UNIVERSITY OF HOUSTON

Annual PhD Review #1

Year 2023

Rabimba Karanjai

May 11, 2023

Contents

Joined the PhD Program in 2020 Fall. Was allowed to come to UH physically and resume degree in Fall 2021.

Prior Work:

1. Mobile multi-party digitally signed documents and techniques for using these allowing detection of tamper - 2021 - US Patent US11025643B2
2. Optimizing Web Virtual Reality - MS Thesis

Courses Taken at UH

- Operating System
- Computer Architecture
- Machine Learning
- Cloud Computing
- Intro Automata & Computability
- Prgrm Analys & Testing

Contents

Confidential Decentralized Transaction

2 Collected Short Stories on Confidential Decentralized Transaction, real word use cases

Today we are going to re-visit some existing problems in Decentralized Transaction systems. Different ways we explored to mitigate them, and extending them to cover real world use cases.

- An event driven framework for smart contract execution
  Mudabbir Kaleem,Keshav Kasichainula,**Rabimba Karanjai**,Lei Xu,Zhimin Gao,Lin Chen,Weidong Shi – ACM DEBS – 2021
- On Conditional Cryptocurrency With Privacy
  Rabimba Karanjai; Lei Xu; Zhimin Gao; Lin Chen; Mudabbir Kaleem; Weidong Shi IEEE ICBC 2021
- Privacy preserving event based transaction system in a decentralized environment
  Rabimba Karanjai,Lei Xu,Zhimin Gao,Lin Chen,Mudabbir Kaleem,Weidong Shi ACM Middleware 2021

Overview of Problems

An event driven framework for smart contract execution - ACM DEBS – 2021

- The current smart contract platforms use a transaction-driven execution model, which requires users to initiate transactions to trigger smart contract execution. This model is inefficient, costly, and unsuitable for many time-sensitive applications that depend on external events.
- The existing solutions for event-driven smart contract execution rely on centralized oracles or trusted third parties to provide event triggers, which introduce security and reliability risks. Moreover, these solutions do not separate event processing from transaction processing, which limits the scalability and performance of smart contracts.
- The current smart contract platforms do not provide a generic and flexible framework for event-driven smart contract execution that can support various types of events, such as time-based, data-based, or user-defined events.

Overview of Problems

On Conditional Cryptocurrency With Privacy - IEEE ICBC – 2021

- The current cryptocurrency systems do not support conditional transactions, which are transactions that depend on the outcomes of certain events, such as sports betting, prediction markets, or insurance claims. Conditional transactions can enable new applications and use cases for cryptocurrencies, such as decentralized finance, peer-to-peer gambling, or smart insurance.
- The existing approaches for conditional transactions rely on smart contracts to lock and release cryptocurrencies based on event triggers, which introduce several drawbacks, such as locking assets, requiring triggering mechanisms, increasing transaction costs, and exposing event conditions to the public.
- The current cryptocurrency systems do not provide privacy protection for conditional transactions, which can leak sensitive information about the users' preferences, beliefs, or risks. Privacy protection can enhance the security and usability of conditional transactions, as well as prevent manipulation or censorship by malicious actors.

Overview of Problems

Privacy preserving event based transaction system in a decentralized environment - ACM Middleware - 2021

- The current transaction systems do not support event-based transactions, which are transactions that depend on the outcomes of certain events, such as sports betting, prediction markets, or insurance claims. Event-based transactions can enable new applications and use cases for data sharing and management, such as decentralized finance, peer-to-peer gambling, or smart insurance.
- The existing approaches for event-based transactions rely on smart contracts to lock and release digital assets based on event triggers, which introduce several drawbacks, such as locking assets, requiring triggering mechanisms, increasing transaction costs, and exposing event conditions to the public.
- The current transaction systems do not provide privacy protection for event-based transactions, which can leak sensitive information about the users' preferences, beliefs, or risks. Privacy protection can enhance the security and usability of event-based transactions, as well as prevent manipulation or censorship by malicious actors.

Overview of Solutions

An event driven framework for smart contract execution - ACM DEBS – 2021

- The paper proposes a new design and implementation of a smart contract platform based on the event-driven execution model. The paper argues that this model is more suitable for many emerging smart contract applications that require timely execution based on events, such as decentralized finance, prediction markets, or insurance claims.
- The paper presents EDSC's design under the Ethereum framework, and shows how it can be easily adapted for other existing smart contract platforms. The paper also demonstrates the implementation and evaluation of EDSC using Ethereum client and reports an average 2.2 to 4.6 times reduced total latency of event triggered smart contracts.
- The paper shows that the proposed system can improve the performance and scalability of smart contracts by using an event-driven execution model that separates event processing from transaction processing. The system also provides a generic and flexible framework for event-driven smart contract execution that can support various types of events, such as time-based, data-based, or user-defined events.

Overview of Solutions

On Conditional Cryptocurrency With Privacy - IEEE ICBC – 2021

- The paper proposes a new design and implementation of a conditional cryptocurrency system with privacy protection. The system allows users to create and transfer confidential conditional coins that are linked to the outcomes of certain events, such as sports betting, prediction markets, or insurance claims.
- The paper demonstrates how to extend the Zerocoin data model and protocol to support confidential conditional coins, and evaluates the system using xJsnark.
- The paper shows that the proposed system can enable free trade of conditional assets and prevent assets from being locked, without relying on any triggering mechanism or exposing event conditions to the public. The system also ensures that the conditional coins are secure, scalable, and compatible with existing cryptocurrency platforms.

Overview of Solutions

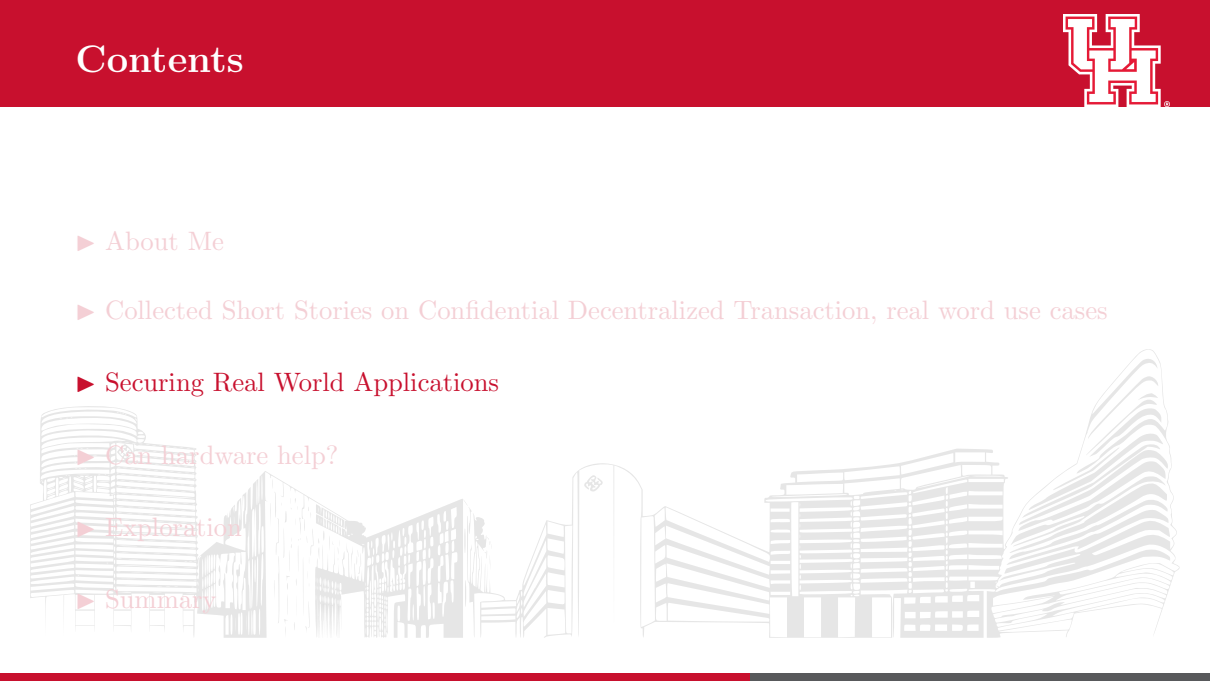
Privacy preserving event based transaction system in a decentralized environment - ACM Middleware - 2021

- The paper presents the design and implementation of a privacy preserving event based UTXO (Unspent Transaction Output) transaction system. The system allows users to create and transfer confidential event based UTXO notes that are linked to the outcomes of certain events, such as sports betting, prediction markets, or insurance claims.
- The paper demonstrates how to extend the Zerocoin data model and protocols to support confidential event based UTXO notes, and evaluates the system using xJsnark.
- The paper shows that the proposed system can enable privacy preserving data sharing and management using event based UTXO notes, without relying on any triggering mechanism or exposing event conditions to the public. The system also ensures that the associations between UTXO notes and events are hidden from the validators.

Problems and Solutions

- EDSC: An Event-Driven Smart Contract Platform
  - Problem: Scalability and performance challenges of current smart contract platforms that use the transaction-driven execution model.
  - Solution: An event-driven execution model that is more suitable for many emerging smart contract applications that require timely execution based on events.
- On Conditional Cryptocurrency With Privacy
  - Problem: Lack of privacy in existing conditional cryptocurrency systems.
  - Solution: A system that encodes the event outcome as part of a cryptocurrency note in a UTXO based system, and ensures that the event conditions and the coin values are hidden from public view using zero-knowledge proofs.
- Privacy preserving event based transaction system in a decentralized environment
  - Problem: Lack of privacy in existing event based transaction systems.
  - Solution: A system that encodes the event outcome as part of the UTXO note and protects the event privacy by hiding it with zero-knowledge proof based protocols.

Contents



Decentralized Application Infrastructures

Decentralized Application Infrastructures as Smart Contract Codes - *Distinguished Paper*

Rabimba Karanjai,Keshav Kasichainula,Nour Diallo,Mudabbir Kaleem,Lei Xu,Lin Chen,Weidong Shi - IEEE ICBC - 2022

- The paper proposes a new design and implementation of a smart contract platform that supports decentralized application infrastructures. The paper shows how to extend the TOSCA domain-specific language to model and specify decentralized application infrastructures as smart contract codes.
- The paper demonstrates how to deploy and manage decentralized application infrastructures using smart contract codes on the Ethereum framework, and shows how the design can be easily adapted for other existing smart contract platforms. The paper also evaluates the system using Ethereum client and reports the performance and cost metrics of the system.
- The paper shows that the proposed system can enable full decentralization in general-purpose computing using blockchain technology.

Blockchain Applications of TEE

Lessons Learned from Blockchain Applications of TEE and Implications

Rabimba Karanjai, L Xu, L Chen, F Zhang, Z Gao, W Shi - ACM HASP - 2021

- The paper reviews and analyzes the existing blockchain-based applications that use hardware TEEs for various purposes, such as data privacy, off-chain computation, or consensus enhancement. The paper identifies the common patterns, challenges, and pitfalls of these applications.
- The paper discusses the implications and recommendations for future research on hardware TEEs for blockchain-based applications. The paper suggests some open problems and opportunities for improving the design and implementation of hardware TEEs in general.
- The paper provides a comprehensive survey and taxonomy of the state-of-the-art hardware TEEs and blockchain-based applications that use them. The paper also compares and contrasts the features and limitations of different hardware TEEs and blockchain-based applications.

Contents

Utilizing secure Trusted Execution Environment

Decentralized Translator of Trust:
Supporting Heterogeneous TEE for Critical Infrastructure Protection

Rabimba Karanjai, Rowan Collier, Zhimin Gao, Lin Chen, Xinxin Fan, Taeweon Suh, Weidong Shi and Lei Xu - ACM BSCI - 2023

- Challenges
  - Heterogeneous TEE systems are difficult to interoperate with each other.
  - Existing solutions to this problem are either not scalable or not secure.
- Contributions
  - We propose DHTee, a decentralized coordination mechanism that uses blockchain technology to support the interoperability of devices with different TEE.
  - DHTee offers a unified framework to support heterogeneous TEE systems.
  - DHTee reduces the system management complexity and can be easily extended to support new TEE schemes.
  - DHTee protects information stored on the blockchain without affecting the function to support heterogeneous TEEs.

Contents

Privacy, LLM, Serverless, Decentralization

- Can we support emerging Web3 DAPPS in decentralized multi cloud environment? ("Decentralized FaaS over Multi-Clouds" - Submitted to IEEE Cloud)
- Can a system be designed that exposes serverless functions with integrity guarantees using Trusted Execution Environment?
- Can we build a system where LLM's can be used not only to generate code, but also systematic mathematical proofs accompanying them for verification, without prohibitive overhead
- Can we systematically test and evaluate High Performance Computing codes generated by different LLM's by generating automated test cases (To be submitted to ASPLOS)
- Can we study the pitfalls, problems and bugs introduced when used for generating smart contracts (Will be submitted to BRAIN 2023)
- Can we make a automated Verilog based exploit generator and code verifier for circuits?

Contents

Conclusion

- My research direction in future will pivot more towrads providing security guarantees in code.
- The privacy aspects of those work should mesh up well enough with decentralization aspects of the previous works.
- Exploration of security hardwares as tools for the above two points will also be my point of interest.