rippleimpact | university blockchain research initiative

BLOCKCHAIN TECHNOLOGY
RESEARCH HIGHLIGHTS FROM
UNIVERSITY PARTNERS

UBRI

Forges New Paths in Blockchain Research

2022

Since UBRI's inception in 2018, Ripple has funded over 40 university partnerships, supporting more than 500 research projects and new or modified course curricula for more than 280 university courses. Ongoing academic analysis of blockchain is a key component to advancing its innovation. This summary shares breakthrough academic contributions, made from 2021-2022 by researchers at UBRI supported universities.

The academic contributions referenced in this report range from open source software, academic journal articles and academic conference papers, to books and applications, each identifying common themes and findings as a catalyst for 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.

Contents

Introduction

Since its conceptualization, blockchain technology has witnessed continuous and rapid development, evolving into the foundation of various digital assets, robust cloud computing platforms, and dependable databases for tracking supply chain information. The growth of blockchain technology continues to bring profound changes across industries, not only in computer science, but also law, finance, and economics. This technology has the potential to help build a more trustworthy and efficient digital world. In an effort to further promote the evolution, development, and transformation of blockchain, Ripple founded the University Blockchain Research Initiative (UBRI), a global network of top universities pursuing public education, academic research, technical development, and innovation in blockchain, cryptocurrency, and related financial technologies (FinTech).

01 SECTION

Exploring Blockchain & DeFi

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

Blocks continue to expand, the underlying technology continues to evolve and improve, and decentralized finance (DeFi) protocols continue to popularize. As a result of these advancements, blockchain/DeFi systems have become more difficult to track and analyze, leading to intransparency of blockchain systems thus making it challenging for developers to troubleshoot and improve the systems. It is vital to continue to probe, measure and study 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.

A Taxonomy of Blockchain Oracles: The Truth Depends on the Question

Michael Bartholic, Aron Laszka, Go Yamamoto, Eric W. Burger

In Proceedings of 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).
https://doi.org/10.1109/ICBC54727.2022.9805555

Abstract

Blockchains benefit from guarantees of immutability and reliability due to their high redundancy and distributed nature. They show their value especially when operating between untrusted parties. Their functionality can be extended program-matically by smart contracts, but are limited by high costs of on-chain computation and only being able to truly trust data which is directly included on-chain. To attempt to bridge this limitation, blockchain oracles are introduced as a conceptual solution to act as a trusted source of information within the blockchain. The Oracle Problem emerges as we consider how one can introduce trusted information into a trust-free environment without compromising the validity of the blockchain. Many promising designs for oracle mechanisms have been proposed, but it is not readily apparent how one should assess the applicability of a given mechanism, nor the strengths and features between mechanisms. To be equipped to assess and categorize oracles, we must consider not just the possible answers, but the questions to which these oracles are trying to speak. Categorizing questions by their possible answering populations, we propose a framework for considering oracle questions and the context with which they are posed. We observe that there are limitations to what an oracle can hope to achieve, depending on the nature of the question, while noting the context in which a question exists can change what is viewed as true.

Towards Understanding Cryptocurrency Derivatives: A Case Study of BitMEX

**Kyle Soska, Jin-Dong Dong, Alex Khodaverdian, Ariel Zetlin-Jones,
Bryan Routledge, Nicolas Christin**

In Proceedings of the Web Conference 2021 (WWW).
https://doi.org/10.1145/3442381.3450059

Abstract

Since 2018, the cryptocurrency trading landscape has evolved from a collection of spot markets (fiat for cryptocurrency) to a hybrid ecosystem featuring complex and popular derivatives products. In this paper we explore this new paradigm through a study of BitMEX, one of the first and most successful derivatives platforms for leveraged cryptocurrency trading. BitMEX trades on average over 3 billion dollars worth of volume per day, and allows users to go long or short Bitcoin with up to 100x leverage. We analyze the evolution of BitMEX products—both settled and perpetual offerings that have become the standard across other cryptocurrency derivatives platforms. We additionally utilize on-chain forensics, public liquidation events, and a site-wide chat room to describe the diverse ensemble of amateur and professional traders that forms this community. These traders range from wealthy agents running automated strategies, to individuals trading small, risky positions and focusing on very short time-frames. Finally, we discuss how derivative trading has impacted cryptocurrency asset prices, notably how it has led to dramatic price movements in the underlying spot markets.

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%.

The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work

**Moritz Platt, Johannes Sedlmeir, Daniel Platt, Jiahua Xu, Paolo Tasca,
Nikhil Vadgama, Juan Ignacio Ibañez**

In Proceedings of 2021 IEEE 21st International Conference on Software Quality,
Reliability and Security Companion (QRS-C), 2021, pp. 1135-1144.
https://doi.org/10.1109/QRS-C55045.2021.00168

Abstract

Popular permissionless distributed ledger technology (DLT) systems using proof-of-work (PoW) for Sybil attack resistance have extreme energy requirements, drawing stern criticism from academia, business and the media. DLT systems building on alternative consensus mechanisms, particularly proof-of-stake (PoS), aim to address this downside. In this paper, we take an initial step towards comparing the energy requirements of such systems to understand whether they achieve this goal equally well. While multiple studies have analysed the energy demands of individual blockchains, little comparative work has been done. We approach this research gap by formalising a basic consumption model for PoS blockchains. Applying this model to six archetypal blockchains generates three main findings. First, we confirm the concerns around the energy footprint of PoW by showing that Bitcoin's energy consumption exceeds the energy consumption of all PoS-based systems analysed by at least three orders of magnitude. Second, we illustrate that there are significant differences in energy consumption among the PoS-based systems analysed, with permissionless systems having a larger energy footprint overall owing to their higher replication factor. Third, we point out that the type of hardware that validators use has a considerable impact on whether the energy consumption of PoS blockchains is comparable with or considerably larger than that of centralised systems.

On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols

Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, Arthur Gervais

In 2021 IEEE Symposium on Security and Privacy (SP), pp. 919-936. IEEE, 2021.
https://doi.org/10.1109/SP40001.2021.00113

Abstract

Decentralized Finance (DeFi) is a blockchain-assetenabled finance ecosystem with millions of daily USD transaction volume, billions of locked up USD, as well as a plethora of newly emerging protocols (for lending, staking, and exchanges). Because all transactions, user balances, and total value locked in DeFi are publicly readable, a natural question that arises is: how can we automatically craft profitable transactions across the intertwined DeFi platforms?

In this paper, we investigate two methods that allow us to automatically create profitable DeFi trades, one well-suited to arbitrage and the other applicable to more complicated settings. We first adopt the Bellman-Ford-Moore algorithm with DeFiPoster-ARB and then create logical DeFi protocol models for a theorem prover in DeFiPoster-SMT. While DeFiPoster-ARB focuses on DeFi transactions that form a cycle and performs very well for arbitrage, DeFiPoster-SMT can detect more complicated profitable transactions. We estimate that DeFiPoster-ARB and DeFiPoster-SMT can generate an average weekly revenue of 191.48 ETH (76,592 USD) and 72.44 ETH (28,976 USD) respectively, with the highest transaction revenue being 81.31 ETH (32,524 USD) and 22.40 ETH (8,960 USD) respectively. We further show that DeFiPoster-SMT finds the known economic bZx attack from February 2020, which yields 0.48M USD. Our forensic investigations show that this opportunity existed for 69 days and could have yielded more revenue if exploited one day earlier. Our evaluation spans 150 days, given 96 DeFi protocol actions, and 25 assets.

Looking beyond the financial gains mentioned above, forks deteriorate the blockchain consensus security, as they increase the risks of double-spending and selfish mining. We explore the implications of DeFiPoster-ARB and DeFiPoster-SMT on blockchain consensus. Specifically, we show that the trades identified by our tools exceed the Ethereum block reward by up to 874×. Given optimal adversarial strategies provided by a Markov Decision Process (MDP), we quantify the value threshold at which a profitable transaction qualifies as Miner Extractable Value (MEV) and would incentivize MEV-aware miners to fork the blockchain. For instance, we find that on Ethereum, a miner with a hash rate of 10% would fork the blockchain if an MEV opportunity exceeds 4× the block reward.

Resurrecting Address Clustering in Bitcoin

Malte Möser, Arvind Narayanan

In the 26th International Conference on Financial Cryptography and Data Security (FC),
Grenada, May 2–6, 2022.
https://fc22.ifca.ai/preproceedings/87.pdf

Abstract

Blockchain analysis is essential for understanding how cryptocurrencies like Bitcoin are used in practice, and address clustering is a cornerstone of blockchain analysis. However, current techniques rely on heuristics that have not been rigorously evaluated or optimized. In this paper, we tackle several challenges of change address identification and clustering. First, we build a ground truth set of transactions with known change from the Bitcoin blockchain that can be used to validate the efficacy of individual change address detection heuristics. Equipped with this data set, we develop new techniques to predict change outputs with low false positive rates. After applying our prediction model to the Bitcoin blockchain, we analyze the resulting clustering and develop ways to detect and prevent cluster collapse. Finally, we assess the impact our enhanced clustering has on two exemplary applications.

02 SECTION

Continued Advances in Blockchain

Over the past few years, UBRI partners have contributed to significant innovations in blockchain technology, including proposing more efficient consensus mechanisms, increasing the scalability of existing blockchain systems, securing the block expansion process, making verification more resource-efficient, and more. These advances not only make the blockchain systems more secure and efficient, but also broaden the range of potential use cases, opening up new possibilities.

Achieving Almost All Blockchain Functionalities with Polylogarithmic Storage

Parikshit Hegde, Robert Streit, Yanni Georghiades, Chaya Ganesh, Sriram Vishwanath

In the 26th International Conference on Financial Cryptography and Data Security (FC),
Grenada, May 2–6, 2022.
https://fc22.ifca.ai/preproceedings/173.pdf

Abstract

In current blockchain systems, full nodes that perform all of the available functionalities need to store the entire blockchain. In addition to the blockchain, full nodes also store a blockchain-summary, called the state, which is used to efficiently verify transactions. With the size of popular blockchains and their states growing rapidly, full nodes require massive storage resources in order to keep up with the scaling. This leads to a tug-of-war between scaling and decentralization since fewer entities can afford expensive resources. We present hybrid nodes for proof-of-work (PoW) cryptocurrencies which can validate transactions, validate blocks, validate states, mine, select the main chain, bootstrap new hybrid nodes, and verify payment proofs. With the use of a protocol called trimming, hybrid nodes only retain polylogarithmic number of blocks in the chain length in order to represent the proof-of-work of the blockchain. Hybrid nodes are also optimized for the storage of the state with the use of stateless blockchain protocols. The lowered storage requirements should enable more entities to join as hybrid nodes and improve the decentralization of the system. We define novel theoretical security models for hybrid nodes and show that they are provably secure. We also show that the storage requirement of hybrid nodes is near-optimal with respect to our security definitions.

Bitcontracts: Supporting Smart Contracts in Legacy Blockchains

Karl Wüst, Loris Diana, Kari Kostiainen, Ghassan Karame, Sinisa Matetic, Srdjan Capkun

In 2021 Network and Distributed Systems Security (NDSS) Symposium, Virtual Conference,
February 21-25, 2021.
https://dx.doi.org/10.14722/ndss.2021.24294

Abstract

In this paper we propose Bitcontracts, a novel solution that enables secure and efficient execution of generic smart contracts on top of unmodified legacy cryptocurrencies like Bitcoin that do not support contracts natively. The starting point of our solution is an off-chain execution model, where the contract's issuers appoints a set of service providers to execute the contract's code. The contract's execution results are accepted if a quorum of service providers reports the same result and clients are free to choose which such contracts they trust and use. The main technical contribution of this paper is how to realize such a trust model securely and efficiently without modifying the underlying blockchain. We also identify a set of generic properties that a blockchain system must support so that expressive smart contracts can be added safely, and analyze popular existing blockchains based on these criteria.

Instant Block Confirmation in the Sleepy Model

Vipul Goyal, Hanjun Li, Justin Raizes

In International Conference on Financial Cryptography and Data Security, pp. 65-83.
Springer, Berlin, Heidelberg, 2021.
https://doi.org/10.1007/978-3-662-64331-0_4

Abstract

Blockchain protocols suffer from an interesting conundrum: owning stake in the Blockchain doesn't necessarily mean that the party is willing to participate in day to day operations. This leads to large quantities of stake being owned by parties who do not actually participate in the growth of the blockchain, reducing its security. Pass and Shi captured this concern in the sleepy model, and subsequent work by Pass et al. extended their results into a full Proof of Stake blockchain protocol which can continue to securely progress even when the majority of parties may be offline. However, their protocol requires 10 or more blocks to be added after a transaction first appears in the ledger for it to be confirmed. On the other hand, existing Byzantine Agreement based blockchain protocols such as Algorand confirm transactions as soon as they appear in the ledger, but are unable to progress when users are not online when mandated.

The main question we address is:
Do there exist blockchain protocols which can continue to securely progress even when the majority of parties (resp. stake) may be offline, and confirm transactions as soon as they appear in the ledger?

Our main result shows the answer to this question to be "yes". We present a Proof of Stake blockchain protocol which continues to securely progress so long as more than half of the online stake is controlled by honest parties, and instantly confirms transactions upon appearance in the ledger.

Securely Boosting Chain Growth and Confirmation Speed in PoW Blockchains

Ovia Seshadri, Vinay J Ribeiro, Aditya Kumar

In Proceedings of 2021 IEEE International Conference on Blockchain (Blockchain), 2021, pp. 140-149.
https://doi.org/10.1109/Blockchain53845.2021.00028

Abstract

Proof-of-Work (PoW) blockchains add blocks, and consequently the chain weight, randomly. The blocks added also have a significant network delay owing to their large size. Large delay combined with randomness causes forks that are responsible for many security problems. One can reduce fork occurrences by designing a system with large block intervals and size but this design compromises performance aspects such as confirmation time guarantees. The trade-off between security and performance in PoW blockchain is a well discussed topic in the literature. In this paper, we aim to reduce the conflict between security and performance through our novel concept of Links. Links are small, fast and frequent structures that can be incorporated on any new or existing PoW blockchains. Links help reduce the confirmation time of its underlying blockchain while preserving its consistency security guarantees. Our novel lower-bound growth rate for PoW systems with links in the presence of a general adversary in a partially synchronous network, shows that links provide a more steady chain growth rate than classic PoW systems without links. On a well-established, secure system like Bitcoin, we use the derived growth rate to show that when links are incorporated to Bitcoin, they help reduce its confirmation time from 60 minutes by half to 30 minutes, while retaining the consistency threshold guarantees of the original Bitcoin system. We provide a proof of concept emulation of links in a Bitcoin test bed consisting of 210 nodes having real world latencies between them. We benchmark a system with links against Bitcoin to show links cause negligible network overheads and no compromises on security in terms of orphaned weight due to forks. Our theoretical analyses and experiments can easily be extended to other Nakamoto style PoW systems.

Embedding a Deterministic BFT Protocol in a Block DAG

Maria A. Schett, George Danezis

In Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing (PODC), 177–186.
https://doi.org/10.1145/3465084.3467930

Abstract

This work formalizes the structure and protocols underlying recent distributed systems leveraging block DAGs, which are essentially encoding Lamport's happened-before relations between blocks, as their core network primitives. We then present an embedding of any deterministic Byzantine fault tolerant protocol $\wp$ to employ a block DAG for interpreting interactions between servers. Our main theorem proves that this embedding maintains all safety and liveness properties of $\wp$. Technically, our theorem is based on the insight that a block DAG merely acts as an efficient reliable point-to-point channel between instances of $\wp$ while also using $\wp$ for efficient message compression.

03 SECTION

Cryptography

Cryptography is the cornerstone of blockchain technology. As a powerful tool derived from mathematical concepts and algorithms, cryptography makes it possible to securely transfer information and preserve user privacy. During the last academic year, UBRI-partnered researchers pioneered new work at the forefront of cryptography and achieved many significant results such as: proposing a framework to allow distributed zero-knowledge proof, improving the existing zero-knowledge schema and making it possible to complete in linear-time, and making secret sharing on blockchains more efficient as well as more secure. These innovations not only benefit the blockchain community but also create many possibilities for the broader digital world.

Experimenting with Collaborative zk-SNARKs: Zero-Knowledge Proofs for Distributed Secrets

Alex Ozdemir, Dan Boneh

In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22).
https://www.usenix.org/conference/usenixsecurity22/presentation/ozdemir

Abstract

A zk-SNARK is a powerful cryptographic primitive that provides a succinct and efficiently checkable argument that the prover has a witness to a public NP statement, without revealing the witness. However, in their native form, zk-SNARKs only apply to a secret witness held by a single party. In practice, a collection of parties often need to prove a statement where the secret witness is distributed or shared among them.

We implement and experiment with collaborative zkSNARKs: proofs over the secrets of multiple, mutually distrusting parties. We construct these by lifting conventional zk-SNARKs into secure protocols among N provers to jointly produce a single proof over the distributed witness. We optimize the proof generation algorithm in pairing-based zkSNARKs so that algebraic techniques for multiparty computation (MPC) yield efficient proof generation protocols. For some zk-SNARKs, optimization is more challenging. This suggests MPC "friendliness" as an additional criterion for evaluating zk-SNARKs.

We implement three collaborative proofs and evaluate the concrete cost of proof generation. We find that over a 3Gb/s link, security against a malicious minority of provers can be achieved with approximately the same runtime as a single prover. Security against N −1 malicious provers requires only a 2× slowdown. This efficiency is unusual since most computations slow down by orders of magnitude when securely distributed. This efficiency means that most applications that can tolerate the cost of a single-prover proof should also be able to tolerate the cost of a collaborative proof.

Zero-Knowledge IOPs with Linear-Time Prover and Polylogarithmic-Time Verifier

Jonathan Bootle, Alessandro Chiesa, Siqi Liu

Advances in Cryptology – EUROCRYPT 2022: 41st Annual International Conference
on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway,
May 30 – June 3, 2022, Proceedings, Part II.
https://doi.org/10.1007/978-3-031-07085-3_10

Abstract

Interactive oracle proofs (IOPs) are a multi-round generalization of probabilistically checkable proofs that play a fundamental role in the construction of efficient cryptographic proofs. We present an IOP that simultaneously achieves the properties of zero knowledge, linear-time proving, and polylogarithmic-time verification. We construct a zero-knowledge IOP where, for the satisfiability of an N-gate arithmetic circuit over any field of size Ω(N), the prover uses O(N) field operations and the verifier uses polylog(N) field operations (with proof length O(N) and query complexity polylog(N)). Polylogarithmic verification is achieved in the holographic setting

for every circuit (the verifier has oracle access to a linear-time-computable encoding of the circuit whose satisfiability is being proved).

Our result implies progress on a basic goal in the area of efficient zero knowledge. Via a known transformation, we obtain a zero knowledge argument system where the prover runs in linear time and the verifier runs in polylogarithmic time; the construction is plausibly post-quantum and only makes a black-box use of lightweight cryptography (collision-resistant hash functions).

Storing and Retrieving Secrets on a Blockchain

Vipul Goyal, Abhiram Kothapalli, Elisaweta Masserova, Bryan Parno, Yifan Song

In IACR International Conference on Public-Key Cryptography, pp. 252-282. Springer, Cham, 2022.
https://doi.org/10.1007/978-3-030-97121-2_10

Abstract

A secret sharing scheme enables one party to distribute shares of a secret to n parties and ensures that an adversary in control of t out of n parties will learn no information about the secret. However, traditional secret sharing schemes are often insufficient, especially for applications in which the set of parties who hold the secret shares might change over time. To achieve security in this setting, dynamic proactive secret sharing (DPSS) is used. DPSS schemes proactively update the secret shares held by the parties and allow changes to the set of parties holding the secrets. We propose FaB-DPSS (FAst Batched DPSS) – a new and highly optimized batched DPSS scheme. While previous work on batched DPSS focuses on a single client submitting a batch of secrets and does not allow storing and releasing secrets independently, we allow multiple different clients to dynamically share and release secrets. FaB-DPSS is the most efficient robust DPSS scheme that supports the highest possible adversarial threshold of 1/2. We prove FaB-DPSS secure and implement it. All operations complete in seconds, and we outperform a prior state-of-the-art DPSS scheme by over 6X.

Additionally, we propose new applications of DPSS in the context of blockchains. Specifically, we propose a protocol that uses blockchains and FaB-DPSS to provide conditional secret storage. The protocol allows parties to store secrets along with a release condition, and once a (possibly different) party satisfies this release condition, the secret is privately released to that party. This functionality is similar to extractable witness encryption. While there are numerous compelling applications (e.g., time-lock encryption, one-time programs, and fair multi-party computation) which rely on extractable witness encryption, there are no known efficient constructions (or even constructions based on any well-studied assumptions) of extractable witness encryption. However, by utilizing blockchains and FaB-DPSS, we can easily build all those applications.
We provide an implementation of our conditional secret storage protocol as well as several applications building on top of it.

Giving an Adversary Guarantees (Or: How to Model Designated Verifier Signatures in a Composable Framework)

Ueli Maurer, Christopher Portmann, Guilherme Rito

In International Conference on the Theory and Application of Cryptology and Information Security, pp. 189-219. Springer, Cham, 2021.
https://doi.org/10.1007/978-3-030-92078-4_7

Abstract

When defining a security notion, one typically specifies what dishonest parties cannot achieve. For example, communication is confidential if a third party cannot learn anything about the messages being transmitted, and it is authentic if a third party cannot impersonate the real (honest) sender. For certain applications, however, security crucially relies on giving dishonest parties certain capabilities. As an example, in Designated Verifier Signature (DVS) schemes, one captures that only the designated verifier can be convinced of the authenticity of a message by guaranteeing that any dishonest party can forge signatures which look indistinguishable (to a third party) from original ones created by the sender.

However, composable frameworks cannot typically model such guarantees as they are only designed to bound what a dishonest party can do. In this paper we show how to model such guarantees—that dishonest parties must have some capability—in the Constructive Cryptography framework (Maurer and Renner, ICS 2011). More concretely, we give the first composable security definitions for Multi-Designated Verifier Signature (MDVS) schemes—a generalization of DVS schemes.

The ideal world is defined as the intersection of two worlds. The first captures authenticity in the usual way. The second provides the guarantee that a dishonest party can forge signatures. By taking the intersection we have an ideal world with the desired properties.

We also compare our composable definitions to existing security notions for MDVS schemes from the literature. We find that only recently, 23 years after the introduction of MDVS schemes, sufficiently strong security notions were introduced capturing the security of MDVS schemes (Damgård et al., TCC 2020). As we prove, however, these notions are still strictly stronger than necessary.

04 SECTION

Security in Blockchain

Security is critical for blockchain systems and their users to issue transactions, store valuable information, and retrieve secrets. In order to preserve and strengthen blockchain security, UBRI partners explored possible threat models of blockchain, proposed dependable smart contract creation mechanisms, introduced quicker and more reliable authentication approaches, and modified or developed new comprehensive analysis methodologies. It is believed that blockchain systems and the applications built upon them can become more secure and dependable over time and research will continue to work towards supporting this outcome.

Elysium: Context-Aware Bytecode-Level Patching to Automatically Heal Vulnerable Smart Contracts

Christof Ferreira Torres, Hugo Jonker, Radu State

In the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Limassol, Cyprus on 26-28 October, 2022.
https://doi.org/10.1145/3545948.3545975

Abstract

Fixing bugs is easiest by patching source code. However, source code is not always available: only 0.3% of the ~49M smart contracts that are currently deployed on Ethereum have their source code publicly available. Moreover, since contracts may call functions from other contracts, security flaws in closed-source contracts may affect open-source contracts as well. However, current state-of-the-art approaches that operate on closed-source contracts (i.e., EVM byte- code), such as EVMPatch and SmartShield, make use of purely hard-coded templates that leverage fix patching patterns. As a result, they cannot dynamically adapt to the bytecode that is being patched, which severely limits their flexibility and scalability. For instance, when patching integer overflows using hard-coded templates, a particular patch template needs to be employed as the bounds to be checked are different for each integer size (i.e., one template for uint256, another template for uint64, etc.).

In this paper, we propose Elysium, a scalable approach towards automatic smart contract repair at the bytecode level. Elysium com- bines template-based and semantic-based patching by inferring context information from bytecode. Elysium is currently able to patch 7 different types of vulnerabilities in smart contracts auto- matically and can easily be extended with new templates and new bug-finding tools. We evaluate its effectiveness and correctness using 3 different datasets by replaying more than 500K transactions on patched contracts. We find that Elysium outperforms existing tools by patching at least 30% more contracts correctly. Finally, we also compare the overhead of Elysium in terms of deployment and transaction cost. In comparison to other tools, we find that generally Elysium minimizes the runtime cost (i.e., transaction cost) up to a factor of 1.7, for only a marginally higher deployment cost, where deployment cost is a one-time cost as compared to the runtime cost.

SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning

Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramèr, Giulia Fanti, Ari Juels

In 2021 Network and Distributed Systems Security (NDSS) Symposium, Virtual Conference, February 21-25, 2021.
https://dx.doi.org/10.14722/ndss.2021.24188

Abstract

Incentive mechanisms are central to the functionality of permissionless blockchains: they incentivize participants to run and secure the underlying consensus protocol. Designing incentive-compatible incentive mechanisms is notoriously challenging, however. As a result, most public blockchains today use incentive mechanisms whose security properties are poorly understood and largely untested. In this work, we propose SquirRL, a framework for using deep reinforcement learning to analyze attacks on blockchain incentive mechanisms. We demonstrate SquirRL's power by first recovering known attacks: (1) the optimal selfish mining attack in Bitcoin, and (2) the Nash equilibrium in block withholding attacks. We also use SquirRL to obtain several novel empirical results. First, we discover a counterintuitive flaw in the widely used rushing adversary model when applied to multi-agent Markov games with incomplete information. Second, we demonstrate that the optimal selfish mining strategy identified in a previous work is actually not a Nash equilibrium in the multi-agent selfish mining setting. In fact, our results suggest (but do not prove) that when more than two competing agents engage in selfish mining, there is no profitable Nash equilibrium. This is consistent with the lack of observed selfish mining in the wild. Third, we find a novel attack on a simplified version of Ethereum's finalization mechanism, Casper the Friendly Finality Gadget (FFG) that allows a strategic agent to amplify her rewards by up to 30%. Notably, Buterin et al. show that honest voting is a Nash equilibrium in Casper FFG; our attack shows that when Casper FFG is composed with selfish mining, this is no longer the case. Altogether, our experiments demonstrate SquirRL's flexibility and promise as a framework for studying attack settings that have thus far eluded theoretical and empirical understanding.

Resource-Aware Session Types for Digital Contracts

Ankush Das, Stephanie Balzer, Jan Hoffmann, Frank Pfenning, Ishani Santurkar

In 2021 IEEE 34th Computer Security Foundations Symposium (CSF), pp. 1-16. IEEE, 2021.
https://doi.org/10.1109/CSF51468.2021.00004

Abstract

Programming digital contracts comes with unique challenges, which include (i) expressing and enforcing protocols of interaction, (ii) controlling resource usage, and (iii) preventing the duplication or deletion of a contract's assets. This article presents the design and type-theoretic foundation of Nomos, a programming language for digital contracts that addresses these challenges. To express and enforce protocols, Nomos is based on shared binary session types. To control resource usage, Nomos employs automatic amortized resource analysis. To prevent the duplication or deletion of assets, Nomos uses a linear type system. A monad integrates the effectful session-typed language with a general-purpose functional language. Nomos' prototype implementation features linear-time type checking and efficient type reconstruction that includes automatic inference of resource bounds via off-the-shelf linear optimization. The effectiveness of the language is evaluated with case studies on implementing common smart contracts such as auctions, elections, and currencies. Nomos is completely formalized, including the type system, a cost semantics, and a transactional semantics to deploy Nomos contracts on a blockchain. The type soundness proof ensures that protocols are followed at run-time and that types establish sound upper bounds on the resource consumption, ruling out re-entrancy and out-of-gas vulnerabilities.

Cryptocurrencies with Security Policies and Two-Factor Authentication

Florian Breuer, Vipul Goyal, Giulio Malavolta

In 2021 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 140-158. IEEE, 2021.
https://doi.org/10.1109/EuroSP51992.2021.00020

Abstract

Blockchain-based cryptocurrencies offer an appealing alternative to Fiat currencies, due to their decentralized and borderless nature. However the decentralized settings make the authentication process more challenging: Standard cryptographic methods often rely on the ability of users to reliably store a (large) secret information. What happens if one user's key is lost or stolen? Blockchain systems lack of fallback mechanisms that allow one to recover from such an event, whereas the traditional banking system has developed and deploys quite effective solutions.

In this work, we develop new cryptographic techniques to integrate security policies (developed in the traditional banking domain) in the blockchain settings. We propose a system where a smart contract is given the custody of the user's funds and has the ability to invoke a two-factor authentication (2FA) procedure in case of an exceptional event (e.g., a particularly large transaction or a key recovery request). To enable this, the owner of the account secret-shares the answers of some security questions among a committee of users. When the 2FA mechanism is triggered, the committee members can provide the smart contract with enough information to check whether an attempt was successful, and nothing more.

We then design a protocol that securely and efficiently implements such a functionality: The protocol is round-optimal, is robust to the corruption of a subset of committee members, supports low-entropy secrets, and is concretely efficient. As a stepping stone towards the design of this protocol, we introduce a new threshold homomorphic encryption scheme for linear predicates from bilinear maps, which might be of independent interest.

To substantiate the practicality of our approach, we implement the above protocol as a smart contract in Ethereum and show that it can be used today as an additional safeguard for suspicious transactions, at minimal added cost. We also implement a second scheme where the smart contract additionally requests a signature from a physical hardware token, whose verification key is registered upfront by the owner of the funds. We show how to integrate the widely used universal two-factor authentication (U2F) tokens in blockchain environments, thus enabling the deployment of our system with available hardware.

Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit

Kaihua Qin, Liyi Zhou, Benjamin Livshits, Arthur Gervais

In International Conference on Financial Cryptography and Data Security (FC), pp. 3-32.
Springer, Berlin, Heidelberg, 2021.
https://doi.org/10.1007/978-3-662-64322-8_1

Abstract

Credit allows a lender to loan out surplus capital to a borrower. In the traditional economy, credit bears the risk that the borrower may default on its debt, the lender hence requires upfront collateral from the borrower, plus interest fee payments. Due to the atomicity of blockchain transactions, lenders can offer flash loans, i.e., loans that are only valid within one transaction and must be repaid by the end of that transaction. This concept has lead to a number of interesting attack possibilities, some of which were exploited in February 2020.

This paper is the first to explore the implication of transaction atomicity and flash loans for the nascent decentralized finance (DeFi) ecosystem. We show quantitatively how transaction atomicity increases the arbitrage revenue. We moreover analyze two existing attacks with ROIs beyond 500k%. We formulate finding the attack parameters as an optimization problem over the state of the underlying Ethereum blockchain and the state of the DeFi ecosystem. We show how malicious adversaries can efficiently maximize an attack profit and hence damage the DeFi ecosystem further. Specifically, we present how two previously executed attacks can be “boosted” to result in a profit of 829.5k USD and 1.1M USD, respectively, which is a boost of 2.37× and 1.73×, respectively.

CJ-Sniffer: Measurement and Content-Agnostic Detection of Cryptojacking Traffic

Yebo Feng, Jun Li, Devkishen Sisodia

In the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Limassol, Cyprus on 26-28 October, 2022.
https://doi.org/10.1145/3545948.3545973

Abstract

With the continuous appreciation of cryptocurrency, cryptojacking, the act by which computing resources are stolen to mine cryptocurrencies, is becoming more rampant. In this paper, we conduct a measurement study on cryptojacking network traffic and propose CryptoJacking-Sniffer (CJ-Sniffer), an easily deployable, privacy-aware approach to protecting all devices within a network against cryptojacking. Compared with existing approaches that suffer from privacy concerns or high overhead, CJ-Sniffer only needs to access anonymized, content-agnostic metadata of network traffic from the gateway of the network to efficiently detect cryptojacking traffic. In particular, while cryptojacking traffic is also cryptocurrency mining traffic, CJ-Sniffer is the first approach to distinguishing cryptojacking traffic from user-initiated cryptocurrency mining traffic, making it possible to only filter cryptojacking traffic, rather than blindly filtering all cryptocurrency mining traffic as commonly practiced. After constructing a statistical model to identify all the cryptocurrency mining traffic, CJ-Sniffer extracts variation vectors from packet intervals and utilizes a long short-term memory (LSTM) network to further identify cryptojacking traffic. We evaluated CJSniffer with a packet-level cryptomining dataset. Our evaluation results demonstrate that CJ-Sniffer achieves an accuracy of over 99% with reasonable delays.

05 SECTION

Reshaping The Financial System

Decentralized finance (DeFi) technology can bring transformative changes to the current global financial system, streamlining the transfer of value. During the past academic year, UBRI-partnered researchers continued to work toward this possibility. A wave of new financial derivatives have been 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 trading mechanisms over different blockchain systems. These research achievements are accelerating the financial revolution, making DeFi protocols more inclusive, secure, and efficient.

Enabling the Internet of Value: How Blockchain Connects Global Businesses

Editors: Nikhil Vadgama, Jiahua Xu, Paolo Tasca

Springer Cham, part of the book series: Future of Business and Finance. 2022..
https://doi.org/10.1007/978-3-030-78184-2

Foreword by David Schwartz
It is easy to imagine one of humankind's earliest transfers of value happening over a campfire on a grassy plain or within a cave offering protection from the elements. One human passing food or clothing to another in exchange for something in kind.

For most of humanity's existence, transactions and the sharing of value were like this: payment delivered at the point of exchange; even long-distance transfers of money often involved the actual unit of value with coins or money crossing bodies of water via ocean liners or miles of the Old West on the backs of ponies. There's a reason treasure hunters invest huge sums of money to explore ancient shipwrecks as gold coins still lay at the bottom of the sea where they sank in transit.

For centuries, goods, information, and stores of value all travelled in the physical realm, conveyed by people from one destination to another. The advent of the telegram broke that cycle with information able to travel far ahead of individuals. Today, information can bounce electronically around the world in seconds, free to access, and share with no restrictions.

Unfortunately, stores of value "even when represented as ones and zeros on an electronic ledger" are still subject to outmoded rules of transfer. Unable to move freely, traditional value must stop and start between countries and currencies. Like the hare in its race against the tortoise, speed remains unrealised, instead traveling in fits and starts on its way to its final destination.

This current day, yet thoroughly unmodern, the mismatch between the speed of transit for information, goods, and value persists because today's payment systems were built for yesterday's companies. Today's companies like Amazon, Airbnb, and Uber need to make instant payments to customers, contractors, and small businesses around the world.

On its face, this is impossible because of the patchwork quilt of payment systems that cover the globe, each with distinct rules, processes, and currencies. To compensate, companies and providers must build bridges across these systems manned by payment teams that can sometimes grow to hundreds of employees. And to improve the speed of transactions, each bridge requires pools of money on either end in the local country's currency to create liquidity.

The end result is an enormous investment of cost and effort that is impossible for small companies or providers to match. This leaves the reality of instant value transfer over the world's antiquated money networks the domain of only the largest and wealthiest organisations; today's equivalents of the Medici family or other well-known financial brokers of the past.

However, a new reality for value is growing that has the potential to penetrate these walls and deliver a system of value that once again matches the speed at which goods and information can flow.

Blockchain technology allows for trust-minimised systems without central operators, breaking the monopoly of those able to straddle disparate payment networks by virtue of their size and wealth. Paired with digital assets designed for cross-border transactions, blockchain-based systems can deliver instant transfers of value anywhere in the world.

But we are not there yet. There are still missing pieces to the puzzle. Just as you require a specific address to send physical mail, a phone number to call someone, or an email address to send an email, so we all need unique digital wallet identifiers to send point to point value.

And the networks themselves still cannot work seamlessly in conjunction. Payment systems "whether traditional or blockchain based" have dozens of different methods of integration. We are still missing the Rosetta Stone for value the piece that will make it possible to unify all of these different networks. In short, we do not yet have our Internet of Value. But we know we need it. And that is progress.

DeFi and the Future of Finance

Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro

John Wiley & Sons, 2021.
https://www.wiley.com/en-us/DeFi+and+the+Future+of+Finance-p-9781119836025

Abstract

Our legacy financial infrastructure has both limited growth opportunities and contributed to the inequality of opportunities. Around the world, 1.7 billion are unbanked. Small businesses, even those with a banking relationship, often must rely on high-cost financing, such as credit cards, because traditional banking excludes them from loan financing. High costs also impact retailers who lose 3% on every credit card sales transaction. These total costs for small businesses are enormous by any metric. The result is less investment and decreased economic growth. Decentralized finance, or DeFi, poses a challenge to the current system and offers a number of potential solutions to the problems inherent in the traditional financial infrastructure. While there are many fintech initiatives, we argue that the ones that embrace the current banking infrastructure are likely to be fleeting. We argue those initiatives that use decentralized methods - in particular blockchain technology - have the best chance to define the future of finance.

An Empirical Study of Defi Liquidations: Incentives, Risks, and Instabilities

Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, Arthur Gervais

In Proceedings of the 21st ACM Internet Measurement Conference (IMC 2021).
https://doi.org/10.1145/3487552.3487811

Abstract

Financial speculators often seek to increase their potential gains with leverage. Debt is a popular form of leverage, and with over 39.88B USD of total value locked (TVL), the Decentralized Finance (DeFi) lending markets are thriving. Debts, however, entail the risks of liquidation, the process of selling the debt collateral at a discount to liquidators. Nevertheless, few quantitative insights are known about the existing liquidation mechanisms.

In this paper, to the best of our knowledge, we are the first to study the breadth of the borrowing and lending markets of the Ethereum DeFi ecosystem. We focus on Aave, Compound, MakerDAO, and dYdX, which collectively represent over 85% of the lending market on Ethereum. Given extensive liquidation data measurements and insights, we systematize the prevalent liquidation mechanisms and are the first to provide a methodology to compare them objectively. We find that the existing liquidation designs well incentivize liquidators but sell excessive amounts of discounted collateral at the borrowers' expenses. We measure various risks that liquidation participants are exposed to and quantify the instabilities of existing lending protocols. Moreover, we propose an optimal strategy that allows liquidators to increase their liquidation profit, which may aggravate the loss of borrowers.

SoK: Yield Aggregators in DeFi

Simon Cousaert, Jiahua Xu, Toshiko Matsui

In 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-14. IEEE, 2022.
https://doi.org/10.1109/ICBC54727.2022.9805523

Abstract

Yield farming has been an immensely popular activity for cryptocurrency holders since the explosion of Decentralized Finance (DeFi) in the summer of 2020. In this Systematization of Knowledge (SoK), we study a general framework for yield farming strategies with empirical analysis. First, we summarize the fundamentals of yield farming by focusing on the protocols and tokens used by aggregators. We then examine the sources of yield and translate those into three example yield farming strategies, followed by the simulations of yield farming performance, based on these strategies. We further compare four major yield aggregators—Idle, Pickle, Harvest and Yearn—in the ecosystem, along with brief introductions of others. We systematize their strategies and revenue models, and conduct an empirical analysis with on-chain data from example vaults, to find a plausible connection between data anomalies and historical events. Finally, we discuss the benefits and risks of yield aggregators.

High-Frequency Trading on Decentralized On-Chain Exchanges

Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, Arthur Gervais

In 2021 IEEE Symposium on Security and Privacy (SP), pp. 428-445. IEEE, 2021.
https://doi.org/10.1109/SP40001.2021.00027

Abstract

Decentralized exchanges (DEXs) allow parties to participate in financial markets while retaining full custody of their funds. However, the transparency of blockchain-based DEX in combination with the latency for transactions to be processed, makes market-manipulation feasible. For instance, adversaries could perform front-running — the practice of exploiting (typically non-public) information that may change the price of an asset for financial gain.

In this work we formalize, analytically exposit and empirically evaluate an augmented variant of front-running: sandwich attacks, which involve front- and back-running victim transactions on a blockchain-based DEX. We quantify the probability of an adversarial trader being able to undertake the attack, based on the relative positioning of a transaction within a blockchain block. We find that a single adversarial trader can earn a daily revenue of over several thousand USD when performing sandwich attacks on one particular DEX — Uniswap, an exchange with over 5M USD daily trading volume by June 2020. In addition to a single-adversary game, we simulate the outcome of sandwich attacks under multiple competing adversaries, to account for the real-world trading environment.

A Game-theoretic Analysis of Cross-chain Atomic Swaps with HTLCs

Jiahua Xu, Damien Ackerer, Alevtina Dubovitskaya

In Proceedings of 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), 2021, pp. 584-594.
https://doi.org/10.1109/ICDCS51616.2021.00062

Abstract

To achieve interoperability between unconnected ledgers, hash time lock contracts (HTLCs) are commonly used for cross-chain asset exchange. The solution tolerates transaction failure, and can “make the best out of worst” by allowing transacting agents to at least keep their original assets in case of an abort. Nonetheless, as an undesired outcome, reoccurring transaction failures prompt a critical and analytical examination of the protocol. In this study, we propose a game-theoretic framework to study the strategic behaviors of agents taking part in cross-chain atomic swaps implemented with HTLCs. We study the success rate of the transaction as a function of the exchange rate of the swap, the token price and its volatility, among other variables. We demonstrate that in an attempt to maximize one's own utility as asset price changes, either agent might withdraw from the swap. An extension of our model confirms that collateral deposits can improve the transaction success rate, motivating further research towards collateralization without a trusted third party. A second model variation suggests that a swap is more likely to succeed when agents dynamically adjust the exchange rate in response to price fluctuations.

The Wisdom of Crowds in FinTech: Evidence from Initial Coin Offerings

Jongsub Lee, Tao Li, Donghwa Shin

The Review of Corporate Finance Studies 11, no. 1 (2022): 1-46.
https://doi.org/10.1093/rcfs/cfab014

Abstract

Certification by analysts on a FinTech platform that harnesses the “wisdom of crowds” is associated with successful initial coin offerings (ICOs). We show that favorable ratings by a group of analysts with diverse backgrounds positively predict fundraising success and long-run token performance. Analysts’ ratings also help detect potential fraud ex ante. We document that analysts have career concerns and are incentivized by the platform to issue informative ratings. Overall, our results suggest that a market-based certification process that relies on a diverse group of individuals is at play in financing blockchain startups. (JEL D82, G11, G24, G32, G34, L26).

06 SECTION

Central Bank Digital Currencies

In recent years, 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 national and regional economies more efficient, inclusive, and equitable. To support this transformation, UBRI-partnered researchers have studied this trend thoroughly. They have proposed new CBDC frameworks to make the system more dependable and practical, and have studied existing schema to identify their vulnerabilities and propose potential improvements, all while investigating how to integrate CBDCs into existing systems.

Central Bank Digital Currency: Considerations, Projects, Outlook

Editor: Dirk Niepelt

CEPR eBook series on FinTech & Digital Currencies, 2021.
https://cepr.org/voxeu/columns/central-bank-digital-currency-considerations-projects-outlook

Foreword by Tessa Ogden

Central bank digital currencies (CBDCs) are receiving more attention than ever before. Yet the motivations for issuance vary across countries, as do the policy approaches and technical designs. As yet, no major jurisdiction has launched a CBDC, and many open questions remain. Monetary authorities, fearful of being left behind by innovations in the private sector, have increasingly turned from observers into participants.

This book brings together contributions from academics and experts from monetary authorities and international organisations to provide a detailed and insightful overview of the key considerations of current CBDC developments worldwide. Specific chapters discuss the economic, legal and political implications of CBDC implementation, as well as assessing existing initiatives and reflecting on the future of the digital financial landscape.

What is clear from the research is that there are no ‘right’ choices for monetary authorities when considering CBDC. However, the debate has clearly narrowed and the implications are now better understood, with issues of privacy, politics and information increasingly coming to the fore. Concerns have also broadened beyond the domains of payments, monetary policy and financial stability, which have generated a consensus that parliaments and voters – not just central banks – should actively join the debate.

The book is an output from CEPR’s Research and Policy Network on FinTech and Digital Currencies, which was established in 2018 to generate, coordinate and disseminate impactful research about the optimal policies to deal with these fast-moving changes in financial markets. The eBook provides a useful guide for policymakers to navigate the complex and fast-moving world of financial digitalisation and should help to inform the design of pilot projects and the direction of future research.

CEPR is grateful to Dirk Niepelt for his expert editorship of this eBook. Our thanks also go to Anil Shamdasani for his skilled handling of its production, and to Kirsty McNeill for her contributions towards its production.

CEPR, which takes no institutional positions on economic policy matters, is delighted to provide a platform for an exchange of views on this important topic.

Platypus: A Central Bank Digital Currency with Unlinkable Transactions and Privacy Preserving Regulation

Karl Wüst, Kari Kostiainen, Noah Delius, Srdjan Capkun

Cryptology ePrint Archive, 2021.
https://eprint.iacr.org/2021/1443

Abstract

Due to the popularity of blockchain-based cryptocurrencies, the increasing digitalization of payments, and the constantly reducing role of cash in society, central banks have shown an increased interest in deploying central bank digital currencies (CBDCs) that could serve as a digital cash-equivalent. While most recent research on CBDCs focuses on blockchain technology, it is not clear that this choice of technology provides the optimal solution. In particular, the centralized trust model of a CBDC offers opportunities for different designs.

In this paper, we depart from blockchain designs and instead build on ideas from traditional e-cash schemes. We propose a new style of building digital currencies that combines the transaction processing model of e-cash with an account-based fund management model. We argue that such a style of building digital currencies is especially well-suited to CBDCs. We also design the first such digital currency system, called Platypus, that provides strong privacy, high scalability, and expressive but simple regulation, which are all critical features for a CBDC. Platypus achieves these properties by adapting techniques similar to those used in anonymous blockchain cryptocurrencies like Zcash to fit our account model and applying them to the e-cash context.

Digital Currencies: The US, China, And The World At A Crossroads

Editors: Darrell Duffie, Elizabeth Economy

Hoover Institution Press, 2022.
https://www.hoover.org/research/digital-currencies-us-china-and-world-crossroads

Abstract

Central bank digital currencies have taken flight globally, and China is boldly leading the way. How will China's digital currency, the e-CNY, serve the political and economic agenda of China's authoritarian government? What are its implications for the world economy, international security, and the leading role of the United States in global payments and finance? How might the e-CNY and its underlying and related technologies be adopted by other countries? How do we weigh the potential gains in efficiency against the risks to privacy and security? How should the United States respond? To answer these questions, the Hoover Institution brought together distinguished experts in national security, finance, economics, central banking, technology policy, and computer science. This volume presents their findings and proposes a pathway toward revitalizing US financial leadership on the international stage in the digital age. The United States must respond to a spectrum of key policy concerns raised by the e-CNY and improve incentives for innovation and competition in its own payment systems. It should expedite development of technology and standards for a possible digital dollar. And it should

advocate for democratic norms of privacy, accountability, transparency, and security in shaping the global rules surrounding central bank digital currencies.

Assessing the Impact of Central Bank Digital Currency on Private Banks

David Andolfatto

The Economic Journal 131, no. 634 (2021): 525-540.
https://doi.org/10.1093/ej/ueaa073

Abstract

This paper investigates how a central bank digital currency can be expected to impact a monopolistic banking sector. The paper's framework of analysis combines the Diamond (1965) model of government debt with the Klein (1971) and Monti (1972) model of a monopoly bank. The paper finds that the introduction of a central bank digital currency has no detrimental effect on bank lending activity and may, in some circumstances, even serve to promote it. Competitive pressure leads to a higher monopoly deposit rate which reduces profit but expands deposit funding through greater financial inclusion and desired saving. An appeal to available theory and evidence suggests that a properly designed central bank digital currency is not likely to threaten financial stability.

07 SECTION

Blockchain Use Cases for Social Good

The dependable, traceable, immutable, and decentralized features of blockchain-based systems make this technology applicable to myriad industries. Recent developments in this space have shed light on the potential to optimize how civil society functions, improving a wide range of applications including medical systems, cyber-physical systems, smart grids, media communication systems, and other socially impactful use cases. These use cases can have a profound impact on social structures, enabling greater inclusion and equity.

Technical Design and Development of a Self-Sovereign Identity Management Platform for Patient-Centric Health Care using Blockchain Technology

Daniel Toshio Harrell, Muhammad Usman, Ladd Hanson, Mustafa Abdul-Moheeth, Ishav Desai, Jahnavi Shriram, Eliel de Oliveira, John Robert Bautista, Eric T. Meyer, Anjum Khurshid

Blockchain in Healthcare Today, 2022.
https://www.blockchainhealthcaretoday.com/index.php/journal/article/view/196

Abstract

Objective: Clinical data in the United States are highly fragmented, stored in numerous different databases, and are defined by service providers or clinical specialties rather than by individuals or their families. As a result, linking or aggregating a complete record for a patient is a major technological, legal, and operational challenge. One of the factors that has made clinical data integration so difficult to achieve is the lack of a universal ID for everyone. This leads to other related problems of having to prove identity at each interaction with the health system and repeatedly providing basic information on demographics, insurance, payment, and medical conditions. Traditional solutions that require complex governance, expensive technology, and risks to privacy and security of the data have failed adequately to solve this interoperability problem. We describe the technical design decisions of a patient-centric decentralized health identity management system using the blockchain technology, called MediLinker, to address some of these challenges.

Design: Our multidisciplinary research group developed and implemented an identity wallet, which uses the blockchain technology to manage verifiable credentials issued by healthcare clinics, banks, and insurance companies. To manage patient's self-sovereign identity, we leveraged the Hyperledger Indy blockchain framework to store patient's decentralized identifiers (DIDs) and the schemas or format for each credential type. In contrast, the credentials containing patient data are stored 'off-ledger' in each person's wallet and accessible via a computer or smartphone. We used Hyperledger Aries as a middleware layer (API: Application Programming Interface) to connect Hyperledger Indy with the front-end, which was developed using a JavaScript framework, ReactJS (Web Application) and React Native (iOS Application).

Results: MediLinker allows users to store their personal data on digital wallets, which they control. It uses a decentralized trusted identity using Hyperledger Indy and Hyperledger Aries. Patients use MediLinker to register and share their information securely and in a trusted system with healthcare and other service providers. Each MediLinker wallet can have six credential types: health ID with patient demographics, insurance, medication list including COVID-19 vaccination status, credit card, medical power of attorney (MPOA) for guardians of pediatric or geriatric patients, and research consent. The system allows for in-person and remote granting and revoking of such permissions for care, research, or other purposes without repeatedly requiring physical identity documents or enrollment information.

Conclusion: We successfully developed and tested a blockchain-based technical architecture, described in this article, as an identity management system that may be operationalized and scaled for future implementation to improve patient experience and control over their personal information.

Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System

Basudeb Bera, Sourav Saha, Ashok Kumar Das, Athanasios V. Vasilakos

In IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5744-5761, April 1, 2021.
https://doi.org/10.1109/JIOT.2020.3030308

Abstract

We design a new blockchain-based access control protocol in IoT-enabled smart-grid system, called DBACP-IoTSG. Through the proposed DBACP-IoTSG, the data is securely brought to the service providers from their respective smart meters (SMs). The peer-to-peer (P2P) network is formed by the participating service providers, where the peer nodes are responsible for creating the blocks from the gathered data securely from their corresponding SMs and adding them into the blockchain after validation of the blocks using the voting-based consensus algorithm. In our work, the blockchain is considered as private because the data collected from the consumers of the SMs are private and confidential. By the formal security analysis under the random oracle model, nonmathematical security analysis and software-based formal security verification, DBACP-IoTSG is shown to be resistant against various attacks. We carry out the experimental results of various cryptographic primitives that are needed for comparative analysis using the widely used multiprecision integer and rational arithmetic cryptographic library (MIRACL). A detailed comparative study reveals that DBACP-IoTSG supports more functionality features and provides better security apart from its low communication and computation costs as compared to recently proposed relevant schemes. In addition, the blockchain implementation of DBACP-IoTSG has been performed to measure computational time needed for the varied number of blocks addition and also the varied number of transactions per block in the blockchain.

AI-Envisioned Blockchain-Enabled Signature-Based Key Management Scheme for Industrial Cyber-Physical Systems

Ashok Kumar Das, Basudeb Bera, Sourav Saha, Neeraj Kumar, Ilsun You, Han-Chieh Chao

In IEEE Internet of Things Journal, vol. 9, no. 9, pp. 6374-6388, May 1, 2022.
https://doi.org/10.1109/JIOT.2021.3109314

Abstract

This article proposes a new blockchain-envisioned key management protocol for artificial intelligence (AI)-enabled industrial cyber–physical systems (ICPSs). The designed key management protocol enables key establishment among the Internet of Things (IoT)-enabled smart devices and their respective gateway nodes. The blocks partially constructed with secure data from smart devices by fog servers are provided to cloud servers that are responsible for completing blocks, and then mining those blocks for verification and addition in the blockchain. The most important application of the private blockchain construction is to apply AI algorithms for accurate predictions in Big data analytics. A detailed security analysis along with formal security verification show that the proposed scheme resists various potential attacks in an ICPS environment. Moreover, practical testbed experiments have been conducted using the multiprecision integer and rational arithmetic cryptographic library (MIRACL). Furthermore, a detailed comparative analysis shows superiority of the proposed scheme over recent relevant schemes. In addition, the practical implementation using the blockchain for the proposed scheme demonstrates the total computational costs when the number of transactions per block and also the number of blocks mined in the blockchain are varied.

An Implementation of Fake News Prevention by Blockchain and Entropy-based Incentive Mechanism

Chien-Chih Chen, Yuxuan Du, Richards Peter, Wojciech Golab

In Proceedings of 2021 IEEE International Conference on Big Data (Big Data), 2021, pp. 2476-2486.
https://doi.org/10.1109/BigData52589.2021.9671778

Abstract

Fake news is undoubtedly a significant threat to democratic countries nowadays because existing technologies can quickly and massively produce fake videos, articles, or social media messages based on the rapid development of artificial intelligence and deep learning. Therefore, human assistance is critical if current automatic fake new identification technologies desire to improve accuracy. Given this situation, prior research has proposed to add a quorum, a group of appraisers trusted by users to verify the authenticity of the information, to the fake news prevention systems. This paper proposes a stake-based incentive mechanism to diminish the negative effect of malicious behaviors on a quorum-based fake news prevention system. Moreover, we use Hyperledger Fabric, Schnorr signatures, and human appraisers to implement a practical prototype of a quorum-based fake news prevention system. Then we conduct necessary case analyses and experiments to realize how dishonest participants, crash failures, and scale impact our system. The outcomes of the case analyses and experiments show that our mechanisms are feasible and provide an analytical basis for developing fake news prevention systems.

Blockchain-based Smart Contracts as New Governance Tools for the Sharing Economy

Stefania Fiorentino, Silvia Bartolucci

Cities, Volume 117, 2021.
https://doi.org/10.1016/j.cities.2021.103325

Abstract

Examples of sharing economy platforms are proliferating, generating new concerns on the exploitation of local resources, ethical and intellectual properties. Necessary changes are required to the regulatory frameworks of our cities. This paper proposes an application of blockchain technology for planning governance purposes. This new cutting-edge technology, currently under-exploited in applications for smart cities planning, may represent a fundamental building block for the digitalization of the sector. We propose blockchain-based management systems (BMSs) as new governance tools to improve traceability, transparency, and decentralization of transactions in the sharing economy. We build a BMS prototype for the management of co-working spaces (CWSs). In particular, we show how a blockchain can be used to track transactions between users (e.g., rent payments), and to advertise or store information about a given space (e.g., building specifications, IP conceived within the space). A large amount of data will be permanently and securely stored on ledger and made available to both institutions and corporations, providing a wide range of new governance tools and services to local authorities of the future. Similar BMSs can be developed for different types of buildings or public services purposes.

08 SECTION

Law, Policy, and Regulation

More comprehensive regulation in FinTech is essential to ensuring these technologies serve society's best interests and enable competition and innovation.

Most UBRI-partnered researchers agree that laws and regulations that apply to traditional financial markets have been slow to adapt to technologies like blockchain and cryptocurrency. UBRI partners are helping define future financial supervisory and regulatory models that can inform appropriate policies and regulations.

Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem

Yuta Takanashi, Shin'ichiro Matsuo, Eric Burger, Clare Sullivan, James Miller, Hirotoshi Sato

Stanford Journal of Blockchain Law & Policy 2020.
https://heinonline.org/HOL/P?h=hein.journals/sjblp3&i=1
https://heinonline.org/HOL/P?h=hein.journals/sjblp3&i=117

Abstract

Financial regulators around the world regulate financial intermediaries and activities to achieve their regulatory goals including investor/consumer protection, financial stability and prevention of financial crimes, and in so doing address various market failures. These objectives are needed in the social interest regardless of the technologies used by the financial system.

Blockchain technology and any financial ecosystem based on it have technical characteristics including decentralization, autonomization, anonymization and globalization, which could undermine the ability of regulators to achieve regulatory goals. Especially when it comes to preventing financial crimes, these characteristics could have significant negative impact on the ability of regulators. The intergovernmental Financial Action Task Force "FATF" recognizes these issues and is tackling them by issuing multiple guidelines; however, it seems that such efforts are falling behind rapid technological developments. Thus, financial regulators must discover ways to achieve regulatory goals even in a blockchain-based financial ecosystem. This situation is similar to the case of telecommunication regulators during the rise of the Internet. The Internet complicated their regulatory goals including intellectual property rights protection and contents regulation. Thus, their relevant experiences provide a good reference. In the face of such difficulties in cyberspace, it was suggested to invoke not just law but also social norms, market mechanisms and architecture (software and hardware) to achieve a certain level of oversight. In fact, various stakeholders cooperated towards utilizing these modes of oversight in order to address issues brought by the Internet. Based on the lessons from the Internet, financial regulators should recognize that cooperation between multi-stakeholders would be beneficial for them, and they should actively play a role towards establishing a cooperative environment among stakeholders. Especially because code embedded in a blockchain system could determine the level of oversight on the activities within a blockchain-based financial ecosystem, regulators should consider ways to cooperate with engineering communities developing code despite often disparate incentives and mindsets. Once regulators successfully establish a cooperative relationship with the engineering community and can together develop code that facilitates mechanisms to achieve regulatory goals, they still must empower society to use such code in order to actually achieve regulatory goals, which requires consideration on alignment with social norms and market competitiveness; thus, regulators must cooperate with other stakeholders including businesses and users.

Through these considerations, this paper concludes that regulators should establish multi-stakeholder governance mechanisms within a blockchain-based financial ecosystem by improving cooperation among stakeholders. The final part of this paper provides some thoughts on relevant open questions, which we will continue to work on.

The SEC, Digital Assets, and Game Theory

Yuliya Guseva

Journal of Corporation Law. 46 (2020): 629.
https://heinonline.org/HOL/P?h=hein.journals/jcorl46&i=661

Abstract

The Securities and Exchange Commission (SEC) has not provided a clear rule to digital asset market participants concerning the nature of cryptoassets, namely, how to determine whether an asset is a security subject to the federal securities laws or something else, like a commodity regulated outside of the purview of the securities statutes. Instead of a formal rule, the SEC has chosen a more flexible modus operandi of enforcement actions in reliance on the functional definition embedded in the Supreme Court Howey decision interpreting the term "investment contract." This Article examines empirical data and develops a model suggesting that, despite the underlying indeterminacy associated with functional definitions and regulation by enforcement, the SEC attempted to reduce information losses and improved regulatory clarity by following a set of well-defined strategies during the first years of its crypto-enforcement efforts. Unfortunately, recent enforcement actions may upend these initially successful game strategies and undermine the efficacy of the techniques the SEC used to minimize the downsides of functional definitions and the regulation via enforcement tactics. As a result, the fabric of cooperation between the innovators and the SEC may be broken, leading to a suboptimal outcome for all market participants and the Commission itself These problems are particularly important in the rapidly evolving world of crypto, DeFi, and fintech.

A Conceptual Framework for Digital-Asset Securities: Tokens and Coins as Debt and Equity

Yuliya Guseva

Maryland Law Review. 80 (2020): 166.
https://heinonline.org/HOL/P?h=hein.journals/mllr80&i=166

Abstract

The article offers a novel approach to the threshold questions on the applicability of securities law to digital assets. The clarity of this framework should be useful to courts, regulators, and market participants. Digital-asset development involves two stages, and securities law is essential only in Stage One. However, federal securities law may apply post-launch and post-asset-delivery, i.e., during the Second Stage of a digital asset project, but in a limited way. During Stage Two, there can be two distinct and separate types of assets – a non-security-token (or coin) and a bond - simultaneously circulating after the project has been deployed and tokens distributed. In addition, there are two groups of digital asset purchasers: the initial investors who own tokens post-delivery and post-platform-launch and the subsequent token purchasers. They exist concurrently. These two cohorts of market participants have completely divergent expectations concerning the role of the issuer in the operation of the platform and the valuation of digital assets. Only the initial “bondholders” have claims against the issuer in Stage Two.

Crypto-Enforcement Around the World

Douglas S. Eakeley, Yuliya Guseva, Leo Choi, Katarina Gonzalez

Southern California Law Review. Postscript 94 (2020): 99.
https://heinonline.org/HOL/P?h=hein.journals/pstscrpt94&i=99

Abstract

The market for cryptoassets is burgeoning as distributed ledger technology transforms financial markets. With the extraordinary growth in the crypto-markets comes the need for regulation to promote efficiency, capital formation, and innovation while protecting investors. With the need for regulation comes enforcement. The blockchain revolution in capital and financial markets has already attracted the attention of enforcement agencies in many jurisdictions. In this Article, we elaborate on crypto-related enforcement and report on the results of the Enforcement Survey conducted by the Rutgers Center for Corporate Law and Governance Fintech and Blockchain Research Program.

We find that the United States Securities and Exchange Commission ("SEC" or "Commission") brings more enforcement actions against digital-asset issuers, broker-dealers, exchanges, and other crypto-market participants than any other major crypto-jurisdiction. By the same token, its enforcement entails more serious penalties. In addition to reviewing the international data, we provide detailed comparisons of the crypto-enforcement actions of the United States Commodity Futures Trading Commission ("CFTC") and the crypto-enforcement program of the SEC. Whereas SEC enforcement has been relatively stable, CFTC cases have been trending up. By contrast, enforcement in foreign jurisdictions seems to be subsiding. Our data raise theoretical questions on regulation via enforcement, its effect on financial innovation, and regulatory competition.

In Part I, we start with discussing the pros and cons of regulation by enforcement, as well as its consequences for innovation and a possible outflow of capital. Part II describes the methodology of the research. Part III presents the main findings. Parts IV and V discuss SEC and CFTC enforcement data, respectively, while Part VI compares the enforcement actions of the two regulators.

Trust in Context: The Impact of Regulation on Blockchain and DeFi

Balazs Bodo, Primavera de Filippi

Amsterdam Law School Legal Studies Research Paper No. 2022-07; Institute for Information Law Research Paper No. 2022-01.
http://dx.doi.org/10.2139/ssrn.4051842

Abstract

Trust is a key resource in financial transactions. Traditional financial institutions, and novel blockchain-based decentralized financial services (DeFi) rely on fundamentally different sources of trust and confidence. The former relies on heavy regulation, trusted intermediaries, clear rules (and restrictions) on market competition, and long standing informal expectations on what banks and other financial intermediaries are supposed to do or not to do. The latter rely on blockchain technology to provide confidence in the outcome of rules encoded in protocols and smart contracts. Their main promise is to create confidence in the way the blockchain architecture enforces rules, rather than to trust banks, regulators, markets. In this article, we compare the trust architectures surrounding these two financial systems. We provide a deeper analysis of how proposed regulation in the blockchain space affects the code- and confidence-based architectures which so far have underwrote DeFi. We argue that despite the solid safeguards and guarantees which code can offer, the confidence in DeFi is still very much dependent on more traditional trust-enhancing mechanisms, such as code governance, and anti-fraud regulation to address some of the issues which currently plague this domain, and which have no immediate, purely software-based solutions. What is more, given the risks of bugs or scams in the DeFi space, regulation and trusted intermediaries may need to play a more active role, in order for DeFi to gain the trust of the next generation of users.

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

清華大學
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

M UNIVERSITY OF MICHIGAN

UNIVERSITY *of* NICOSIA

USP Universidade de São Paulo

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

UNIVERSITY OF WYOMING

Royal University of Bhutan

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 40 university partnerships, supporting more than 500 research projects and new or modified course curricula for more than 280 university courses.