rippleimpact | university blockchain research initiative

UBRI Forges New Paths in Blockchain Research

We thank Yebo Feng for his extensive research and dedicated support scanning through hundreds of academic pieces to hand select the best of 2020-2021.

Contents

Introduction

Ongoing academic analysis of the past, present and future of blockchain is a key component in developing advanced insight and identifying promising innovations for a still relatively new and complex technology. Given the vast number of publications in blockchain and related fields, identifying relevant and applicable research can be a daunting task. This summary aims to alleviate these logistical challenges by identifying and organizing breakthrough academic contributions made from 2020-2021 by researchers at universities that are supported through the University Blockchain Research Initiative (UBRI).*

The academic contributions referenced in this report range from open source software, academic journal articles, and academic conference papers, to books and applications, with the hope that this information may identify common themes and findings and catalyze further cutting-edge scientific discovery and technological innovation. This summary is also intended to enable academic knowledge exchange and collaboration, and to inspire future research.

*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.

1

A Deep Dive on Blockchain Today

Since the onset of mainstream adoption of blockchain-based systems and digital financial technologies, both use cases and end users have grown dramatically.

Blocks continue to expand, and the underlying technology continues to evolve and improve. As early blockchain systems have advanced and broadened, they have become more difficult to track and analyze. Therefore, it is vital to continue to probe, measure and analyze current “live” blockchain systems to evaluate the effectiveness of their design, understand the real-world implications of the technology, and inspire future applications, scientific theories, and system designs.

Stability and Scalability of Blockchain Systems

Aditya Gopalan, Abishek Sankararaman, Anwar Walid, Sriram Vishwanath

In Proceedings of the ACM on Measurement and Analysis of Computing Systems, 4(2), 1-35.
https://doi.org/10.1145/3392153

Abstract

The blockchain paradigm provides a mechanism for content dissemination and distributed consensus on Peer-to-Peer (P2P) networks. While this paradigm has been widely adopted in industry, it has not been carefully analyzed in terms of its network scaling with respect to the number of peers. Applications for blockchain systems, such as cryptocurrencies and IoT, require this form of network scaling. In this paper, we propose a new stochastic network model for a blockchain system. We identify a structural property called one-endedness, which we show to be desirable in any blockchain system as it is directly related to distributed consensus among the peers. We show that the stochastic stability of the network is sufficient for the one-endedness of a blockchain. We further establish that our model belongs to a class of network models, called monotone separable models. This allows us to establish upper and lower bounds on the stability region. The bounds on stability depend on the connectivity of the P2P network through its conductance and allow us to analyze the scalability of blockchain systems on large P2P networks. We verify our theoretical insights using both synthetic data and real data from the Bitcoin network.

Revisiting Transactional Statistics of High-scalability Blockchains

Benjamin Livshits, Daniel Perez, Jiahua Xu

In Proceedings of the ACM Internet Measurement Conference (IMC), pp. 535-550. 2020.
https://doi.org/10.1145/3419394.3423628

Abstract

Scalability has been a bottleneck for major blockchains such as Bitcoin and Ethereum. Despite the significantly improved scalability claimed by several high-profile blockchain projects, there has been little effort to understand how their transactional throughput is being used. In this paper, we examine recent network traffic of three major high-scalability blockchains—EOSIO, Tezos and XRP Ledger (XRPL)—over a period of seven months. Our analysis reveals that only a small fraction of the transactions are used for value transfer purposes. In particular, 96% of the transactions on EOSIO were triggered by the airdrop of a currently valueless token; on Tezos, 76% of throughput was used for maintaining consensus; and over 94% of transactions on XRPL carried no economic value. We also identify a persisting airdrop on EOSIO as a DoS attack and detect a two-month-long spam attack on XRPL. The paper explores the different designs of the three blockchains and sheds light on how they could shape user behavior.

The Cost of Bitcoin Mining Has Never Really Increased

Yo-Der Song, Tomaso Aste

Frontiers in Blockchain 3 (2020): 44.
https://doi.org/10.3389/fbloc.2020.565497

Abstract

The Bitcoin network is burning a large amount of energy for mining. In this paper, we estimate the lower bound for the global mining energy cost for a period of 10 years from 2010 to 2020, taking into account changes in energy costs, improvements in hashing technologies and hashing activity. We estimate energy cost for Bitcoin mining using two methods: Brent Crude oil prices as a global standard and regional industrial electricity prices weighted by the share of hashing activity. Despite a 10-billion-fold increase in hashing activity and a 10-million-fold increase in total energy consumption, we find the cost relative to the volume of transactions has not increased nor decreased since 2010. This is consistent with the perspective that, in order to keep the Blockchain system secure from double spending attacks, the proof or work must cost a sizable fraction of the value that can be transferred through the network. We estimate that in the Bitcoin network this fraction is of the order of 1%.

Bitcoin: A Natural Oligopoly

Nick Arnosti, Matt Weinberg

In 10th Innovations in Theoretical Computer Science, ITCS 2019 (p. 5).
https://arxiv.org/abs/1811.08572

Abstract

Although Bitcoin was intended to be a decentralized digital currency, in practice, mining power is quite concentrated. This fact is a persistent source of concern for the Bitcoin community. We provide an explanation using a simple model to capture miners' incentives to invest in equipment. In our model, n miners compete for a prize of fixed size. Each miner chooses an investment q_i, incurring cost $c_i q_i$, and then receives reward $\frac{q_i^\alpha}{\sum_j q_j^\alpha}$, for some $\alpha \geq 1$. When $c_i = c_j$ for all i, j, and $\alpha = 1$, there is a unique equilibrium where all miners invest equally. However, we prove that under seemingly mild deviations from this model, equilibrium outcomes become drastically more centralized. In particular,

- When costs are asymmetric, if miner i chooses to invest, then miner j has market share at least $1 - \frac{c_j}{c_i}$. That is, if miner j has costs that are (e.g.) 20% lower than those of miner i, then miner j must control at least 20% of the total mining power.
- In the presence of economies of scale $(\alpha > 1)$, every market participant has a market share of at least $1 - \frac{1}{\alpha}$, implying that the market features at most $\frac{\alpha}{\alpha - 1}$ miners in total.

We discuss the implications of our results for the future design of cryptocurrencies. In particular, our work further motivates the study of protocols that minimize "orphaned blocks", proof-of-stake protocols, and incentive compatible protocols.

Dynamics of Fintech Terms in News and Blogs and Specialization of Companies of The Fintech Industry

Fabio Ciulla, Rosario N. Mantegna

Chaos: An Interdisciplinary Journal of Nonlinear Science 30, no. 8 (2020): 083112.
https://doi.org/10.1063/5.0004487

Abstract

We perform a large scale analysis of a list of fintech terms in (i) news and blogs in the English language and (ii) professional descriptions of companies operating in many countries. The occurrence and the co-occurrence of fintech terms and locutions show a progressive evolution of the list of fintech terms in a compact and coherent set of terms used worldwide to describe fintech business activities. By using methods of complex networks that are specifically designed to deal with heterogeneous systems, our analysis of a large set of professional descriptions of companies shows that companies having fintech terms in their description present over-expressions of specific attributes of country, municipality, and economic sector. By using the approach of statistically validated networks, we detect geographical and economic over-expressions of a set of companies related to the multi-industry, geographically, and economically distributed fintech movement.

We present a study of the rapid development of a highly innovative industry. Specifically, we investigate the fintech industry, i.e., the industry developing technological innovations, technology-based products, and services for the financial sector. This industry presents a rather fast dynamics and a worldwide diffusion. These aspects make an analysis based on a big data approach very difficult due to the unavoidable variety, biases, and inconsistencies of the best available databases. In our study, we overcome these limitations by using the methodology of statistically validated networks (SVNs). In fact, this methodology is able to highlight over-expressed relationships between pairs of elements of bipartite networks obtained from heterogeneous sets. By investigating a list of terms used in a large corpus of news and blogs and in a large collection of professional descriptions of companies working worldwide, and by using the methodology of statistically validated networks, we detect over-expressions of some fintech terms in the descriptions of companies with specific attributes of geographical location and of economic activity.

Proof-of-Stake Mining Games with Perfect Randomness

Matheus V. X. Ferreira, S. Matthew Weinberg

In Proceedings of the 22nd ACM Conference on Economics and Computation (EC 2021).
https://arxiv.org/abs/2107.04069

Abstract

Proof-of-Stake blockchains based on a longest-chain consensus protocol are an attractive energy-friendly alternative to the Proof-of-Work paradigm. However, formal barriers to "getting the incentives right" were recently discovered, driven by the desire to use the blockchain itself as a source of pseudorandomness.

We consider instead a longest-chain Proof-of-Stake protocol with perfect, trusted, external randomness (e.g. a randomness beacon). We produce two main results.

First, we show that a strategic miner can strictly outperform an honest miner with just 32.8% of the total stake. Note that a miner of this size cannot outperform an honest miner in the Proof-of-Work model. This establishes that even with access to a perfect randomness beacon, incentives in Proof-of-Work and Proof-of-Stake longest-chain protocols are fundamentally different.

Second, we prove that a strategic miner cannot outperform an honest miner with 30.8% of the total stake. This means that, while not quite as secure as the Proof-of-Work regime, desirable incentive properties of Proof-of-Work longest-chain protocols can be approximately recovered via Proof-of-Stake with a perfect randomness beacon.

The space of possible strategies in a Proof-of-Stake mining game is significantly richer than in a Proof-of-Work game. Our main technical contribution is a characterization of potentially optimal strategies for a strategic miner, and in particular, a proof that the corresponding infinite-state MDP admits an optimal strategy that is positive recurrent.

2

Continued Advances in Blockchain and FinTech

Over the past few years, UBRI partners have contributed to significant innovations in blockchain and financial technologies, proposing new Byzantine fault tolerance consensus mechanisms, mutable blockchain systems, secure smart contract creation mechanisms, adaptive blockchain application interfaces, and more. These advances not only make the blockchain system more secure and efficient, but also broaden the range of possible use cases, opening up new possibilities.

FastPay: High-Performance Byzantine Fault Tolerant Settlement

Mathieu Baudet, George Danezis, Alberto Sonnino

In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT), pp. 163-177. 2020.
https://doi.org/10.1145/3419614.3423249

Abstract

FastPay allows a set of distributed authorities, some of which are Byzantine, to maintain a high-integrity and availability settlement system for pre-funded payments. It can be used to settle payments in a native unit of value (crypto-currency), or as a financial side-infrastructure to support retail payments in fiat currencies. FastPay is based on Byzantine Consistent Broadcast as its core primitive, foregoing the expenses of full atomic commit channels (consensus). The resulting system has low-latency for both confirmation and payment finality. Remarkably, each authority can be sharded across many machines to allow unbounded horizontal scalability. Our experiments demonstrate intra-continental confirmation latency of less than 100ms, making FastPay applicable to point of sale payments. In laboratory environments, we achieve over 80,000 transactions per second with 20 authorities—surpassing the requirements of current retail card payment networks, while significantly increasing their robustness.

Policy-based Chameleon Hash for Blockchain Rewriting with Black-box Accountability

Yangguang Tian, Nan Li, Yingjiu Li, Pawel Szalachowski, Jianying Zhou

In Annual Computer Security Applications Conference (ACSAC), pp. 813-828. 2020.
https://doi.org/10.1145/3427228.3427247

Abstract

Policy-based chameleon hash is a useful primitive for blockchain rewriting. It allows a party to create a transaction associated with an access policy, while another party who possesses enough rewriting privileges satisfying the access policy can rewrite the transaction. However, it lacks accountability. The chameleon trapdoor holder may abuse his/her rewriting privilege and maliciously rewrite the hashed object in the transaction without being identified. In this paper, we introduce policy-based chameleon hash with black-box accountability (PCHBA). Black-box accountability allows an attribute authority to link modified transactions to responsible transaction modifiers in case of dispute, in which any public user identifies those transaction modifiers from interacting with an access device/blackbox. We first present a generic framework of PCHBA. Then, we present a practical instantiation, showing its practicality through implementation and evaluation analysis.

Unveiling The Importance and Evolution of Design Components Through The "Tree of Blockchain"

Florian Spychiger, Paolo Tasca, Claudio J. Tessone

Frontiers in Blockchain 3 (2021): 60.
https://doi.org/10.3389/fbloc.2020.613476

Abstract

This study covers the evolutionary development of blockchain technologies over the last 11 years (2009–2019) and sheds lights on potential areas of innovation in heretofore unexplored sub-components. For this purpose, we collected and analyzed detailed data on 107 different blockchain technologies and studied their component-wise technological evolution. The diversity of their designs was captured by deconstructing the blockchains using the Tasca-Tessone taxonomy to build what we call the "tree of blockchain" composed of blockchain main and sub-components. With the support of information theory and phylogenetics, we found that most design explorations have been conducted within the components in the areas of consensus mechanisms and cryptographic primitives. We also show that some sub-components like Consensus Immutability and Failure Tolerance, Access and Control layer, and Access Supply Management have predictive power over other sub-components. We finally found that few dominant design models—the genetic driving clusters of Bitcoin, Ethereum, and XRP—influenced the evolutionary paths of most of the succeeding blockchains.

Decrypting Distributed Ledger Design—Taxonomy, Classification and Blockchain Community Evaluation

Mark C. Ballandies, Marcus M. Dapp, Evangelos Pournaras

Cluster Computing (2021): 1-22.
https://doi.org/10.1007/s10586-021-03256-w

Abstract

More than 1000 distributed ledger technology (DLT) systems raising $600 billion in investment in 2016 feature the unprecedented and disruptive potential of blockchain technology. A systematic and data-driven analysis, comparison and rigorous evaluation of the different design choices of distributed ledgers and their implications is a challenge. The rapidly evolving nature of the blockchain landscape hinders reaching a common understanding of the techno-socio-economic design space of distributed ledgers and the cryptoeconomies they support. To fill this gap, this paper makes the following contributions: (i) A conceptual architecture of DLT systems with which (ii) a taxonomy is designed and (iii) a rigorous classification of DLT systems is made using real-world data and wisdom of the crowd. (iv) A DLT design guideline is the end result of applying machine learning methodologies on the classification data. Compared to related work and as defined in earlier taxonomy theory, the proposed taxonomy is highly comprehensive, robust, explanatory and extensible. The findings of this paper can provide new insights and better understanding of the key design choices evolving the modeling complexity of DLT systems, while identifying opportunities for new research contributions and business innovation.

A Language-Based Approach to Smart Contract Engineering

John Kolb

Dissertation, University of California, Berkeley, 2020.
https://www2.eecs.berkeley.edu/Pubs/TechRpts/2020/EECS-2020-220.pdf

Abstract

Blockchain-based smart contracts have emerged as a popular means of enforcing agreements among a collection of parties without a prior assumption of trust. However, it has proven difficult to write correct contracts that are robust when operating in the adversarial environment of public blockchains. This thesis evaluates the ability of a domain-specific contract programming language to support the expression and systematic testing of practical smart contracts. We present the design, implementation, and evaluation of Quartz, a contract language based on the state machine model of execution.

The design and evaluation of Quartz is grounded in a suite of case study smart contracts. These are intended to span a wide range of application scenarios and design patterns encountered in practice by contract developers. The language's implementation is organized around the translation of a contract to two targets: a formal specification expressed in TLA+ and an implementation expressed in Solidity. Through its support for model checking contract specifications, Quartz enables the discovery of implementation flaws identical to those that have compromised real-world smart contracts. Moreover, its generated Solidity code imposes at most minor execution overhead compared to equivalent handwritten code. Finally, we discuss Quartz's future potential to validate contracts against economic notions of correctness, which are often central concerns in contract design yet are not addressed by current verification techniques.

A Blockchain-based Trust System for Decentralised Applications: When Trustless Needs Trust

Nguyen Truonga, Gyu Myoung Lee, Kai Sun, Florian Guitton, YiKe Guo

Future Generation Computer Systems (2021).
https://doi.org/10.1016/j.future.2021.05.025

Abstract

Blockchain technology has been envisaged to commence an era of decentralised applications and services (DApps) without the need for a trusted intermediary. Such DApps open a marketplace in which services are delivered to end-users by contributors which are then incentivised by cryptocurrencies in an automated, peer-to-peer, and trustless fashion. However, blockchain, consolidated by smart contracts, only ensures on-chain data security, autonomy and integrity of the business logic execution defined in smart contracts. It cannot guarantee the quality of service of DApps, which entirely depends on the services' performance. Thus, there is a critical need for a trust system to reduce the risk of dealing with fraudulent counterparts in a blockchain network. These reasons motivate us to develop a fully decentralised trust framework deployed on top of a blockchain platform, operating along with DApps in the marketplace to demoralise deceptive entities while encouraging trustworthy ones. The trust system works as an underlying decentralised service providing a feedback mechanism for end-users and maintaining trust relationships among them in the ecosystem accordingly. We believe this research fortifies the DApps ecosystem by introducing an universal trust middleware for DApps as well as shedding light on the implementation of a decentralised trust system.

3

Security in Blockchain

Security is the foundation of blockchain technology. In order to preserve and strengthen this foundation, UBRI partners have explored possible threat models of blockchain, proposed advanced cryptography and encryption algorithms, and modified or developed entirely new comprehensive analysis methodologies. UBRI-supported researchers believe that blockchains and financial technologies can become more secure and dependable over time - in part, in anticipation of more powerful computing and security threats from bad actors - and they will continue to work towards supporting this outcome.

Compositional Security for Reentrant Applications

Ethan Cecchetti, Siqiu Yao, Haobin Ni, Andrew C. Myers

In Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P 2021), 2021.
https://www.cs.cornell.edu/andru/papers/oakland21/

Abstract

The disastrous vulnerabilities in smart contracts sharply remind us of our ignorance: we do not know how to write code that is secure in composition with malicious code. Information flow control has long been proposed as a way to achieve compositional security, offering strong guarantees even when combining software from different trust domains. Unfortunately, this appealing story breaks down in the presence of reentrancy attacks. We formalize a general definition of reentrancy and introduce a security condition that allows software modules like smart contracts to protect their key invariants while retaining the expressive power of safe forms of reentrancy. We present a security type system that provably enforces secure information flow; in conjunction with run-time mechanisms, it enforces secure reentrancy even in the presence of unknown code; and it helps locate and correct recent high-profile vulnerabilities.

BlockSci: Design and Applications of a Blockchain Analysis Platform

Harry Kalodner, Malte Möser, Kevin Lee, Steven Goldfeder, Martin Plattner, Alishah Chator, ArvindNarayanan

In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), pp. 2721-2738. 2020.
https://www.usenix.org/conference/usenixsecurity20/presentation/kalodner

Abstract

Analysis of blockchain data is useful for both scientific research and commercial applications. We present BlockSci, an open-source software platform for blockchain analysis. BlockSci is versatile in its support for different blockchains and analysis tasks. It incorporates an in-memory, analytical (rather than transactional) database, making it orders of magnitudes faster than using general-purpose graph databases. We describe BlockSci's design and present four analyses that illustrate its capabilities, shedding light on the security, privacy, and economics of cryptocurrencies.

Replay Attacks and Defenses Against Cross-shard Consensus in Sharded Distributed Ledgers

Alberto Sonnino, Shehar Bano, Mustafa Al-Bassam, George Danezis

In Proceedings of 2020 IEEE European Symposium on Security and Privacy (Euro S&P), pp. 294-308. 2020.
https://doi.org/10.1109/EuroSP48549.2020.00026

Abstract

We present a family of replay attacks against sharded distributed ledgers targeting cross-shard consensus protocols, such as the recently proposed Chainspace and Omniledger. They allow an attacker, with network access only, to double-spend or lock resources with minimal efforts. The attacker can act independently without colluding with any nodes, and succeed even if all nodes are honest; most of the attacks can also exhibit themselves as faults under periods of asynchrony. These attacks are effective against both shard-led and client-led cross-shard consensus approaches. We present Byzcuit-a new cross-shard consensus protocol that is immune to those attacks. We implement a prototype of Byzcuit and evaluate it on a real cloud-based testbed, showing that our defenses impact performance minimally, and overall performance surpasses previous works.

Winkle: Foiling Long-Range Attacks in Proof-of-Stake Systems

Sarah Azouvi, George Danezis, Valeria Nikolaenko

In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, pp. 189-201. 2020.
https://doi.org/10.1145/3419614.3423260

Abstract

Winkle protects any validator-based byzantine fault tolerant consensus mechanisms, such as those used in modern Proof-of-Stake blockchains, against long-range attacks where old validators' signature keys get compromised. Winkle is a decentralized secondary layer of client-based validation, where a client includes a single additional field into a transaction that they sign: a hash of the previously sequenced block. The block that gets a threshold of signatures (confirmations) weighted by clients' coins is called a "confirmed" checkpoint. We show that under plausible and flexible security assumptions about clients the confirmed checkpoints can not be equivocated. We discuss how client key rotation increases security, how to accommodate for coins' minting and how delegation allows for faster checkpoints. We evaluate checkpoint latency experimentally using Bitcoin and Ethereum transaction graphs, with and without delegation of stake.

Proof-Carrying Data without Succinct Arguments

Benedikt Bunz, Alessandro Chiesa, William Lin, Pratyush Mishra, Nicholas Spooner

In 2021 Annual International Cryptology Conference (CRYPTO 2021).
https://eprint.iacr.org/2020/1618

Abstract

Proof-carrying data (PCD) is a powerful cryptographic primitive that enables mutually distrustful parties to perform distributed computations that run indefinitely. Known approaches to construct PCD are based on succinct non-interactive arguments of knowledge (SNARKs) that have a succinct verifier or a succinct accumulation scheme.

In this paper we show how to obtain PCD without relying on SNARKs. We construct a PCD scheme given any non-interactive argument of knowledge (e.g., with linear-size arguments) that has a split accumulation scheme, which is a weak form of accumulation that we introduce.

Moreover, we construct a transparent non-interactive argument of knowledge for R1CS whose split accumulation is verifiable via a (small) constant number of group and field operations. Our construction is proved secure in the random oracle model based on the hardness of discrete logarithms, and it leads, via the random oracle heuristic and our result above, to concrete efficiency improvements for PCD.

Along the way, we construct a split accumulation scheme for Hadamard products under Pedersen commitments and for a simple polynomial commitment scheme based on Pedersen commitments. Our results are supported by a modular and efficient implementation.

Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms

Crystal Andrea Roma, Chi-En Amy Tai, M. Anwar Hasan

IEEE Access 9 (2021): 71295-71317.
https://doi.org/10.1109/ACCESS.2021.3077843

Abstract

Classical cryptographic schemes in use today are based on the difficulty of certain number theoretic problems. Security is guaranteed by the fact that the computational work required to break the core mechanisms of these schemes on a conventional computer is infeasible; however, the difficulty of these problems would not withstand the computational power of a large-scale quantum computer. To this end, the post-quantum cryptography (PQC) standardization process initiated by the National Institute of Standards and Technology (NIST) is well underway. In addition to the evaluation criteria provided by NIST, the energy consumption of these candidate algorithms is also an important criterion to consider due to the use of battery-operated devices, high-performance computing environments where energy costs are critical, as well as in the interest of green computing. In this paper, the energy consumption of PQC candidates is evaluated on an Intel Core i7-6700 CPU using PAPI, the Performance API. The energy measurements are categorized based on their proposed security level and cryptographic functionality. The results are then further subdivided based on the underlying mechanism used in order to identify the most energy-efficient schemes. Lastly, IgProf is used to identify the most energy-consuming subroutines within a select number of submissions to highlight potential areas for optimization.

4

Blockchain for Social Good

The dependable, traceable, immutable, and decentralized features of blockchain-based systems make this technology applicable to more than just financial and Internet sectors. Recent developments in this space have shed light on its potential to optimize how civil society functions, improving a wide range of applications including medical systems, welfare systems, electrical grids, supply chains, and other socially impactful use cases. Blockchain also shows promise as a tool for making financial systems and services more inclusive, affordable and participatory—a growing focus for university researchers globally.

Applying Blockchain Technology to Address the Crisis of Trust During the COVID-19 Pandemic

Anjum Khurshid

JMIR medical informatics 8, no. 9 (2020): e20477.
https://doi.org/10.2196/20477

Abstract

Background: The widespread death and disruption caused by the COVID-19 pandemic has revealed deficiencies of existing institutions regarding the protection of human health and well-being. Both a lack of accurate and timely data and pervasive misinformation are causing increasing harm and growing tension between data privacy and public health concerns.

Objective: This aim of this paper is to describe how blockchain, with its distributed trust networks and cryptography-based security, can provide solutions to data-related trust problems.

Methods: Blockchain is being applied in innovative ways that are relevant to the current COVID-19 crisis. We describe examples of the challenges faced by existing technologies to track medical supplies and infected patients and how blockchain technology applications may help in these situations.

Results: This exploration of existing and potential applications of blockchain technology for medical care shows how the distributed governance structure and privacy-preserving features of blockchain can be used to create “trustless” systems that can help resolve the tension between maintaining privacy and addressing public health needs in the fight against COVID-19.

Conclusions: Blockchain relies on a distributed, robust, secure, privacy-preserving, and immutable record framework that can positively transform the nature of trust, value sharing, and transactions. A nationally coordinated effort to explore blockchain to address the deficiencies of existing systems and a partnership of academia, researchers, business, and industry are suggested to expedite the adoption of blockchain in health care.

Using Blockchain Technology to Mitigate Challenges in Service Access for the Homeless and Data Exchange Between Providers: Qualitative Study

Anjum Khurshid, Vivian Rajeswaren, Steven Andrews

Journal of Medical Internet Research 22, no. 6 (2020): e16887.
https://doi.org/10.2196/16887

Abstract

Background: In the homeless population, barriers to housing and supportive services include a lack of control or access to data. Disparate data formats and storage across multiple organizations hinder up-to-date intersystem access to records and a unified view of an individual's health and documentation history. The utility of blockchain to solve interoperability in health care is supported in recent literature, but the technology has yet to be tested in real-life conditions encompassing the complex regulatory standards in the health sector.

Objective: This study aimed to test the feasibility and performance of a blockchain system in a homeless community to securely store and share data across a system of providers in the health care ecosystem.

Methods: We performed a series of platform demonstrations and open-ended qualitative feedback interviews to determine the key needs and barriers to user and stakeholder adoption. Account creation and data transactions promoting organizational efficiency and improved health outcomes in this population were tested with homeless users and service providers.

Results: Persons experiencing homelessness and care organizations could successfully create accounts, grant and revoke data sharing permissions, and transmit documents across a distributed network of providers. However, there were issues regarding the security of shared data, user experience and adoption, and organizational preparedness for service providers as end users. We tested a set of assumptions related to these problems within the project time frame and contractual obligations with an existing blockchain-based platform.

Conclusions: Blockchain technology provides decentralized data sharing, validation, immutability, traceability, and integration. These core features enable a secure system for the management and distribution of sensitive information. This study presents a concrete evaluation of the effectiveness of blockchain through an existing platform while revealing limitations from the perspectives of user adoption, cost-effectiveness, scalability, and regulatory frameworks.

Blockchain Technology in the Food Industry: A Review of Potentials, Challenges and Future Research Directions

Abderahman Rejeb, John G. Keogh, Suhaiza Zailani, Horst Treiblmaier, Karim Rejeb

Logistics 4, no. 4 (2020): 27.
https://doi.org/10.3390/logistics4040027

Abstract

Blockchain technology has emerged as a promising technology with far-reaching implications for the food industry. The combination of immutability, enhanced visibility, transparency and data integrity provides numerous benefits that improve trust in extended food supply chains (FSCs). Blockchain can enhance traceability, enable more efficient recall and aids in risk reduction of counterfeits and other forms of illicit trade. Moreover, blockchain can enhance the integrity of credence claims such as sustainably sourced, organic or faith-based claims such as kosher or halal by integrating the authoritative source of the claim (e.g., the certification body or certification owner) into the blockchain to verify the claim integrity and reassure business customers and end consumers. Despite the promises and market hype, a comprehensive overview of the potential benefits and challenges of blockchain in FSCs is still missing. To bridge this knowledge gap, we present the findings from a systematic review and bibliometric analysis of sixty-one (61) journal articles and synthesize existing research. The main benefits of blockchain technology in FCSs are improved food traceability, enhanced collaboration, operational efficiencies and streamlined food trading processes. Potential challenges include technical, organizational and regulatory issues. We discuss the theoretical and practical implications of our research and present several ideas for future research.

The Influence of Blockchain-based Food Traceability On Retailer Choice: The Mediating Role of Trust

Marion Garaus, Horst Treiblmaier

Food Control 129 (2021): 108082.
https://doi.org/10.1016/j.foodcont.2021.108082

Abstract

In the last decades, numerous food scandals have attracted policy makers' interest and subsequently induced retailers to actively improve food safety. Blockchain technology allows consumers to track the flow of food products and reduce food fraud, such as counterfeiting, dilution, or adulteration. Using three experiments conducted with Austrian business students as well as an online convenience sample, we investigate how the traceability of food products impacts consumers' trust in the retailer and subsequently influences consumers' retailer choice. Our model further considers retailer familiarity and the disclosure of blockchain benefits as important moderators of the impact of blockchain-based traceability systems on trust in the retailer. The model was tested using ANOVA, ANCOVA, and Hayes' PROCESS models. In terms of

fostering consumer trust, the findings show that retailers who are unfamiliar to consumers profit more from the use of blockchain technology than do better-known retailers. Moreover, informing consumers about specific blockchain benefits strengthens the positive effects of a blockchain-based traceability system.

Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda

Horst Treiblmaier, Abderahman Rejeb, Andreas Strebinger

Smart Cities 3, no. 3 (2020): 853-872.
https://doi.org/10.3390/smartcities3030044

Abstract

The term “Smart City” denotes a comprehensive concept to alleviate pending problems of modern urban areas which have developed into an important work field for practitioners and scholars alike. However, the question remains as to how cities can become “smart”. The application of information technology is generally considered a key driver in the “smartization” of cities. Detailed frameworks and procedures are therefore needed to guide, operationalize, and measure the implementation process as well as the impact of the respective technologies. In this paper, we discuss blockchain technology, a novel driver of technological transformation that comprises a multitude of underlying technologies and protocols, and its potential impact on smart cities. We specifically address the question of how blockchain technology may benefit the development of urban areas. Based on a comprehensive literature review, we present a framework and research propositions. We identify nine application fields of blockchain technology in the smartization of cities: (1) healthcare, (2) logistics and supply chains, (3) mobility, (4) energy, (5) administration and services, (6) e-voting, (7) factory, (8) home and (9) education. We discuss current developments in these fields, illustrate how they are affected by blockchain technology and derive propositions to guide future research endeavors.

Community Energy Groups: Can They Shield Consumers from the Risks of Using Blockchain for Peer-to-Peer Energy Trading?

Alexandra Schneiders, David Shipworth

Energies 14, no. 12 (2021): 3569.
https://doi.org/10.3390/en14123569

Abstract

Peer-to-peer (P2P) energy trading is emerging as a new mechanism for settling the exchange of energy between renewable energy generators and consumers. P2P provides a mechanism for local balancing when it is facilitated through distributed ledgers (`blockchains'). Energy communities across Europe have uncovered the potential of this technology and are currently running pilots to test its applicability in P2P energy trading. The aim of this paper is to assess, using legal literature and legislation, whether the legal forms available to energy communities in the United Kingdom (UK) can help resolve some of the uncertainties around the individual use of blockchain for P2P energy trading. This includes the legal recognition of `prosumers', the protection of their personal data, as well as the validity of `smart contracts' programmed to trade energy on the blockchain network. The analysis has shown that legal entities, such as Limited Liability Partnerships and Co-operative Societies, can play a crucial role in providing the necessary framework to protect consumers engaging in these transactions. This is particularly the case for co-operatives, given that they can hold members liable for not respecting the rules set out in their (compulsory) governing document. These findings are relevant to other European countries, where the energy co-operative model is also used.

5

Reshaping The Financial System

New financial technologies will bring potentially transformative changes to the current global financial system. Central Banks are experimenting with digital currencies (CBDCs) as a complement to traditional fiat currencies due to their secure, efficient structure. Central Banks are also exploring the potential for CBDCs to make their national and regional economies more efficient, inclusive, and equitable. A wave of new financial derivatives continue to be brought to market, decentralized finance protocols have been proposed to better manage digital assets, and a new generation of trading platforms has brought users fairer and more effective bidding mechanisms.

Liquidations: DeFi on a Knife-edge

Daniel Perez, Sam M. Werner, Jiahua Xu, Benjamin Livshits

The 25th International Conference on Financial Cryptography and Data Security (FC 2021).
https://fc21.ifca.ai/papers/144.pdf

Abstract

The trustless nature of permissionless blockchains renders overcollateralization a key safety component relied upon by decentralized finance (DeFi) protocols. Nonetheless, factors such as price volatility may undermine this mechanism. In order to protect protocols from suffering losses, undercollateralized positions can be liquidated. In this paper, we present the first in-depth empirical analysis of liquidations on protocols for loanable funds (PLFs). We examine Compound, one of the most widely used PLFs, for a period starting from its conception to September 2020. We analyze participants' behavior and risk-appetite in particular, to elucidate recent developments in the dynamics of the protocol. Furthermore, we assess how this has changed with a modification in Compound's incentive structure and show that variations of only 3% in an asset's dollar price can result in over 10m USD becoming liquidable. To further understand the implications of this, we investigate the efficiency of liquidators. We find that liquidators' efficiency has improved significantly over time, with currently over 70% of liquidable positions being immediately liquidated. Lastly, we provide a discussion on how a false sense of security fostered by a misconception of the stability of non-custodial stablecoins, increases the overall liquidation risk faced by Compound participants.

A Digital Currency Architecture for Privacy and Owner-Custodianship

Geoffrey Goodell, Hazem Danny Al-Nakib, Paolo Tasca

Future Internet 13, no. 5 (2021): 130.
https://doi.org/10.3390/fi13050130

Abstract

In recent years, electronic retail payment mechanisms, especially e-commerce and card payments at the point of sale, have increasingly replaced cash in many developed countries. As a result, societies are losing a critical public retail payment option, and retail consumers are losing important rights associated with using cash. To address this concern, we propose an approach to digital currency that would allow people without banking relationships to transact electronically and privately, including both e-commerce purchases and point-of-sale purchases that are required to be cashless. Our proposal introduces a government-backed, privately-operated digital currency infrastructure to ensure that every transaction is registered by a bank or money services business, and it relies upon non-custodial wallets backed by privacy-enhancing technology, such as blind signatures or zero-knowledge proofs, to ensure that transaction counterparties are not revealed. Our approach to digital currency can also facilitate more efficient and transparent clearing, settlement, and management of systemic risk. We argue that our system can restore and preserve the salient features of cash, including privacy,

owner-custodianship, fungibility, and accessibility, while also preserving fractional reserve banking and the existing two-tiered banking system. We also show that it is possible to introduce regulation of digital currency transactions involving non-custodial wallets that unconditionally protect the privacy of end-users.

Digital Currency and Economic Crises: Helping States Respond

Geoffrey Goodell, Hazem Danny Al-Nakib, Paolo Tasca

Systemic Risk Centre (SRC) Special Papers SP 20.

https://www.systemicrisk.ac.uk/publications/special-papers/digital-currency-and-economic-crises-helping-states-respond

Abstract

The current crisis, at the time of writing, has had a profound impact on the financial world, introducing the need for creative approaches to revitalising the economy at the micro level as well as the macro level. In this informal analysis and design proposal, we describe how infrastructure for digital assets can serve as a useful monetary and fiscal policy tool and an enabler of existing tools in the future, particularly during crises, while aligning the trajectory of financial technology innovation toward a brighter future. We propose an approach to digital currency that would allow people without banking relationships to transact electronically and privately, including both internet purchases and point-of-sale purchases that are required to be cashless. We also propose an approach to digital currency that would allow for more efficient and transparent clearing and settlement, implementation of monetary and fiscal policy, and management of systemic risk. The digital currency could be implemented as central bank digital currency (CBDC), or it could be issued by the government and collateralised by public funds or Treasury assets. Our proposed architecture allows both manifestations and would be operated by banks and other money services businesses, operating within a framework overseen by government regulators. We argue that now is the time for action to undertake development of such a system, not only because of the current crisis but also in anticipation of future crises resulting from geopolitical risks, the continued globalisation of the digital economy, and the changing value and risks that technology brings.

Assets On The Blockchain: An Empirical Study of Tokenomics

Yuen C.Lo, Francesca Medda

Information Economics and Policy 53 (2020): 100881.

https://doi.org/10.1016/j.infoecopol.2020.100881

Abstract

Digital tokens linked to financial and economic ventures may have multiple functions and uses. In this work, we examine the relationship between various token functions and the market price of

the corresponding token. We consider 86 venture related blockchain tokens, and develop the analysis through a stepwise testing of four hypotheses using panel ordinary least squares with cluster-robust standard errors. We find that token functions are statistically significant in relation to token prices. In the absence of an established legal framework, we argue that our results complements recent regulatory actions identifying tokens to be investment contracts in a common venture.

AuditChain: A Trading Audit Platform Over Blockchain

Guy R. Vishnia, Gareth W. Peters

Frontiers in Blockchain 3 (2020): 9.
https://doi.org/10.3389/fbloc.2020.00009

Abstract

A blockchain architecture and solution is proposed to audit processing under exchange regulation for trading activity of exchanges. A particular focus is made on dark pools and periodic auctions. An architecture of the solution is described conceptually and an implementation of the proposed solution is made in .NET framework in C# via a RESTful API for chain interaction with the periodic auction venue. The framework proof of concept is tested for different efficiency and latency considerations. This opens the concept to significantly more detailed and extensive developments.

Entrepreneurial Finance and Moral Hazard: Evidence From Token Offerings

Paul P. Momtaz

Journal of Business Venturing (2020): 106001.
https://doi.org/10.1016/j.jbusvent.2020.106001

Abstract

This paper provides the first evidence of a moral hazard in signaling in an entrepreneurial finance context, by examining token offerings or Initial Coin Offerings (ICOs). Entrepreneurs' ability to signal quality is crucial to succeeding in the competition for growth capital. However, the absence of institutions that verify endogenous signals may induce a moral hazard in signaling. Consistent with this hypothesis, artificial linguistic intelligence indicates that token issuers systematically exaggerate information disclosed in whitepapers. Exaggerating entrepreneurs raise more funds in less time, suggesting that investors do not see through this practice initially. Eventually, the crowd learns about the exaggeration bias through trading with other investors. The resulting investor disappointment causes the cryptocurrency to depreciate and the probability of platform failure to increase.

6

Policy and Regulation

The majority of UBRI researchers agree that clearer and more comprehensive regulation in FinTech is essential to ensuring these technologies serve society's best interests and enable, not stifle, competition and innovation. Regulation should support a fully functioning and interoperable global economy, provide effective protection of consumers and collective public rights, enable continued adoption of FinTech, and support future development of blockchain technology. Researchers generally agree that in many countries laws and regulations that apply to traditional financial markets have been slow to adapt to financial technologies like blockchain and cryptocurrency. UBRI partners are playing an important role in defining future financial supervisory and regulatory models that can help inform appropriate policies and regulations.

The Law of Blockchain

Georgios Dimitropoulos

Washington Law Review: 95 (2020): 1117.

https://www.law.uw.edu/wlr/print-edition/print-edition/vol-95/3/the-law-of-blockchain

Abstract

Blockchain technology is a new general-purpose technology that poses significant challenges to the existing state of law, economy, and society. Blockchain has one feature that makes it even more distinctive than other disruptive technologies: it is, by nature and design, global and transnational. Moreover, blockchain operates based on its own rules and principles that have a law-like quality. What may be called the lex cryptographia of blockchain has been designed based on a rational choice vision of human behavior. Blockchain adopts a framing derived from neoclassical economics, and instantiates it in a new machinery that implements rational choice paradigms using blockchain in a semi-automatic way, across all spheres of life, and without regard to borders. Accordingly, a global law and crypto-economics movement is now emerging owing to the spread of blockchain.

This Article suggests that such a rational choice paradigm is an insufficient foundation for the future development of blockchain. It seeks to develop a new understanding of blockchain and its regulation through code according to the emerging "law and political economy" framework. Blockchain is much more than a machine that enables the automation of transactions according to a rational choice framework. Blockchain should instead be understood as a technological infrastructure. Acknowledging the infrastructural dimension of blockchain technology may help identify a new role for the law in its interaction with blockchain, as well as for government in its interaction with the new technology. More precisely, identifying blockchain as an "infrastructural commons" helps us recognize that law and regulation should not be relegated to the role of merely facilitating the operation of the invisible hand of the market by and within blockchain, but should rather acquire more active roles, such as safeguarding access on non-discriminatory terms to users, on a model with net neutrality and other public utility safeguards. The Article closes by proposing a "law and political economy" framework for blockchain that is based on principles of publicness, trust, and interoperability.

Transactional Scripts in Contract Stacks

Shaanan Cohney, David A. Hoffman

Minnesota Law Review: 105 (2020): 319.

https://dx.doi.org/10.2139/ssrn.3523515

Abstract

In conventional transactions, written contracts usually memorialize the terms of the commercial exchange. For deals in which some of the goods being transferred and the forum for the trade are digitized — as in the case of cryptocurrencies — parties may use computer code rather than a written contract to record their terms. Such pieces of code are sometimes called "smart

contracts" because they perform many of the same functions as contracts but are expressed in a computing language. Coded exchanges embody a potentially revolutionary contracting innovation. But they are difficult to assimilate into traditional contracting terminology, conceptual framing, and doctrine.

This Article begins by distilling the central legally and practically significant type of smart contracts — what we call "transactional scripts." It then develops an account of how these scripts, which operate on public blockchains, are created, the economic barriers to their adoption, and how they produce errors of legal significance. This account, in turn, allows us to more rigorously and accessibly situate transactional scripts in existing legal doctrine.

Commentators are enthusiastic about scripts in part because, the story goes, they are "self-executing" and require no third-party adjudicators. Yet we show that optimism to be unfounded by documenting how scripts, like ordinary contracts, can result in misunderstanding, frustrated intent, and failure.

When code misdelivers, disappointed parties will seek legal recourse. We argue that jurists should situate scripts within other legally operative statements and disclosures, or contract stacks. Precision about the relationship between script and stack sustains a novel framework, rooted in old doctrines of interpretation, parol evidence and equity, that will help jurists compile answers to the private law problems that digitized exchange entails.

VAT Treatment of Cryptocurrency Intermediation Services

Tina Ehrke-Rabel, Lily Zechner

Intertax 48, no. 5 (2020).

https://kluwerlawonline.com/journalarticle/Intertax/48.5/TAXI2020046

Abstract

The bitcoin blockchain was construed as a self-regulating system that would eliminate financial institutions serving as trusted third parties. Instead however, various new intermediaries emerged carrying out economic activities related to the blockchain. The most common 'gateways' are cryptocurrency exchange platforms and wallet providers. Moreover, bitcoin's main purpose has shifted from means of payment to speculation. In this article, the authors assess how the mentioned gateways are to be treated for value added tax purposes and challenge the Hedqvist-decision of the European Court of Justice against the backdrop of how bitcoins are being used today.

Crowd Arbitration: Blockchain Dispute Resolution

Aleksei Gudkov

Legal Issues in the Digital Age 2020.
https://lida.hse.ru/article/view/11780/12568

Abstract

Internet technology makes digital value transactions between anonymous individuals possible, but leaves unanswered the question of how to resolve disputes between unidentified parties. Blockchain dispute resolution platforms provide a response to this problem. In the social dispute resolution systems for blockchain currently in use, pseudo anonymous jurors can resolve disputes between pseudo anonymous parties. This paper presents Kleros as the most illustrative blockchain dispute resolution platform BDRP. To describe the features of the Kleros dispute resolution platform and the qualification of jurors, this research employs an online dispute resolution survey of both the jurors and stakeholders of the Kleros platform. This study raises important questions about key elements of procedural justice in resolution platforms for blockchain disputes. The research underlines the pros and cons of dispute resolution for crowdsourced blockchain and contributes to the further development of online dispute resolution systems. It tests the wisdom of the crowd as the core attribute of the resolution process in crowdsource disputes. Crowdsource mass dispute resolution, coupled with cooperative jurors and blockchain technology, could ensure greater effectiveness and fairness of the dispute resolution process, especially the adjudication of online small claims disputes.

UBRI University Partners



About UBRI

The University Blockchain Research Initiative (UBRI) is a global network of leading universities pursuing research, technology development, teaching and knowledge sharing on blockchain, cryptocurrency and related topics. UBRI was founded in 2018 by Ripple, a global blockchain-based financial technology company. Since UBRI's inception, Ripple has provided funding to more than 40 universities, which have produced hundreds of research projects, established new and modified curriculum for hundreds of university courses, and supported conferences and other academic convenings.