rippleimpact | university blockchain research initiative

BLOCKCHAIN TECHNOLOGY RESEARCH HIGHLIGHTS FROM UNIVERSITY PARTNERS

UBRI

Embracing New Horizons in Blockchain Research and Innovation

2025

The University Blockchain Research Initiative (UBRI), launched by Ripple in 2018, has established a global network of over 60 academic partners to drive research and education in blockchain and digital assets. Through strategic funding, collaboration, and the exchange of ideas, UBRI empowers faculty and students to explore real-world blockchain applications, shape academic programs, and train the next generation of leaders in decentralized finance (DeFi) and emerging technologies.

This 2024–2025 report highlights the exceptional academic output of UBRI-affiliated institutions, showcasing journal publications, conference papers, books, and active research efforts. These contributions address critical and emerging themes including stablecoins, DeFi, and AI integration, while supporting Ripple's long-term vision for innovation in the blockchain space.

As blockchain continues to evolve and gain traction across industries, UBRI remains a vital catalyst for rigorous, forward-thinking academic inquiry. We invite you to explore the insights captured in this report and see how UBRI-supported researchers are helping shape the future of this technology and its global impact.

*The materials in this report are based on work that may be supported or partially supported by Ripple under the University Blockchain Research Initiative (UBRI) program. Any opinions, findings, conclusions, or recommendations expressed in the materials are those of the authors and do not necessarily reflect the views of Ripple. Additionally, the XRP Ledger (XRPL) is a decentralized public blockchain based on open-source technology to which a global group of businesses and developers contribute (including Ripple).

Copyright © 2025 Ripple. All rights reserved.

Contents

Introduction 4

Stablecoins and Real-Word Assets (RWA) 5

DeFi Infrastructure 9

Cryptographic Security and Oracle Design 13

AI-Driven Governance and Consensus Mechanisms 17

Blockchain Interoperability and Regulatory Fragmentation 21

Institutional Design and Social Impact of Blockchain 25

Conclusion 28

UBRI University Partners 29

Copyright © 2025 Ripple. All rights reserved.

Introduction

The transformative potential of blockchain continues to grow across industries; from reimagining financial infrastructure and digital assets to redefining governance, identity, and compliance in an increasingly decentralized world. As the global landscape evolves, academic research remains essential in shaping the future of blockchain by providing critical insights, rigorous analysis, and innovative frameworks for real-world adoption.

Ripple's University Blockchain Research Initiative (UBRI) plays a key role in advancing this mission. Through its philanthropic commitment to global academic collaboration, UBRI has empowered top researchers and institutions to explore frontier topics in blockchain, pushing the boundaries of what is technologically and economically possible.

This year's report covers the 2024–2025 academic cycle and highlights cutting-edge work produced by UBRI partners across six thematic areas. These topics reflect the most pressing challenges and opportunities in blockchain development today including the rise of stablecoins and tokenized real-world assets (RWAs) and new models for DeFi infrastructure.

The research also explores privacy-preserving central bank digital currency (CBDC) design, oracle resilience, and the integration of AI in consensus and governance systems. Other contributions examine challenges around regulatory fragmentation and interoperability across chains and jurisdictions, as well as the broader institutional and societal impact of blockchain.

Together, these studies emphasize the importance of academic research in driving the blockchain ecosystem forward and underscore UBRI's commitment to open inquiry and innovation across disciplines. Looking ahead, Ripple and its UBRI partners remain focused on leveraging blockchain to build a more inclusive, efficient, and transparent future.

Copyright © 2025 Ripple. All rights reserved.

01 —— SECTION

Stablecoins and Real-Word Assets (RWA)

Stablecoins and tokenized assets are catalyzing the next phase of financial innovation by enhancing efficiency, transparency, and programmability in digital markets. This section explores critical design decisions in privacy-preserving tokenization, such as frameworks that balance privacy with regulatory compliance in offline transactions. It also examines key adoption drivers, evolving legal frameworks, and the interplay between public and private sectors, providing a broader perspective on how tokenization can enable more resilient and inclusive financial systems.

Copyright © 2025 Ripple. All rights reserved.

Privacy and Compliance Design Options in Offline Central Bank Digital Currencies

Panagiotis Michalopoulos, Odunayo Olowookere, Nadia Pocher

IEEE Transactions on Network and Service Management, 2025

https://www.eecg.utoronto.ca/~veneris/TNSM25.pdf

Abstract

Many central banks are researching and piloting digital versions of fiat money, specifically retail central bank digital currencies (CBDCs). Core to many discussions revolving around these systems' design is the ability to perform transactions even without network connectivity. While this approach is generally believed to provide additional degrees of freedom for user privacy, the lack of direct involvement of third parties in these offline transfers also interferes with key regulatory requirements that need to be accommodated in the financial space. This paper presents a compliance-by-design approach to evaluate technologies that can balance privacy with anti-money laundering and counter-terrorism financing (AML/CFT) measures. It classifies privacy design options and corresponding technical building blocks for offline CBDCs, along with their impact on AML/CFT measures, and outlines commonalities and differences between offline and online solutions. As such, it provides a conceptual framework for further techno-legal assessments and implementations.

Adoption of Central Bank Digital Currencies: A Data-Driven Exploration of Key Influential Factors

Arshpreet Singh, Mohamad Sadegh Sangari, Atefeh Mashatan

Americas Conference on Information Systems (AMCIS), 2025

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1147&context=amcis2025

Abstract

Central Bank Digital Currency (CBDC) is a digital form of fiat currency issued and regulated by central banks. Understanding the drivers and barriers for CBDC adoption is crucial for helping the key stakeholders determine the important areas and concerns that need to be addressed to ensure a successful integration of CBDCs in the financial system. This paper employs a data-driven approach to understand major themes regarding CBDC adoption in news articles using topic modeling, followed by aspect-based sentiment analysis (ABSA) to prioritize the factors influencing CBDC adoption. The findings highlight digital infrastructure, digital economy, and financial innovation as top adoption drivers, and security, user trust, and policy and regulations as the major barriers. The data-driven approach of using ABSA to rank a list of drivers and barriers is the first of its kind and can be generalized to rank factors in other domains.

Copyright © 2025 Ripple. All rights reserved.

Carbono 21: Promoting Forestation Through Digital Assets

Pedro H. B. Correia, Marcos A. S. Simplicio Jr.

Brazilian Symposium on Computer Networks and Distributed Systems (SBRC), 2025

https://sol.sbc.org.br/index.php/sbrc_estendido/article/view/35878

Abstract

Despite its environmental benefits, forestation is often overlooked in favor of more profitable crops with negative environmental impacts. In response, this work promotes forestation through tokenization, creating financial incentives for landowners who plant trees. Forested areas and green assets are transformed into Non-Fungible Tokens (NFTs) on a consortium blockchain. Their metadata is automatically updated via satellite-based deforestation tracking systems, something unseen in the literature. The solution also contributes to distributed systems and the environment by proposing several transparency mechanisms – often lacking in forestation efforts and permissioned blockchains –, enabling authorities to audit the transaction and utilization of green assets.

On the Coexistence of Stablecoins and Central Bank Digital Currencies

Yuliya Guseva, Sangita Gazi, Douglas Eakeleys

Law and Contemporary Problems, 2024

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4709282

Abstract

Money is not a simple concept. It is a complex construct consisting of public and private elements. A significant portion of it originates from private-sector entities like banks, against which other private parties have contractual claims. This longstanding partnership between public and private institutions in creating and supplying money is deeply embedded in economic history and, arguably, even the Constitution of the United States. Over the centuries, federal law has specified which firms issue the safest private money and, in doing so, placed private banks in a somewhat privileged position. Non-bank financial firms, for example, typically do not have access to the Fed-provided rails of the clearing and settlement system for inter-bank payments and the master accounts at the Fed.

These regulatory fundamentals of the private-public economic partnership are long-standing but imperfect. To name a few issues, banks fail; banks have flaws in their operational coverage and do not serve every part of our economy, with millions of unbanked and underbanked residents in the United States; and the current payment systems exhibit inefficiencies and high costs in transfers, clearing, and settlement. These issues highlight that the public-private money system and its regulatory framing are not ideal, militating in favor of reform.

The traditional avenue for improving efficiencies and reducing transaction costs is innovation accompanied by relevant regulatory changes that ensure that innovations do not broadly

Copyright © 2025 Ripple. All rights reserved.

generate negative externalities affecting consumers, financial markets, and the economy. In this Article, we consider two technology-based initiatives: “central bank digital currencies” (CBDCs) (digital money designed as a representation of fiat money with universal accessibility and the status of a legal tender) and “stablecoins” (privately issued cryptoassets relying on blockchain technology and aiming to maintain stable value, often through collateralization by other assets that have value).

These public and private innovations are often presented as a study in contrast and competing products. From a policy perspective, CBDCs are described as safer public money, while stablecoins are pictured as risky private alternatives raising systemic risk concerns. Regulators also worry that stablecoins could create unwanted competition for fiat currencies.

In this Article, we change this standard perspective by focusing on how stablecoins may help us reconsider the foundations of the public-private money partnership as it exists to solve the inefficiencies of the current bank-focused system. We identify the pros and cons of the relationship between stablecoins and CBDCs. The United States is unlike many other countries in its historical approach to public monetary sovereignty and the importance of private money and financial institutions. The public does not need to oust the private. Instead, carefully regulated private initiatives should be preserved lest the United States loses the efficiencies of private innovation. Simultaneously, it is self-evident that these assets need to be regulated.

Our exploration into the coexistence of stablecoins and CBDCs reveals a complex and evolving landscape of technological innovation in the payment and financial sectors. We underscore the need for a nuanced understanding of both private and public digital money, highlighting their distinct roles, potential benefits, and inherent risks within the global financial ecosystem. While stablecoins offer innovative solutions and contribute to diversification within the financial and payment sectors, their regulatory challenges and risk factors necessitate careful oversight. Conversely, the emergence of CBDCs represents a significant step by central banks in modernizing monetary systems and potentially enhancing financial inclusion, but these developments raise their own sets of challenges and risks.

A key overarching observation is that public money, including CBDCs, and private money, such as stablecoins, will continue to coexist. Regulators need to adapt to this evolving coexistence and plurality of monetary instruments and create reliable regulatory safeguards for this public-private economic partnership. Better, smarter guardrails for the evolving coexistence of private and public money must simultaneously capitalize on the benefits of private innovation, control its negative externalities, safeguard financial stability, and protect consumers.

Copyright © 2025 Ripple. All rights reserved.

02 —— SECTION

DeFi Infrastructure

DeFi continues to transform financial services by reducing intermediaries, but it also introduces new risks across governance and security. This section features research on defending smart contracts against oracle manipulation, detecting price manipulation attacks, and introducing AI-driven governance models to improve decision-making. Insights into the dual role of Decentralized Autonomous Organizations (DAOs), highlight the complex dynamics of decentralized systems. These studies contribute to building more robust, adaptive, and transparent DeFi Infrastructure.

Copyright © 2025 Ripple. All rights reserved.

Safeguarding DeFi Smart Contracts Against Oracle Deviations

Xun Deng, Sidi Mohamed Beillahi, Cyrus Minwalla, Han Du, Andreas Veneris, Fan Long

International Conference on Software Engineering (ICSE), 2024
https://dl.acm.org/doi/abs/10.1145/3597503.3639225

Abstract

This paper presents OVer, a framework designed to automatically analyze the behavior of decentralized finance (DeFi) protocols when subjected to a "skewed" oracle input. OVer firstly performs symbolic analysis on the given contract and constructs a model of constraints. Then, the framework leverages an SMT solver to identify parameters that allow its secure operation. Furthermore, guard statements may be generated for smart contracts that may use the oracle values, thus effectively preventing oracle manipulation attacks. Empirical results show that OVer can successfully analyze all 10 benchmarks collected, which encompass a diverse range of DeFi protocols. Additionally, this paper illustrates that current parameters utilized in the majority of benchmarks are inadequate to ensure safety when confronted with significant oracle deviations. It shows that existing ad-hoc control mechanisms such as introducing delays are often in-sufficient or even detrimental to protect the DeFi protocols against the oracle deviation in the real-world.

DeFi Attacks and the Role of DAOs

Bianca Kremer, Kanye Ye Wang

Decentralised Autonomous Organisation Regulation: Principles and Perspective for the Future, 2024
https://viewer.content-select.com/pdf/viewer?id=1&id_type=isbn&identifiers=9783161637018&signature=8b2c79abeb77146af4574ecf9f2063adc18c1e56&ses

Abstract

Decentralized Finance (DeFi) represents an innovative alternative to the traditional financial system and is driven by blockchain technology. While it has witnessed significant growth, it has also been plagued by a range of security breaches, including hacks and other malicious attacks, leading to significant financial losses. By 2022, such attacks within the DeFi ecosystem amounted to an alarming $3.8 billion. Within this landscape, Decentralized Autonomous Organizations (DAOs), a pioneering model of bottom-up coordination, have emerged as both potential mitigators of risk and, paradoxically, potential attack vectors. In this paper, we explore the multifunctional role of DAOs within DeFi attacks. We examine their proactive involvement in preventing, mitigating, and responding to such attacks, while also being susceptible targets. Through case studies involving DAOs, we provide insights into how DAOs operate in DeFi.

Copyright © 2025 Ripple. All rights reserved.

DeFort: Automatic Detection and Analysis of Price Manipulation Attacks in DeFi Applications

Maoyi Xie, Ming Hu, Ziqiao Kong, Cen Zhang, Yebo Feng, Haijun Wang, Yue Xue, Hao Zhang, Ye Liu, Yang Liu

ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), 2024
https://doi.org/10.1145/3650212.3652137

Abstract

Although Decentralized Finance (DeFi) applications facilitate tamper-proof transactions among multiple anonymous users, since attackers can access the smart contract bytecode directly, vulnerabilities in the transaction mechanism, contract code, or third-party components can be easily exploited to manipulate token prices, leading to financial losses. Since price manipulation often relies on specific states and complex trading sequences, existing detection tools have limitations in addressing this problem. In addition, to swiftly identify the root cause of an attack and implement targeted defense and remediation measures, auditors typically prioritize understanding the methodology behind the attack, emphasizing 'how' it occurred rather than simply confirming its existence. To address these problems, this paper presents a novel automatic price manipulation detection and analysis framework, named DeFort, which contains a price manipulation behavior model to guide on-chain detection, multiple price monitoring strategies to detect pools with abnormal token prices, and various profit calculation mechanisms to confirm attacks. Based on behavioral models, DeFort can automatically locate transactions and functions that cause abnormal price fluctuations and identify attackers and victims. Experimental results demonstrate that DeFort can outperform state-of-the-art price manipulation detection methods. Furthermore, after monitoring 441 real-world projects for two months, DeFort successfully detected five price manipulation attacks.

Liquidity Provision on Blockchain-based Decentralized Exchanges

Agostino Capponi, Ruizhe Jia

Review of Financial Studies, 2025
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805095

Abstract

We show that the infrastructure of decentralized exchanges (DEXs) subjects liquidity providers (LPs) to a tragedy of the commons. LPs lack incentives to exit liquidity pools to prevent arbitrage losses, as these are collectively shared, while withdrawal costs are borne individually. Arbitrage rents primarily flow to validators as infrastructure fees, with the median arbitrageur transferring 96% of profits. Proposed solutions—speed technology, alternative sequencing rules, and flexible pricing curves—fail to reduce these rents. Leveraging the Silicon Valley Bank crisis as a natural experiment, we show that LPs defensively adopt more convex pricing curves to mitigate adverse selection risks.

Copyright © 2025 Ripple. All rights reserved.

Game Theoretic Liquidity Provisioning in Concentrated Liquidity Market Makers

Weizhao Tang, Rachid El-Azouzi, Cheng Han Lee, Ethan Chan, Giulia Fanti

PACM-MACS, 2025
https://dl.acm.org/doi/abs/10.1145/3711700

Abstract

Automated marker makers (AMMs) are decentralized exchanges that enable the automated trading of digital assets. Liquidity providers (LPs) deposit digital tokens, which can be used by traders to execute trades, which generate fees for the investing LPs. In AMMs, trade prices are determined algorithmically, unlike classical limit order books. Concentrated liquidity market makers (CLMMs) are a major class of AMMs that offer liquidity providers flexibility to decide not only how much liquidity to provide, but in what ranges of prices they want the liquidity to be used. This flexibility can complicate strategic planning, since fee rewards are shared among LPs. We formulate and analyze a game theoretic model to study the incentives of LPs in CLMMs. Our main results show that while our original formulation admits multiple Nash equilibria and has complexity quadratic in the number of price ticks in the contract, it can be reduced to a game with a unique Nash equilibrium whose complexity is only linear. We further show that the Nash equilibrium of this simplified game follows a waterfilling strategy, in which low-budget LPs use up their full budget, but rich LPs do not. Finally, by fitting our game model to real-world CLMMs, we observe that in liquidity pools with risky assets, LPs adopt investment strategies far from the Nash equilibrium. Under price uncertainty, they generally invest in fewer and wider price ranges than our analysis suggests, with lower-frequency liquidity updates. In such risky pools, by updating their strategy to more closely match the Nash equilibrium of our game, LPs can improve their median daily returns by $116, which corresponds to an increase of 0.009% in median daily return on investment (ROI). At maximum, LPs can improve daily ROI by 0.855% when they reach Nash equilibrium. In contrast, in stable pools (e.g., of only stablecoins), LPs already adopt strategies that more closely resemble the Nash equilibrium of our game.

Copyright © 2025 Ripple. All rights reserved.

03 SECTION

Cryptographic Security and Oracle Design

Foundational trust in blockchain systems depends on advanced cryptographic protections and secure oracle mechanisms. Research in this section advances both, introducing quantum-resistant ledger designs, hybrid cryptographic schemes, and improved oracle structures for decentralized data feeds. Innovative applications include multi-party computation for auditing, decentralized counting oracles, and large language models (LLMs) for vulnerability detection. Together, these works strengthen blockchain security against evolving threats and promote more reliable offchain data integration.

Copyright © 2025 Ripple. All rights reserved.

Benchmarking LLMs and LLM-based Agents in Practical Vulnerability Detection for Code Repositories

Alperen Yildiz, Sin G. Teo, Yiling Lou, Yebo Feng, Chong Wang, Dinil Mon Divakaran

Association for Computational Linguistics (ACL), 2025

https://arxiv.org/abs/2503.03586

Abstract

Large Language Models (LLMs) have shown promise in software vulnerability detection, particularly on function-level benchmarks like Devign and BigVul. However, real-world detection requires interprocedural analysis, as vulnerabilities often emerge through multi-hop function calls rather than isolated functions. While repository-level benchmarks like ReposVul and VulEval introduce interprocedural context, they remain computationally expensive, lack pairwise evaluation of vulnerability fixes, and explore limited context retrieval, limiting their practicality.

We introduce JitVul, a JIT vulnerability detection benchmark linking each function to its vulnerability-introducing and fixing commits. Built from 879 CVEs spanning 91 vulnerability types, JitVul enables comprehensive evaluation of detection capabilities. Our results show that ReAct Agents, leveraging thought-action-observation and interprocedural context, perform better than LLMs in distinguishing vulnerable from benign code. While prompting strategies like Chain-of-Thought help LLMs, ReAct Agents require further refinement. Both methods show inconsistencies, either misidentifying vulnerabilities or over-analyzing security guards, indicating significant room for improvement.

CountChain: A Decentralized Oracle Network for Counting Systems

Behkish Nassirzadeh, Stefanos Leonardos, Albert Heinle, Anwar Hasan, Vijay Ganesh

IEEE International Conference on Blockchain (ICBC), 2024

https://www.computer.org/csdl/proceedings-article/blockchain/2024/515900a324/20l5lOKa1ZC

Abstract

Blockchain integration in industries like online advertising is hindered by its connectivity limitations to off-chain data. These industries heavily rely on precise counting systems to collect and analyze off-chain data. This requires mechanisms, often called oracles, to feed off-chain data into smart contracts. However, current oracle solutions are ill-suited for counting systems since the oracles do not know when to expect the data, posing a significant challenge. To address this, we present CountChain, a decentralized oracle network for counting systems. In CountChain, data is received by all oracle nodes, and any node can submit a proposition request. Each proposition contains enough data to evaluate the occurrence of an event. Only randomly selected nodes participate in a game to evaluate the truthfulness of each proposition by providing proof and some stake. Finally, the propositions with the outcome of True increments the counter in a smart contract. Thus, instead of a contract calling oracles for data, in CountChain, the oracles call a smart contract when the data is available. Furthermore,

Copyright © 2025 Ripple. All rights reserved.

we present a formal analysis and experimental evaluation of the system's parameters on over half a million data points to obtain optimal system parameters. In such conditions, our gametheoretical analysis demonstrates that a Nash equilibrium exists wherein all rational parties participate with honesty.

Toxic Decoys: A Path to Scaling Privacy-Preserving Cryptocurrencies

Christian Cachin, François-Xavier Wicht

Proceedings on Privacy Enhancing Technologies (PoPETs), 2025
https://petsymposium.org/popets/2025/popets-2025-0165.pdf

Abstract

Anonymous cryptocurrencies attracted much attention over the past decade, yet ensuring both integrity and privacy in an open system remains challenging. Their transactions preserve privacy because they do not reveal on which earlier transaction they depend, specifically which outputs of previous transactions are spent. However, achieving privacy imposes a significant storage overhead due to two current limitations. First, the set of potentially unspent outputs of transactions grows indefinitely because the design hides cryptographically which one have been consumed; and, second, additional data must be stored for each spent output to ensure integrity, that is, to prevent that it can be spent again. We introduce a privacy-preserving payment scheme that mitigates these issues by randomly partitioning unspent outputs into fixed-size bins. Once a bin has been referenced in as many transactions as its size, it is pruned from the ledger. This approach reduces storage overhead while preserving privacy. We first highlight the scalability benefits of using smaller untraceability sets instead of considering the entire set of outputs, as done in several privacy-preserving cryptocurrencies. We then formalize the security and privacy notions required for a scalable, privacy-preserving payment system and analyze how randomized partitioning plays a key role in both untraceability and scalability. To instantiate our approach, we provide constructions based on Merkle trees and one based on cryptographic accumulators. We finally show the storage benefits of our scheme and analyze its resilience against large-scale flooding attacks using empirical transaction data.

From Theory to Implementation of Quantum-Safe Ledgers with XRPL as a Case Study

Atharva Lele, Vaibhav Agarwal, Hitesh Tewari

International Conference on Blockchain Computing and Applications (BCCA), 2025

Abstract

The Ripple-developed XRP Ledger (XRPL) is fundamental for securing blockchain transactions efficiently. However, the rise of quantum computing threatens the cryptographic algorithms the XRPL relies on, for example Secp256k1 and Ed25519-donna for securing transactions and validating digital signatures. Shor's and Grover's algorithms can break the security of Secp256k1 and Ed25519-donna which will make them vulnerable to attack. To mitigate this critical threat, we propose integrating Post-Quantum Cryptographic (PQC) algorithms into XRPL. Our focus is on the NIST standardized CRYSTALS-Dilithium candidate, which is a lattice-based algorithm

Copyright © 2025 Ripple. All rights reserved.

that offers robust security against classical and quantum attacks. By incorporating CRYSTALS-Dilithium alongside existing classical algorithms, a smooth transition to quantum resistance is enabled while also ensuring backward compatibility. This requires modifications to the XRPL protocol, key management infrastructure, and transaction validation process. Our approach not only strengthens XRPL against future threats, but also sets a standard for quantum-resistant blockchain security.

GrAC: Graph-Based Anonymous Credentials from Identity Graphs on Blockchain

Wenyi Tang, Shankha Shubhra Mukherjee, Seongho Park, Changhao Chenli, Hyunok Oh, Jihye Kim, Taeho Jung

IEEE Blockchain Conference, 2024
https://www.computer.org/csdl/proceedings-article/blockchain/2024/515900a113/20I5gYt6NUc

Abstract

With the growing need for privacy and self-sovereign identity, traditional identity management relying on centralized data registries not only represents single points of failure but also lacks transparency and control over users' identity information. With the built-in tamper-proofness and transparency, blockchain has been widely studied to accommodate the challenges in traditional identity management. Still, it usually comes with privacy concerns due to its public accessibility. Anonymous credentials take advantage of the recent progress in zero-knowledge proof, allowing the unlinkable presentation of only the necessary attributes for a service to guarantee anonymity. However, the existing anonymous credentials require a secondary issuer to verify and manage the anonymized credentials, which compromises the overall transparency and causes indirect management of the user's identity. In this paper, we propose GrAC, a blockchain-based identity management system based on a novel identity graph, which allows users and identity providers to securely store and manage identity information on the blockchain without intermediate entities. GrAC also includes an anonymous authentication protocol suite based on zero-knowledge proof, allowing users to generate one-time anonymous credentials that selectively reveal minimal information to the service provider for authentication. The analysis and evaluations show that GrAC has a reasonable overhead and provides adequate anonymity protection while removing the need for intermediate issuers.

Copyright © 2025 Ripple. All rights reserved.

04 SECTION

AI-Driven Governance and Consensus Mechanisms

AI technologies are introducing new possibilities for enhancing governance, security, and efficiency in decentralized systems. This section examines how AI can improve the governance of decentralized organizations, strengthen consensus protocols through fuzz-testing, and optimize protocol performance via advanced data analysis. By merging blockchain and AI, these studies lay the groundwork for smarter, more adaptive, and resilient consensus and governance frameworks.

Copyright © 2025 Ripple. All rights reserved.

Auto.gov: Learning-Based Governance for Decentralized Finance (DeFi)

Jiahua Xu, Yebo Feng, Daniel Perez, Benjamin Livshits

IEEE Transactions on Services Computing, 2025
https://ieeexplore.ieee.org/document/10937069?denied=

Abstract

Decentralized finance (DeFi) is an integral component of the blockchain ecosystem, enabling a range of financial activities through smart-contract-based protocols. Traditional Decentralized finance (DeFi) governance typically involves manual parameter adjustments by protocol teams or token holder votes, and is thus prone to human bias and financial risks, undermining the system's integrity and security. While existing efforts aim to establish more adaptive parameter adjustment schemes, there remains a need for a governance model that is both more efficient and resilient to significant market manipulations. In this paper, we introduce “Auto.gov”, a learning-based governance framework that employs a Deep Q-network (DQN) Reinforcement learning (RL) strategy to perform semi-automated, data-driven parameter adjustments. We create a DeFi environment with an encoded action-state space akin to the Aave lending protocol for simulation and testing purposes, where Auto.gov has demonstrated the capability to retain funds that would have otherwise been lost to price oracle attacks. In tests with real-world data, Auto.gov outperforms the benchmark approaches by at least 14% and the static baseline model by tenfold, in terms of the preset performance metric—protocol profitability. Overall, the comprehensive evaluations confirm that Auto.gov is more efficient and effective than traditional governance methods, thereby enhancing the security, profitability, and ultimately, the sustainability of DeFi protocols.

Rocket: A System-Level Fuzz-Testing Framework for the XRPL Consensus Algorithm

Wishaal Kanhai, Ivar van Loon, Yuraj Mangalgi, Thijs Van der Valk, Lucas Witte, Annibale Panichella, Mitchell Olsthoorn, Burcu Kulahcioglu Ozkan

18th IEEE International Conference on Software Testing, Verification and Validation (ICST), 2025
https://www.computer.org/csdl/proceedings-article/icst/2025/10988979/26S4EBOHJ0A

Abstract

Byzantine fault tolerant algorithms are critical for achieving consistency and reliability in distributed systems, especially in the presence of faults or adversarial behavior. The consensus algorithm used by the XRP Ledger falls into this category. In practice, the implementation of these algorithms is prone to errors, which can lead to undesired behavior in the system. This paper introduces Rocket, a fuzz-testing framework designed for the XRPL consensus algorithm. Rocket enables researchers and developers to automatically inject network and process faults into a locally simulated network of XRPL validator nodes to test if the system behaves as expected. This technique has previously been shown to be effective in finding implementation errors. Rocket has been designed to focus on extensibility and ease of use, enabling users to run complex test scenarios with minimal setup.

Copyright © 2025 Ripple. All rights reserved.

Kite: How to Delegate Voting Power Privately

Kamilla Nazirkhanova, Vrushank Gunjur, X. Pilli Cruz-De Jesus, Dan Boneh

arXiv, 2025

https://arxiv.org/abs/2501.05626

Abstract

Ensuring the privacy of votes in an election is crucial for the integrity of a democratic process. Often, voting power is delegated to representatives (e.g., in congress) who subsequently vote on behalf of voters on specific issues. This delegation model is also widely used in Decentralized Autonomous Organizations (DAOs). Although several existing voting systems used in DAOs support private voting, they only offer public delegation. In this paper, we introduce Kite, a new protocol that enables private delegation of voting power for DAO members. Voters can freely delegate, revoke, and re-delegate their power without revealing any information about who they delegated to. Even the delegate does not learn who delegated to them. The only information that is recorded publicly is that the voter delegated or re-delegated their vote to someone. Kite accommodates both public and private voting for the delegates themselves.

We analyze the security of our protocol within the Universal Composability (UC) framework. We implement Kite as an extension to the existing Governor Bravo smart contract on the Ethereum blockchain, that is widely used for DAO governance. Furthermore, we provide an evaluation of our implementation that demonstrates the practicality of the protocol. The most expensive operation is delegation due to the required zero-knowledge proofs. On a consumer-grade laptop, delegation takes between 7 and 167 seconds depending on the requested level of privacy.

A 9-dimensional Analysis of GossipSub over the XRP Ledger Consensus Protocol

IEEE Network Operations and Management Symposium (NOMS), 2024

From The Quarterly Journal of Economics, 2024

https://ieeexplore.ieee.org/document/10575688

Abstract

This work shows a 9-dimensional analysis of the behavior and performance of Gossipsub according to the parameterization of the mesh. GossipSub is the state-of-the-art framework for safe and fast message dissemination on blockchains. This study focuses on its application in the quorum-based consensus of the XRP Ledger. Using data science techniques, we cluster sets of parameters, identify correlations between dimensions, and develop a decision tree for informed parameter selection. Contributions include demonstrating the adaptability of GossipSub for alternative consensus models, analyzing how parameters impact network performance and behavior, and providing a method for parameterization to meet specific network requirements.

Copyright © 2025 Ripple. All rights reserved.

The Evolution of AI Governance

Simon Chesterman, Yuting Gao, Jungpil Hahn, Valerie Sticher

Computer, 2024
https://www.computer.org/csdl/magazine/co/2024/09/10660604/1ZPP4D3zAvS

Abstract

Many companies and a growing number of governments have guides, frameworks, or principles on their use of artificial intelligence (AI). Analyzing the evolving practice of releasing such documents and the language they use offers important insights into how norms around AI are spreading and changing — and where they might go next.

Copyright © 2025 Ripple. All rights reserved.

05 —— SECTION

Blockchain Interoperability and Regulatory Fragmentation

Interoperability and regulatory fragmentation remain central barriers to the global adoption of blockchain technology. Research in this section investigates the market impact of inconsistent regulatory enforcement, offers benchmarking tools to evaluate blockchain performance across networks, and analyzes emerging legal challenges such as the rise of AI-powered arbitration. Together, these studies underscore the importance of harmonized standards and cross-chain frameworks to enable seamless, compliant, and scalable blockchain systems.

Copyright © 2025 Ripple. All rights reserved.

Reinforcing RCTs with Multiple Priors while Learning about External Validity

Frederico Finan, Demian Pouzo

arXiv, 2024

https://arxiv.org/abs/2112.09170

Abstract

This paper introduces a framework for incorporating prior information into the design of sequential experiments. These sources may include past experiments, expert opinions, or the experimenter's intuition. We model the problem using a multi-prior Bayesian approach, mapping each source to a Bayesian model and aggregating them based on posterior probabilities. Policies are evaluated on three criteria: learning the parameters of payoff distributions, the probability of choosing the wrong treatment, and average rewards. Our framework demonstrates several desirable properties, including robustness to sources lacking external validity, while maintaining strong finite sample performance.

Blockchain Interoperability: Implications for EU Competition Law and Data Protection Law

Klaudia Majcher, Marco Botta

EUI Working Paper, 2025

https://cadmus.eui.eu/server/api/core/bitstreams/acda0f04-2b5d-5912-bed9-86495d79cd5f/content

Abstract

Since the launch of Bitcoin in 2009, blockchain technology has undergone significant development and demonstrated its potential to revolutionize several industries. Distributed Ledger Technologies (DLTs) enable the transparent recording and secure sharing of data across a network of participants in a decentralized manner. However, the adoption of DLTs has been hindered by the existence of numerous protocols and diverging standards, leading to the creation of isolated 'walled gardens' where each blockchain operates independently. Achieving interoperability between different blockchains is thus essential for the broader application of blockchain technology beyond cryptocurrencies.

So far, blockchain interoperability has been analysed primarily from a technical perspective, with a noticeable gap in scholarly contributions addressing its legal implications. This article is the first attempt to examine how EU competition law and data protection law will be affected by, and can support, the evolution towards interoperable blockchains. To this objective, it first provides the background by briefly explaining blockchain interoperability and its underlying mechanisms, as well as demonstrates the benefits of fostered interoperability and the challenges preventing it from fully materializing. As regards a competition law assessment, our analysis identified three potential areas that might be affected by blockchain interoperability: collusion and information exchanges, anti-competitive foreclosure, and standardization. A data protection analysis focuses on evaluating the potential impacts of blockchain interoperability on the principles of accountability, data minimization, and purpose limitation, as well as on the rights of individuals, particularly the 'right to be forgotten'.

Copyright © 2025 Ripple. All rights reserved.

The article concludes that blockchain interoperability does not introduce entirely new legal challenges beyond those already identified in the existing literature on blockchain's compatibility with competition law and data protection law. However, it has the potential to exacerbate these challenges. By enhancing the degree of data sharing among different parties, blockchain interoperability may foster collusion and complicate compliance with the GDPR. At the same time, blockchain interoperability could lower market entry barriers and reduce market concentration, thereby decreasing the risk of foreclosure practices. Our analysis also revealed that, in the near future, particular attention should be paid to the standardization efforts surrounding blockchain interoperability, which are likely to become a crucial nexus between blockchain technology and competition law.

Robots Replacing Human Arbitrators: The Legal Dilemma

Robert Walters

Information & Communications Technology Law, 2025
https://www.tandfonline.com/doi/full/10.1080/13600834.2024.2408155#abstract

Abstract

Robots are slowly replacing humans in many areas of the economy. This paper compares the current-day arbitration laws of Australia, Cayman Islands, European Union, India, Indonesia, Japan, Singapore, Qatar, Philippines, the United Kingdom, and the United States, which are considered arbitration friendly. The paper confirms that the respective arbitration laws do not clearly and unequivocally provide for a robot to be used as an arbitrator. It is well understood that robots today do not have the emotional or social intelligence, such as bias, that a human naturally brings to the arbitration table. There are four streams of studies on this issue: AI-powered arbitrator, AI arbitration, AI-assisted arbitration, and a robot as arbitrator. However, none of these is clearly defined by arbitration law. This paper argues that the current day laws do not provide for robots to replace the human arbitrator, and must retain the status quo. Any law reform to allow a robot to replace the human arbitrator, would be a jump too far, and would significantly diminish the long-standing reputation that arbitration has as an effective legal mechanism for resolving international commercial and investor-state disputes.

Copyright © 2025 Ripple. All rights reserved.

Distributed Ledgers and Secure Multi-Party Computation for Auditing and Financial Reporting

Sean Shun Cao, Lin William Cong, Baozhong Yang

Management Science, 2024
https://pubsonline.informs.org/doi/10.1287/mnsc.2023.02577

Abstract

To understand the disruption and implications of distributed ledger technologies for financial reporting and auditing, we analyze firm misreporting, auditor monitoring and competition, and regulatory policy in a unified model. A federated blockchain for financial reporting and auditing can improve verification efficiency not only for transactions in private databases but also for cross-chain verifications through privacy-preserving computation protocols. Despite the potential benefit of blockchains, private incentives for firms and first-mover advantages for auditors can create inefficient under-adoption or partial adoption that favors larger auditors. Although a regulator can help coordinate the adoption of technology, endogenous choice of transaction partners by firms can still lead to adoption failure. Our model also provides an initial framework for further studies of the costs and implications of the use of distributed ledgers and secure multiparty computation in financial reporting, including the positive spillover to discretionary auditing and who should bear the cost of adoption.

Copyright © 2025 Ripple. All rights reserved.

06 —— SECTION

Institutional Design and Social Impact of Blockchain

The impact of blockchain has extended beyond digital assets to broader institutional and societal applications.

This section explores this reach, including how blockchain can improve data security through decentralized identity systems, influence market dynamics under liquidity constraints, and shape consumer trust in financial services. Additionally, it examines the systemic risks in interconnected digital markets. These insights highlight blockchain's potential to foster safer, fairer, and more efficient digital economies.

Copyright © 2025 Ripple. All rights reserved.

The Dynamic Effects of Blockchain-based Identity Management Adoption on Data Breaches

Sarah Mulombo Mulaji, Irwin Brown, Sumarie Roodt

Proceedings of the 57th Hawaii International Conference on System Sciences, 2024

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1847&context=hicss-57

Abstract

The purpose of this research was to explore the dynamics associated with the adoption of blockchain-based identity management to illustrate its effects on data breach rates. A comprehensive literature review was conducted, and data was analysed using the system dynamics technique of causal loop diagram. The analysis identified key circular causal relationships which show how data breach rates could be reduced by adopting a blockchain-based identity management system like self-sovereign identity.

Large Orders in Small Markets: Execution with Endogenous Liquidity Supply

Agostino Capponi, Albert J. Menkveld, Hongzhong Zhang

Review of Finance, 2025

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326313

Abstract

We model the execution of a large uninformed sell order in the presence of strategic competitive market makers. We solve for the unique symmetric equilibrium of the model in closed form. Analysis of this equilibrium reveals that large orders unequivocally benefit market makers, while smaller investors stand to benefit only if the order trades with a sufficiently high intensity. The equilibrium results further provide a rationale for the empirically observed patterns of (i) shorter orders trading at higher intensities, and (ii) price pressures potentially subsiding before large orders stop executing.

FinTech Services from BigTech Companies

Thomas Puschmann, Engjull Halimi

Systems Research and Behavioral Science, 2024

https://onlinelibrary.wiley.com/doi/full/10.1002/sres.3029#:~:text=The%20examples%20of%20innovative%20banking,which%20was%20not%20pursued%20further.

Abstract

The so-called BigTech companies Amazon, Alphabet, Apple and Meta and are constantly attempting to grow into new business areas. Due to their expertise in data analysis, they have managed to quickly establish themselves in many industries as digital ecosystems and, as part of this strategy, are also expanding their footprint in financial services. However, the biggest challenge that BigTech companies are facing in financial services is customer acceptance. This paper contributes to the emerging field of digital ecosystems and the acceptance of sensitive services by users. Although the BigTech firms have gained much attention, only little empirical analysis is available. This paper aims to shed light on the determinants of customer acceptance of BigTech banking services. Based on a survey in Switzerland this research

Copyright © 2025 Ripple. All rights reserved.

develops an analytic model to identify and test the relevant determinants. The results indicate that the strongest significant influences were found in subjective risk and trust which clearly demonstrates the still-existing incumbents' advantage over the BigTech companies.

Federated Learning in Smart Healthcare: A Survey of Applications, Challenges, and Future Directions

Mohammad Nasajpour, Seyedamin Pouriyeh, Reza M. Parizi, Meng Han, Fatemeh Mosaiyebzadeh, Liyuan Liu, Yixin Xie, Daniel Macêdo Batista

Electronics, 2025

https://doi.org/10.3390/electronics14091750

Abstract

In recent years, novel technologies in smart healthcare systems have opened significant opportunities for diagnosis and treatment across various medical fields. Federated Learning (FL), a decentralized machine learning approach, trains shared models using local data from devices like wearables and hospital systems without transferring sensitive information, offering a promising solution to privacy challenges in areas such as cancer prediction, COVID-19 detection, drug discovery, and medical image processing. This literature survey reviews FL architectures (e.g., FedHealth, PerFit), applications, and recent advancements, demonstrating their impact on healthcare through enhanced predictive models for patient care. Key findings include improved accuracy in wearable-based diagnostics and secure multi-institutional collaboration, though limitations persist. We also highlight open challenges, such as security risks, communication costs, and data heterogeneity, which require further research attention.

Copyright © 2025 Ripple. All rights reserved.

07 —— SECTION

Conclusion

Remarkable progress has been made in blockchain research across academia, and sharing these new discoveries remains more important than ever.

This year, UBRI's focus has been on tokenization, DeFi infrastructure, cryptographic security, AI-driven governance, interoperability, and the broader institutional and social impacts of blockchain. Leading universities around the world have contributed valuable research driving these fields forward.

With these critical advancements in blockchain technology, UBRI remains committed to fostering academic excellence and promoting open knowledge in the blockchain space. Looking ahead, we are excited to see our research partners apply their findings to real-world systems like the XRP Ledger, accelerating blockchain's global development with energy and ambition.

Copyright © 2025 Ripple. All rights reserved.

UBRI University Partners

Copyright © 2025 Ripple. All rights reserved.

About UBRI

To further promote the evolution, development, and transformation of blockchain, Ripple founded the University Blockchain Research Initiative (UBRI), a global network of top universities pursuing public education, academic research, technical development, and innovation in blockchain, cryptocurrency, and related financial technologies (FinTech). Since UBRI's inception in 2018, Ripple has funded over 60 university partnerships, supporting a significant number of research projects and contributing to the modification or creation of hundreds of university courses.

To learn more about the University Blockchain Research Initiative, visit ripple.com/ubri.

Copyright © 2025 Ripple. All rights reserved.