Research Papers on 'Blockchain'

Google Scholar

Semantic Scholar

IEEE Xplore

PubMed

Paper 1:

A Practical Rollup Escape Hatch Design

Date: 2025-03-31

Time: 11:55:10

Authors:

Francisco Gomes Figueira, Martin Derka, Ching Lun Chiu, Jan Gorzny

Summary:

- A rollup network is a type of popular "Layer 2" scaling solution for general purpose "Layer 1" blockchains like Ethereum. Rollups networks separate execution of transactions from other aspects like consensus, processing transactions off of the Layer 1, and posting the data onto the underlying layer for security. While rollups offer significant scalability advantages, they often rely on centralized operators for transaction ordering and inclusion, which also introduces potential risks. If the operator fails to build rollup blocks or propose new state roots to the underlying Layer 1, users may lose access to digital assets on the rollup. An escape hatch allows users to bypass the failing operator and withdraw assets directly on the Layer 1. We propose using a time-based trigger, Merkle proofs, and new resolver contracts to implement a practical escape hatch for these networks. The use of novel resolver contracts allow user owned assets to be located in the Layer 2 state root, including those owned by smart contracts, in order to allow users to escape them. This design ensures safe and verifiable escape of assets, including ETH, ERC-20 and ERC-721 tokens, and more, from the Layer 2.

Click here for more

Paper 2:

Blockchain for Federated Learning in the Internet of Things: Trustworthy Adaptation, Standards, and the Road Ahead

Date: 2025-03-31

Time: 08:19:18

Authors:

Farhana Javed, Engin Zeydan, Josep Mangues-Bafalluy, Kapal Dev, Luis Blanco

Summary:

- As edge computing gains prominence in Internet of Things (IoTs), smart cities, and autonomous systems, the demand for real-time machine intelligence with low latency and model reliability continues to grow. Federated Learning (FL) addresses these needs by enabling distributed model training without centralizing user data, yet it remains reliant on centralized servers and lacks built-in mechanisms for transparency and trust. Blockchain and Distributed Ledger Technologies (DLTs) can fill this gap by introducing immutability, decentralized coordination, and verifiability into FL workflows. This article presents current standardization efforts from 3GPP, ETSI, ITU-T, IEEE, and O-RAN that steer the integration of FL and blockchain in IoT ecosystems. We then propose a blockchain-based FL framework that replaces the centralized aggregator, incorporates reputation monitoring of IoT devices, and minimizes overhead via selective on-chain storage of model updates. We validate our approach with IOTA Tangle, demonstrating stable throughput and block confirmations, even under increasing FL workloads. Finally, we discuss architectural considerations and future directions for embedding trustworthy and resource-efficient FL in emerging 6G networks and vertical IoT applications. Our results underscore the potential of DLT-enhanced FL to meet stringent trust and energy requirements of next-generation IoT deployments.

Click here for more

Paper 3:

Detecting Functional Bugs in Smart Contracts through LLM-Powered and Bug-Oriented Composite Analysis

Date: 2025-03-31

Time: 04:39:51

Authors:

Binbin Zhao, Xingshuang Lin, Yuan Tian, Saman Zonouz, Na Ruan, Jiliang Li, Raheem Beyah, Shouling Ji

Summary:

- Smart contracts are fundamental pillars of the blockchain, playing a crucial role in facilitating various business transactions. However, these smart contracts are vulnerable to exploitable bugs that can lead to substantial monetary losses. A recent study reveals that over 80% of these exploitable bugs, which are primarily functional bugs, can

evade the detection of current tools. The primary issue is the significant gap between understanding the high-level logic of the business model and checking the low-level implementations in smart contracts. Furthermore, identifying deeply rooted functional bugs in smart contracts requires the automated generation of effective detection oracles based on various bug features. To address these challenges, we design and implement PROMFUZZ, an automated and scalable system to detect functional bugs, in smart contracts. In PROMFUZZ, we first propose a novel Large Language Model (LLM)-driven analysis framework, which leverages a dual-agent prompt engineering strategy to pinpoint potentially vulnerable functions for further scrutiny. We then implement a dual-stage coupling approach, which focuses on generating invariant checkers that leverage logic information extracted from potentially vulnerable functions. Finally, we design a bug-oriented fuzzing engine, which maps the logical information from the high-level business model to the low-level smart contract implementations, and performs the bug-oriented fuzzing on targeted functions. We compare PROMFUZZ with multiple state-of-the-art methods. The results show that PROMFUZZ achieves 86.96% recall and 93.02% F1-score in detecting functional bugs, marking at least a 50% improvement in both metrics over state-of-the-art methods. Moreover, we perform an in-depth analysis on real-world DeFi projects and detect 30 zero-day bugs. Up to now, 24 zero-day bugs have been assigned CVE IDs.

Click here for more

Paper 4:

Comprehensive Survey towards Security Authentication Methods for Satellite Communication Systems

Date: 2025-03-30

Time: 01:57:15

Authors:

Yunfei Meng, Changbo Ke, Zhiqiu Huang

Summary:

- Satellite communication systems (SatCom) is a brand-new network that uses artificial Earth satellites as relay stations to provide communication services such as broadband Internet access to various users on land, sea, air and in space. It features wide coverage, relatively high transmission rates and strong anti-interference capabilities. Security authentication is of crucial significance for the stable operation and widespread application of satellite communication systems. It can effectively prevent unauthorized access, ensuring that only users and devices that pass security authentication can access the satellite network. It also ensures the confidentiality, integrity, and availability of data during transmission and storage, preventing data from being stolen, tampered with, or damaged. By means of literature research and comparative analysis, this paper carries out on a comprehensive survey towards the security authentication methods used by SatCom. This paper first summarizes the existing SatCom authentication methods as five categories, namely, those based on cryptography, Blockchain, satellite orbital information, the AKA protocol and physical hardware respectively. Subsequently, a comprehensive comparative analysis is carried out on the above-mentioned five categories of security authentication methods from four dimensions, i.e., security, implementation difficulty and cost, applicable scenarios and real-time performance, and the final comparison results are following obtained. Finally, prospects are made for several important future research directions of security authentication methods for SatCom, laying a well foundation for further carrying on the related research works.

Click here for more

Paper 5:

Ethereum Price Prediction Employing Large Language Models for Short-term and Few-shot Forecasting

Date: 2025-03-29

Time: 19:04:28

Authors:

Eftychia Makri, Georgios Palaiokrassas, Sarah Bouraga, Antigoni Polychroniadou, Leandros Tassiulas

Summary:

- Cryptocurrencies have transformed financial markets with their innovative blockchain technology and volatile price movements, presenting both challenges and opportunities for predictive analytics. Ethereum, being one of the leading cryptocurrencies, has experienced significant market fluctuations, making its price prediction an attractive yet complex problem. This paper presents a comprehensive study on the effectiveness of Large Language Models (LLMs) in predicting Ethereum prices for short-term and few-shot forecasting scenarios. The main challenge in training models for time series analysis is the lack of data. We address this by leveraging a novel approach that adapts existing pre-trained LLMs on natural language or images from billions of tokens to the unique characteristics of Ethereum price time series data. Through thorough experimentation and comparison with traditional and contemporary models, our results demonstrate that selectively freezing certain layers of pre-trained LLMs achieves state-of-the-art performance in this domain. This approach consistently surpasses benchmarks across multiple metrics, including Mean Squared Error (MSE), Mean Absolute Error (MAE), and Root Mean Squared Error (RMSE), demonstrating its effectiveness and robustness. Our research not only contributes to the existing body of knowledge on LLMs but also provides practical insights in the cryptocurrency prediction domain. The adaptability of pre-trained LLMs to handle the nature of Ethereum prices suggests a promising direction for future research, potentially including the integration of sentiment analysis to further refine forecasting accuracy.

Click here for more

Paper 6:

Enhanced Smart Contract Reputability Analysis using Multimodal Data   Fusion on Ethereum

Date: 2025-03-29

Time: 12:07:37

Authors:

Cyrus Malik, Josef Bajada, Joshua Ellul

Summary:

- The evaluation of smart contract reputability is essential to foster trust in decentralized ecosystems. However, existing methods that rely solely on code analysis or transactional data, offer limited insight into evolving trustworthiness. We propose a multimodal data fusion framework that integrates code features with transactional data to enhance reputability prediction. Our framework initially focuses on AI-based code analysis, utilizing GAN-augmented opcode embeddings to address class imbalance, achieving 97.67% accuracy and a recall of 0.942 in detecting illicit contracts, surpassing traditional oversampling methods. This forms the crux of a reputability-centric fusion strategy, where combining code and transactional data improves recall by 7.25% over single-source models, demonstrating robust performance across validation sets. By providing a holistic view of smart contract behaviour, our approach enhances the model's ability to

assess reputability, identify fraudulent activities, and predict anomalous patterns. These capabilities contribute to more accurate reputability assessments, proactive risk mitigation, and enhanced blockchain security.

Click here for more

Paper 7:

SoK: Security Analysis of Blockchain-based Cryptocurrency

Date: 2025-03-28

Time: 05:21:30

Authors:

Zekai Liu, Xiaoqi Li

Summary:

- Cryptocurrency is a novel exploration of a form of currency that proposes a decentralized electronic payment scheme based on blockchain technology and cryptographic theory. While cryptocurrency has the security characteristics of being distributed and tamper-proof, increasing market demand has led to a rise in malicious transactions and attacks, thereby exposing cryptocurrency to vulnerabilities, privacy issues, and security threats. Particularly concerning are the emerging types of attacks and threats, which have made securing cryptocurrency increasingly urgent. Therefore, this paper classifies existing cryptocurrency security threats and attacks into five fundamental categories based on the blockchain infrastructure and analyzes in detail the vulnerability principles exploited by each type of threat and attack. Additionally, the paper examines the attackers' logic and methods and successfully reproduces the vulnerabilities. Furthermore, the author summarizes the existing detection and defense solutions and evaluates them, all of which provide important references for ensuring the security of cryptocurrency. Finally, the paper discusses the future development trends of cryptocurrency, as well as the public challenges it may face.

Click here for more

Paper 8:

Smart treaties: A path to binding agreements in international relations?

Date: 2025-03-27

Time: 14:07:49

Authors:

Niklas Valentin Lehmann

Summary:

- Can we create binding agreements between nations? Recently, scholars have argued that blockchain technology enables us to do so. Given that this could greatly affect the anarchical world order implied by state sovereignty, this remarkable claim is investigated thoroughly. By focusing on the technical implementation of smart contracts between nations, this article finds that the potential to create binding agreements using blockchain technology is far more limited than recently suggested.

Click here for more

Paper 9:

Unveiling Latent Information in Transaction Hashes: Hypergraph Learning for Ethereum Ponzi Scheme Detection

Date: 2025-03-27

Time: 12:52:47

Authors:

Junhao Wu, Yixin Yang, Chengxiang Jin, Silu Mu, Xiaolei Qian, Jiajun Zhou, Shanqing Yu, Qi Xuan

Summary:

- With the widespread adoption of Ethereum, financial frauds such as Ponzi schemes have become increasingly rampant in the blockchain ecosystem, posing significant threats to the security of account assets. Existing Ethereum fraud detection methods typically model account transactions as graphs, but this approach primarily focuses on binary transactional relationships between accounts, failing to adequately capture the complex multi-party interaction patterns inherent in Ethereum. To address this, we propose a hypergraph modeling method for the Ponzi scheme detection method in Ethereum, called HyperDet. Specifically, we treat transaction hashes as hyperedges that connect all the relevant accounts involved in a transaction. Additionally, we design a two-step hypergraph sampling strategy to significantly reduce computational complexity. Furthermore, we introduce a dual-channel detection module, including the hypergraph detection channel and the hyper-homo graph detection channel, to be compatible with existing detection methods. Experimental results show that, compared to traditional homogeneous graph-based methods, the hyper-homo graph detection channel achieves significant performance improvements, demonstrating the superiority of hypergraph in Ponzi scheme detection. This research offers innovations for modeling complex relationships in blockchain data.

Click here for more

Paper 10:

Process Channels: A New Layer for Process Enactment Based on Blockchain State Channels

Date: 2025-03-26

Time: 22:44:30

Authors:

Fabian Stiehle, Ingo Weber

Summary:

- For the enactment of inter-organizational business processes, blockchain can guarantee the enforcement of process models and the integrity of execution traces. However, existing solutions come with downsides regarding throughput scalability, latency, and suboptimal tradeoffs between confidentiality and transparency. To address these issues, we propose to change the foundation of blockchain-based business process execution: from on-chain smart contracts to state channels, an overlay network on top of a blockchain. State channels allow conducting most transactions off-chain while mostly retaining the core security properties offered by blockchain. Our proposal, process channels, is a model-driven approach to enacting processes on state channels, with the aim to retain the desired blockchain properties while reducing the on-chain footprint as much as possible. We here focus on the principled approach of state channels as a platform, to enable manifold future optimizations in various directions, like latency and confidentiality. We implement our approach prototypical and evaluate it both qualitatively (w.r.t. assumptions and guarantees) and quantitatively (w.r.t. correctness and gas cost). In short, while the initial deployment effort is higher with state channels, it typically pays off after a few process instances; and as long as the new assumptions hold, so do the guarantees.

Click here for more

Paper 11:

Precise Static Identification of Ethereum Storage Variables

Date: 2025-03-26

Time: 16:22:08

Authors:

Sifis Lagouvardos, Yannis Bollanos, Michael Debono, Neville Grech, Yannis Smaragdakis

Summary:

- Smart contracts are small programs that run autonomously on the blockchain, using it as their persistent memory. The predominant platform for smart contracts is the Ethereum VM (EVM). In EVM smart contracts, a problem with significant applications is to identify data structures (in blockchain state, a.k.a. "storage"), given only the deployed smart contract code. The problem has been highly challenging and has often been considered nearly impossible to address satisfactorily. (For reference, the latest state-of-the-art research tool fails to recover nearly all complex data structures and scales to under 50% of contracts.) Much of the complication is that the main on-chain data structures (mappings and arrays) have their locations derived dynamically through code execution. We propose sophisticated static analysis techniques to solve the identification of on-chain data structures with extremely high fidelity and completeness. Our analysis scales nearly universally and recovers deep data structures. Our techniques are able to identify the exact types of data structures with 98.6% precision and at least 92.6% recall, compared to a state-of-the-art tool managing 80.8% and 68.2% respectively. Strikingly, the analysis is often more complete than the storage description that the compiler itself produces, with full access to the source code.

Click here for more

Paper 12:

A Survey of Secure Semantic Communications

Date: 2025-03-26

Time: 15:35:20

Authors:

Rui Meng, Song Gao, Dayu Fan, Haixiao Gao, Yining Wang, Xiaodong Xu, Bizhu Wang, Suyu Lv, Zhidi Zhang, Mengying Sun

Summary:

- Semantic communication (SemCom) is regarded as a promising and revolutionary technology in 6G, aiming to transcend the constraints of ``Shannon's trap" by filtering out redundant information and extracting the core of effective data. Compared to traditional communication paradigms, SemCom offers several notable advantages, such as reducing the burden on data transmission, enhancing network management efficiency, and optimizing resource allocation. Numerous researchers have extensively explored SemCom from various perspectives, including network architecture, theoretical analysis, potential technologies, and future applications. However, as SemCom continues to evolve, a multitude of security and privacy concerns have arisen, posing threats to the confidentiality, integrity, and availability of SemCom systems. This paper presents a comprehensive survey of the technologies that can be utilized to secure SemCom. Firstly, we elaborate on the entire life cycle of SemCom, which includes the model training, model transfer, and semantic information transmission phases. Then, we identify the security and privacy issues that emerge during these three stages. Furthermore, we summarize the techniques available to mitigate these security and privacy threats, including data cleaning, robust learning, defensive strategies against backdoor attacks, adversarial training, differential privacy, cryptography, blockchain technology, model compression, and physical-layer security. Lastly, this paper outlines future research directions to guide researchers in related fields.

Click here for more