Expanding the Scope of Distributed Consensus

RFI Topic Area 2

Applications and Barriers to Consensus Protocols (ABC)

Organization:
Carnegie Mellon University

Type of Organization:
Other Educational

Technical POC
Vipul Goyal
CMU Computer Science Department
5000 Forbes Ave
Pittsburgh, PA 15213
Tel: (412) 593 4000
E-Mail: goyal@cs.cmu.edu

Administrative POC
Janise Loell
Research Administrator
5000 Forbes Ave
Pittsburgh, PA 15213
Tel: (412) 268-5597
E-Mail: osp@andrew.cmu.edu

Technical Contributors
Nicolas Christin, Vipul Goyal, Norman Sadeh, and Ariel Zetlin-Jones
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213

1 Goals and Impact

Blockchains, or distributed consensus technologies, hold tremendous promise for organically handling private, secure data, which in turn could have a dramatic impact across a number of strategically important application domains spanning across both DoD and civilian scenarios. Realizing this promise requires new, powerful innovations in distributed consensus technology. These innovations will allow the use of blockchains outside the scope of existing applications such as cryptocurrencies or supply chain management protocols. Evaluating the promise of such innovations requires a careful, quantitative understanding of the risks inherent with transferring secure data to the blockchain. Neither the full potential of blockchain nor the risks associated with its use are fully understood at this point. Research and innovation are critically needed right now to determine how to maximize the potential of this nascent technology and how to undertake corrective actions to determine and minimize its risks.

We propose to significantly expand the reach of blockchain by enabling the storage of and computation on data stored in secret-shared form. We outline a vision to determine and quantify the (currently unknown) risks associated with the use of blockchain technologies. We also propose the use of novel, economic incentives to reduce the risks associated with known threat-points in existing implementations of blockchain.

Expanding the Scope of Blockchain Applications. Storing (classified) data in a decentralized fashion (using secret-sharing) has obvious economic benefits. First, this type of storage avoids a single point of attack since an adversary would have to compromise several settings potentially located on different networks, and, running a different operating system. Second, this type of storage avoids giving a single entity (such as the AWS cloud) excessive control and data collection abilities. With the rapid rise in industry concentration, especially among the firms concentrated in new technologies that are collecting ever larger amounts of data on each user's behavior, the importance of latter benefit would appear to be growing. Other potential applications include supporting democratically-minded activities that would otherwise run the risk of state censorship and repression, thereby promoting democratic values that are a cornerstone of our nation and of our foreign policy. We would also explore the use of Blockchains in the context of IoT devices to, e.g., decentralize data collection, and, crowd-source the location of IoT devices accurately (even in the presence of adversarial entities).

Understanding and Dealing with Blockchain Risks. The risks and costs associated with blockchain implementation are currently less clear. While much media has been focused on the energy costs that arise in maintaining a blockchain ledger, our research emphasizes both known and unknown security risks—that is, risks that threaten the security or permanence of blockchain data. For instance, blockchain infrastructure hinges on miners to codify the network consensus about the state of the ledger. Blockchain protocols circumvent impossibility results on distributed consensus among byzantine parties by assuming economic rationality of the network participants. However, little work has so far been done in quantifying how deviations from perfect participant rationality can impact ledger security—researchers have started investigating game-theoretic and other models of possible attacks (e.g., selfish mining, bribery attacks), but a more general theory to understand the trade-offs between the strength of the security guarantees provided and the economic incentives at play is urgently needed.

2 Technical Plan

Our proposal consists of two interrelated parts: first, the determination and careful measurement of the risks associated with existing implementations of blockchain technology. Second, we propose significant advancements in the capabilities of distributed consensus mechanisms as well as the economic incentives that ensure the security and permanence of data stored on the blockchain.

2.1 Determining and Measuring Blockchain Risks

We have so far very limited understanding of how economic incentives shape blockchain security. The naive view is that the blockchain is secure if a majority of the network behaves properly. However, this has been shown to be untrue under certain conditions [ES14]. More generally, the value of the assets secured on the blockchain might be sufficiently high, that attackers may find it economically rational to spend the amount of money needed to either bribe or convince miners to rewrite history.

We argue that, as a research community, we need to first measure potential instances of malicious behavior in practice, by looking into existing ledgers for evidence of abnormal behavior (e.g., causes and consequences of denial-of-service attacks on existing ledgers). Indeed, existing blockchains provide an ecologically valid environment (since people are playing with actual money) to measure deviant behavior in practice, and better understand the rational trade-offs malicious participants make. This work would take advantage of the many different blockchains already deployed today. At the same time, we also envision conducting empirical studies such as competitions involving automated agents, human subjects or both, where participants are encouraged to compete under interesting conditions not found in the wild yet. This would be similar to work conducted in automated trading over the past 15+ years - see for instance, the supply chain trading agent competition co-designed by one of the proposers, as a way of exploring strategic behaviors under realistic supply chain trading competitions [AS05,CAS+05].

Second, informed by (but not limited to) these measurements, we argue that we need to develop new theoretical frameworks (e.g., based on game theory) to help us fundamentally understand such tradeoffs.

2.2 Expanding the Reach of Blockchains

Our aims in development are twofold. First, we propose to develop a new and powerful distributed consensus technology. Our technology would enable the miners to jointly store secret data in a secret-shared form. In addition, our technology would allow one to perform useful computation on the stored secret data, This would allow one to essentially emulate a full-fledged trusted cloud capable of storing and computing on classified data. A few compelling applications follow:

Decentralized secure storage with access control. Storing classified data securely is one of the biggest challenges in the world of cyber-security. There is no shortage of high profile cases of data leak: from credit card numbers, to passwords, to personal information such as social security numbers, or classified government memos. Our technology will allow us to realize decentralized storage. The classified data would be stored in a secret shared form with the miners (or the consensus nodes) using, e.g., Shamir secret sharing. In fact, to improve efficiency, the data could first be encrypted using a random key, and, only the key could be secret shared among the miners.

Towards retrieval of the data, there are several options. The retrieval could be based on the attributes or the credentials which the user holds. Any user could post a (signed) request to recover a subset of the stored data along with a certificate of his credentials. Only if the credentials are appropriate, the miners would individually release their shares of the key to this user. Given a sufficient number of shares, the user would be able to recover the secret key and hence decrypt the data. Since various miners might be corrupted and give out incorrect shares, Reed-Solomon decoding could be used to tolerate errors. The reconstruction could be time-based. For example, HBO could store the latest Game of Thrones episode and ask the miners to release the decryption key only at 9PM on the coming Sunday. In general, one could write an arbitrary program to specify the access policy.

Moving beyond storage. Our broader goal is to move from a centralized trusted cloud to a distributed cloud (emulated by the miners). The distributed cloud will provide all the functionality that a trusted cloud can without having the strong trust assumptions or a single point of failure. To achieve our goal, we need to go beyond just storing sensitive data. While a trusted cloud must indeed store sensitive data, it must also perform useful computations on the stored data. Examples include answering database queries, performing a keyword search, or, performing a data mining operation. We propose to allow computations on private data using cryptographic techniques of secure multi-party computation (MPC).

Economic Incentives. Our second aim is to propose significant improvements to the decentralized economic incentives that play a critical role in validating and securing data on the blockchain. Existing blockchains, based on the proof-of-work consensus protocol necessarily feature a time lag of roughly one hour before users can "trust" the information on the blockchain. In Bitcoin, this lag results in a settlement lag before parties are willing to exchange real goods and services in exchange for tokens. In other blockchain applications, this lag would result in possibly a pure information lag. The time delay plays a key role in securing the data on the blockchain from malicious attacks by those attempting to overwrite the history of the data for personal gain.

One currently recognized type of attack is the so-called 51% attack. This attack may be deployed by a miner, or group of miners that control more than 51% of a blockchain networks mining capacity. Given sufficient mining capacity, a miner may over-write elements in previous blocks of data and then subsequently mine new blocks fast enough to outpace the rest of the network. Eventually, the malicious miners blockchain would become long enough and the protocol would recommend all users switch to the malicious miners chain making this altered chain the new "valid data.

Our research develops new mechanisms to disincentive these types of attacks on the security of blockchain data with alternative economic incentives. We develop a new, game-theoretic model and show that the usefulness of a 51% is a feature of the specific implementation of blockchain used in Bitcoin and other proof-of-work based applications. Importantly, it is not a limitation of the technology. In other words, we show that there exist alternative protocols that can implement blockchain record-keeping while eliminating miners incentives to attempt 51% attacks using economic incentives. Constructing these incentives requires careful monitoring of the history of blockchain and providing differential economic incentives (rewards or punishments) as miners propose alternative ledgers. Extensions of this work will allow us to determine the minimum lag needed to prevent such attacks and to ensure security of blockchain data.

3 Bio and Capabilities

Nicolas Christin is an Associate Research Professor at Carnegie Mellon University, jointly appointed in the School of Computer Science, and the Department of Engineering and Public Policy. He is affiliated with the Institute for Software Research, and a core faculty in CyLab, the university-wide information security institute. His research interests are in computer and information systems security; most of his work is at the boundary of systems and policy research. Papers he co-authored won several awards including best paper awards at USENIX Security (twice) and ACM CHI, the 2016 Google Security and Privacy Research award, and the 2018 IEEE Cybersecurity Award for Practice.

Vipul Goyal is an Associate Professor in the Computer Science Department at CMU. Previously, he was a researcher in the Cryptography and Complexity group at Microsoft Research, India. Dr. Goyal is a winner of several honors including a 2016 ACM CCS test of time award, a Microsoft Research graduate fellowship, and, a Google outstanding graduate student award. He was named to the Forbes magazine 30 under 30 list of people changing science and healthcare in 2013. His research has received media coverage at popular science publications such as MIT technology reviews, Slashdot, and, Nature news. He has published over 70 technical papers at top conferences in cryptography such as at Crypto, Eurocrypt, STOC, FOCS, and, ACM CCS.

Norman Sadeh is a Professor in the School of Computer Science at Carnegie Mellon University, where he is affiliated with the Institute for Software Research, the Human Computer Interaction Institute and the CyLab Security and Privacy Institute. Norman is also co-founder and co-director of the Masters Program in Privacy Engineering, director of the School of Computer Sciences Mobile Commerce Lab and co-founder of the Schools PhD program in Societal Computing. His research interests span mobile and IoT, cybersecurity, privacy, machine learning, artificial intelligence and related public policy issues

Ariel Zetlin-Jones is an Associate Professor of Economics at the Tepper School of Business, Carnegie Mellon University. His research focuses on developing a better understanding of the workings of financial markets with implications for the design of optimal financial regulations. His research has been published in the American Economic Review, the Journal of Political Economy, and the Journal of Monetary Economics.

References

[AS05] R Arunachalam, NM Sadeh, *The supply chain trading agent competition*, Electronic Commerce Research and Applications 4 (1), 66-84.

[CAS+05] J Collins, R Arunachalam, NM Sadeh, J Eriksson, N Finne, S Janson, *The supply chain management game for the 2005 trading agent competition*, Carnegie-Mellon University.

[ES14] Eyal, Ittay, and Emin Gn Sirer. *Majority is not enough: Bitcoin mining is vulnerable*. In Proceedings of Financial Cryptography and Data Security: 18th International Conference, FC 2014 (N. Christin and R. Safavi-Naini, editors). Barbados, March 3-7, 2014.