Gmail **Satoshi Nakamoto <nakamoto.satoshi.b@gmail.com>**

10 new citations to your articles

Google Scholar Alerts <scholaralerts-noreply@google.com> Mon, Sep 22 at 23:07
To: <nakamoto.satoshi.b@gmail.com>

Efficient Three-party ECDSA Signature Based on Replicated Secret Sharing with Identifiable Abort

W Cheng, Q Feng, C Zeng, Y Peng, M Luo, X Yang… - IEEE Transactions on …, 2025

The private key is the only credential that can control and access account assets in the blockchain. Once the private key is leaked or stolen, the user loses control of the assets. The current mainstream solution is a threshold signature scheme based on secure multi-party computation, which can privately calculate the signature value without recovering the complete private key. However, most existing solutions are based on homomorphic or oblivious transmission, which have problems such as …

- Cites: Bitcoin: A Peer-to-Peer Electronic Cash System

Threshold Signatures with Verifiably Timed Combining and Message-Dependent Tracing

M Li, H Ding, Y Chen, Y Qiao, Z Zhang, L Zhu, M Conti - IEEE Transactions on …, 2025

Threshold Signature (TS) is one of the fundamental cryptographic primitives adopted in many practical applications. Current Threshold, Accountable, and Private Signature (TAPS) schemes suffer from delayed combining, unverifiable combining, and message-independent tracing. More precisely, a malicious combiner may delay the combination of signature shares and replace some signature shares from honest signers with ones from colluding signers, and an unrestricted tracer can reveal …

- Cites: Bitcoin: A Peer-to-Peer Electronic Cash System

CRCT: Compact Ring Confidential Transactions Based on Sum Arguments

J Duan, W Wang, L Wang, L Gu, L Zhu - IEEE Transactions on Information Forensics …, 2025

Ring Confidential Transactions (RingCT) is a classic cryptographic protocol for anonymous transactions on blockchains, currently used in the popular anonymous cryptocurrency Monero. The proof size of RingCT transactions is linearly related to the ring size, which limits the use of larger ring sizes due to the significant communication overhead it incurs. However, reducing the ring size also leads to decreased anonymity. Therefore, in recent years, many studies have focused on …

- Cites: Bitcoin: A Peer-to-Peer Electronic Cash System

SAT-IOTA: A Cybersecurity Reinforcement Framework for Blockchain-Driven Space Satellites Utilizing Anomaly Prediction

AN Bikos, SAP Kumar - IEEE Journal on Miniaturization for Air and Space …, 2025

This paper introduces SAT-IOTA, a lightweight and AI-driven cybersecurity framework designed for blockchain-powered satellite infrastructures. Unlike traditional detection approaches, SAT-IOTA employs predictive anomaly analytics combined with a Sliding Window (SW) machine learning mechanism to proactively identify and mitigate security threats in space-air-ground integrated networks (SAGINs). The proposed framework integrates IOTA distributed ledger technology …

- Cites: Bitcoin: a peer-to-peer electronic cash system. Whitepaper (2008)

[HTML] Optimizing blockchain file storage: enhancing performance and reducing ledger size with adaptive compression and advanced data structures

M Tmeizeh, C Rodríguez-Domínguez… - Cluster Computing, 2025

Ensuring the digital preservation of files and data in an immutable environment is essential for maintaining security, integrity, and trust. The decentralized architecture, robust security, and reliability of blockchain position it as a leading solution for storage technologies requiring tamper-proof integrity. This work presents an enhanced version of a previously published framework, introducing a technique to optimize on-chain file storage efficiency. The proposed solution leverages a …

- Cites: Bitcoin: A peer-to-peer electronic cash system. 2008

Modelling Open Source Blockchain Software Health with Factor Analysis

J Nijsse, A Litchfield - 2025 5th International Conference on Computer …, 2025

Software health is an elusive concept with no consensus on its constituents and metrics, and little work in the blockchain domain. Since the inception of Bitcoin, the proliferation of blockchain projects and tokens has also resulted in numerous victims harmed by scammers quickly copying code, creating phishing sites, and luring investors into unhealthy projects. We model blockchain software health by exploratory factor analysis to identify the latent constructs of general Public Interest in …

- Cites: Bitcoin: A Peer-to-Peer Electronic Cash System

[PDF] LoChain: A Decentralized and Privacy-Preserving Blockchain Protocol for Mobility Data Management

MMS Bouderbala, D Demirag, S Gambs - The International Archives of the …, 2025

Mobility data has become a strategic asset in urban planning, crisis management and smart city operations. However, centralized systems for mobility tracking raise severe privacy concerns as they have the ability to directly link individuals to their movements. To address these issues, we propose LoChain, a decentralized protocol that enables the privacy-preserving collection and processing of mobility data based on blockchain technology. More precisely, LoChain replaces precise coordinates …

- Cites: Bitcoin: A Peer-to-Peer Electronic Cash System

Secure Data Sharing and End-to-End Encryption in Federated Cloud Computing Systems

O Dewangan, PK Tamrakar, A Guru, A Shrivastava… - … International Conference on …, 2025

Rapid increase of data and cloud boom has altered the requirement for secure and scalable data sharing mechanisms. The problem with federated cloud computing security lies in combining several cloud service providers together: the confidentiality, integrity, and controlled access cannot be guaranteed, which is very challenging. This research is contended to develop a secure framework for data sharing in federated cloud domains with the use of end-to-end encryption (E2EE) as …

- Cites: Bitcoin: A Peer-to-Peer Electronic Cash System

Designing Business Models through Sustainable and Digital Innovation

D Binci, NM Gusmerotti, C Cerruti - 2025

Sustainability today is not simply a constraint or compliance issue-it is an innovation process that redefines how companies conceive their value proposition, organize supply chains, engage stakeholders, and govern transformation. This book places business models at the center of that redefinition, framing Business Model Innovation (BMI) as a critical lever to align economic performance with social and environmental value creation. Bridging academic rigor and practical relevance, this volume offers …

- Cites: Bitcoin: A Peer-to-Peer Electronic Cash System

[PDF] Blockchain Consensus Mechanisms

P Bains - 2025

Consensus mechanisms underpin the effective operation of blockchains by ensuring a single consistent and honest ledger. The design and implementation of these consensus mechanisms can improve or impede the ability of regulatory and supervisory authorities to achieve their objectives and mandates. This paper provides an update to the Fintech Note Blockchain Consensus Mechanisms: A Primer for Supervisors (2022) by reviewing the growth of existing consensus …

- Cites: A peer-to-peer electronic cash system
