Blockchain Security

A survey of Techniques and Research Directions

Ahmed Yehia

Computer Engineering Department Kuwait University

November 10, 2021



- Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- **6** Process Security In Blockchain
- 6 Data Security in Blockchains
- Questions



Introduction

•00

- Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- 5 Process Security In Blockchain
- 6 Data Security in Blockchains

Introduction

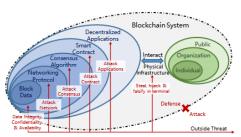
- Blockchain
 - Data blocks chained sequentially according to chronological order
 - Distributed ledger; infeasible to tamper with
- Applications
 - Cryptocurrencies
 - Smart contracts
 - Non-Fungible Tokens (NFTs)

The Properties of Distributed Ledger Technology (DLT)



• Blockchain Security

- Threat Types
 - Internal or Peripheral
 - Malevolent or Unintentional
- Threats are addressed by
 - Detection
 - Prevention
 - Appropriate Response
- Today's research is too technical; limited real-life considerations



- Introduction
- 2 Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- 5 Process Security In Blockchain
- 6 Data Security in Blockchains
- Questions

Related Work

- Lin and Liao (DOI: 10.6633/IJNS.201709.19(5).01)
 - A review of blockchain security issues in terms of majority attack, data scale, etc.
 - Problem not comprehensive enough
- Li et al. (DOI: 10.1016/j.future.2017.08.020)
 - Blockchain attacks and their real-life counterparts
 - Problem neglects business application scenarios
- Joshi et al. (DOI: 10.3934/mfc.2018007)
 - Consensus protocols from the aspect of data security and privacy
 - Problem Misses other aspects such as smart contracts
- Pattern: security is not considered holistically



- Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- 5 Process Security In Blockchain
- 6 Data Security in Blockchains

Objective and Approach

- Objective survey blockchain security challenges in light of different parts of system
- Approach View blockchain security in terms of
 - Process level
 - Data level
 - Infrastructure level
- The Process-Data-Infrastructure framework PDI

- Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- 5 Process Security In Blockchain
- 6 Data Security in Blockchains

- Security Conceptual View Oracle View of Security
 - Data Security
 - Fraud Prevention
 - Compliance Enablement
- Security Reference Architecture IBM Framework
 - Holistic view of security
 - Includes business, technology, and service
- How does the PDI framework compare?

Oracle View IBM Framework PDI Framework **Blockchain System** Security Governance, Risk Decentralized App. Fraud Detection **Process Level** Management & Compliance **Business Applications** Monitorina & Profilina **Smart Contract** Industrial Applications Access Controls **Implementations** People and Identity Violation Detection Smart Contract Laver Operation Standard Audit & Behavior Algorithm & Distribution & Regulations Analysis Data & Information Mechanism Fraud Detection & Risk prediction Consensus Layer **Data Security** Authorization Certificate Access Controls Application & Process **Data Level** Distributed Synchronize. Encryption & Masking Fault Tolerance Cryptography & Devices, Platforms, & Encryption Media Network, Server, Terminal Networking Layer In Transit In Use Computing & Access Control Retrieval Data Verification Physical Infrastructure **Privacy & Consensus** Compliance Enable P2P Network Risk Management Data Layer Controls & Reporting Infrastructure Level Common Policy, Event Hash & Chain Struct. Attestation & Terminal Handling & Reporting Merkle Tree & Timestamp **Analysis** Network Data Block & Encryption Profession Managed Physical Identity & Access al Services Services Infrastruct. Server/Node Management Physical Infrastructure

- Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- **6** Process Security In Blockchain
- 6 Data Security in Blockchains

- Requires practitioner to agree on and enforce set of secure policies
- Complicated due to multiple tasks and governance
- Aspects of process security
 - Smart Contract
 - · Business Level
 - Virtual Machine Level
 - Contract Code Level
 - Implementing Scenarios
 - Standards and regulations
 - Fraud detection and risk management



Security of Smart Contracts

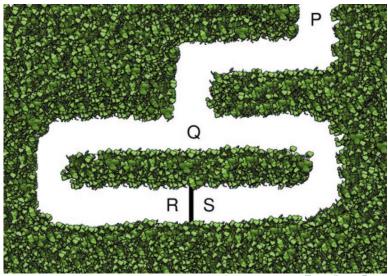
- Programs automatically executed on distributed networks
- No external trusted third-party; mutual distrust
- Need to execute *correctly* and be protected against *malevolence*
- Issues on the level of
 - Business (unauthorized access, malicious infection, unpredictable state)
 - Virtual Machine (stack size limit, randomness generation, time constraints)
 - Code (call to the unknown, gasless send, deadlocked state)
- To combat such issues, analysis of smart contracts bytecode and semantics is necessary
- Tools such as Securify could help



Implementation Security of Blockchain

- Internet of Things
 - Goal full autonomous data processing and exchange
 - Challenges Transactions per second, privacy violation, DoS
 - Possible solution Robust identification and authentication of devices
- Shared economy
 - Goal Enforce demander-supplier agreements
 - Challenges Privacy violation of parties of interest
 - Possible solution Zero-knowledge proof

Zero-knowledge Proof - Ali Baba's Cave



Operation Standards and Regulations

- Blockchain technical challenges
 - Scalability, performance, and interoperability
- Blockchain management challenges
 - Integration with complex institutional, regulatory, social, economic, and physical systems
- Standardization of blockchain technologies is key in solving such issues
- However, standardization may stifle progress and introduce new risks

Operation Standards and Regulations

Type	Group/Content
World Wide Web	Credentials Community Group, Digital
Consortium (W3C)	Verification Community Group,
	Blockchain Community Group, Verifiable
	Claims Working Group, Interledger
	Community Group, Web Ledger Protocol
ISO TC 307	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27
Standards Australia	Roadmap for Blockchain Standards
International	Focus Group on DLT (FG DLT)
Telecommunications Union	
IEEE	Blockchain and DLT
SWIFT	Blockchain and DLT
European Union	General Data Protection Regulation
	(GDPR)
China Electronics	Reference architecture of blockchain
Standardization Institute	



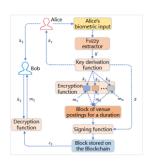
Fraud Detection and Prevention

- Types of fraud that affect blockchain
 - Objective fraud
 - Subjective fraud
 - Rating fraud
- Fraud detection and prevention via
 - Preventative control (risk prediction)
 - Detective control (detection of existing fraud / attacks)

- 1 Introduction
- 2 Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- 5 Process Security In Blockchain
- 6 Data Security in Blockchains
- Questions

Access Control in Blockchains

- Access Control in Blockchain
 - In research, access control is achieved by
 - Smart Contract
 - Attribute-Based Encryption (ABE) schema (CP-ABE)
 - Challenge ABE schema requires mutability for revocation; blockchains are immutable
 - Solution Fine-grained control; access is given per-item
 - Example: hybrid fine-grained access control model proposed by Adams (DOI: https://doi.org/10.1002/spy2.97)



Computation Techniques on Encrypted Data in Blockchains

- Computing techniques on encrypted blockchain data
 - Homomorphic encryption
 - · Working on data while it's still encrypted
 - Secure multi-party computation
 - · Work on joint input together while keeping each node's input secure
 - Trusted computing
 - Offload computation to other participants while still ensuring validity of result

- 1 Introduction
- 2 Related Work
- 3 Objective and Approach
- 4 Framework of Blockchain Security
- 5 Process Security In Blockchain
- 6 Data Security in Blockchains
- Questions

Questions

The floor is open for questions