ripple

BLOCKCHAIN TECHNOLOGY
RESEARCH HIGHLIGHTS FROM
UNIVERSITY PARTNERS

# UBRI

# Advancing Blockchain Research with Real-World Impact

2026

The University Blockchain Research Initiative (UBRI), launched by Ripple in 2018, continues to expand its global footprint, fostering a network of over 60 premier academic partners to drive pioneering research and foundational education in digital assets. By supplying funding, strategic resources, and open-source collaboration, UBRI empowers global faculty and students to transform academic programs, explore daily-life applications of blockchain technologies, and cultivate the next generation of leaders in decentralized finance.

This 2025–2026 report showcases the remarkable academic output of UBRI-supported researchers, highlighting breakthrough publications. Motivated by the rapid acceleration of the technological landscape, this year's UBRI-supported research reflects three major areas of momentum:  a) The rise of autonomous and AI-enabled financial infrastructure; b) The continued maturation of tokenized assets and digital markets; c) Foundational advances in security, privacy, and post-quantum cryptography.

We invite you to explore the insights captured within this report and witness how academic brilliance is translating complex theory into utility for users. These collaborative contributions are not only expanding the boundaries of computer science, economics, and governance but are also building the infrastructure required for the broader blockchain ecosystem to thrive globally.

*The materials in this report are based on work that may be supported or partially supported by Ripple under the University Blockchain Research Initiative 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 is a decentralized public blockchain based on open-source technology to which a global group of businesses and developers contribute (including Ripple).

Contents

## Introduction

Blockchain's transformative potential continues to mature on a global scale, shifting from early-stage experimentation to a realistic transformation of financial infrastructure and decentralized governance. As this landscape grows more complex, rigorous academic research remains indispensable. By providing deep analytical frameworks, economic insights, and empirical findings, academia bridges the gap between theoretical potential and secure, real-world institutional adoption of digital assets.

Central to this progress is Ripple's University Blockchain Research Initiative (UBRI). Driven by a philanthropic commitment to global academic collaboration, UBRI provides top-tier universities and researchers with the resources required to investigate frontier domains, pushing the limits of modern computer science, economics, finance, social science, and governance.

This year's report captures the 2025–2026 academic cycle, showcasing the vital contributions of UBRI partners across eight core dimensions of Blockchain: Security and Privacy, Post-Quantum Cryptography, Consensus Protocols, Autonomous Agents, Mechanism Design, Tokenization of Real World Assets, Financial Markets, and Governance and Social Impact.

Additionally, the research analyzes regulatory fragmentation and the socio-environmental impacts of decentralized finance (DeFi) technology. These contributions demonstrate that DeFi has matured into practical applications, such as basic income programs and pension plans, proving the power of open academic inquiry to advance the ecosystem. Moving forward, Ripple and its UBRI partners remain committed to anchoring global innovation in scientific excellence to build an efficient, transparent, and inclusive future.

01 —— SECTION

## Security and Privacy

# As decentralized and interconnected systems expand globally, safeguarding network integrity, transaction records, and user data becomes paramount.

This section examines cutting-edge methodologies and automated tools designed to mitigate risk and enhance privacy across digital infrastructures.

Featured research highlights advancements across all critical dimensions of network resilience. Software supply chain security is addressed by Cargo Scan, an interactive program analysis tool that streamlines third-party Rust dependency reviews by isolating potentially dangerous side-effects. Structural fault tolerance is enhanced by a multiplex flow network model designed to prevent cascading failures across interdependent network layers. Beyond these technical areas, users' privacy perceptions towards personal health records stored on blockchain is analyzed using advanced statistical methods.

The interdisciplinary advancements from our research partners reinforce the foundational trust, privacy, and systemic robustness necessary for institutional-grade digital infrastructures.

## Auditing Rust Crates Effectively

**Lydia Zoghbi, David Thien, Ranjit Jhala, Deian Stefan, and Caleb Stanford**

European Symposium on Programming, 2026
https://dl.acm.org/doi/10.1007/978-3-032-22723-2_15

Abstract

We introduce Cargo Scan, the first interactive program analysis tool designed to help developers audit third-party Rust code. Real systems written in Rust rely on thousands of transitive dependencies. These dependencies are as dangerous in Rust as they are in other languages (e.g., C or JavaScript)— and auditing these dependencies today means manually inspecting every line of code. Unlike for most industrial languages, though, we can take advantage of Rust's type and module system to minimize the amount of code that developers need to inspect to the code that is potentially dangerous. Cargo Scan models such potentially dangerous code as effects and performs a side-effects analysis, tailored to Rust, to identify effects and track them across crate and module boundaries. In most cases (69.2%) developers can inspect flagged effects and decide whether the code is potentially dangerous locally. In some cases, however, the safety of an effect depends on the calling context— how a function is called, potentially by a crate the developer imports later. Hence, Cargo Scan tracks context-dependent information using a call-graph, and collects audit results into composable and reusable audit files. In this paper, we describe our experience auditing Rust crates with Cargo Scan. In particular, we audit the popular client and server HTTP crate, hyper, and all of its dependencies; our experience shows that Cargo Scan can reduce the auditing burden of potentially dangerous code to a median of 0.2% of lines of code when compared to auditing whole crates. Looking at the Rust ecosystem more broadly, we find that Cargo Scan can automatically classify ~3.5K of the top 10K crates on crates.io as safe; of the crates that do require manual inspection, we find that most of the potentially dangerous side-effects are concentrated in roughly 3% of these crates.

## Analysis and Optimization of Robustness in Multiplex Flow Networks Against Cascading Failures

**Orkun İrsoy and Osman Yağan**

IEEE Transactions on Network Science and Engineering, 2025
https://ieeexplore.ieee.org/document/11129154

Abstract

Networked systems are susceptible to cascading failures, where the failure of an initial set of nodes propagates through the network, often leading to system-wide failures. In this work, we propose a multiplex flow network model to study robustness against cascading failures triggered by random failures. The model is inspired by systems where nodes carry or support multiple types of flows, and failures result in the redistribution of flows within the same layer rather than between layers. To represent different types of interdependencies between the layers of the multiplex network, we define two cases of failure conditions: layer independent overload and layer influenced overload. We provide recursive equations and their solutions to calculate the steady-state fraction of surviving nodes, validate them through a set of simulation experiments, and discuss optimal load-capacity allocation strategies. Our results demonstrate

that allocating the total excess capacity to each layer proportional to the mean effective load in the layer and distributing that excess capacity equally among the nodes within the layer ensures maximum robustness. The proposed framework for different failure conditions allows us to analyze the two overload conditions presented and can be extended to explore more complex interdependent relationships.

## Optimistic or Uncomfortable? Examining Privacy Perceptions of Immigrants Towards Blockchain-based Personal Health Record Adoption Intentions

**Dane Vanderkooi and Atefeh Mashatan**

59th Hawaii International Conference on System Sciences, 2026
https://hdl.handle.net/10125/111848

Abstract

Personal medical health records (PHRs) have improved patient access and control over personal health information. However, adoption rates remain low due to barriers, including accessibility and privacy concerns. These challenges are further amplified among immigrants through digital divides. Solutions such as blockchain-based PHRs have been touted to alleviate challenges while providing agency to patients. Yet, implementing blockchain elicits novel privacy challenges. As such, this study explores immigrant adoption intentions towards blockchain-based PHR systems from a privacy perspective. An extended privacy calculus model is developed to include technology perceptions, optimism, discomfort, cultural dimensions, uncertainty avoidance and collectivism. The model was tested using cross-sectional survey data, which were analyzed using partial least squares structural equation modelling (PLS-SEM). The results support the majority of the model hypotheses. Technological optimism and uncertainty avoidance enhance perceived adoption benefits while discomfort raises privacy risks. Risks and benefits are then weighed against each other to determine adoption intentions.

02 —— SECTION

## Cryptography in the Post-Quantum Era

# Quantum computing threatens to break today's digital security.

To protect tomorrow’s networks, researchers deploy post-quantum cryptography, ensuring systems stay mathematically secure without sacrificing transaction speed.

Recent breakthroughs from our research partners bridge the gap between theory and practice by tackling three core challenges: a): Uncovering hidden security vulnerabilities in standard signature schemes so they can be fixed before global adoption. b): Eliminating heavy computational lag in post-quantum zero-knowledge proofs by using optimized algorithms. c): Create the ultimate blueprint for resilient, confidential ledger systems.

These research projects ensure emerging digital ecosystems remain secure against future quantum threats without sacrificing performance.

## A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures

**Michele Battagliola, Riccardo Longo, Federico Pintore, Edoardo Signorini, and Giovanni Tognolini**

Mediterranean Journal of Mathematics, 2025
https://link.springer.com/article/10.1007/s00009-025-02882-7

Abstract

Signature schemes from multi-round interactive proofs are becoming increasingly relevant in post-quantum cryptography. A prominent example is CROSS, recently admitted to the second round of the NIST on-ramp standardisation process for post-quantum digital signatures. While the security of these constructions relies on the Fiat–Shamir transform, in the case of CROSS the use of the fixed-weight parallel-repetition optimisation makes the security analysis fuzzier than usual. A recent work has shown that the fixed-weight parallel repetition of a multi-round interactive proof is still knowledge sound, but no matching result appears to be known for the non-interactive version. In this paper, we provide two main results. First, we explicitly prove the EUF-CMA security of CROSS, filling a gap in the literature. We do this by showing that, in general, the Fiat–Shamir transform of an HVZK and knowledge-sound multi-round interactive proof is EUF-CMA secure. Second, we present a novel forgery attack on signatures obtained from fixed-weight repetitions of 5-round interactive proofs, substantially improving upon a previous attack on parallel repetitions due to Kales and Zaverucha. Our new attack has particular relevance for CROSS, as it shows that several parameter sets achieve a significantly lower security level than claimed, with reductions up to 24% in the worst case.

## Accelerating Post-quantum Secure zkSNARKs by Optimizing Additive FFT

**Mohammadtaghi Badakhshan, Susanta Samanta, and Guang Gong**

Selected Areas in Cryptography, 2025
https://dl.acm.org/doi/10.1007/978-3-032-10536-3_13

Abstract

Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zkSNARKs) are increasingly utilized across diverse applications. While significant advances have been made in the development of post-quantum secure zkSNARKs, these schemes face challenges, including substantial computational complexity. In this paper, we propose leveraging the Cantor special basis in post-quantum secure zkSNARKs operating over binary extension fields. This approach enables the optimization of the additive Fast Fourier Transform (FFT) algorithm in Aurora, a post-quantum secure zkSNARK, by replacing the previously used Gao–Mateer FFT with the Cantor and LCH FFTs. Our implementation demonstrates a significant reduction in computation time for Aurora, with the potential to accelerate other zkSNARKs utilizing additive FFTs. Additionally, we present a detailed theoretical analysis of the computational costs of the Cantor FFT algorithm, providing exact counts of additions, multiplications, and precomputation overhead. Furthermore, we analyze the FFT call complexity within the encoding of the Rank-1 Constraint System in the Aurora zkSNARK.

# The Zcash Protocol Explained: A Journey into Privacy-Preserving Cryptography

**Atharva Lele and Hitesh Tewari**

IEEE International Conference on Distributed Ledger Technologies, 2025
https://ieeexplore.ieee.org/abstract/document/11466938

Abstract

Privacy in blockchain-based cryptocurrencies has become a critical area of research and development. This is driven by the transparent nature of public ledgers and the growing demand for confidential transactions. This study provides a comprehensive exposition of a prominent privacy-enhancing protocol, Zcash. We begin by elucidating the design and operation of Tornado Cash, a smart contract-based mixer on Ethereum that leverages zero-knowledge proofs to enable unlinkable transactions. Building on this foundation, we explore the Zcash protocol, tracking its evolution from Bitcoin and its innovative use of zk-SNARKs. We also examine the intricate mechanisms that highlight its privacy guarantees, including circuit design, Merkle tree structures and transaction relations. By systematically analyzing and comparing these protocols, this study aims to clarify their inner workings, highlight their strengths and limitations, and provide information on the future of privacy in decentralized finance.

03 —— SECTION

## Building Consensus and Trust

# Modern blockchain architecture relies on achieving distributed trust and identity verification without central authorities.

To protect evolving networks, current research focuses on developing frameworks that maintain robust consensus while decentralizing digital identity, specifically targeting operational bottlenecks and structural vulnerabilities.

One framework addresses this by introducing a blockchain-native Public Key Infrastructure (PKI) built on the XRP Ledger (XRPL). By leveraging native XRPL fields and NFT capabilities, this system manages and revokes X.509 certificates, removing the need for traditional, centralized Certificate Authorities. To improve network flexibility at the protocol level, another paper introduces an asynchronous, randomized DAG-based consensus protocol. This approach accommodates asymmetric trust models, allowing individual participants to define their own quorum parameters while maintaining "common-core" validation across the system. A timely evaluation of the blockchain trilemma maps out the ongoing tension between governance token concentration, centralized infrastructure layers, and the practical challenges of achieving true decentralization.

These works advance the technical foundation required to keep decentralized networks trusted, resilient, and scalable.

## A Blockchain-Native PKI: Secure X.509 Certificate Management on the XRP Ledger

**Harsha Vardhan, Prab Hiranayachatri, Atharva Lele, and Hitesh Tewari**

2025 IEEE International Conference on Distributed Ledger Technologies
https://ieeexplore.ieee.org/abstract/document/11466670

Abstract

Public Key Infrastructure (PKI) is foundational to secure digital communication, yet its traditional reliance on centralized Certificate Authorities (CAs) introduces significant risks, costs, and operational bottlenecks. This paper presents a novel, fully decentralized approach to PKI by leveraging the XRP Ledger (XRPL) blockchain for the issuance, storage, retrieval, and revocation of X. 509 certificates. The core methodology stores certificates directly within XRPL transactions using the native Memos field, offering a lightweight, immutable, and cost-effective solution without requiring modifications to the underlying protocol. To enhance certificate lifecycle management and enable native on-chain revocation, we also introduce a complementary approach that uses Non-Fungible Tokens (NFTs) to store certificate data and metadata. NFT-based storage supports features such as instant revocation through burning or flagging, and enables additional transparency and auditability. Certificate retrieval involves querying transaction history or owned NFTs, decoding and reassembling the data if chunked, and validating the reconstructed X. 509 certificate using standard tools. We implement a Python-based web application that exposes RESTful APIs for certificate lifecycle management, secure messaging, and encrypted email, demonstrating seamless integration with existing PKI-aware applications. Our evaluation shows that this architecture drastically reduces operational costs compared to traditional CAs while enhancing transparency, auditability, and resilience. This work demonstrates the feasibility and advantages of blockchain-native PKI, paving the way for scalable, trust minimized, and user-centric digital identity management.

## DAG-based Consensus with Asymmetric Trust

**Ignacio Amores-Sesar, Christian Cachin, Juan Villacis, and Luca Zanolini**

Proceedings of the ACM Symposium on Principles of Distributed Computing, 2025
https://dl.acm.org/doi/10.1145/3732772.3733527

Abstract

In protocols with asymmetric trust, each participant is free to make its own individual trust assumptions about others, captured by an asymmetric quorum system. This contrasts with ordinary, symmetric quorum systems and with threshold models, where all participants share the same trust assumption. It is already known how to realize reliable broadcasts, shared-memory emulations, and binary consensus with asymmetric quorums. In this work, we introduce Directed Acyclic Graph (DAG)-based consensus protocols with asymmetric trust. To achieve this, we extend the key building-blocks of the well-known DAG-Rider protocol to the asymmetric model. Counter to expectation, we find that replacing threshold quorums with their asymmetric counterparts in the existing constant-round gather protocol does not result in a sound asymmetric gather primitive. This implies that asymmetric DAG-based consensus protocols, specifically those based on the existence of common-core primitives, need new ideas in an asymmetric-trust model. Consequently, we introduce the first asymmetric protocol

for computing a common core, equivalent to that in the threshold model. This leads to the first randomized asynchronous DAG-based consensus protocol with asymmetric quorums. It decides within an expected constant number of rounds after an input has been submitted, where the constant depends on the quorum system.

## Promises and Perils of Decentralization in the Blockchain Age

**Mariia Petryk, Christoph Mueller-Bloch, Jungpil Hahn, Hanna Halaburda, Ola Henfridsson, Daniel Obermeier, and Youngjin Yoo**

International Conference on Information Systems, 2025
https://icis2025.aisconferences.org/events/panels/

Abstract

Blockchain technology promises to disrupt information-based markets through decentralized governance, challenging the dominance of centralized digital platforms. Information Systems (IS) scholars have examined blockchain's key affordances – distributed value capture, transparency, smart contracts, and token-driven growth – across diverse domains such as supply chains, social media, and digital identity. Yet, empirical evidence reveals persistent centralization in practice, raising concerns about the viability and desirability of blockchain-enabled decentralization. Challenges include governance token concentration, centralized system layers, and trade-offs in the "blockchain trilemma" of scalability, security, and decentralization. Building on the evidence, this panel aims to foster critical discussion around the feasibility, relevance, and research implications of blockchain decentralization.

04 —— SECTION

## Autonomous Decentralized Systems

# Modern machine learning, Large Language Models (LLMs), and Agentic AI are catalyzing the next phase of the decentralized finance ecosystem by providing intelligence, automation, and advanced analytics directly into the blockchain.

This section explores how autonomous agents and advanced algorithms are moving beyond passive data processing to actively secure and optimize decentralized systems.

Featured research highlights a multi-tiered convergence between intelligent systems and distributed ledgers. Comprehensive surveys map out the foundational interplay, core research opportunities, and common misconceptions surrounding the integration of cryptography and artificial intelligence. This synergy manifests in decentralized governance, where autonomous decision-makers evaluate, interpret, and align complex DAO voting proposals with human intentions. System security is reinforced through specialized machine learning frameworks. The research teams also show how market integrity may be safeguarded via Graph Neural Networks, alongside cross-network transfer learning methodologies that bypass data bottlenecks to predict financial fraud.

These breakthroughs from our partners pave the way for a more autonomous, secure, and resilient intelligent decentralized ecosystem.

## Profit or Deceit? Mitigating Pump and Dump in DeFi via Graph and Contrastive Learning

**Cong Wu, Jing Chen, Jiahong Li, Jiahua Xu, Ju Jia, Yutao Hu, Yebo Feng, Yang Liu, and Yang Xiang**

IEEE Transactions on Information Forensics and Security, 2025
https://ieeexplore.ieee.org/document/11106506

Abstract

Pump-and-Dump (PD) schemes pose a significant threat to the stability and fairness of Decentralized Finance (DeFi) markets, often resulting in substantial financial losses for investors. The early and accurate detection of these schemes is crucial for preserving trust in the rapidly expanding cryptocurrency ecosystem. However, existing detection methods primarily rely on post-event analysis and heuristic-based approaches, which are often inadequate for real-time and precise identification of PD activities. In this paper, we present PUMPWATCHER, an innovative framework that employs Graph Neural Networks (GNNs) and contrastive learning to detect PD schemes by modeling transaction behaviors within temporal graphs. PUMPWATCHER integrates advanced transaction graph construction, temporal GNNs, and contrastive learning techniques to enhance node and edge representations, thereby improving the detection of intricate and covert PD operations. We validate PUMPWATCHER on a dataset from Uniswap, encompassing 924,508 transactions across 858 tokens within December 2022. The results show that PUMPWATCHER outperforms state-of-the-art models, achieving a superior balanced accuracy of 92.3%, while significantly minimizing false positives and negatives. These outcomes highlight its potential to set a new standard in real-time detection of market manipulation, paving the way for more secure and resilient DeFi ecosystems.

## Crypto x AI, AI x Crypto: A Survey

**Sarah Allen, Pranay Anchuri, James Austgen, Maryam Bahrani, Samuel Breckenridge, Aaron Buchwald, Christian Cachin, Andrés Fábrega, Jared Fernandez, James Hsin-yu Chiang, Marwa Mouallem, Roi Bar-Zur, Neil DeSilva, Ittay Eyal, Giulia Fanti, Ari Juels, Andrew Miller, Christian Sillaber, Dani Vilardell, Pramod Viswanath, Wenhao Wang, Matt Weinberg, Sen Yang, Jianzhu Yao, and Fan Zhang**

The Initiative for CryptoCurrencies & Contracts, 2026
https://arxiv.org/abs/2606.13892

Abstract

The intersection of crypto x AI is spawning papers, products, online posts, and companies. All the surrounding buzz, though, obscures what exactly has been done, what the opportunities and challenges are, and what open questions deserve attention. This survey paper asks what AI can do for blockchain-based technologies (broadly construed as “crypto”) (crypto x AI), and vice versa (AI x crypto). We systematize existing work, summarize key takeaways, highlight open research questions, and offer a perspective on pervasive industry misconceptions, concluding that AI and crypto are still in the very early stages of meaningful integration.

## DAO-AI: Evaluating Collective Decision-Making through Agentic AI in Decentralized Governance

**Agostino Capponi, Alfio Gliozzo, Chunghyun Han, and Junkyu Lee**

Preprint from arXiv and Columbia University, 2025
https://arxiv.org/abs/2510.21117

Abstract

This paper presents a first empirical study of agentic AI as autonomous decision-makers in decentralized governance. Using more than 3K proposals from major protocols, we build an agentic AI voter that interprets proposal contexts, retrieves historical deliberation data, and independently determines its voting position. The agent operates within a realistic financial simulation environment grounded in verifiable blockchain data, implemented through a modular composable program (MCP) workflow that defines data flow and tool usage via Agentics framework. We evaluate how closely the agent's decisions align with the human and token-weighted outcomes, uncovering strong alignments measured by carefully designed evaluation metrics. Our findings demonstrate that agentic AI can augment collective decision-making by producing interpretable, auditable, and empirically grounded signals in realistic DAO governance settings. The study contributes to the design of explainable and economically rigorous AI agents for decentralized financial systems.

## Cross-Network Transfer Learning for Cryptocurrency Fraud Detection

**Denizhan Dalgıç and Şerif Bahtiyar**

ICT Systems Security and Privacy Protection, 2026
https://link.springer.com/chapter/10.1007/978-3-032-27993-4_18

Abstract

The lack of labeled data in the new generation of blockchain networks, such as XRP Ledger (XRPL), which also suffers from the lack of labeled data, is a notable deficiency. This work addresses the well-known "labeled data bottleneck problem" using Cross-Network Transfer Learning, postulating the universality of the fraud network structure. This research investigates the efficiency of three different adaptation mechanisms, Renaming, Scaled Transformation, and Synthetic Generation, to successfully transfer data from Bitcoin network to XRPL network. Experimental results indicate the attainment of 0.927 and 0.878 F1-score performances for transactions and wallet classification models, respectively when they are trained from transformed data. The solution also achieves the best performance using real XRPL distribution parameters with the Distribution-Based Synthetic Generation approach, which confirms the feasibility of the proposed approach.

# BreachT5: Ensembling CodeT5+ Models for Multi-Label Vulnerability Detection in Smart Contracts

**Gregorio Dalia, Tat Luat Nguyen, Andrea Di Sorbo, Corrado Visaggio, and Annibale Panichella**

Proceedings of the 8th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB '26), 2026

https://dl.acm.org/doi/10.1145/3786157.3788570

Abstract

Ethereum smart contracts manage billions in digital assets, and vulnerability detection is critical given the immutability of deployed code and the irreversible nature of transactions. However, existing tools such as Slither rely on rigid, rule-based analysis, and general-purpose language models like ChatGPT often miss rare or context-dependent bugs. To address these limitations, this paper presents BreachT5, an ensemble of two fine-tuned CodeT5+ models designed for multi-label vulnerability detection in Solidity contracts. We first fine-tune a 220M parameter model on over 67,000 real contracts labeled with the Smart Contract Weakness Classification (SWC), revealing intrinsic detection differences across vulnerability types. We then explore the performance of a 770M variant, which improves accuracy on frequent classes but underperforms on rare ones. To balance this trade-off, BreachT5 combines both models via soft voting with per-class thresholds. Our results on the BCCC-SCsVuls2024 dataset show that BreachT5 achieves 0.556 Macro-F1 and 0.612 Micro-F1, outperforming the two standalone models, Slither, and GPT-5 in multi-label vulnerability detection.

05 —— SECTION

## Mechanism Design: Overcoming Inefficiency and Improving Utilities

# Aligning economic incentives and optimizing resource utilization are critical to overcoming structural bottlenecks and arbitrage strategies in decentralized protocols.

To protect the ecosystem from censorship and Maximum Extractable Value (MEV) attacks, researchers are developing mechanisms aimed at curbing exploitative behavior, such as front-running, and maximizing execution efficiency.

Featured research addresses these vulnerabilities by optimizing the game-theoretic and physical dimensions of distributed infrastructure. Research dimensions include: A novel protocol utilizes Wesolowski's Verifiable Delay Function (VDF) to keep transaction contents confidential until a cryptographic puzzle is solved; Economic models demonstrate that block propagation latencies and mining power concentration cause significant systemic waste; Empirical analysis reveals that while private mempools prevent traditional sandwich attacks, they remain highly vulnerable to cross-layer attacks; Novel smart-contract bargaining frameworks effectively mitigate inefficiencies found in traditional financial networks; Research evaluates the economic benefits and risks of Decentralized Exchanges (DEXs) to propose designs that maximize investor outcomes.

By constraining exploitative strategies and eliminating structural waste, these advancements ensure that next-generation decentralized networks remain economically incentive-compatible and efficient, thereby making utility generation more egalitarian for all participants.

## Timelock Shield: A Robust Defense Against MEV and Censorship Attacks in Blockchain

**Saksham Agrawal and Vinay J. Ribeiro**

Crypto Valley Conference on Blockchain Technology, 2025

https://ieeexplore.ieee.org/document/11068800

Abstract

Blockchain's security relies on cryptographic principles to resist tampering and fraud. However, vulnerabilities such as Maximum Extractable Value (MEV) and Censorship attacks persist, where malicious actors exploit knowledge of pending transactions or bribe miners to manipulate execution. While some state-of-the-art methods aim to counter these attacks through trusted setups and fair ordering, they compromise decentralization. Alternative solutions based on commit-and-reveal are decentralized but vulnerable to DoS and deferred reveal attacks.
We introduce Timelock Shield, a decentralized protocol to counteract MEV and censorship attacks. Timelock Shield utilizes timelock encryption and delayed transaction execution related to a particular smart contract. Timelock encryption ensures that the transaction contents remain confidential until a cryptographic puzzle is resolved, and delayed execution allows the state of the smart contract related to that transaction to be updated later. Crucially, the protocol operates without requiring a trusted setup, directly addressing the vulnerabilities of existing methods and significantly enhancing both security and applicability. We present a detailed game-theoretic analysis of the complex incentive structure of the protocol for various participants, demonstrating the ineffectiveness of censorship attempts and the impracticality of MEV strategies. Furthermore, we detail the implementation of Timelock Shield's key features based on Wesolowski's Verifiable Delay Function (VDF), which enables the generation of encrypted transactions, decryption, proof generation, and transaction verification. Drawing from our experimental analysis, we offer insight into the selection of VDF parameters and deadlines used in the protocol to better align with real-world computational durations.

## How the interplay between power concentration, competition, and propagation affects the resource efficiency of distributed ledgers

**Paolo Barucca, Carlo Campajola, and Jiahua Xu**

PNAS Nexus, 2026

https://academic.oup.com/pnasnexus/article/5/5/pgag135/8691350

Abstract

Forks in the Bitcoin network arise as a natural consequence of competition within its Proof-of-Work consensus protocol, but lead to resource inefficiencies and compromise network security. The frequency of forks, therefore, serves as a critical indicator of a distributed ledger's operational efficiency. We model the fork rate in a network of heterogeneous miners as a function of the number of miners, their hash rate distribution, and block propagation times within the peer-to-peer infrastructure. Empirical evidence demonstrates that fork rates are well-approximated by the ratio of the median block propagation time to mining time. Our model provides a theoretical foundation for this relationship while also capturing the fork rate's additional dependency on miner heterogeneity. Our work establishes a robust mathematical setting for investigating

factors often unobservable from existing empirical data, such as power concentration, competition, and asymmetric propagation times in distributed networks. Using this as a null model, we can detect anomalies in the historical fork rate, e.g. around 2016, indicating either high concentration of mining power or strongly heterogeneous latency in the Bitcoin network. We also estimate the mining power wasted in mining blocks on top of a nonlatest block, which potentiates accidental forks. The wastage amounts to approximately 16,000 MW in the most recent year, equivalent to half of the power generated in the United Kingdom.

## Rolling in the Shadows: Analyzing the Extraction of MEV Across Layer-2 Rollups

**Christof Ferreira Torres, Albin Mamuti, Ben Weintraub, Cristina Nita-Rotaru, and Shweta Shinde**

ACM SIGSAC Conference on Computer and Communications Security, 2024
https://dl.acm.org/doi/10.1145/3658644.3690259

Abstract

The emergence of decentralized finance has transformed asset trading on the blockchain, making traditional financial instruments more accessible while also introducing a series of exploitative economic practices known as Maximal Extractable Value (MEV). Concurrently, decentralized finance has embraced rollup-based Layer-2 solutions to facilitate asset trading at reduced transaction costs compared to Layer-1 solutions such as Ethereum. However, rollups lack a public mempool like Ethereum, making the extraction of MEV more challenging. In this paper, we investigate the prevalence and impact of MEV on Ethereum and prominent rollups such as Arbitrum, Optimism, and zkSync over a nearly three-year period. Our analysis encompasses various metrics including volume, profits, costs, competition, and response time to MEV opportunities. We discover that MEV is widespread on rollups, with trading volume comparable to Ethereum. We also find that, although MEV costs are lower on rollups, profits are also significantly lower compared to Ethereum. Additionally, we examine the prevalence of sandwich attacks on rollups. While our findings did not detect any sandwiching activity on popular rollups, we did identify the potential for cross-layer sandwich attacks facilitated by transactions that are sent across rollups and Ethereum. Consequently, we propose and evaluate the feasibility of three novel attacks that exploit cross-layer transactions, revealing that attackers could have already earned approximately 2 million USD through cross-layer sandwich attacks.

## Smart Contracting in Network Markets

**Darrell Duffie and Chaojun Wang**

Finance Theory Group, 2026

https://www.financetheory.org/papers/smart-contracting-in-network-markets

Abstract

With complete-information bilateral bargaining in network settings, holdup is eliminated when contracts across the network are agreed atomically (all or none) via a smart contract. Applications include over-the-counter trading, syndicated lending, multi-tranche securitizations, third-party financed purchases, and bookbuilding. Under a novel extensive-form bargaining protocol, any firm can give a “greenlight” to the terms of a contract proposed to that firm, which automatically converts those terms into a binding contract if the terms proposed to all other firms also receive greenlights. In any Perfect Bayesian Equilibrium with Markov strategies, firms immediately agree on socially efficient contracts that equalize expected gains across firms.

## The evolution of decentralized exchange: Risks, benefits, and oversight

**Campbell R. Harvey, Joel Hasbrouck, and Fahad Saleh**

Research Policy, 2026

https://www.sciencedirect.com/science/article/abs/pii/S0048733325002331

Abstract

A decentralized exchange, or DEX, is an application deployed on a blockchain that allows investors to exchange digital assets. We focus on the most prominent type of DEX, an Automated Market Maker (AMM), where pricing terms are determined by a preset exchange rate formula. This technology has several unique features, including accessibility to all investors, transparency of pricing, and near simultaneity of execution and settlement. In particular, trading via a DEX is feasible for any asset tokenized on a blockchain. In turn, given that assets such as stocks and bonds could be easily tokenized, it is particularly important to understand the risks posed by DEXs. This paper examines both the benefits and risks for investors from DEXs, explores the role of private and public liquidity pools, and analyzes possible regulatory approaches.

06 —— SECTION

## Tokenization and Real World Assets: Progress and Future Directions

# Transforming physical and financial assets into programmable digital tokens unlocks liquidity, fractional ownership, and infrastructural democratization.

This section explores the evolving landscape of asset tokenization, tracking its industrial implementation from abstract value exchange to concrete physical assets.

Featured research highlights how distributed architectures bridge the legacy financial system with the broader digital economy across several cross-disciplinary dimensions. At the institutional layer, structural analyses from the World Economic Forum clarify the core advantages of asset tokenization, focusing on transparency, market flexibility, and shared records, while accompanying toolkits map the regulatory taxonomy and business ecosystem of stablecoins as vital conduits for global payments. Moving beyond purely digital instruments, these tokenization principles are extended to Real-World Assets (RWAs) through frameworks that leverage machine learning and satellite-driven digital twins to precisely monitor and optimize agricultural and forestry biomass assets. The applications of real-world tokenization in socially important issues are evaluated through novel tokenization frameworks designed to channel retail capital from defined 401(k) and IRA retirement plans directly into public infrastructure projects.

These novel frameworks illustrate how tokenization bridges our physical world with an inclusive, transparent, and efficient digital economy.

## Asset Tokenization in Financial Markets: The Next Generation of Value Exchange

**Cameron Nili and Sandra Waliczek**

The World Economic Forum, 2025

https://reports.weforum.org/docs/WEF_Asset_Tokenization_in_Financial_Markets_2025.pdf

Abstract

Tokenization presents a transformative digital asset ownership model, fundamentally reshaping global financial markets. When effectively implemented, tokenization can significantly enhance transparency, accessibility, operational and cost efficiency and market flexibility, allowing participants to transact at any time and anywhere. The core advantage of tokenization lies in democratizing financial market access, enabled by trusted infrastructure.

## The Stablecoin Toolkit

**Kevin Werbach**

Wharton Initiative on Financial Policy and Regulation, 2026

https://bdap.wharton.upenn.edu/wp-content/uploads/2026/01/Stablecoin-Toolkit.pdf

Abstract

Stablecoins are essential elements of the digital asset world. More broadly, stablecoins promise to bridge the gap between the traditional financial system and the digital asset realm. With recent and proposed regulatory regimes providing clarity for institutions, these instruments are poised to become even more significant in financial markets. Stablecoins represent a potential direction for the future of money and payments globally, overcoming the limitations of legacy market infrastructure and offering novel capabilities. Although interest in stablecoins among both financial market participants and policy-makers has increased dramatically, attention has focused on a limited portion of the market. This report provides a comprehensive overview of the stablecoin world today, including the business ecosystem, categories of approaches, and use cases. A second report in the series will focus on the legal and regulatory considerations for stablecoins, highlighting approaches in major jurisdictions.

## A machine-learning enabled digital-twin framework for next generation precision agriculture and forestry

**Tarek I. Zohdi**

Computer Methods in Applied Mechanics and Engineering, 2024

https://www.sciencedirect.com/science/article/abs/pii/S0045782524005061

Abstract

This work utilizes the modern synergy between flexible, rapid, simulations and quick assimilation of data in order to develop next-generation tools for precise biomass management of large-scale agricultural and forestry systems. Additionally, when integrated with satellite and drone-based digital elevation technologies, the results lead to digital replicas of physical systems, or so-called digital-twins, which offer a powerful framework by which to optimally manage agricultural and forestry assets. Specifically, this enables the investigation of inverse problems seeking to ascertain ideal parameter combinations, such as the number of plants/trees, plant/

tree spacing, light intensity, water availability, soil resources, available planting surface area, initial seedling size, genetic variation, etc. to obtain optimal system performance. Towards this goal, a digital-twin framework is developed, consisting of a rapid computational physics engine to simulate an agricultural installation, containing thousands of growing, interacting, plants/trees. This model is then driven by a machine-learning algorithm to obtain optimal parameter sets that match observed statistical representations of a time series of growing agricultural canopy surfaces, measured by digital elevation models. Model simulations are provided to illustrate the approach and to show how such a tool can be used for large-scale biomass management.

## Tokenized IRA Infrastructure Accounts: Can Defined 401(k) Pension Plans Close the Finance Gap?

**Peter Adriaens, Minseo Park, Chaofeng Wang, and Yifeng Tian**

Journal of Management in Engineering, 2026
https://ascelibrary.org/doi/10.1061/JMENEA.MEENG-7074

Abstract

Infrastructure is the backbone of societies and economies, from power generation facilities to transportation systems and water networks. A widening gap exists between the need for resilient infrastructure and available public financing, exacerbating socioeconomic disparities in the US and globally. Public sector financing of infrastructure is subject to political influences and budgetary priorities, while private investment models are limited to institutional investors such as pension funds and insurance companies. Hence, current financing models leave a significant fraction of capital from private resources untapped for public infrastructure, including retail investors and more efficient capital (Tian et al. 2020). Three major narratives are emerging to unlock retail capital for infrastructure finance: (1) shifting defined pension plan investment policies, (2) expanding tokenized financing and infrastructure data assetization, and (3) strengthening regulatory/technical capabilities to drive adoption. Since the emergence of cryptocurrencies, applications of blockchain, a fusion of distributed ledger technology (DLT) and encryption technologies, have been considered for pilot use cases of infrastructure tokenization in the energy, real estate, and smart city contexts (Chung et al. 2023). While digital finance is rapidly growing as an alternative platform to transform traditional financing structures, there is a dearth of knowledge on the regulatory, social, and technical barriers for implementation of tokenization in public infrastructure projects. The potential role for unlocking trillions in defined pension plan contributions to execute on this premise may come from the emergence of real-world asset (RWA) tokenization. RWA tokenization involves converting the rights to an asset (e.g., real estate, energy, financing, or services) into a digital token on a blockchain, dramatically changing how these assets are financed, handled, traded, and perceived. This digital transformation has significantly increased liquidity, accessibility, and efficiency in asset management. Is there an opportunity to leverage these innovations for retail investors to become involved in public infrastructure financing? Recent proposed policies for retirement account participation in private markets may well facilitate new investments in infrastructure through tokenization.

07 —— SECTION

## Financial Markets: Risks, Impacts, and Opportunities

# The rapid integration of digital assets into global economic systems highlights the critical need to understand underlying financial market dynamics.

To help participants navigate volatile markets, researchers are developing frameworks to analyze risks and unlock opportunities directly onchain.

Featured research bridges onchain transaction data and asset pricing theory to enhance systemic stability. Network architecture analysis reveals that while short-term retail users amplify price fluctuations, a stable backbone of long-term wallets preserves the core integrity of the XRPL during market swings. In addition, traditional asset valuation models are refined by introducing a new pricing method that accounts for changing investor risk preferences, dramatically slashing option pricing errors. Our understanding of the decentralized market infrastructure is further strengthened by mapping automated market makers (AMMs) to exotic financial options, mathematically matching the hidden costs of providing liquidity to the option's natural time decay. By providing analytical clarity, optimizing onchain transaction dynamics, and reducing valuation errors, these combined advancements ensure that the next-generation decentralized ecosystem remains resilient during times of high volatility.

## Backbone Structure in the XRP Transaction Network During Price Fluctuation

**Krongtum Sankaewtong and Yuichi Ikeda**

Proceedings of Blockchain Kaigi, 2025

https://journals.jps.jp/doi/abs/10.7566/JPSCP.44.011009?mobileUi=0f

Abstract

As one of the largest cryptocurrencies and a cornerstone of international remittance, XRP exhibits distinctive transactional patterns during episodes of market volatility. In this study, we distinguish a subset of wallets who remain active in each weekly snapshot of a 22-week observation period from the entire XRP wallet base, enabling us to examine how these persistently engaged wallets, compared to short-term users, influence onchain behavior. We employ graph-theoretical tools, including community detection, bow-tie decomposition, and Hodge decomposition, to reveal how network structure and flow metrics align with price dynamics. Our findings indicate that short-term users amplify price fluctuations and create imbalances that signal potential price peaks and increases in short transaction loops and outward flows. In contrast, the persistently engaged wallets form a stable backbone within the Giant Strongly Connected Component (GSCC), maintaining loop-dominated and reciprocal transactions. This core endures persists even as short-term users enter and exit, underscoring the pivotal role of persistently engaged wallets in preserving network stability. Moreover, several on-chain signals, such as changes in community structure, degree correlations, and short transaction cycles, serve as statistically significant early indicators of impending price surges, emphasizing the network's sensitivity to user-driven shifts. Our results highlight how short-term and persistently engaged wallets collectively shape XRP's transaction network, shedding light on broader mechanisms of cryptocurrency market dynamics and financial system integration.

## Option Pricing with Time-Varying Volatility Risk Aversion

**Peter Reinhard Hansen and Chen Tong**

The Review of Financial Studies, 2026

https://academic.oup.com/rfs/article-abstract/39/3/875/8239980?redirectedFrom=fulltextf

Abstract

We introduce a pricing kernel with time-varying volatility risk aversion to explain the observed time variations in the shape of the pricing kernel. When combined with the Heston-Nandi GARCH model, this framework yields a tractable option pricing model in which the variance risk ratio (VRR) emerges as a key variable. We show that the VRR is closely linked to economic fundamentals, as well as sentiment and uncertainty measures. A novel approximation method provides analytical option pricing formulas, and we demonstrate substantial reductions in pricing errors through an empirical application to the S&P 500 index, the CBOE VIX, and option prices.

# Modeling Loss-Versus-Rebalancing in Automated Market Makers via Continuous-Installment Options

**Srisht Fateh Singh, Reina Ke Xin Li, Samuel Gaskin, Yuntao Wu, Jeffrey Klinck, Panagiotis Michalopoulos, Zissis Poulos, and Andreas Veneris**

Conference on Advances in Financial Technologies, 2025
https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.AFT.2025.6

Abstract

This paper mathematically models a constant-function automated market maker (CFAMM) position as a portfolio of exotic options, known as perpetual American continuous-installment (CI) options. This model replicates an AMM position's delta at each point in time over an infinite time horizon, thus taking into account the perpetual nature and optionality to withdraw of liquidity provision. This framework yields two key theoretical results: (a) It proves that the AMM's adverse-selection cost, loss-versus-rebalancing (LVR), is analytically identical to the continuous funding fees (the time value decay or theta) earned by the at-the-money CI option embedded in the replicating portfolio. (b) A special case of this model derives an AMM liquidity position's delta profile and boundaries that suffer approximately constant LVR, up to a bounded residual error, over an arbitrarily long forward window. Finally, the paper describes how the constant volatility parameter required by the perpetual option can be calibrated from the term structure of implied volatilities and estimates the errors for both implied volatility calibration and LVR residual error. Thus, this work provides a practical framework enabling liquidity providers to choose an AMM liquidity profile and price boundaries for an arbitrarily long, forward-looking time window where they can expect an approximately constant, price-independent LVR. The results establish a rigorous option-theoretic interpretation of AMMs and their LVR, and provide actionable guidance for liquidity providers in estimating future adverse-selection costs and optimizing position parameters.

08 —— SECTION

## Governance and Social Impact of the Blockchain Ecosystem

# Decentralized technologies hold profound potential to drive environmental sustainability, advance inclusion, and optimize public welfare.

This section explores how the blockchain ecosystem addresses pressing societal and ecological challenges by bringing digital innovation and better governance.

The included research highlights these real-world applications across several key areas. It studies the role of voting mechanisms in information aggregation. It examines how blockchain can strengthen data integrity and standardize sustainability reporting while navigating energy-consumption challenges. It looks at how blockchain optimizes regional basic income programs for vulnerable populations. Additionally, the papers from our research partners illustrate how sustainable digital finance empowers the unbanked population by providing mobile access to loans and savings for them. On the environment protection side, our research partners explore the tokenization of environmental preservation, such as reforestation and carbon credits, alongside the cloud security needed to protect these green platforms from digital threats.

These pioneering studies demonstrate how the convergence of technology, finance, and sustainability can offer scalable solutions to combat poverty, inequality, and climate change.

## Balancing Power in Decentralized Governance: Quadratic Voting and Information Aggregation

**Alon Benhaim, Brett Hemenway Falk, and Gerry Tsoukalas**

Management Science, 2025
https://pubsonline.informs.org/doi/10.1287/mnsc.2024.08469

Abstract

In decentralized governance, quadratic voting (QV)—where the cost of acquiring voting power is convex—optimally aggregates voter preferences, outperforming simpler linear voting (LV) mechanisms when voters have complete information. But what if they do not? We show that uncertainty not only breaks QV optimality but can also cause it to underperform LV. Intuitively, this is because cost convexity can disincentivize better-informed voters from adequately conveying their private information. The optimal mechanism varies with the distribution of stakes and information among voters, implying that QV's known advantages in preference aggregation do not readily extend to common-value information aggregation settings.

## Blockchain's role in environmental sustainability: Bibliometric insights from scopus

**Ganesh D. Bhatt and Ali Emdad**

Green Technologies and Sustainability, 2025
https://www.sciencedirect.com/science/article/pii/S2949736125000703

Abstract

Blockchain technology is increasingly acknowledged as a transformative tool for advancing environmental sustainability. Although blockchain has the potential to enhance transparency, trust, and accountability, research on blockchain's sustainability applications remains fragmented with inconsistent methodologies and limited integration of theoretical frameworks. One major barrier to achieving sustainability goals is the lack of standardized verification systems, which hinders regulatory oversight and consistent assessment of environmental claims. This study employs bibliometric analysis using the Scopus database and analytical tools such as VOSviewer to systematically examine the research landscape. By identifying key trends, influential authors, and thematic research clusters, this study synthesizes blockchain's roles in environmental sustainability. Our findings indicate that blockchain strengthens data integrity, enhances sustainability reporting, and promotes stakeholder collaboration across environmental sectors. However, challenges such as scalability, energy-intensive consensus mechanisms, and regulatory uncertainty persist. This study contributes to the literature by clarifying foundational concepts, identifying research gaps, and proposing directions for future work in blockchain-based sustainability frameworks.

## How Cryptocurrency Could Improve Basic Income Programs: A Design Science Research Approach

**Marcelo Henrique de Araujo, Eduardo H. Diniz, Adrian K. Cernev, Lauro Gonzalez, and Luiz A. Silva de Faria**

Information Technology for Development, 2026
https://aisel.aisnet.org/itd/vol32/iss1/18/

Abstract

Basic income policies attracted a lot of attention from policymakers and researchers during the pandemic. Considering the evidence of these policies' effectiveness, many believe that they are here to stay, keeping local governments prepared for new emergency crises. In this paper, we investigate the use of blockchain to improve digital payment platforms for basic income. We analyse the case of the Brazilian city of Maricá, where a basic income programme created by the local government for the most vulnerable residents is paid in Mumbucas — a local currency accepted only within the city. With more than 70,000 Mumbuca users in a city of 200,000 inhabitants, the initiative in Maricá has become one of the world's largest regional basic income programmes. We adopt the design science research (DSR) approach to analyse the case and propose improvements to the existing platform, considering this implementation as two entangled sub-artefacts: the public policy and the digital local currency. We conclude the case analysis by proposing alternatives for improving the artefact with a blockchain solution. This study contributes to the discussion regarding basic income, local currencies, blockchain digital platforms, and the DSR approach for producing impactful research in the information and communication technologies for development (ICT4D) field.

## Sustainable Digital Finance: Introduction

**Ingrid-Gabriela Hoven, Soh Young In, and Thomas Puschmann**

Financial Innovation and Technology, 2026
https://link.springer.com/book/10.1007/978-3-032-02983-6

Abstract

In many parts of the world, bank accounts and the financial control that they provide are seamlessly woven into the fabric of daily life. Yet, in many developing countries, they remain a gateway to opportunity that millions of people still lack. For a woman trader in a rural village, life without a bank account once meant struggling to save, plan, or grow her livelihood. The arrival of a mobile banking app changed everything: she could secure a small loan in the morning, buy produce to sell at the market, and repay the loan by the evening. Digital finance was more than a convenience. It transformed her business, empowered her to invest in her children's education, and gave her control over a future she once thought unattainable. Every day, similar stories are unfolding across the globe, underscoring the profound potential of digital finance to reshape lives and redefine how the world conducts business. As we navigate an era of rapid global transformation, the convergence of digital technology, finance, and sustainability is no longer a distant frontier; it is increasingly the cornerstone of sustainable development. When harnessed correctly, digital finance offers an unparalleled opportunity to improve lives, align financial systems with development priorities, meaningfully engage citizens, and better address global challenges such as climate change, poverty, and inequality.

09 —— SECTION

## Conclusion

# This year's UBRI report underscores a remarkable chapter of acceleration and maturation in academic blockchain research.

As decentralized technology evolves at a breakneck pace, the open, global exchange of scientific discovery has never been more vital. This cycle's focus has transcended early-stage optimization to confront the foundational realities of the digital age—spanning tokenization, intelligent DeFi infrastructure, post-quantum cryptographic security, autonomous AI-driven governance, and the multifaceted legal and social impacts of decentralized systems.

Across the eight core thematic areas presented, leading global universities have contributed indispensable frameworks that directly advance the security and utility of the broader ecosystem. These achievements stand as a testament to the power of cross-disciplinary collaboration, proving that the most complex challenges in scalability, privacy, and compliance are solved when industry support meets uninhibited academic inquiry.

UBRI remains deeply committed to fostering this culture of academic excellence and championing open-access knowledge in the blockchain space. Looking toward the future, we look forward to witnessing our research partners apply these paradigm-shifting insights to real-world architectures like the XRP Ledger (XRPL). Together, Ripple and its academic network are not merely observing the evolution of digital finance—we are anchoring its global development with unprecedented energy, rigor, and ambition.

# UBRI University Partners

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.