rippleimpact | university blockchain research initiative

BLOCKCHAIN TECHNOLOGY RESEARCH HIGHLIGHTS FROM UNIVERSITY PARTNERS

UBRI

Relentlessly Pursuing Blockchain Research and Innovation

2024

Since its launch in 2018, Ripple's University Blockchain Research Initiative (UBRI) has been instrumental in forming partnerships with nearly 60 universities, supporting a diverse array of research projects and reshaping numerous academic programs. The relentless pursuit of academic exploration in blockchain technology is crucial for sparking innovation and facilitating its adoption in institutional frameworks.

This report highlights the groundbreaking academic contributions made by UBRI-supported researchers between 2023-2024. These remarkable works include journal articles, conference papers, and books, delving into key themes and insights that drive further scientific discovery and technological advancement, while aligning with Ripple's future product line developments. This year, as we shift our focus to stablecoins, interoperability, and AI applications in blockchain, we are thrilled to see our research partners achieving outstanding results in these cutting-edge fields.

We invite you to delve into this report, uncovering how academic brilliance is shaping the future of blockchain technology, driving global innovation, and transforming industries worldwide. These efforts are not only pushing the boundaries of what's possible but also laying the foundation for Ripple to become an industry leader.

*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).

Contents

Introduction 4

Exploring Interoperability, L2 Solutions, and Optimization 5

Blockchain and Smart Contract Security: From AI to Decentralized Solutions 11

Advancing Consensus, Cryptography and Zero-knowledge Proofs 15

Innovating Decentralized Finance (DeFi) 18

Evolving FinTech, Digital Payments, and Governance 22

Promoting Blockchain for Good and Sustainability 27

Conclusion 32

UBRI University Partners 33

Introduction

Blockchain's influence on future developments is undeniable. Industries worldwide are eager to harness the enhancements offered by blockchain technology; from minimizing global payment frictions and promoting fairer financial services to the digitization of tangible assets and providing constant market access—the potential of blockchain is vast.

Recognizing that academic research is essential for driving blockchain advancements, UBRI relentlessly pursues groundbreaking studies, widespread knowledge sharing, and technological progress. Thanks to Ripple's substantial philanthropic investment in blockchain research, top universities globally have been inspired to explore blockchain's extensive capabilities.

Over the years, the UBRI network has grown to include numerous university partners across various continents, supporting a multitude of research initiatives and achieving numerous fellowships and scholarships. This year, Ripple's focus has shifted to stablecoins, interoperability, and AI applications in blockchain, and we are pleased to see our partners achieve remarkable results in these areas. Furthermore, as UBRI partners gain more experience with blockchain, we will jointly explore more academic research on the XRP Ledger.

Therefore, this report aims to showcase the outstanding blockchain research conducted by UBRI partners between 2023-2024, highlighting the ongoing integration of blockchain into global industries. These studies underscore the essential role of academic efforts in shaping the blockchain domain and the boundless potential of international collaborative innovation.

This year's report covers six main categories, each reflecting the latest advancements in blockchain technology across different sectors. Firstly, it explores strategies for enhancing interoperability, Layer 2 solutions, and optimization. Secondly, it showcases methods to enhance blockchain and smart contract security using AI or decentralized solutions. Thirdly, it examines advancements in consensus mechanisms, cryptography, and zero-knowledge proofs. Additionally, it highlights innovations in decentralized finance (DeFi). It also analyzes the impact of blockchain, cryptocurrencies, stablecoins, and Central Bank Digital Currencies (CBDCs) on FinTech, digital payments, and governance. Finally, it promotes blockchain for good and sustainability.

These studies illustrate the critical role of academic research in advancing the blockchain field and highlight the immense potential of global collaborative innovation.

01 —— SECTION

Exploring Interoperability, L2 Solutions, and Optimization

Enhancing scalability, increasing security, and improving execution efficiency are fundamental research areas driving the advancement of blockchain technology.

The papers in this category delve into various innovative strategies, including enhancing message propagation, predicting market risks, improving blockchain execution, increasing liquidity, and even implementing intelligent transportation systems. Moreover, these groundbreaking studies offer valuable insights and practical solutions, thereby driving technological progress. Ultimately, they support the future development of blockchain technology, solidifying its role as the backbone of interoperability and Layer 2 solutions.

To Squelch or not to Squelch: Enabling Improved Message Dissemination on the XRP Ledger

Lucian Trestioreanu, Flaviene Scheidt, Wazen Shbair, Jerome Francois, Damien Mlagoni, Radu State

From NOMS 2024-2024 IEEE Network Operations and Management Symposium
https://hal.science/hal-04621124/document

Abstract

With the large increase in the adoption of blockchain technologies, their underlying peer-to-peer networks must also scale with the demand. In this context, previous works highlighted the importance of ensuring efficient and resilient communication for the underlying consensus and replication mechanisms. However, they were mainly focused on mainstream, Proof-of-Work-based Distributed Ledger Technologies like Bitcoin or Ethereum. In this paper, the problem is investigated in the context of consensus-validation-based blockchains, like the XRP Ledger. The latter relies on a Federated Byzantine Agreement (FBA) consensus mechanism, which is proven to have good scalability in regards to transaction throughput. However, it is known that significant increases in the size of the XRP Ledger network would be challenging to achieve. The main reason is the flooding mechanism used to disseminate the messages related to the consensus protocol, which creates many duplicates in the network. Squelching is a recent solution proposed for limiting this duplication; however, it was never evaluated quantitatively in real-life scenarios involving the XRPL production network. In this paper, our aim is to assess this mechanism using a real-life controllable testbed and the XRPL production network, to assess its benefit and compare it to alternative solutions relying on Named Data Networking and on a gossip-based approach.

A Trading Strategy Based on BitCoin High and Low Prices: The Role of an Evolving Fuzzy Model for Interval-valued Time Series Forecasting

Leandro Maciel

From IEEE International Conference on Fuzzy Systems, 2023
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10309799

Abstract

This paper evaluates the predictability of high and low Bitcoin prices and the profitability of a trading strategy based on these forecasts. As high and low prices can be seen as interval-value time series, an evolving fuzzy system to model and forecast interval data is suggested to capture the time-varying, nonlinear, and uncertain dynamics of the cryptocurrency market. The model is composed of fuzzy functional rules in which its structure and functionality are updated as data are input. It is also designed to process interval-valued data, where high and low prices are used to represent the corresponding interval bounds. Antecedents of the rules are updated using participatory learning to cluster interval-valued time series, and consequents are computed using weighted recursive least squares based on intervals' center and range. In addition to the evaluation of predictability through accuracy metrics, a simple trading strategy is constructed based on high and low price forecasts to determine entry and exit signals, composing an economic criterion. Empirical results indicated that the fuzzy model is able

to produce accurate forecasts of high and low prices of Bitcoin, and a higher level of return adjusted by risk is achieved when these forecasts are used to perform a trading strategy in comparison with the competitive approaches.

Specular: Towards Secure, Trust-minimized Optimistic Blockchain Execution

Zhe Ye, Ujval Misra, Jiajun Cheng, Wenyang Zhou, Dawn Song

From 2024 IEEE Symposium on Security and Privacy

https://www.computer.org/csdl/proceedings-article/sp/2024/313000a171/1V5U7c5x1Li

Abstract

An optimistic rollup (ORU) scales a blockchain's throughput by delegating computation to an untrusted remote chain (L2), refereeing any state claim disagreements between mutually distrusting L2 operators via an interactive dispute resolution protocol. State-of-the-art ORUs employ a monolithic dispute resolution protocol that tightly couples an L1 referee with a specific L2 client binary, oblivious to the system's higher-level semantics. We argue that this approach (1) magnifies monoculture failure risk by precluding trust-minimized and permissionless participation using operator-chosen client software; (2) leads to an unnecessarily large and difficult-to-audit TCB; and (3) suffers from a frequently triggered, yet opaque upgrade process, both further increasing auditing overhead and broadening the governance attack surface.
To address these concerns, we outline a methodology for designing a secure and resilient ORU with a minimal TCB, by facilitating opportunistic 1-of-N-version programming. Due to its unique challenges and opportunities, we ground this work concretely in the context of the Ethereum ecosystem, where ORUs have gained significant traction. Specifically, we design a semantically aware proof system, natively targeting the EVM and its instruction set. We present an implementation in a new ORU, Specular, that opportunistically leverages Ethereum's existing client diversity with minimal source modification, demonstrating our approach's feasibility.

DEEPER: A Shared Liquidity Decentralized Exchange Design for Low Trading Volume Tokens to Enhance Average Liquidity

Srisht Fateh Singh, Panagiotis Michalopoulos, Andreas Veneris

From International Journal of Network Management, 2024

https://doi.org/10.1002/nem.2261

Abstract

This paper presents DEEPER, a design for a decentralized exchange that enhances liquidity via reserve sharing. By doing this, it addresses the problem of shallow liquidity in low trading volume token pairs. Shallow liquidity impairs the functioning of on-chain markets by creating room for unwanted phenomena such as high slippage and sandwich attacks. DEEPER solves this by allowing liquidity providers of multiple trading pairs against a common token to share liquidity. This is achieved by creating a common reserve pool for the shared token that is accessible by each trading pair. Independent from the shared liquidity, providers are free to

add liquidity to individual token pairs without any restriction. The trading between one token pair does not affect the price of other token pairs even though the reserve of the shared token changes.The proposed design is an extension of concentrated liquidity automated mar-ket maker DEXs that is simple enough to be implemented on smart contracts.This is demonstrated by providing a template for a hook-based smart contract that adds our custom functionality to UNISWAP V4. Experiments on historical prices show that for a batch consisting of eight trading pairs, DEEPER enhances liquidity by over 2.6–5:9. The enhancement in liquidity can be increased fur-ther by increasing the participating tokens in the shared pool. While providing shared liquidity, liquidity providers should be cautious of certain risks and pit-falls, which are described. Overall, DEEPER enables the creation of fair markets for low trading volume token pairs.

Blockchain-Based Efficient Access Control With Handover Policy in IoV-Enabled Intelligent Transportation System

Sandip Roy, Sourav Nandi, Raj Maheshwari, Sachin Shetty, Ashok Kumar Das, Pascal Lorenz

From IEEE Transactions on Vehicular Technology, 2023

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10285436

Abstract

Recent advances in Internet technology and IoT devices have facilitated researchers to foster a wide range of Intelligent Transportation Systems (ITS) that improve the quality of automated transportation by addressing real-time safety and traffic management issues. The participating ITS agents, such as smart cars and roadside equipment, are required to communicate urgently through an open (unsecured) wireless channel in an unattended setting. To address the security issues, several vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) authentication and access control protocols have been proposed in recent times. However, fast-moving vehicles need to set up frequent authentication with different roadside units, which induces high computation and communication overheads. Consequently, it becomes a bottleneck for the resource-limited vehicle onboard unit devices. As the blockchain supports decentralized storage with data integrity and transparency, in this article, we design a secure and lightweight Internet of Vehicles (IoV)-enabled blockchain-based access control protocol with a handover authentication facility (we call it BACHP-IoV, in short). The handover authentication mechanism exploits no computation-costly cryptographic primitives. Once the transactions or messages have been securely gathered by a roadside unit (RSU), RSU_j, residing in a group of vehicles Vh_i, will form a partial block, which is later forwarded to a cloud server node in the Peer-to-Peer (P2P) cloud servers blockchain network for converting it into a full block. Next, the full blocks are mined using a voting-based consensus algorithm. In addition, the in-charge trusted authority TA uploads information about the registered vehicles, such as randomized masked passwords and random secrets, to the blockchain. Thus, an RSU_j can check the authenticity of a particular vehicle as well. We prove the security strength of the proposed BACHP-IoV by using the well-known Real-or-Random (ROR)-based random oracle model, the ProVerif 2.03 simulation tool, and informal security analysis. We have implemented the proposed BACHP-IoV through network simulator 3 (NS-3) and blockchain, and the simulation results demonstrate that BACHP-IoV is practical in a real-life scenario. A detailed comparative analysis also shows that BACHP-IoV provides significantly better security and efficiency than the existing competing schemes.

Interplay of Cryptocurrencies with Financial and Social Media Indicators: An Entropy-Weighted Neural-MADM Approach

Jéfferson Augusto Colombo, Tanzina Akhter, Peter Wanke, Md. Abul Kalam Azad, Yong Tan, Seyyed A. Edalatpanah, Jorge Antunes

From Journal of Operational and Strategic Analytics, 2023
https://library.acadlore.com/JOSA/2023/1/4/JOSA_01.04_02.pdf

Abstract

In the rapidly evolving domain of digital finance, the interplay between cryptocurrencies and external variables such as financial and social media indicators warrants thorough examination. This investigation employs a novel, entropy-weighted Multiple Attribute Decision Making (MADM) model to decipher these intricate relationships. The study's foundation is an expansive dataset, meticulously compiled to encompass a broad spectrum of financial data alongside diverse social media indicators. Central to this analysis is the employment of the Stepwise Weight Assessment Ratio Analysis (SWARA) method, meticulously applied to ascertain the relative importance of various social media indicators. Complementing this, the Complex Proportional Assessment (COPRAS) methodology is adeptly utilized to derive utility functions for each cryptocurrency under scrutiny. The analytical prowess of neural network regressions is harnessed to delineate the influence exerted by a multitude of financial indicators on these utility functions.

The findings of this research are pivotal in understanding the dynamics within the cryptocurrency market. Bitcoin and Ripple emerge as pivotal entities, primarily functioning as primary conduits for market shocks. In contrast, Ethereum is identified as a stabilizing force, predominantly absorbing such fluctuations. A nuanced aspect of this study is the differential impact of social media indicators on various cryptocurrencies. Bitcoin and Ethereum display a negative correlation with these indicators, suggesting a complex, possibly inverse relationship with social media dynamics. Conversely, Litecoin, Dogecoin, and Ripple exhibit a positive responsiveness, indicating a heightened susceptibility to social media attention, sentiment, and prevailing uncertainty.

SyncPCN/PSyncPCN: Payment Channel Networks without Blockchain Synchrony

Oğuzhan Ersoy, Jérémie Decouchant, Satwik Prabhu Kumble, Stefanie Roos

From AFT '22: Proceedings of the 4th ACM Conference on Advances in Financial Technologies
https://doi.org/10.1145/3558535.3559779

Abstract

Payment channel networks (PCNs) enhance the scalability of blockchains by allowing parties to conduct transactions off-chain, i.e., without broadcasting every transaction to all blockchain participants. To conduct transactions, a sender and a receiver can either establish a direct payment channel with a funding blockchain transaction or leverage existing channels in a multi-hop payment. The security of PCNs usually relies on the synchrony of the underlying blockchain, i.e., evidence of misbehavior needs to be published on the blockchain within a time limit. Alternative payment channel proposals that do not require blockchain synchrony rely on quorum certificates and use a committee to register the transactions of a channel. However, these proposals do not support multi-hop payments, a limitation we aim to overcome.

In this paper, we demonstrate that it is, in fact, impossible to design a multi-hop payment protocol with both network asynchrony and faulty channels, i.e., channels that may not correctly follow the protocol. We then detail two committee-based multi-hop payment protocols that respectively assume synchronous communications and possibly faulty channels, or asynchronous communication and correct channels. The first protocol relies on possibly faulty committees instead of the blockchain to resolve channel disputes and enforces privacy properties within a synchronous network. The second one relies on committees that contain at most f faulty members out of 3f + 1 and successively delegate to each other the role of eventually completing a multi-hop payment. We show that both protocols satisfy the security requirements of a multi-hop payment and compare their communication complexity and latency.

02 —— SECTION

Blockchain and Smart Contract Security: From AI to Decentralized Solutions

The security of blockchain and smart contracts is paramount in modern digital finance. To bolster the stability and reliability of these systems, researchers are developing a range of innovative technologies. For instance, simulation analysis of decentralized decision-making processes reveals that adjusting certain parameters can significantly enhance security. Additionally, lightweight schemes designed to prevent transaction reordering attacks address practical security threats effectively. Meanwhile, in-depth research on blockchain censorship underscores the challenges posed by external sanctions on neutrality and security.

Furthermore, leveraging blockchain transparency and digital footprints to combat crypto-enabled crimes showcases the technology's potential in enhancing digital security. Moreover, using machine learning models to predict and identify risks highlights AI's crucial role in improving the security of P2P marketplaces. Collectively, these studies illustrate a variety of methods, from AI to decentralized solutions, all aimed at enhancing the security of blockchain and smart contracts.

Understanding Decentralization of Decision-Making Power in Proof-of-Stake Blockchains: An Agent-Based Simulation Approach

Christoph Mueller-Bloch, Jonas Valbjørn Andersen, Jason Spasovski, Jungpil Hahn

From European Journal of Information Systems, 2024

https://www.tandfonline.com/doi/epdf/10.1080/0960085X.2022.2125840?needAccess=true

Abstract

Blockchain systems allow for securely keeping shared records of transactions in a decentralized way. This is enabled by algorithms called consensus mechanisms. Proof-of-work is the most prominent consensus mechanism, but it is environmentally unsustainable. Here, we focus on proof-of-stake, its best-known alternative. Importantly, decentralized decision-making power is not an inherent feature of blockchain systems but a technological possibility. Numerous security incidents illustrate that decentralized control cannot be taken for granted. We therefore study how key parameters affect the degree of decentralization in proof-of-stake blockchain systems.

Based on a real-world implementation of a proof-of-stake blockchain system, we conduct agent-based simulations to study how a range of parameters impact decentralization. The results suggest that high numbers of initial potential validator nodes, large transactions, a high number of transactions, and a very high or very low positive validator network growth rate increase decentralization. We find weak support for an impact of changes in transaction fees and initial stake distributions.

Our study highlights how blockchain challenges our understanding of decentralization in information systems research and contributes to understanding the governance mechanisms that lead to decentralization in proof-of-stake blockchain systems. Additionally, it aids in designing proof-of-stake blockchain systems that are prone to decentralization and, therefore, more secure.

Eating Sandwiches: Modular and Lightweight Elimination of Transaction Reordering Attacks

Orestis Alpos, Ignacio Amores-Sesar, Christian Cachin, Michelle Yeo

From International Conference on Principles of Distributed Systems (OPODIS 2023)

https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.OPODIS.2023.12

Abstract

Traditional blockchains grant the miner of a block full control not only over which transactions are included but also their order. This constitutes a major flaw discovered with the introduction of decentralized finance, allowing miners to perform Miner Extractable Value (MEV) attacks. In this paper, we address the issue of sandwich attacks by providing a construction that takes as input a blockchain protocol and outputs a new blockchain protocol with the same security but in which sandwich attacks are not profitable. Furthermore, our protocol is fully decentralized, requiring no trusted third parties or heavy cryptography primitives, and carries a linear increase in latency and minimal computation overhead.

Blockchain Censorship

Anton Wahrstätter, Jens Ernstberger, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikołaj Barczentewicz, Arthur Gervais

From WWW '24: Proceedings of the ACM on Web Conference 2024
https://dl.acm.org/doi/pdf/10.1145/3589334.3645431

Abstract

Permissionless blockchains promise resilience against censorship by a single entity. This suggests that deterministic rules, not third-party actors, decide whether a transaction is appended to the blockchain. In 2022, the U.S. Office of Foreign Assets Control (OFAC) sanctioned a Bitcoin mixer and an Ethereum application, challenging the neutrality of permissionless blockchains. In this paper, we formalize, quantify, and analyze the security impact of blockchain censorship. We start by defining censorship, followed by a quantitative assessment of current censorship practices. We find that 46% of Ethereum blocks were made by censoring actors complying with OFAC sanctions, indicating the significant impact of OFAC sanctions on the neutrality of public blockchains. We discover that censorship affects not only neutrality but also security. After Ethereum's transition to Proof-of-Stake (PoS), censored transactions faced an average delay of 85%, compromising their security and strengthening sandwich adversaries.

An Anatomy of Crypto-Enabled Cybercrimes

Lin William Cong, Campbell R. Harvey, Daniel Rabetti, Zong-Yu Wu

From SSRN, 2024
http://dx.doi.org/10.2139/ssrn.4188661

Abstract

The advent of cryptocurrencies and digital assets holds the promise of improving financial systems by offering cheap, quick, and secure transfer of value. However, it also opens up new payment channels for cybercrimes. Assembling a diverse set of public on-chain and off-chain, proprietary and hand-collected data, including attacker-victim negotiations and dark web conversations in Russian, we present an initial anatomy of crypto-enabled cybercrimes, highlighting relevant economic issues and proposing areas for future research. Among others, we find ransomware, as the most dominant organized crypto-enabled cybercrime, entails criminal gangs that operate like firms who adopt modern revenue models and carefully manage their reputations. We suggest that blanket restrictions on cryptocurrency usage may prove counterproductive. Instead, blockchain transparency enables effective forensics for tracking, monitoring, and shutting down dominant cybercriminal organizations, which potentially facilitates a more secure and reliable crypto ecosystem in the longer term.

Identifying Risky Vendors in Cryptocurrency P2P Marketplaces

Taro Tsuchiya, Alejandro Cuevas, Nicolas Christin

From WWW '24: Proceedings of the ACM on Web Conference 2024
https://dl.acm.org/doi/pdf/10.1145/3589334.3645475

Abstract

Peer-to-Peer (P2P) cryptocurrency exchanges are two-sided marketplaces, similar to eBay, where individuals can offer to sell cryptocurrencies in exchange for payment. Due to disintermediation, these marketplaces trade off increased privacy for higher risk (e.g., scams/fraud). Although these marketplaces use feedback systems to encourage healthier transactions, anecdotal evidence suggests that feedback often fails to capture vendor-associated risks. This work documents the online safety of cryptocurrency P2P marketplaces, identifies underlying issues in feedback-based reputation systems, and proposes improved mechanisms for predicting and monitoring risky accounts.

We collect data from two cryptocurrency marketplaces, Paxful and LocalCoinSwap (LCS), for 12 months (06/2022–06/2023). The data includes over 396,000 listings, 67,000 vendors, and 4.7 million feedback entries for Paxful; and about 52,000 listings, 14,000 users, and 146,000 feedback entries for LCS.

First, we show that the current feedback system does not sufficiently convey enough information about risky vendors and is susceptible to reputation manipulation through user collusion and automation. Second, by combining various publicly available information, we build machine learning models to predict account suspension, achieving a 0.86 F1-score and 0.93 AUC for Paxful. Third, while our models appear to have limited transferability across markets, we identify which features most help account suspension across platforms. Finally, we perform a month-long online evaluation to show that our models are significantly more successful than mere feedback-based reputation schemes at predicting which users will be suspended in the future.

03 —— SECTION

Advancing Consensus, Cryptography and Zero-knowledge Proofs

Cryptography is the bedrock of secure blockchain systems, ensuring transaction integrity, confidentiality, and authenticity.

To tackle emerging threats, researchers are not only enhancing the robustness of consensus mechanisms but also exploring innovative cryptographic constructs. For instance, the significant focus on zero-knowledge proofs has transformed them into essential components of blockchain. Moreover, advancements in threshold signature schemes, particularly those tailored for post-quantum cryptography, are boosting the security and resilience of digital signatures. Altogether, these studies demonstrate how innovative cryptographic approaches and robust consensus mechanisms can effectively address both current and future security challenges in distributed systems.

Federated Byzantine Agreement Protocol Robustness to Targeted Network Attacks

Vytautas Tumas, Sean Rivera, Damien Magoni, Radu State

From 2023 IEEE Symposium on Computers and Communications (ISCC)
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10217935

Abstract

Federated Byzantine Agreement protocols, as applied in the XRP Ledger and Stellar, use voting to reach a consensus. Participants in these protocols select whom to trust in the network and effectively communicate with their trustees to reach an agreement on transactions. Most trustees, for example, 80% in the XRP Ledger, must agree on the same transactions for them to appear in the blockchain. However, disruptions to the communication between the trustees can prevent them from reaching an agreement, thus halting the blockchain.

In this paper, we propose a novel robustness metric to measure the tolerance of Federated Byzantine Agreement protocols to node failures. We show that the XRP Ledger Consensus Protocol is vulnerable to targeted attacks. Specifically, an attacker only needs to disconnect 9% of the highest-degree nodes to halt the blockchain. We propose a mitigation strategy that maintains critical XRP Ledger network topology properties while increasing the robustness up to 45%.

Cutting the GRASS: Threshold Group Action Signature Schemes

Michele Battagliola, Giacomo Borin, Alessio Meneghetti, Edoardo Persichetti

From Topics in Cryptology – CT-RSA 2024
https://eprint.iacr.org/2023/859.pdf

Abstract

Group actions are fundamental mathematical tools, with a long history of use in cryptography. Indeed, the action of finite groups at the basis of the discrete logarithm problem is behind a very large portion of modern cryptographic systems. With the advent of post-quantum cryptography, however, other group actions, such as isogeny-based ones, received interest from the cryptographic community, attracted by the possibility of translating old discrete logarithm-based functionalities.

Usually, research focuses on abelian group actions; however in this work we show that isomorphism problems which stem from non-abelian cryptographic group actions can be viable building blocks for threshold signature schemes. In particular, we construct a full N-out-of-N threshold signature scheme, and discuss the efficiency issues arising from extending it to the generic T-out-of-N case. To give a practical outlook on our constructions, we instantiate them with two different flavors of code-based cryptographic group actions, respectively at the basis of the LESS and MEDS signature schemes, two of NIST's candidates in the recent call for post-quantum standardization.

HyperPlonk: Plonk with Linear-Time Prover and High-Degree Custom Gates

Binyi Chen, Benedikt Bünz, Dan Boneh, Zhenfei Zhang

From EUROCRYPT 2023
https://doi.org/10.1007/978-3-031-30617-4_17

Abstract

Plonk is a widely used succinct non-interactive proof system that uses univariate polynomial commitments. Plonk is quite flexible: it supports circuits with low-degree “custom” gates as well as circuits with lookup gates (a lookup gate ensures that its input is contained in a predefined table). For large circuits, the bottleneck in generating a Plonk proof is the need for computing a large FFT.

We present HyperPlonk, an adaptation of Plonk to the boolean hypercube, using multilinear polynomial commitments. HyperPlonk retains the flexibility of Plonk but provides several additional benefits. First, it avoids the need for an FFT during proof generation. Second, and more importantly, it supports custom gates of much higher degree than Plonk without harming the running time of the prover. Both of these can dramatically speed up the prover’s running time. Since HyperPlonk relies on multilinear polynomial commitments, we revisit two elegant constructions: one from Orion and one from Virgo. We show how to reduce the Orion opening proof size to less than 10 KB (an almost factor 1000 improvement) and show how to make the Virgo FRI-based opening proof simpler and shorter.

A Lower Bound on the Length of Signatures Based on Group Actions and Generic Isogenies

Dan Boneh, Jiaxin Guan, Mark Zhandry

From EUROCRYPT 2023
https://doi.org/10.1007/978-3-031-30589-4_18

Abstract

We give the first black box lower bound for signature protocols that can be described as group actions, which include many based on isogenies. We show that, for a large class of signature schemes making black box use of a (potentially non-abelian) group action, the signature length must be $\Omega(\lambda^2/\log\lambda)$. Our class of signatures generalizes all known signatures that derive security exclusively from the group action, and our lower bound matches the state of the art, showing that the signature length cannot be improved without deviating from the group action framework.

04 —— SECTION

Innovating Decentralized Finance (DeFi)

Decentralized Finance (DeFi) is transforming traditional financial systems by leveraging blockchain technology to create open, transparent, and accessible financial services. As a result, advances in DeFi are significantly improving market efficiency and liquidity, while also introducing robust security measures to guard against manipulation and attacks. However, it's important to note that researchers have identified operational risks stemming from decentralized governance, including protocol, oracle, and systemic risks. On the flip side, innovations in smart contracts and governance tokens are reshaping traditional financial practices, effectively addressing issues like transparency and moral hazard. Thus, while DeFi brings numerous benefits, it also necessitates careful consideration of its inherent risks and ongoing innovations

The Impact of Derivatives on Spot Markets: Evidence From the Introduction of Bitcoin Futures Contracts

Patrick Augustin, Alexey Rubtsov, Donghwa Shin

From Management Science, 2023
https://doi.org/10.1287/mnsc.2023.4900

Abtract
Cryptocurrencies provide a unique opportunity to identify how derivatives impact spot markets. They are fully fungible, trade across multiple spot exchanges at different prices, and futures contracts were selectively introduced on bitcoin (BTC) exchange rates against the USD in December 2017. Following the futures introduction, we find a significantly greater increase in cross-exchange price synchronicity for BTC–USD relative to other exchange rate pairs, as demonstrated by an increase in price correlations and a reduction in arbitrage opportunities and volatility. We also find support for an increase in price efficiency, market quality, and liquidity. The evidence suggests that futures contracts allowed investors to circumvent arbitrage frictions associated with short sale constraints, arbitrage risk associated with block confirmation time, and market segmentation. Overall, our analysis supports the view that the introduction of BTC–USD futures was beneficial to the bitcoin spot market by making the underlying prices more informative.

SecPLF: Secure Protocols for Loanable Funds Against Oracle Manipulation Attacks

Sanidhay Arora, Yingjiu Li, Yebo Feng, and Jiahua Xu

From ASIA CCS '24: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security
https://dl.acm.org/doi/pdf/10.1145/3634737.3637681

Abstract
The evolving landscape of Decentralized Finance (DeFi) has raised critical security concerns, especially pertaining to Protocols for Loanable Funds (PLFs) and their dependency on price oracles, which are susceptible to manipulation. The emergence of flash loans has further amplified these risks, enabling increasingly complex oracle manipulation attacks that can lead to significant financial losses. Responding to this threat, we first dissect the attack mechanism by formalizing the standard operational and adversary models for PLFs. Based on our analysis, we propose SecPLF, a robust and practical solution designed to counteract oracle manipulation attacks efficiently. SecPLF operates by tracking a price state for each cryptoasset, including the recent price and the timestamp of its last update. By imposing price constraints on the price oracle usage, SecPLF ensures a PLF only engages a price oracle if the last recorded price falls within a defined threshold, thereby negating the profitability of potential attacks. Our evaluation based on historical market data confirms SecPLF's efficacy in providing high-confidence prevention against arbitrage attacks that arise due to minor price differences. SecPLF delivers proactive protection against oracle manipulation attacks, offering ease of implementation, oracle-agnostic property, and resource and cost efficiency.

Decentralized Finance: Protocols, Risks, and Governance

Agostino Capponi, Garud Iyengar, Jay Sethuraman

From Foundations and Trends® in Privacy and Security, 2023
http://dx.doi.org/10.1561/3300000036

Abstract

Financial markets are undergoing an unprecedented transformation. Technological advances have brought major improvements to the operations of financial services. While these advances promote improved accessibility and convenience, traditional finance shortcomings like lack of transparency and moral hazard frictions continue to plague centralized platforms, imposing societal costs. In this monograph, we argue how these shortcomings and frictions may be mitigated by the decentralized finance (DeFi) ecosystem. We delve into the workings of smart contracts, the backbone of DeFi transactions, with an emphasis on those underpinning token exchange and lending services. We highlight the pros and cons of the novel form of decentralized governance introduced via the ownership of governance tokens. We argue that the current DeFi infrastructure introduces operational risks to users, which we segment into five primary categories: consensus mechanisms, protocol, oracle, frontrunning, and systemic risks. We conclude by emphasizing the need for future research to focus on the scalability of existing blockchains, the improved design and interoperability of DeFi protocols, and the rigorous auditing of smart contracts.

Digital Collateral

Paul Gertler, Brett Green, Catherine Wolfram

From The Quarterly Journal of Economics, 2024
https://academic.oup.com/qje/advance-article/doi/10.1093/qje/qjae003/7588833

Abstract

A new form of secured lending using “digital collateral” has recently emerged, most prominently in low- and middle-income countries. Digital collateral relies on lockout technology, which allows the lender to temporarily disable the flow value of the collateral to the borrower without physically repossessing it. We explore this new form of credit in a model and a field experiment using school-fee loans digitally secured with a solar home system. Securing a loan with digital collateral drastically reduced default rates (by 19 percentage points) and increased the lender’s rate of return (by 49 percentage points). Using a variant of the Karlan and Zinman (2009) methodology, we decompose the total effect on repayment and find that roughly two-thirds is attributable to moral hazard, and one-third to adverse selection. In addition, access to digitally secured school-fee loans significantly increased school enrollment and school-related expenditures without detrimental effects on households’ balance sheets.

Safeguarding DeFi Smart Contracts against Oracle Deviations

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

From ACM/IEEE Proceedings of the 46th International Conference on Software Engineering, 2024
https://doi.org/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 also illustrates that current parameters utilized in the majority of benchmarks are inadequate to ensure safety when confronted with significant oracle deviations.

05 —— SECTION

Evolving FinTech, Digital Payments, and Governance

Blockchain technology, cryptocurrencies, and central bank digital currencies (CBDCs) are profoundly reshaping FinTech, digital payments, and governance structures. Our partners have delved into the practical challenges and innovative solutions in blockchain governance, uncovering factors driving consumer resistance to crypto payments and the economic implications of blockchain and crypto assets. Moreover, they have examined decentralized market structures, regulatory approaches, and the future financial systems influenced by technological advancements. Additionally, the legal and arbitration frameworks in the digital economy, as well as the competitive dynamics between traditional payment firms, cryptocurrencies, stablecoins, and CBDCs, are key areas of focus. These explorations underscore the evolving FinTech landscape, highlighting the interplay between technological innovation and regulatory frameworks, and ultimately shaping the future of global finance.

Blockchain Governance in the Wild

Kevin Werbach, Primavera Di Filippi, Gina Pieters, Joshua Tan

From Cryptoeconomic Systems, 2024
https://doi.org/10.21428/58320208.ebd76eea

Abstract

The key function of blockchains and decentralized applications (dApps) built upon them is to reach consensus with minimal centralization or hierarchy across many independent, economically-motivated actors. We call governance the collection of procedures, rules, and norms that allow these actors to make and implement decisions. Governance is a challenge found in all human societies. While many blockchain enthusiasts believe that all governance can be encoded within software minimizing or removing centralization, actual blockchain governance experiences involving many contributors and significant assets tend to differ from the pristine abstractions described in initial whitepapers.

What is Driving Consumer Resistance to Crypto-payment? A Multianalytical Investigation

Mohamad Sadegh Sangari, Atefeh Mashatan

From Psychology & Marketing, 2024
https://onlinelibrary.wiley.com/doi/epdf/10.1002/mar.21935

Abstract

Despite the extensive interest in cryptocurrencies over the past years, their application as a means of payment in e-commerce and retail purchases continues to be much slower than anticipated. This paper investigates the underlying mechanisms and elements that drive consumer resistance in this space. Drawing upon the stimulus-organism-response paradigm and the innovation resistance theory, the paper explores how the characteristics of the current cryptocurrency landscape contribute to different factors associated with crypto-payment rejection. Our findings from empirical and experimental studies reveal how ecosystem volatility and the lack of structural assurances for cryptocurrencies foster negative consumer perceptions, leading to resistance against crypto-payment use. The paper develops new insights into the main predictors of consumer resistance to crypto-payment, which is a precursor to the mainstream use of cryptocurrencies. Moreover, it sheds light on the interactions among context-specific, psychological, and functional determinants of behavioral consumer response.

Advances in Blockchain and Crypto Economics

Bruno Biais, Agostino Capponi, Lin William Cong, Vishal Gaur, Kay Giesecke

From Management Science, 2023
https://doi.org/10.1287/mnsc.2023.intro.v69.n11

Abstract

Over the past decade, blockchains and cryptocurrencies have taken a central stage in financial technology (FinTech) innovation. In 2020–2021, as the academic finance and management community began actively investigating this domain, we issued a call for papers for a special issue to encourage interdisciplinary research in this emerging area. This section of Management Science presents the first systematic collection of knowledge, both theoretical and empirical, focusing on blockchain economics, crypto assets, decentralized finance, and Web3 ecosystems. We describe the editorial protocol employed for this special issue (now included in this volume as a special section), summarize what we learn about the field, and introduce the 15 articles included in the special section. We also offer several observations to highlight foundational issues in the new field and to guide future research in this exciting new area at the intersection of technology and finance.

Decentralized Markets and Self-Regulation

Yuliya Guseva

From George Washington Law Review, 2024
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4677538

Abstract

Distributed ledger technology, such as blockchains, is changing financial markets by creating a new foundation for transacting with digital assets. Simultaneously, blockchain-enabled intermediaries—cryptoexchanges—have emerged to trade, broker, and settle transactions with digital assets, including native cryptoassets and other tokenized assets. U.S. regulators seek to place cryptoexchanges within the ambit of existing regulation and registration requirements for legacy intermediaries. A critical underexplored corollary of this approach is converting cryptoexchanges into legacy self-regulatory organizations (SROs) or members of such SROs. Put differently, U.S. agencies are bringing not only conventional regulation but also self-regulation into blockchain-enabled markets. Unfortunately, in imposing the traditional model without reform, policymakers risk ignoring the considerable economic potential of the new technologies. Their approach should also fail to precisely target the risks, transaction costs, and negative externalities of digital asset trading.

To offer solutions, the Article examines the digital asset market structure and microstructure, its intermediaries, and associated transaction costs. Comparing centralized cryptoexchanges, decentralized cryptoexchanges, and legacy trading venues, the Article explains why cryptoexchanges cannot optimally address the risks of digital asset markets without bespoke regulatory guardrails. Agreeing with the basic intuition to introduce formal self-regulation, the Article refines possible self-regulatory models. The proposed frameworks would aggregate the decentralized knowledge of individual participants in the global blockchain-enabled market to ensure better coordination and well-informed regulation. Building on market expertise, the new SROs would educate the regulators about ongoing market developments and risks, promote

regulatory efficiency, and improve digital asset trading. The proposed approach would also reduce the costs of coordination among heterogeneous and globally dispersed participants in blockchain-enabled markets and nudge them toward self-regulatory and technological solutions to transactional problems in a comprehensive manner.

Financial System 2030

Thomas Puschmann

From Springer Nature, 2024

https://link.springer.com/book/10.1007/978-3-031-55700-2

Abstract

The financial system is currently confronted with tremendous challenges from the global economy, trade, politics, demographics, and most recently from enormous technological advancements. These developments have the capacity to change the existing financial system fundamentally. This book addresses how technological developments and digitalization will impact the future of financial systems.

This book is based on the results of a series of ten roundtables with high-level experts on the future of the financial system. Experts from academia, supranational institutions, central banks, commercial banks, regulators, start-ups, technology companies, venture capital firms, think tanks, foundations, and other visionaries from five continents developed potential scenarios of the financial system 2030 over a time horizon of five years. The book presents the results of these discussions, which are structured along the 'Vaduz Architecture'. This newly introduced concept distinguishes different dimensions for the future financial system, including information technologies, nation states and (de-) regulation.

Commercial and Arbitration Law of the Digital Economy: A Comparison of Asian, European and North American Jurisdictions

Robert Walters

From Routledge Taylor & Francis Group, 2025

https://www.routledge.com/Commercial-and-Arbitration-Law-of-the-Digital-Economy-A-Comparison-of-Asian-European-and-North-American-Jurisdictions/Walters/p/book/9781032443287

Abstract

This book discusses the importance of the digital economy and its most pressing challenge: the onset of quantum and critical technology. It looks at how its implementation, either on its own or coupled with artificial intelligence, impacts commercial and arbitration law.

International trade and investment are increasingly being integrated within national security policy and the law to protect the nation state. A failure to safeguard personal and commercial data will allow other state and non-state actors to set the rules that do not align with the values of the rule of law and transnational rules-based system. This book argues that it is necessary to establish a principles-based approach to governing the development and use of these

technologies. Chapters touch on the application of smart contracts, arbitration, as well as mergers and acquisitions and their potential weaponisation in the digital economy due to their ability to transcend national security. Elements of intellectual property, particularly patents and trademarks, and how international legal instruments have directed national law-making are also explored.

This is a useful reference for governments, regulators, legal, technologists and policy experts. This is also of interest to scholars looking at personal and commercial data in relation to intellectual property, contracts and international commercial arbitration law.

06 —— SECTION

Promoting Blockchain for Good and Sustainability

Blockchain technology holds immense potential to drive social good and sustainability. Our partners' research spans various applications, including sustainable agriculture financing, supply chain management, renewable energy integration, green fintech, and the oil and gas industry. These studies showcase blockchain's benefits in reducing carbon emissions, enhancing transparency, and promoting responsible governance. Moreover, they demonstrate how blockchain can address current environmental and social challenges by highlighting the synergy between technological innovation and governance frameworks. Through these explorations, blockchain technology is reaffirmed as a powerful tool for advancing global sustainability and promoting social good.

Blockchain Technology for Pay-for-outcome Sustainable Agriculture Financing: Implications for Governance and Transaction Costs

Kenneth Hsien Yung Chung, Peter Adriaens

From Environmental Research Communications, 2024
https://doi.org/10.1088/2515-7620/ad16f0

Abstract

Pay-for-outcome financing mechanisms have been used to address agricultural runoffs to overcome the inefficiencies associated with push-based solutions, which are dependent on subsidies or philanthropic funding. As a market-based approach, pay-for-outcome platforms seek to incentivize sustainable practices, compensated by beneficiaries of the positive outcomes. Execution of pay-for-outcome financing mechanisms in an agriculture context is a complex transaction, involving investors, farmers, third-party verifiers of outcomes, government and corporate beneficiaries, and thus requires a costly governance structure. Effective governance mechanisms are needed to meet the transaction costs identified in performance measurements. This study investigates the efficacy of blockchain technology to address transaction costs in pay-for-outcome financing for sustainable agriculture. Through a proof-of-concept, this study quantifies and explores the potential cost-saving benefits of utilizing blockchain. The proof-of-concept is an application of blockchain within a pay-for-outcome incentive model, namely the Soil and Water Outcomes Fund, for sustainable agriculture. Utilizing the Ethereum blockchain, transactions are facilitated through crypto wallets and a hybrid smart contract, while precipitation is used as a proxy for agricultural runoff measurements. Drawing from Transaction Cost Economics theory, a discussion is presented on how blockchains can reduce transaction costs, enhancing the governance and efficiency of pay-for-outcome mechanisms. Furthermore, the article presents blockchain transaction fees in the context of the scale of operations, considering the total number of participants in the Soil and Water Outcomes Fund. Our findings indicate that blockchain technology has the capacity to simplify intricate transactions, boost measurement accuracy, cut administrative expenses, and foster trust and transparency among stakeholders, thereby reducing the overall transaction costs associated with pay-for-outcome incentives. While blockchain has its limitations and is not a universally applicable solution for every type of transaction cost, we believe that blockchains are well-suited to facilitate pay-for-outcome financing such as the Soil and Water Outcomes Fund.

Privacy-Preserving Ownership Transfer: Challenges and An Outlined Solution Based on Zero-Knowledge Proofs

Mohammadtaghi Badakhshan, Guang Gong

From 2023 IEEE 9th World Forum on Internet of Things (WF-IoT)
https://ieeexplore.ieee.org/abstract/document/10539396

Abstract

Although employing blockchain in supply chain management (SCM) can provide benefits in numerous aspects such as traceability, transparency, and more, using public blockchain for

SCM may compromise the privacy of the supply chain participants and their business secrets. In this paper, we review recent papers that integrate blockchain with SCM and the papers that propose privacy-preserving approaches for public blockchain. Then, we identify the problem in the existing solutions. Additionally, we present an outline of a framework that enables entities in a supply chain to upload their data records anonymously. This framework preserves unlinkability when transferring product ownership. The proposed scheme allows data auditors, who can be the end customers of a supply chain, to access a product's history and verify the authenticity of the data while preserving the privacy of the data uploader. We demonstrate that supply chain data records follow a directed acyclic graph (DAG), similar to the data structure that maintains data records in version control systems (VCS). Hence, this insight could make the framework applicable for anonymous version control systems based on blockchain.

ECC-EXONUM-eVOTING: A Novel Signature Based e-Voting Scheme Using Blockchain and Zero Knowledge Property

Suman Majumder, Sangram Ray, Dipanwita Sadhukhan, Mou Dasgupta, Ashok Kumar Das, Youngho Park

From IEEE Open Journal of the Communications Society, 2023
https://doi.org/10.1109/OJCOMS.2023.3348468

Abstract
Traditional voting systems mainly comprise of paper polling, electronic ballot system (EVM), mechanical devices, etc., and demand the physical presence of the voters. In the new age of digitization, the electronic voting system has come up with a unique facility to cast votes from any discreet place. However, the e-voting system has to face several challenges regarding security and privacy. To overcome such obstructions, blockchain is introduced in e-voting applications that preserve anonymity, security, and consistency of voter-related information with the help of Merkle tree and hash digest. Hence, any discrepancy can immediately be detected whenever the hash values of the respective block have been modified and consequently, the whole block is discarded. In this research, a novel e-voting scheme is proposed following the decentralized service-oriented architecture of Exonum private blockchain, hybrid consensus algorithm, and Elliptic Curve Diffie-Helmen (ECDH) protocol to agree upon a secure session key among different participants. Moreover, the proposed scheme (ECC-EXONUM-eVOTING) employs a zero-knowledge protocol and is customized to work over idemix technologies with a blind signature scheme. Numerous well-known cryptographic attacks are analyzed formally using the probabilistic random oracle model and informally for validating the security strength of ECC-EXONUM-eVOTING. As a result, it is found that the proposed scheme is well-defended against all potential security concerns. Furthermore, the scheme is simulated using both Automated Validation of Internet Security Protocols and Applications (AVISPA) and Scyther tools to demonstrate the proposed scheme is not prone to any security attacks. Finally, it is concluded that the proposed scheme is well-suited for secure e-voting applications.

Data Science of Renewable Energy Integration: The Nexus of Energy, Environment, and Economic Growth

Yuichi Ikeda

From Springer Nature, 2024
https://link.springer.com/book/10.1007/978-981-99-8779-5

Abstract

This book covers various data scientific approaches to analyze the issue of grid integration of renewable energy for which the grid flexibility is the key to cope with its intermittency. It provides readers with the scope to view renewable energy integration as establishing a distributed energy network instead of the traditional centralized energy system. Specifically, quantitative valuation system-wise of the levelized cost of energy, which includes both initial cost and various operational costs, enables readers to optimize energy systems in order to minimize economic cost and environmental impact. It is noted, however, that the high cost of integrating renewable energy on a large scale might slow economic growth considerably. Topics addressed in the book also include statistical comparative study of the relationship between energy and economic growth, a graphical model of determinant factors for foreign direct investment in renewable energy, the coupled oscillator model and unit commitment model to capture intermittency of renewable energy, and the network model of evolving micro-grids. The book explains desired innovation to reduce the integration cost significantly using innovative technologies such as energy storage with hydrogen production and vehicle-to-grid technology. Illustrated by careful analysis of selected examples of renewable integration using different types of grid flexibility, this volume is indispensable to readers who make policy recommendations to establish the distributed energy network integrated with large-scale renewable energy by disentangling the nexus of energy, environment, and economic growth.

Sustainable Oil and Gas Using Blockchain

Soheil Saraji, Si Chen

From Springer International Publishing, 2023
https://doi.org/10.1007/978-3-031-30697-6

Abstract

As the world shifts towards a sustainable energy future, the oil and gas industry faces significant challenges and opportunities. Focusing on the development of a sustainable O&G industry, the book delves into the role of climate and financial markets in the energy sector, applications of blockchain in sustainable energy development, and the challenges of legal and regulatory issues in applying blockchain technology. It provides insight into how the energy industry is already working on reducing carbon emissions and paving the way to a sustainable future with detailed examples of reducing methane emissions, carbon credit markets, sustainable aviation fuels, and plastics. The book also examines how O&G companies could further their sustainability initiatives using blockchain technology for emission data monitoring, carbon capture, utilization, storage, and supply-chain management to develop clean products.

Green Fintech: Developing a Research Agenda

Thomas Puschmann, Valentyn Khmarskyi

From Corporate Social Responsibility and Environmental Management, 2024
https://doi.org/10.1002/csr.2675

Abstract

Digitalization and sustainability have been the core drivers of transformation of the financial industry in recent years. In this context, green fintech plays a major role,which, however, is still an unexplored field in business, information systems and finance research. This paper conducts a systematic literature analysis and develops a research agenda based on a framework, which is derived from clustering 74 academic research papers. The framework consists of the four clusters strategy, organization,technology, and potentials along nine dimensions. The research agenda reveals that green fintech is still a very premature field of research. The analysis shows that areas like customer- and government-related services, insurance-oriented approaches andSDGs which focus on life on land and life below water are still rare and that most of the approaches focus on blockchain technology, while other financial technologies like artificial intelligence are still underrepresented.

07 —— SECTION

Conclusion

This year's UBRI report showcases the impressive strides in blockchain research within academia. As blockchain technology races forward, spreading new discoveries across the globe becomes increasingly vital. This year, we've zeroed in on stablecoins, interoperability, and AI applications in blockchain. Esteemed institutions worldwide have launched research projects that have significantly advanced these fields.

The report covers six main categories, each highlighting the latest advancements in blockchain technology across various sectors. UBRI is set to continue cementing its status as a beacon of excellence in the blockchain world and a shining example of the decentralization of knowledge. Looking ahead, we are eager to see our research partners apply their groundbreaking findings to the XRPL, driving the global advancement of blockchain technology with confidence and excitement.

UBRI University Partners

Australian National University
Carnegie Mellon University
Cornell University
TU Delft
Duke University
ETH zürich
FGV
Georgetown University
ITAM
International Institute of Information Technology Hyderabad
KU The University of Kansas
Korea University
Kyoto University
MIT
Morgan State University
NUS National University of Singapore
Northeastern University
NYU Abu Dhabi
Princeton University
Háskólinn í Reykjavík
Rutgers Law School
Toronto Metropolitan University
Stanford University
Tsinghua University
The University of North Carolina at Chapel Hill
UKCBT
Universität Bern
Berkeley University of California
University of Cape Town
University of Oregon
University of Michigan
University of Nicosia
東京大学 The University of Tokyo
uni.lu Université du Luxembourg
University of Oxford
Penn
Texas The University of Texas at Austin
University of Waterloo
University of Zurich
Università di Trento
USP Universidade de São Paulo
University of Toronto
Columbia University in the City of New York
Trinity College Dublin
ie Business School
Victoria University Melbourne Australia
ASU Arizona State University
Portland State University
EPITA
Royal University of Bhutan
NOVA School of Business & Economics
University of Wyoming
EUI
Northwestern Kellogg
EBS Universität
Nanyang Technological University Singapore
Yonsei University

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 almost 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.