rippleimpact | university blockchain research initiative

BLOCKCHAIN TECHNOLOGY
RESEARCH HIGHLIGHTS FROM
UNIVERSITY PARTNERS

UBRI

Powers Breakthroughs in Blockchain Research

2023

Since the inception of the University Blockchain Research Initiative (UBRI) in 2018, Ripple has funded over 50+ university partnerships, supporting hundreds of research projects and influencing countless university courses. Ongoing academic analysis of blockchain is essential to technological progress and institutional adoption of blockchain technologies.

This summary shares breakthrough academic contributions made from 2022-2023 by researchers at UBRI supported universities. The academic contributions referenced in this report range from academic journal and conference papers to books, each identifying common themes and findings which catalyze further scientific discovery and technological innovation.

*The materials in this report are based upon work that may be supported or partially supported by Ripple under the University Blockchain Research Initiative (UBRI) program. Any opinions, findings, and 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 for which a worldwide group of businesses and developers contribute (including Ripple).

Contents

Introduction

The role of blockchain in shaping the future is inextricable. Disparate industries worldwide are interested in the improvements that can be realized using blockchain technology; from reducing frictions in global payments and providing greater equity for financial services, to tokenization of real-world assets and around-the-clock market access—the possibilities with blockchain are endless.

Academic research is crucial for blockchain innovation, which is why UBRI aims to foster an array of groundbreaking research, knowledge dissemination, and technological advancements. With Ripple's $80M philanthropic pledge to blockchain research, the world's premier universities were galvanized into action to explore and understand the vast capabilities of blockchain technology.

The UBRI network has expanded to include a significant number of university collaborators across multiple continents, supporting a wide range of research projects and earning a substantial number of awards in the form of fellowships and scholarships. In contrast to last year's report, research on Central Bank Digital Currencies (CBDCs) has evolved to focus more on regulation—no doubt in connection with the growth in global adoption. This report also highlights a greater number of academic papers focusing on the XRP Ledger, many of which have been published in leading academic journals, indicating its importance across this community.

An additional section on Taxonomy has been included to showcase the burgeoning interest in this subject as it relates to blockchain. The papers throughout this section can be used as a tool to help researchers narrow down their field of study and understand the implications of innovation across the blockchain industry.

This report aims to highlight the exceptional blockchain research from UBRI partners between 2022-2023, illuminating the path to blockchain's continued integration into global industries. These studies represent the pivotal role of academic endeavors in shaping the blockchain landscape and the immeasurable potential of global collaborative innovation.

01 SECTION

Refining Distributed Ledger Technology

Distributed ledger technology (DLT) enables various participants to store and coordinate transactions over a dispersed network of nodes, without the need for a central authority. Diverse studies shed light on enhancing communication efficiency, introducing novel distributed structures, and layering consensus protocols to enhance security and scalability. Additionally, they address latency issues in P2P networks. Concurrency issues and incentive schemes receive notable attention throughout this section, as do the dynamics of transaction fees. Together, these works underscore the multifaceted endeavors to elevate and adapt DLT across various contexts.

XRP-NDN Overlay: Improving the Communication Efficiency of Consensus-Validation based Blockchains with an NDN

Lucian Trestioreanu, Wazen M. Shbair, Flaviene Scheidt de Cristo, Radu State

In NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium (pp. 1-5).
https://doi.org/10.1109/NOMS56928.2023.10154402

Abstract

With growing adoption of Distributed Ledger Technologies, their networks must scale while maintaining efficient communication for the underlying consensus and replication mechanisms. New content distribution concepts like Named Data Networking create opportunities to achieve this. We present and evaluate XRP-NDN overlay, a solution to increase communication efficiency for consensus-validation blockchains like XRP Ledger. We send consensus messages over different communication models and show that the chosen model lowers the number of messages at node level to minimum, while maintaining or improving performance by leveraging overlay advantages.

Tiramisu: Layering Consensus Protocols for Scalable and Secure Blockchains

Anurag Jain, Sanidhay Arora, Sankarshan Damle, Sujit Gujar

In 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-3).
https://doi.org/10.1109/ICBC54727.2022.9805562

Abstract

Cryptocurrencies are poised to revolutionize the modern economy by democratizing commerce. These currencies operate on top of blockchain-based distributed ledgers. Existing permissionless blockchain-based protocols offer unparalleled benefits like decentralization, anonymity, and transparency. However, these protocols suffer in performance which hinders their widespread adoption. In particular, high time-to-finality and low transaction rates keep them from replacing centralized payment systems such as the Visa network. Permissioned blockchain protocols offer attractive performance guarantees, but they are not considered suitable for deploying decentralized cryptocurrencies due to their centralized nature. Researchers have developed several multi-layered blockchain protocols that combine both permissioned and permissionless blockchain protocols to achieve high performance along with decentralization. The key idea with existing layered blockchain protocols in literature is to divide blockchain operations into two layers and use different types of consensus to manage each layer. However, many such works come with the assumptions of honest majority which may not accurately reflect the real world where the participants may be self-interested or rational. These assumptions may render the protocols susceptible to security threats in the real world, as highlighted by the literature focused on exploring game-theoretic attacks on these protocols. We generalize the “layered” approach taken by existing protocols in the literature and present a framework to analyze the system in the BAR Model and provide a generalized game-theoretic analysis of such protocols. Using our analysis, we identify the critical system parameters required for a distributed ledger’s secure operation in a more realistic setting.

Strategic Latency Reduction in Blockchain Peer-to-Peer Networks

Weizhao Tang, Lucianna Kiffer, Giulia Fanti, Ari Juels

Proceedings of the ACM on Measurement and Analysis of Computing Systems, 7(2), 1-33.
https://doi.org/10.1145/3589976

Abstract

Most permissionless blockchain networks run on peer-to-peer (P2P) networks, which offer flexibility and decentralization at the expense of performance (e.g., network latency). Historically, this tradeoff has not been a bottleneck for most blockchains. However, an emerging host of blockchain-based applications (e.g., decentralized finance) are increasingly sensitive to latency; users who can reduce their network latency relative to other users can accrue (sometimes significant) financial gains. In this work, we initiate the study of strategic latency reduction in blockchain P2P networks. We first define two classes of latency that are of interest in blockchain applications. We then show empirically that a strategic agent who controls only their local peering decisions can manipulate both types of latency, achieving 60% of the global latency gains provided by the centralized, paid service bloXroute, or, in targeted scenarios, comparable gains. Finally, we show that our results are not due to the poor design of existing P2P networks. Under a simple network model, we theoretically prove that an adversary can always manipulate the P2P network's latency to their advantage, provided the network experiences sufficient peer churn and transaction activity.

Charlotte: A Web of Composable Authenticated Distributed Data Structures

Isaac Sheff, Xinwen Wang, Kushal Babel, Haobin Ni, Robbert van Renesse, Andrew C. Myers

ACM Trans. Comput. Syst. (July 2023).
https://doi.org/10.1145/3607534

Abstract

Cross-domain applications are rapidly adopting blockchain techniques for immutability, availability, integrity, and interoperability. However, for most applications, global consensus is unnecessary and may not even provide sufficient guarantees.

We propose a new distributed data structure: Attested Data Structures (ADS), which generalize not only blockchains, but also many other structures used by distributed applications. As in blockchains, data in ADSs is immutable and self-authenticating. ADSs go further by supporting application-defined proofs (attestations). Attestations enable applications to plug in their own mechanisms to ensure availability and integrity.

We present Charlotte, a framework for composable ADSs. Charlotte deconstructs conventional blockchains into more primitive mechanisms. Charlotte can be used to construct blockchains, but does not impose the usual global-ordering overhead. Charlotte offers a flexible foundation for interacting applications that define their own policies for availability and integrity. Unlike traditional distributed systems, Charlotte supports heterogeneous trust: different observers have their own beliefs about who might fail, and how. Nevertheless, each observer has a

consistent, available view of data.

Charlotte's data structures are interoperable and composable: applications and data structures can operate fully independently, or can share data when desired. Charlotte defines a language-independent format for data blocks and a network API for servers.

To demonstrate Charlotte's flexibility, we implement several integrity mechanisms, including consensus and proof of work. We explore the power of disentangling availability and integrity mechanisms in prototype applications. The results suggest that Charlotte can be used to build flexible, fast, composable applications with strong guarantees.

IRS: An Incentive-compatible Reward Scheme for Algorand

Maizi Liao, Wojciech Golab, Seyed Majid Zahedi

In Proceedings of the 2023 International Conference on Autonomous Agents and Multiagent Systems (AAMAS '23). 661–669.
https://dl.acm.org/doi/10.5555/3545946.3598697

Abstract

Founded in 2017, Algorand is one of the world's first carbon-negative, public blockchains inspired by proof of stake. Algorand uses a Byzantine agreement protocol to add new blocks to the blockchain. The protocol can tolerate malicious users as long as a supermajority of the stake is controlled by non-malicious users. The protocol achieves about 100x more throughput compared to Bitcoin and can be easily scaled to millions of nodes. Despite its impressive features, Algorand lacks a reward-distribution scheme that can effectively incentivize nodes to participate in the protocol. In this work, we study the incentive issue in Algorand through the lens of game theory. We model the Algorand protocol as a Bayesian game and propose a novel reward scheme to address the incentive issue in Algorand. We derive necessary conditions to ensure that participation in the protocol is a Bayesian Nash equilibrium under our proposed reward scheme even in the presence of a malicious adversary. We also present quantitative analysis of our proposed reward scheme by applying it to two real-world deployment scenarios. We estimate the costs of running an Algorand node and simulate the protocol to measure the overheads in terms of computation, storage, and networking.

Empirical Analysis of EIP-1559: Transaction Fees, Waiting Time, and Consensus Security

Yulin Liu, Yuxuan Lu, Kartik Nayak, Fan Zhang, Luyao Zhang, Yinhong Zhao

In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 2099-2113).
https://doi.org/10.1145/3548606.3559341

Abstract

A transaction fee mechanism (TFM) is an essential component of a blockchain protocol. However, a systematic evaluation of the real-world impact of TFMs is still absent. Using rich data from the Ethereum blockchain, the mempool, and exchanges, we study the effect of EIP-1559, one of the earliest-deployed TFMs that depart from the traditional first-price auction paradigm. We conduct a rigorous and comprehensive empirical study to examine its causal effect on blockchain transaction fee dynamics, transaction waiting times, and consensus security. Our results show that EIP-1559 improves the user experience by mitigating intrablock differences in the gas price paid and reducing users' waiting times. However, EIP-1559 has only a small effect on gas fee levels and consensus security. In addition, we find that when Ether's price is more volatile, the waiting time is significantly higher. We also verify that a larger block size increases the presence of siblings. These findings suggest new directions for improving TFMs.

02 SECTION

Exploring Cryptography, Authentication and Attack Analysis

Cryptography is more than just the foundation of blockchain; it's the protective shield for data, user identities, and security on a ledger. Researchers are continuously improving the efficiency and exploring the applications of zero-knowledge proofs (zk-proofs) which have transcended from mere theory to an indispensable piece of blockchain applications. In addition, advanced code-based signcryption schemes, which combine both encryption and digital signatures, are among the prime examples of using cryptography to enhance the security and privacy of a blockchain. Other examples include authentication methods based on blockchain and key agreement schemes, as well as privacy protection authentication in smart grids and energy systems. Moreover, researchers also offer solutions to front-running attacks on the XRP Ledger and potential threats to proof-of-stake blockchains.

Succinct Non Interactive Arguments of Knowledge from Supersingular Isogenies

Paulo L. Barreto, Marcos A. Simplicio Jr, Gustavo H. M. Zanon

In Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (pp. 181-194). SBC.
https://doi.org/10.5753/sbseg.2022.225292

Abstract

A succinct non-interactive argument of knowledge (SNARK) enables a party to convince another of some statement (typically, knowledge of some information) by means of a short argument, while ensuring it is infeasible for an adversary to create a short argument of the opposite statement. We hereby describe a SNARK for CSI-FiSh signatures, whose security stems from hard problems involving supersingular isogenies. Although the scheme looks analogous to a SNARK for conventional Schnorr signatures, it is non-trivial in that, as we also show, a similar SNARK for another isogeny-based signature scheme (SQISign) is not viable. As a bonus, we also discuss how to drastically reduce the memory needed to implement the CSIDH framework required by CSI-FiSh signatures.

Orion: Zero Knowledge Proof with Linear Prover Time

Tiancheng Xie, Yupeng Zhang, Dawn Song

In Annual International Cryptology Conference (pp. 299-328)
https://doi.org/10.1007/978-3-031-15985-5_11

Abstract

Zero-knowledge proof is a powerful cryptographic primitive that has found various applications in the real world. However, existing schemes with succinct proof size suffer from a high overhead on the proof generation time that is super-linear in the size of the statement represented as an arithmetic circuit, limiting their efficiency and scalability in practice. In this paper, we present Orion, a new zero-knowledge argument system that achieves O(N) prover time of field operations and hash functions and O(log2 N) proof size. Orion is concretely efficient and our implementation shows that the prover time is 3.09 s and the proof size is 1.5 MB for a circuit with 220 multiplication gates. The prover time is the fastest among all existing succinct proof systems, and the proof size is an order of magnitude smaller than a recent scheme proposed in Golovnev et al. 2021.

In particular, we develop two new techniques leading to the efficiency improvement. (1) We propose a new algorithm to test whether a random bipartite graph is a lossless expander graph or not based on the densest subgraph algorithm. It allows us to sample lossless expanders with an overwhelming probability. The technique improves the efficiency and/or security of all existing zero-knowledge argument schemes with a linear prover time. The testing algorithm based on densest subgraph may be of independent interest for other applications of expander graphs. (2) We develop an efficient proof composition scheme, code switching, to reduce the proof size from square root to polylogarithmic in the size of the computation. The scheme is built on the encoding circuit of a linear code and shows that the witness of a second zero-knowledge argument is the same as the message in the linear code. The proof composition only introduces a small overhead on the prover time.

Speeding Up Multi-Scalar Multiplication over Fixed Points Towards Efficient zkSNARKs

Guiwen Luo, Shihui Fu, Guang Gong

IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(2), 358–380.
https://doi.org/10.46586/tches.v2023.i2.358-380

Abstract

The arithmetic of computing multiple scalar multiplications in an elliptic curve group then adding them together is called multi-scalar multiplication (MSM). MSM over fixed points dominates the time consumption in the pairing-based trusted setup zero-knowledge succinct non-interactive argument of knowledge (zkSNARK), thus for practical applications we would appreciate fast algorithms to compute it. This paper proposes a bucket set construction that can be utilized in the context of Pippenger's bucket method to speed up MSM over fixed points with the help of precomputation. If instantiating the proposed construction over BLS12-381 curve, when computing n-scalar multiplications for $n = 2e$ ($10 \le e \le 21$), theoretical analysis indicates that the proposed construction saves more than 21% computational cost compared to Pippenger's bucket method, and that it saves 2.6% to 9.6% computational cost compared to the most popular variant of Pippenger's bucket method. Finally, our experimental result demonstrates the feasibility of accelerating the computation of MSM over fixed points using large precomputation tables as well as the effectiveness of our new construction.

BUAKA-CS: Blockchain-enabled User Authentication and Key Agreement Scheme for Crowdsourcing System

Mohammad Wazid, Ashok Kumar Das, Rasheed Hussain, Neeraj Kumar, Sandip Roy

Journal of Systems Architecture, 123, 102370.
https://doi.org/10.1016/j.sysarc.2021.102370

Abstract

Crowdsourcing is a practice of using collective intelligence of a group in order to achieve a common goal to solve complex problems in an innovative way. It involves obtaining information and opinions from a group of participants who submit their data (i.e., solutions) via the Internet using some applications. The application domains, where crowdsourcing can be used, include, but not limited to, healthcare, environment, public safety, disaster management, and transportation. Despite the unprecedented advantages of crowdsourcing, security and privacy are rising concerns that need to be addressed. Therefore, it is crucially important to provide effective solutions that address the security and privacy issues in crowdsourcing systems. To this end, the salient features of blockchain technology such as immutability, decentralization, transparency and resiliency can play a pivotal role to address the afore-mentioned security challenges. To fill these gaps, in this paper, we propose a new blockchain-based user authentication and key agreement scheme for crowdsourcing (BUAKA-CS) through lightweight cryptographic techniques. The security of the BUAKA-CS is proved through the formal method and also through other mathematical methods that depict the resilience of BUAKA-CS against various types of possible attacks. Moreover, the robustness of BUAKA-CS against possible attacks is proved through widely-recognized automated software validation tools. We also compare BUAKA-CS with other existing schemes and prove its out performance in terms of security, functionality, computation and communication costs. Finally, we conduct the extensive blockchain-based simulations to measure the impact of BUAKA-CS on the performance of the system.

Privacy-Preserving Blockchain-Based Authentication in Smart Energy Systems

Anusha Vangala, Ashok Kumar Das

In Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems
(pp. 1208-1214).
https://doi.org/10.1145/3560905.3568179

Abstract

Smart Energy Systems (SES) are the need of the hour, given the looming dangers of power crises amid changing climatic conditions. However, sensitive data play a critical role in such systems deserving high privacy and security protection. This paper proposes a novel blockchain-based authentication scheme that preserves privacy using the zero-knowledge protocol. During informal analysis, the proposed scheme shows resistance to various attacks such as man-in-the-middle attacks, replay attacks, impersonation attacks, privileged insider attacks, and ephemeral secret leakage attacks. The formal security verification using AVISPA regards the scheme as safe. In addition, the scheme supports critical features such as anonymity and untraceability within limited computational and communicational costs. A simulation of blockchain using Node.js shows only a linear increase in computation time with an increase in the number of blocks, and transactions, and an exponential increase with the number of nodes.

BPPS: Blockchain-Enabled Privacy-Preserving Scheme for Demand-Response Management in Smart Grid Environments

KiSung Park; JoonYoung Lee; Ashok Kumar Das; Youngho Park

IEEE Transactions on Dependable and Secure Computing, 20(2), 1719-1729.
https://doi.org/10.1109/TDSC.2022.3163138

Abstract

With the ongoing revolutionary growth of the industrial Internet of Things and smart grid networks, smart grid (SG) communication has been acknowledged as a next-generation network for intelligent and efficient electric power transmission. In SG networks, smart meters (SMs) generally send requests for electricity demand to service providers (SPs), which deal with the requests for efficient energy distribution. However, SGs experience many security issues with the deployed SMs and untrusted wireless communication. To tackle these security issues, we propose a privacy-preserving authentication scheme for demand response management in SGs, called BPPS. It can resist various attacks and achieve secure mutual authentication with key agreement; moreover, it provides integrity of demand-response data using blockchain.

Moreover, we perform the informal and formal (mathematical) security analysis to confirm that BPPS is secure against various attacks and achieves session key security, respectively. Furthermore, we conduct the performance and simulation analysis for SGs using NS3 and Ethereum testnet. Consequently, BPPS provides high-level security and can be applied to actual SG networks.

A Ripple for Change: Analysis of Frontrunning in the XRP Ledger

Vytautas Tumas, Beltran Borja Fiz Pontiveros, Christof Ferreira Torres, Radu State

In 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-9).
https://doi.org/10.1109/ICBC56567.2023.10174999

Abstract

Blockchains are disrupting traditional finance by reducing the number of intermediaries and providing transparency. Blockchains, however, come with their own set of prominent issues. One such challenge is frontrunning. Attackers try to influence the transaction order so that their transaction executes before their victims' transaction. While frontrunning is a well-studied topic on Ethereum, it is unknown whether other blockchains are also susceptible to such attacks. One proposed defence strategy against frontrunning attacks is to randomize the transaction execution order. XRP Ledger is the highest-value blockchain to use such a strategy. Furthermore, it runs a Decentralized Exchange, which provides ample frontrunning opportunities. Therefore, in the context of XRP Ledger, we examine whether randomized transaction order provides sufficient protection against frontrunning. Our results show that the mechanism embedded in the XRP Ledger protocol is insufficient to prevent these attacks. We showcase two strategies to perform frontrunning attacks. The first, “naive” strategy, uses randomly generated accounts, whereas the second uses carefully selected accounts to improve the attack's success. Based on our analysis of the XRP Ledgers' historical data, we estimate that attackers could generate up to approx. 1.4M USD profit over two months, provided they succeeded to frontrun every opportunity.

A Code-Based Hybrid Signcryption Scheme

Jean Belo Klamti, M. Anwarul Hasan

Journal of Mathematical Cryptology, 17(1), 20220002.
https://doi.org/10.1515/jmc-2022-0002

Abstract

A key encapsulation mechanism (KEM) that takes as input an arbitrary string, i.e., a tag, is known as tag-KEM, while a scheme that combines signature and encryption is called signcryption. In this article, we present a code-based signcryption tag-KEM scheme. We utilize a code-based signature and an IND CCA2 - (adaptive chosen ciphertext attack) secure version of McEliece’s encryption scheme. The proposed scheme uses an equivalent subcode as a public code for the receiver, making the NP-completeness of the subcode equivalence problem be one of our main security assumptions. We then base the signcryption tag-KEMto design a code-based hybrid signcryption scheme. A hybrid scheme deploys asymmetric- as well as symmetric-key

encryption. We give security analyses of both our schemes in the standard model and prove that they are secure against IND CCA2 - (indistinguishability under adaptive chosen ciphertext attack) and SUF CMA - (strong existential unforgeability under chosen message attack).

Bitcoin Enhanced Proof-of-Stake Security: Possibilities and Impossibilities

Ertem Nusret Tas; David Tse; Fangyu Gai; Sreeram Kannan; Mohammad Ali Maddah-Ali; Fisher Yu

In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 126-145)
https://doi.org/10.1109/SP46215.2023.10179426

Abstract

Bitcoin is the most secure blockchain in the world, supported by the immense hash power of its Proof-of-Work miners. Proof-of-Stake chains are energy-efficient, have fast finality but face several security issues: susceptibility to non-slashable long-range safety attacks, low liveness resilience and difficulty to bootstrap from low token valuation. We show that these security issues are inherent in any PoS chain without an external trusted source, and propose a new protocol, Babylon, where an off-the-shelf PoS protocol checkpoints onto Bitcoin to resolve these issues. An impossibility result justifies the optimality of Babylon. A use case of Babylon is to reduce the stake withdrawal delay: our experimental results show that this delay can be reduced from weeks in existing PoS chains to less than 5 hours using Babylon, at a transaction cost of less than 10K USD per annum for posting the checkpoints onto Bitcoin.

03 SECTION

Evaluating Decentralized Finance (DeFi) and Exchange Dynamics

Decentralized exchanges leveraging Automated Market Maker protocols contribute to the adoption of Decentralized Finance (DeFi). Yet, as the crypto market sees participation from non-crypto native industries, arbitrage opportunities in mature cryptocurrencies are set to wane. On another front, Decentralized Autonomous Organizations (DAOs) are redefining organizational norms given their distinctive governance structures. As such, researchers are finding new ways to evaluate crypto markets and governance using advanced analytical techniques including the market impact of trading behaviors.

SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols

Jiahua Xu, Krzysztof Paruch, Simon Cousaert, Yebo Feng

ACM Computing Surveys, 55(11), 1-50.
https://doi.org/10.1145/3570639

Abstract

As an integral part of the decentralized finance (DeFi) ecosystem, decentralized exchanges (DEXs) with automated market maker (AMM) protocols have gained massive traction with the recently revived interest in blockchain and distributed ledger technology (DLT) in general. Instead of matching the buy and sell sides, automated market makers (AMMs) employ a peer-to-pool method and determine asset price algorithmically through a so-called conservation function. To facilitate the improvement and development of AMM-based decentralized exchanges (DEXs), we create the first systematization of knowledge in this area. We first establish a general AMM framework describing the economics and formalizing the system's state-space representation. We then employ our framework to systematically compare the top AMM protocols' mechanics, illustrating their conservation functions, as well as slippage and divergence loss functions. We further discuss security and privacy concerns, how they are enabled by AMM-based DEXs' inherent properties, and explore mitigating solutions. Finally, we conduct a comprehensive literature review on related work covering both DeFi and conventional market microstructure.

Arbitrage in the Market for Cryptocurrencies

Tommy Crépellière, Matthias Pelster, Stefan Zeisberger

Journal of Financial Markets, 100817.
https://doi.org/10.1016/j.finmar.2023.100817

Abstract

Arbitrage opportunities in markets for cryptocurrencies are well-documented. In this paper, we confirm that they exist; however, their magnitude decreased greatly from April 2018 onward. Analyzing various trading strategies, we show that it is barely possible to exploit existing price differences since then. We discuss and test several mechanisms that may be responsible for the increased market efficiency and find that informed trading is correlated with a reduction in arbitrage opportunities.

Reaching for Yield in Decentralized Financial Markets

Patrick Augustin, Roy Chen-Zhang, Donghwa Shin

Available at SSRN 4063228.
http://dx.doi.org/10.2139/ssrn.4063228

Abstract

Among the ecosystem of decentralized financial services, yield farming is a complex investment strategy with hidden downside risks providing opportunities for passively earning income. We characterize the risk and return characteristics of yield farming and show that yield farms

dynamically compete for liquidity by offering high yields that are advertised as salient headline rates. Levering the full history of transactions available through blockchain data, we show that investors chase farms with high yields and that those farms with the highest headline rates record the most negative risk-adjusted returns. That underperformance is amplified by small investment stakes and investor mistakes. Overall, our evidence is consistent with salience theory that may underpin reaching for yield behavior. We exploit heterogeneity in shocks to the information set of yield farmers to show that improved information disclosure and reduction in product complexity reduces yield chasing and improves investor performance. Since yield farming is easily accessible to retail investors, our analysis has important implications for the regulation of decentralized finance.

Decentralized Governance and Digital Asset Prices

Ian Appel, Jillian Grennan

Available at SSRN 4367209

http://dx.doi.org/10.2139/ssrn.4367209

Abstract

Decentralized Autonomous Organizations ("DAOs") are crypto-native organizations run without centralized management. Instead, managerial and financial decisions are made by token holders via a decentralized voting process. Taking advantage of the transparency of blockchains, we gather data on DAOs and 10,764 of their improvement proposals. We offer a novel classification of DAOs' objectives and governance structures. We also examine the relation between governance and performance. Aspects of governance that promote broad participation in decision-making or enhance security are associated with positive abnormal returns. Barriers to the adoption of improvement proposals are associated with negative abnormal returns. Overall, our findings provide some of the first evidence on the governance of this new organizational form.

Cryptoasset Networks: Flows and Regular Players in Bitcoin and XRP

Hideaki Aoyama ,Yoshi Fujiwara, Yoshimasa Hidaka ,Yuichi Ikeda

PloS one, 17(8), e0273068.

https://doi.org/10.1371/journal.pone.0273068

Abstract

Cryptoassets flow among players as recorded in the ledger of blockchain for all the transactions, comprising a network of players as nodes and flows as edges. The last decade, on the other hand, has witnessed repeating bubbles and crashes of the price of cryptoassets in exchange markets with fiat currencies and other cryptos. We study the relationship between these two important aspects of dynamics, one in the bubble/crash of price and the other in the daily network of crypto, by investigating Bitcoin and XRP. We focus on “regular players” who frequently appear on a weekly basis during a period of time including bubble/crash, and quantify each player’s role with respect to outgoing and incoming flows by defining flow-weighted frequency. During the most significant period of one-year starting from the winter of

2017, we discovered the structure of three groups of players in the diagram of flow-weighted frequency, which is common to Bitcoin and XRP in spite of the different nature of the two cryptos. By examining the identity and business activity of some regular players in the case of Bitcoin, we can observe different roles of them, namely the players balancing surplus and deficit of cryptoassets (Bal-branch), those accumulating the cryptoassets (In-branch), and those reducing it (Out-branch). Using this information, we found that the regime switching among Bal-, In-, Out-branches was presumably brought about by the regular players who are not necessarily dominant and stable in the case of Bitcoin, while such players are simply absent in the case of XRP. We further discuss how one can understand the temporal transitions among the three branches.

Projecting XRP Price Burst by Correlation Tensor Spectra of Transaction Networks

Abhijit Chakraborty, Tetsuo Hatsuda, Yuichi Ikeda

Scientific Reports, 13(1), 4718
https://doi.org/10.1038/s41598-023-31881-5

Abstract

Cryptoassets are becoming essential in the digital economy era. XRP is one of the large market cap cryptoassets. Here, we develop a novel method of correlation tensor spectra for the dynamical XRP networks, which can provide an early indication for XRP price. A weighed directed weekly transaction network among XRP wallets is constructed by aggregating all transactions for a week. A vector for each node is then obtained by embedding the weekly network in continuous vector space. From a set of weekly snapshots of node vectors, we construct a correlation tensor. A double singular value decomposition of the correlation tensors gives its singular values. The significance of the singular values is shown by comparing with its randomize counterpart. The evolution of singular values shows a distinctive behavior. The largest singular value shows a significant negative correlation with XRP/USD price. We observe the minimum of the largest singular values at the XRP/USD price peak during the first week of January 2018. The minimum of the largest singular value during January 2018 is explained by decomposing the correlation tensor in the signal and noise components and also by evolution of community structure.

Is Your Digital Neighbor a Reliable Investment Advisor?

Daisuke Kawai, Alejandro Cuevas, Bryan Routledge, Kyle Soska, Ariel Zetlin-Jones, Nicolas Christin

In Proceedings of the ACM Web Conference 2023 (WWW '23), pp. 3581-3591)
https://doi.org/10.1145/3543507.3583502

Abstract

The web and social media platforms have drastically changed how investors produce and consume financial advice. Historically, individual investors were often relying on newsletters and related prospectus backed by the reputation and track record of their issuers. Nowadays, financial advice is frequently offered online, by anonymous or pseudonymous parties with little at stake. As such, a natural question is to investigate whether these modern financial "influencers" operate in good faith, or whether they might be misleading their followers intentionally. To start answering this question, we obtained data from a very large cryptocurrency derivatives exchange, from which we derived individual trading positions. Some of the investors on that platform elect to link to their Twitter profiles. We were thus able to compare the positions publicly espoused on Twitter with those actually taken in the market. We discovered that 1) staunchly "bullish" investors on Twitter often took much more moderate, if not outright opposite, positions in their own trades when the market was down, 2) their followers tended to align their positions with bullish Twitter outlooks, and 3) moderate voices on Twitter (and their own followers) were on the other hand far more consistent with their actual investment strategies. In other words, while social media advice may attempt to foster a sense of camaraderie among people of like-minded beliefs, the reality is that this is merely an illusion, which may result in financial losses for people blindly following advice.

04 SECTION

Advancing Regulatory and Legal Frameworks

Regulation of digital assets and blockchain technology remains nascent and fragmented across industries and regions. With the rise of DAOs and advancements in digital asset valuation and allocation models, academic research can provide insights for future regulatory guidelines, ensuring secure global interoperability of blockchain systems to harness the full potential of this technology.

How Should We Regulate Cryptocurrencies via Consensus?: A Strategic Framework for Optimal Legal Transaction Throughput

Aditya Ahuja, Vinay Ribeiro, Ranjan Pal

Distributed Ledger Technologies: Research and Practice, 2(1), 1-20.
https://doi.org/10.1145/3567593

Abtract

Permissionless blockchain consensus protocols have been leveraged for defining decentralized economies for the (commercial or private) trade of virtual and physical assets, using cryptocurrencies. In most instances, the assets being traded are regulated, which mandates that the legal right to their trade and their trade value are determined by the governmental regulator of the jurisdiction in which the trade occurs. Unfortunately, existing blockchains do not formalize proposal of legal cryptocurrency transactions, as part of the execution of their respective consensus protocols, resulting in illegal activities in the associated crypto-economies. In this contribution, unlike existing non-consensus solutions, which are prone to be more compute-time and audit-time intensive, we present a novel regulatory framework for blockchain protocols, for ensuring legal transaction confirmation as part of the blockchain consensus. As per our regulatory framework, we derive, through a stochastic game analysis, block proposal strategies under which legal transaction throughput supersedes throughput of traditional transactions, which are, in the worst case, an indifferentiable mix of legal and illegal transactions. Finally, we show that when a majority of the consensus protocol participants are licensed by the regulator to propose legal transactions, there exists a fair consensus execution policy to maximize the legal transaction throughput in the blockchain network.

The Global Challenge of Digital Asset Regulations

Bianca Kremer, Kevin Werbach

In Competition Policy International TechREG Chronicle, February 2022 Issue
https://bdap.wharton.upenn.edu/cpi-regtech-the-global-challenge-of-digital-asset-regulation/

Abstract

Digital assets add complexity to an already complex global financial system. Jurisdictions around the world are adopting measures to respond to ongoing developments. As activity grows, bespoke legal regimes are either in place, in development, or under discussion around the world. Regulatory interest now extends beyond token offerings and exchanges to include stablecoins, decentralized finance (“DeFi”), non-fungible tokens (“NFTs”) and decentralized autonomous organizations (“DAOs”). In this article, we take a bird’s eye view of the global state of digital asset regulation. While some countries have adopted a hostile posture, most regulators are attempting to balance concerns about potential harms against potential benefits. Despite concerns about uncertainty and fragmentation, the regulatory environment is gradually adapting to the novel challenges of digital assets and blockchain-based financial services.

Regulation of Cryptoassets (2nd Edition)

Carol Goforth, Yuliya Guseva

West Academic Publishing, 2023
https://faculty.westacademic.com/Book/Detail/339461

Abstract

The materials in this book are designed to look at cryptoassets and the expanding world of cryptotransactions to examine the regulatory regimes surrounding these assets and markets and how those regimes are developing. Because the technology behind and legal reaction to crypto are evolving so rapidly and are still in the early stages, it is not possible to create a traditional casebook that focuses only on settled judicial opinions to illustrate relevant legal issues and rules. These materials therefore look at various statutes, rules, and regulatory structures that predate the advent of crypto along with mission and informational statements promulgated by the agencies most closely involved with regulation of cryptoassets and cryptotransactions. The book also covers recent administrative and judicial decisions addressing crypto-related issues and involving cryptoasset and fintech firms, as well as a range of other materials such as pleadings, briefs, agency guidelines and proposed regulations, and academic commentary. The book examines a broad range of regulatory regimes, and although it focuses primarily on U.S. federal law, it also introduces applicable state law, international law, and European Union law.

Digital Assets and Regulatory Fragmentation: The SEC versus the CFTC

Yuliya Guseva, Irena Hutton

Boston College Law Review (forthcoming 2023), Available at SSRN.
https://ssrn.com/abstract=4249503

Abstract

In 2022, the White House released a regulatory framework calling for a whole-of-government approach to digital asset innovations. Although justified and necessary, this systems-based strategy discounts the reality that U.S. financial regulation is fundamentally fragmented. There are signs of a turf war between the major digital asset regulators (the SEC and the CFTC). Both agencies claim jurisdiction over overlapping classes of digital assets, and several congressional bills recently proposed to radically redistribute this jurisdiction.

Policy reforms under the conditions of regulatory fragmentation need empirical data comparing the effect of actions of the regulators involved. Empirical literature on digital asset innovations, however, has not paid sufficient attention to the impact of the U.S.-specific factors such as regulatory fragmentation. Nor has it explored the importance of U.S. regulators to global digital asset markets. We aim to fill this gap, contribute to scholarship on financial innovation, and equip policymakers with necessary empirical data.

Our empirical study compares how the SEC and the CFTC regulate crypto primarily via enforcement and how the global digital asset market reacts to the agencies. The market distinguishes between the Commissions and reacts particularly negatively to SEC enforcement.

It is erroneous to assume, however, that this is because crypto markets reject formal law or strong enforcement. Digital asset prices exhibit a more positive reaction to U.S.-led antifraud efforts, indicating that investors understand the value of market integrity. The unfavorable reaction to regulation may be explained by who enforces substantive law (the CFTC or the SEC). We provide theoretical explanations and underscore that, while U.S.-led enforcement is generally viewed as costly, some types of regulation may have the potential to improve market quality with positive valuation implications. We hope that our analysis will provide new information to scholars and policymakers in evaluating the merits of financial reforms, addressing the current fragmentation in financial regulation, resolving turf wars, and advancing the efforts to promote a "whole-of-government" approach to digital asset innovation.

Decentralized Autonomous Organization Toolkit

David Gogel, Bianca Kremer, Aiden Slavin, Kevin Werbach

World Economic Forum (2023, January 17).
https://www.weforum.org/reports/decentralized-autonomous-organization-toolkit/

Abstract

Collaboratively governed and code-driven, decentralized autonomous organizations (DAOs) are engaged in nothing less than an experiment to reimagine how we connect, collaborate and create. Although DAOs today manage billions of dollars' worth of assets, engage millions of contributors and operate across industries as diverse as finance and philanthropy, basic questions regarding operations, governance, law and policy are only just beginning to be addressed by policy-makers, regulators and entrepreneurs. The result of a collaboration involving more than 100 experts spanning the public and private sectors, the DAO Toolkit provides resources for developers, policy-makers and other stakeholders seeking to engage with the DAO ecosystem.

Digital Assets: Pricing, Allocation and Regulation

Reena Aggarwal, Paolo Tasca

Cambridge University Press, 2023
https://books.google.ca/books?id=Y5sM0AEACAAJ

Abstract

he book deepens our understanding of the complex inter-relations between traditional and digital assets. The first of its kind to present a comprehensive review of studies on valuation and pricing of digital assets in general, it introduces new models of portfolio strategies with digital assets.

05 SECTION

Conducting Taxonomy, Benchmarking, Validation and State-of-Art Surveys

Blockchain programmability can, at times, be a bit daunting given the intricacies and complexity, but this is where the technical possibilities shine. From taxonomy and benchmarking to smart contract validation, the framework and trustworthiness of a blockchain is tested in the details. Moreover, cutting-edge surveys in the areas of benchmarking, DeFi and layer-2 protocols are providing valuable insight into consensus algorithms, yield farming, smart contract validation and monitoring, as well as peer-to-peer network topology analysis.

Benchmarking Blockchains: The Case of XRP Ledger and Beyond

Marios Touloupou, Klitos Christodoulou, Antonis Inglezakis, Elias Iosif, Marinos Themistocleous

In Proceedings of the 55th Hawaii International Conference on System Sciences, 2022
http://hdl.handle.net/10125/80070

Abstract

Blockchain and Distributed Ledger Technologies appear to be at a worldwide threshold of acceptance and adoption. Since their inception, several innovative projects have been proposing solutions to the blockchain trilemma, improving blockchain features and its technical limitations. However, the adoption of blockchain as a technology requires a comprehensive understanding and characterization of its technical aspects. The latter introduces an uncertainty for an organization to decide which blockchain protocol best meets its needs and demands. In general, there is a lack of proper testing and software engineering practices for assessing the usage of different blockchain protocols and understanding their performance. Toward that direction, this paper presents an architecture for a blockchain benchmarking framework that aims at the deployment and evaluation of different blockchain protocols. Moreover, we introduce a set of modules for testing and evaluating their behavior under different test-cases and scenarios. To illustrate the usefulness of the proposed architecture we demonstrate an instantiation with the deployment of a private XRPL Network. The experiments conducted in this work were focused on how XRPL behaves under heavy load.

A Systematic Literature Review Toward a Blockchain Benchmarking Framework

Marios Touloupou, Marinos Themistocleous, Elias Iosif, Klitos Christodoulou

IEEE Access
https://doi.org/10.1109/ACCESS.2022.3188123

Abstract

Blockchain is a disruptive technology that focuses on the safe exchange of data between several distributed applications. Despite its widespread adoption, there are areas that require further research towards the understanding of their performance characteristics. In addition, consensus algorithms, a vital part of blockchain, require a more comprehensive understanding of their technical principles and characteristics. Along with the design of different types of consensus algorithms, several challenges, such as system scalability and power consumption, have been raised. Therefore, more comprehensive research is needed to investigate the degree to which consensus algorithms are built and how they perform. To this end, this study extends the body of knowledge and contributes towards the assessment of blockchain protocol performance. We present a comprehensive taxonomy of selected studies on blockchain performance, identifying similarities and differences while attempting to identify existing work on simulators and benchmarking frameworks that aim to explore the performance of blockchain-enabled consensus algorithms.

A Taxonomy for Decentralized Finance

Johannes Rude Jensen, Victor von Wachter, Omri Ross

Complex Systems Informatics and Modeling Quarterly, (26), 46-54.
https://doi.org/10.7250/csimq.2021-26.03

Abstract

Decentralized Finance ('DeFi') has gained tremendous momentum over the past three years by using novel approaches to disintermediating financial institutions in the provision of financial services. However, empirical research in this field is still rare, and a more comprehensive understanding of the domain is a missing component in academic research. This paper develops a taxonomy based on a comprehensive literature analysis to structure this emerging field systematically. The taxonomy includes three perspectives (strategy, organization, technology) and seven dimensions (blockchain, value proposition, token type, business process, price mechanism, protocol type, integration type) as well as thirty-six characteristics. The application of the taxonomy to 278 DeFi start-ups reveals that most of the DeFi start-ups focus on Ethereum (36.3%) and have a focus on analytics and automation (52%), while, surprisingly only a few incorporate decentralized governance approaches (3.3%), provide decentralized exchanges (14%) or integrate off-chain data.

Topology Analysis of the XRP Ledger

Vytautas Tumas, Sean Rivera, Damien Magoni, Radu State

In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 1277-1284).
https://doi.org/10.1145/3555776.3577611

Abstract

XRP Ledger is one of the oldest, well-established blockchains. Despite the popularity of the XRP Ledger, little is known about its underlying peer-to-peer network. The structural properties of a network impact its efficiency, security and robustness. We aim to close the knowledge gap by providing a detailed analysis of the XRP overlay network.

In this paper we examine the graph-theoretic properties of the XRP Ledger peer-to-peer network and its temporal characteristics. We crawl the XRP Ledger over two months and collect 1,290 unique network snapshots. We uncover a small group of nodes that act as a networking backbone. In addition, we observe a high network churn, with a third of the nodes changing every five days. Our findings have strong implications for the resilience and safety of the XRP Ledger.

Verifying SOLIDITY Smart Contracts via Communication Abstraction in SMARTACE

Scott Wesley, Maria Christakis, Jorge A. Navas, Richard Trefler, Valentin Wüstholz, Arie Gurfinkel

In Verification, Model Checking, and Abstract Interpretation: 23rd International Conference, VMCAI 2022, Proceedings 23 (pp. 425-449).
https://doi.org/10.1007/978-3-030-94583-1_21

Abstract

Solidity smart contract allow developers to formalize financial agreements between users. Due to their monetary nature, smart contracts have been the target of many high-profile attacks. Brute-force verification of smart contracts that maintain data for up to users is intractable. In this paper, we present SmartACE, an automated framework for smart contract verification. To ameliorate the state explosion induced by large numbers of users, SmartACE implements local bundle abstractions that reduce verification from arbitrarily many users to a few representative users. To uncover deep bugs spanning multiple transactions, SmartACE employs a variety of techniques such as model checking, fuzzing, and symbolic execution. To illustrate the effectiveness of SmartACE, we verify several contracts from the popular OpenZeppelin library: an access-control policy and an escrow service. For each contract, we provide specifications in the Scribble language and apply fault injection to validate each specification. We report on our experience integrating Scribble with SmartACE, and describe the performance of SmartACE on each specification.

A Framework of Runtime Monitoring for Correct Execution of Smart Contracts

R. K. Shyamasundar

In International Conference on Blockchain (ICBC 2022), pp. 92-116
https://doi.org/10.1007/978-3-031-23495-8_7

Abstract

Smart contracts have been subjected to several attacks that have exploited various vulnerabilities of languages like Solidity, which has resulted in huge financial losses. The functioning and deployment of smart contracts are somewhat different from classical programming environments. Once a smart contract is up and running, changing it, is very complicated and nearly infeasible as the contract is expected to be immutable when created. If we find a defect in a deployed smart contract, a new version of the contract has to be created and deployed with concurrence from the stakeholders. Further, when a new version of an existing contract is deployed, data stored in the previous contract does not get transferred automatically to the newly refined contract. We have to manually initialize the new contract with the past data which makes it very cumbersome and not very trustworthy. As neither updating a contract nor rolling back an update is possible, it greatly increases the complexity of implementation and places a huge responsibility while being deployed initially on the blockchain.

The main rationale for smart contracts has been to enforce contracts safely among the stakeholders. In this paper, we shall discuss a framework for runtime monitoring to prevent the exploitation of a major class of vulnerabilities using the programmers' annotations given in the smart contracts coded in Solidity. We have chosen several phrases for annotation mimicking declarations of concurrent programming languages so that the underlying run-time monitors can be automatically generated. The annotations simply reflect the intended constraints on the execution of programs relative to the object state relative to observables like method calls, exceptions, etc. Such a framework further adds to the advantage of debugging at the source level as the original structure is preserved and also enhances the trust of the user as the run-time monitoring assertion logs provide a rough proof-outline of the contract.

A Survey of Layer-Two Blockchain Protocols

Ankit Gangwal, Haripriya Ravali Gangavalli, Apoorva Thirupathi

Journal of Network and Computer Applications
https://doi.org/10.1016/j.jnca.2022.103539

Abstract

After the success of the Bitcoin blockchain, came several cryptocurrencies and blockchain solutions in the last decade. Nonetheless, Blockchain-based systems still suffer from low transaction rates and high transaction processing latencies, which hinder blockchains' scalability. An entire class of solutions, called Layer-1 scalability solutions, have attempted to incrementally improve such limitations by adding/modifying fundamental blockchain attributes. Recently, a completely different class of works, called Layer-2 protocols, have emerged to tackle the blockchain scalability issues using unconventional approaches. Layer-2 protocols improve transaction processing rates, periods, and fees by minimizing the use of underlying slow and costly blockchains. In fact, the main chain acts just as an instrument for trust establishment and dispute resolution among Layer-2 participants, where only a few transactions are dispatched to the main chain. Thus, Layer-2 blockchain protocols have the potential to transform the domain. However, rapid and discrete developments have resulted in diverse branches of Layer-2 protocols. In this work, we systematically create a broad taxonomy of such protocols and implementations. We discuss each Layer-2 protocol class in detail and also elucidate their respective approaches, salient features, requirements, etc. Moreover, we outline the issues related to these protocols along with a comparative discussion. Our thorough study will help further systematize the knowledge dispersed in the domain and help the readers to better understand the field of Layer-2 protocols.

Reap the Harvest on Blockchain: A Survey of Yield Farming Protocols

Jiahua Xu; Yebo Feng

IEEE Transactions on Network and Service Management, 20(1), 858-869.
https://doi.org/10.1109/TNSM.2022.3222815

Abstract

Yield farming represents an immensely popular asset management activity in decentralized finance (DeFi). It involves supplying, borrowing, or staking crypto assets to earn an income in forms of transaction fees, interest, or participation rewards at different DeFi marketplaces. In this systematic survey, we present yield farming protocols as an aggregation-layer constituent of the wider DeFi ecosystem that interact with primitive-layer protocols such as decentralized exchanges (DEXs) and loanable funds (PLFs) protocol for loanable funds (PLF). We examine the yield farming mechanism by first studying the operations encoded in the yield farming smart contracts, and then performing stylized, parameterized simulations on various yield farming strategies. We conduct a thorough literature review on related work, and establish a framework for yield farming protocols that takes into account pool structure, accepted token types, and implemented strategies. Using our framework, we characterize major yield aggregators in the market including Yearn Finance, Beefy, and Badger DAO. Moreover, we discuss anecdotal attacks against yield aggregators and generalize a number of risks associated with yield farming.

06 SECTION

Dedicated Efforts to Blockchain for Social Good

Blockchain plays a pivotal role in addressing gaps in the global financial system and financial equity as well as promoting sustainable energy. For instance, when integrated with the Internet of Things (IoT), blockchain offers a seamless solution for long-term energy and environmental monitoring. Additionally, asset tokenization on blockchain can drive financial innovation and foster more sustainable systems. The utility of real-world asset tokenization is extensive — ranging from energy trading to environment accounting — and has the power to reshape our approach to sustainability and social giving. A closer look at cryptocurrency engagement during COVID-19 highlights nuanced participation across diverse demographics. Collectively, these insights offer a holistic view of the evolving crypto industry.

Technology-enabled Financing of Sustainable Infrastructure: A Case for Blockchains and Decentralized Oracle Networks

Kenneth Hsien Yung Chung, Dan Li, Peter Adriaens

Technological Forecasting and Social Change, 187, 122258.
https://doi.org/10.1016/j.techfore.2022.122258

Abstract

The capital required to maintain infrastructure in good repair falls short globally. This is commonly referred to as the “infrastructure finance gap”. To address climate change, transitioning from conventional to sustainable infrastructure further imposes financing challenges. This study employs the Model approach to justify and predict how blockchain technologies can leverage infrastructure data to close the finance gap by introducing new financing mechanisms. A semisystematic literature review was carried out for infrastructure finance, sustainable infrastructure and smart cities finance mechanisms, as well as blockchains and oracles. Conventional infrastructure finance via debt and equity lacks benchmarks that reflect the risk-return characteristics of the asset class. Performance-based financing addresses this issue by integrating performance data in valuations. However, a lack of trust in data veracity remains. Blockchains provide trust and transparency in data and transactions. They utilize oracles to access off-chain information for on-chain decision-making. With smart contracts and decentralized oracle networks, a general approach is presented where data from internet-of-things inform on-chain transactions, delivering performance benchmarks that accurately reflect the risk-return characteristics in an infrastructure investment. Capital can then be more readily deployed, thus closing the finance gap. An end-to-end example of financing sustainable stormwater infrastructure, Open Storm, is also presented.

Towards Inclusive and Sustainable Infrastructure Development Through Blockchain-enabled Asset Tokenization: An Exploratory Case Study

Y. Tian, R. E. Minchin, K. Chung, J. Woo and P. Adriaens

In IOP Conference Series: Materials Science and Engineering (Vol. 1218, No. 1, p. 012040)
https://doi.org/10.1088/1757-899X/1218/1/012040

Abstract

Infrastructure development is a key to supporting the economy and building social resilience. Unfortunately, existing infrastructure financing models struggle with multiple issues to close the widening financial gap and integrate environmental, social, and governance (ESG) factors to improve resilience and achieve sustainable growth. With the emergence of innovative technology, blockchain-enabled asset tokenization shows the potential to create a new economic model to integrate non-financial values, such as positive social and environmental impacts, into tradable cryptographic tokens. Tokenization offers opportunities to generate long-term positive social and environmental impacts, along with better financial returns, which further improves the profitability and bankability of infrastructure projects. SolarCoin, WePower Token, and ZiyenCoin are analyzed in this exploratory case study research to demonstrate how blockchain-enabled asset tokenization can be applied to infrastructure development. It

is identified that tokenization promotes inclusiveness and sustainability through shareholder empowerment, incentive monetization, and finance optimization. Obstacles hindering the broader adoption of tokenization and policy implications are also discussed.

Blockchain + IoT Sensor Network to Measure, Evaluate and Incentivize Personal Environmental Accounting and Efficient Energy Use in Indoor Spaces

Nan Ma, Alex Waegel, Max Hakkarainen, William W. Braham, Lior Glass, Dorit Aviv

Applied Energy, 332, 120443.
https://doi.org/10.1016/j.apenergy.2022.120443

Abstract

Electric demand flexibility in buildings is highly dependent on occupant behavior. Evaluating and incentivizing these behaviors can provide grid-responsive support and encourage demand response (DR) participation. To achieve these goals, we developed an infrastructure for connecting Internet of Things (IoT) sensors to a distributed ledger (blockchain network) for long-term monitoring of energy and environmental performance. This study presents a novel Blockchain + IoT paradigm for the building science research community, applied in a real-world application. This Blockchain + IoT Network (BIN) uses Raspberry Pi minicomputers as platforms for connecting sensors to a blockchain network, to provide and analyze real-time indoor environmental quality (IEQ), energy, and carbon intensity data. As part of the study, we propose various metrics to evaluate the environmental footprints of building users. Novel algorithms for normalizing energy usage and carbon intensity, with consideration of a variety of related environmental factors, are executed as smart contracts on the blockchain network. All measurements and the smart contract transactions are reported and visualized on live dashboards. The use of smart contract allocates tokens based on the reward algorithms to incentivize individuals' energy conservation, and similarly to DR pricing, can help influence occupant consumption patterns towards carbon reduction goals. We further test the smart contract's algorithm in relation to real sensor data we have collected in two case studies: single-unit households and carbon intensity in the energy market. The combination of proposed metrics translates measured sensor data into token awards, demonstrates upper and lower limits dictated by the grid generation mix profile, and indicates that there is the potential for load shifting to minimize carbon emissions without considering the scale of consumption.

Blockchain Applications in the Energy Industry

Soheil Saraji, Christelle Khalaf

In Regulatory Aspects of Artificial Intelligence on Blockchain, pp. 159-180
https://doi.org/10.4018/978-1-7998-7927-5.ch008

Abstract

The current energy transition from a fossil-fuel-based economy to a zero-carbon has significantly accelerated in recent years, as the largest emitters have committed to achieving carbon-neutral goals in the next 20-30 years. The energy industry transition is characterized by modernization through digital technologies, increased renewable energy generation, and environmental sustainability. Blockchain technology can play a significant role in providing secure digital distributed platforms facilitating digitization, decarbonization, and decentralization of the energy systems. Several promising blockchain applications in the energy sector are under research and development, including peer-to-peer energy trading; carbon monitoring, management, and trading; and IoT-enabled electric grid management. However, several challenges are slowing down the commercialization of these applications, including outdated legislation and regulations, slow pace of adaptation from the traditional energy industry, and risks associated with the new, untested technology.

COVID-19 Cryptocurrency Investment: Wealth Disparities and Portfolio Diversification

Juliet Elu, Miesha Williams

Journal of Economics, Race, and Policy, 6, 53-59
https://doi.org/10.1007/s41996-022-00108-6

Abstract

The introduction of cryptocurrency and blockchain technology has provided many investors the option to engage in the market, diversify their portfolios, and accumulate wealth. The high return on cryptocurrency during the pandemic has served as an incentive for all ethnic groups to participate in the market. Cryptocurrency is perceived as a hedging instrument for wealth prospects across races during COVID-19. Considering the return on investment, to what extent is blockchain a good hedging instrument for minority investors? Using weekly trade price data from Yahoo Finance, market valuations from coinranking.com, and asset/equity variables from the Federal Reserve Bank, this paper examines investment strategies of different racial/ethnic groups in cryptocurrency during the pandemic in a panel data model from 2019 to 2021. Should investors use public coins such as Bitcoin and Ethereum as part of their investment portfolio mix during the pandemic? We find that an increase in the price of Bitcoin and other cryptocurrencies during the pandemic may repress the investment strategy for marginalized groups.

07 SECTION

Conclusion

This year's UBRI report marks a steady, but significant shift in blockchain research across academia. As the technology evolves, it's important that new findings are able to reach all corners of the world. Esteemed global institutions have unveiled research projects that not only dissect the intricate technicalities of blockchain but also shape international strategies and policies. UBRI will continue to cement its role as a beacon of excellence in the blockchain sphere and a testament to the decentralization of knowledge.

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

جامعة نيويورك ابوظبي NYU Abu Dhabi

Princeton University

Háskólinn í Reykjavík Reykjavik University

Rutgers

Toronto Metropolitan University

Stanford University

清华大学 Tsinghua University

The University of North Carolina at Chapel Hill

UCL

u b Universität Bern

Berkeley University of California

University of Cape Town IYUNIVESITHI YASEKAPA • UNIVERSITEIT VAN KAAPSTAD

O 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 UZH

Università di Trento

USP Universidade de São Paulo

University of Toronto

Columbia University in the City of New York

Trinity College Dublin Coláiste na Tríonóide, Baile Átha Cliath The University of Dublin

ie Business School

Victoria University Melbourne Australia

ASU Arizona State University

Portland State University

EPITA School of Engineering & Computer Science

Royal University of Bhutan

NOVA Nova School of Business & Economics

University of Wyoming

EUI

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 around the world 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 more than 50 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.