 2021	Published: *SoK: oracles from the ground truth to market manipulation* [123]	CTO Ether Capital
Winter 2022		
Summer 2022		
Fall 2022		
Winter 2023	PhD Proposal	
Summer 2023	Follow up research on auditing crypto-assets	
Fall 2023	PhD Seminar	
Winter 2024	Writing the dissertation Follow up research on security of oracles	Head of Security Puffer Finance
Summer 2024	Dissertation defense	

Methodology - SoK

- Many of the chapters fall under “Systemization of Knowledge”
  - Introduced in 2010 at the IEEE Symposium on Security and Privacy ("Oakland" conference)
- “our community... produces too many incremental results that don't always lead to better general understanding... Some of this has been blamed on the lack of appropriate high-visibility venues in which to publish these types of papers since the top security venues (including Oakland research papers) emphasize novel research contributions.”
- “We believe an SoK paper will be at least as valuable of a contribution to our research community as a typical Oakland paper, and expect these papers will be widely read and cited.”