A Review of Crypto Networks

Mian Zhang[1] **and Yuhong Ji**[2]

[1]**College of Art and Science, Roosevelt University**
[2]**College of Education and Human Development, Texas A&M University**

Corresponding author:
Mian Zhang[1]

Email address: mzhang1@mail.roosevelt.edu

ABSTRACT

Bitcoin is a crypto currency system that has been rapidly adopted due to its anonymity and decentralized properties. Blockchain is the underpinning technology that maintains the Bitcoin transaction ledger. The blockchain network operates in a state of consensus, which automatically checks in with itself periodically. One of biggest innovation by Bitcoin system is that it is a new way to develop open networks. Anything that happens on the blockchain is a function of the network as a whole. Crypto networks represent a fundamental shift in the way our society transacts, organizes, and works with each other, which could be explained and deciphered by econophysics of the network itself. From a networking perspective, we reviewed a list of current literatures that studied the crypto networks, mostly Bitcoin transaction networks. We identified the potential research areas that would further provide insights into the design of a more resilient and secure crypto networks.

INTRODUCTION

Bitcoin was originally proposed as a peer-to-peer electronic cash system without relying on the trust of any third parties [1]. It also solves the problem of double-spending. The intrinsic decentralized characteristic of blockchain allows it to propagate information in a peer-to-peer manner. The decentralized approach is consistent in all aspects of the Bitcoin system including data generation, storage, dissemination, and acknowledgement. Blockchain and crypto-networks as the underlying technologies that power Bitcoin has many advantages over traditional internet services. As a self-auditing ecosystem of a digital value, the Bitcoin blockchain network reconciles every transaction that happens in ten-minute intervals.

Unlike traditional giant internet service providers such as Google and Facebook who completely dominate the way to distribute the wealth, the fair distribution of blockchain is built in the protocol from the born time. The blockchain potentially cuts out the middleman for these types of transactions. This enables the developers and users of the platform to grow in a healthy manner, since all the values created by network participants go back to the value creators. Like any other networks, Bitcoin network is no exception when it comes to malicious attacks. One of the notable form of attack against Bitcoin network topology is eclipsing attack by using information propagation knowledge [2]. Hence, it is critical that future crypto-network should be designed as both robust and secure by learning and improving early crypto-network such Bitcoin. We review some preliminary researches in this domain, and in particularly from the perspective of network science and engineering.

A NETWORKING PERSPECTIVE

Bitcoin as fully decentralized global currency has been analyzed from a networking perspective. As information flows among different nodes in bitcoin network, Bitcoin transaction is slow due to the fact that information needs to be propagated across the network to synchronize the ledger replicas. The slow dissemination of information exposes a potential security hole for the malicious attacks. This also causes the blockchain to fork frequently. Some measures have been implemented to mitigate the number of the blockchain forks in the network by 50%. However, a long-term solution is still needed [2]. Bitcoin peer-to-peer network topology can be inferred and utilized by malicious attackers to perform precise attacks such as eclipsing attack. By observing the flooding process of the information flow, a flooding

network's topology can be inferred. A network topology inference method has been proposed along with a proof of concept in real network [3].

Bitcoin's decentralized fair peer-to-peer operation can be attributed to the notion of peers being able to reach a global consensus. The broadcast substrate in Bitcoin protocol is the key components by which peers can communicate with each other. Nodes have been identified to have disproportionate influence on the entire bitcoin network. An efficient and scalable technique called AddressProbe has been proposed to scan the entire network in minutes regularly without affecting bitcoin peers [4]. Estimably 2% of the nodes accounts 75% of mining power. A resilient topological structure has been identified, although it does not resemble a traditional random graph behavior. The degree distribution of Bitcoin's transaction graph converges to a scale-free network over time [5]. A more comprehensive study of network characteristics could be extended to various centrality metrics and temporal graphs [6–15]. Spectral clustering properties of the network can also be studied on Bitcoin transaction networks to compare with scale-free networks [16]. A detailed analysis of Bitcoin network has been performed in [17]. Two phases of bitcoin transaction network has been observed. Before Bitcoin gets popular, large fluctuations in network characteristics such as degree distribution have been observed. After Bitcoin gets wide public attention, the network involvement is driven by preferential attachment.

The same as Bitcoin, Ethereum is a decentralized public blockchain network [18]. Although there are some significant technical distinctions between them, the most important difference is that Bitcoin and Ethereum differ substantially in purpose and capability. While the Bitcoin blockchain is primarily used to keep track of digital currency ownership, the Ethereum blockchain concentrates on executing the programming code of any decentralized application. In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network. Denial-of-service attacks have been identified by exploiting an Ethereum Virtual Machine instruction. The attacker floods the network with that instruction, causing a decrease of its computational power, and a substantial slowdown to the blockchain synchronization process [19].

CONCLUSIONS AND FUTURE WORK

We reviewed the existing researches of crypto networks from a networking science perspective. A list of graph attributes have been studied. The distribution pattern of the currency has been identified from an econophysics perspective. Ethereum and Bitcoin networks are the two major crypto-networks under most extensive research. We expect more researches into other types of crypto-networks. Other aspects of crypto network security could also be studied. Machine learning techniques can be applied to predict the network attack probabilities in the future [20–24].

REFERENCES

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system.

[2] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, pages 1–10. IEEE, 2013.

[3] Till Neudecker, Philipp Andelfinger, and Hannes Hartenstein. Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In *Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences*, pages 358–367. IEEE, 2016.

[4] Andrew Miller, James Litton, Andrew Pachulski, Neal Gupta, Dave Levin, Neil Spring, and Bobby Bhattacharjee. Discovering bitcoin?s public topology and influential nodes. *et al.*, 2015.

[5] Annika Baumann, Benjamin Fabian, and Matthias Lischke. Exploring the bitcoin network. In *WEBIST (1)*, pages 369–374, 2014.

[6] Dongsheng Zhang. Resilience enhancement of container-based cloud load balancing service. Technical report, PeerJ Preprints, 2018.

[7] Dongsheng Zhang. *Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks*. PhD thesis, University of Kansas, 2015.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26911v1 | CC BY 4.0 Open Access | rec: 3 May 2018, publ: 3 May 2018

[8] Dongsheng Zhang and James P.G. Sterbenz. Modelling critical node attacks in MANETs. In *Self-Organizing Systems*, volume 8221 of *Lecture Notes in Computer Science*, pages 127–138. Springer Berlin Heidelberg, 2014.

[9] Dongsheng Zhang and James P. G. Sterbenz. Analysis of Critical Node Attacks in Mobile Ad Hoc Networks. In *Proceedings of the 6th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 171–178, Barcelona, Spain, November 2014.

[10] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. Çetinkaya, and James P.G. Sterbenz. Modelling Wireless Challenges. In *Proceedings of the 18th ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 423–425, Istanbul, August 2012. Extended Abstract.

[11] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. Çetinkaya, and James P.G. Sterbenz. Modelling Attacks and Challenges to Wireless Networks. In *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 806–812, St. Petersburg, October 2012.

[12] Dongsheng Zhang and James P. G. Sterbenz. Measuring the Resilience of Mobile Ad Hoc Networks with Human Walk Patterns. In *Proceedings of the 7th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, Munich, Germany, October 2015.

[13] Dongsheng Zhang and James PG Sterbenz. Robustness Analysis and Enhancement of MANETs using Human Mobility Traces. *Journal of network and systems management*, 24(3):653–680, 2016.

[14] Dongsheng Zhang and James P. G. Sterbenz. Robustness analysis of mobile ad hoc networks using human mobility traces. In *Proceedings of the 11th International Conference on Design of Reliable Communication Networks (DRCN)*, Kansas City, USA, March 2015.

[15] Dongsheng Zhang and James P. G. Sterbenz. Measuring the resilience of mobile ad hoc networks with human walk patterns. In *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 161–168, Oct 2015.

[16] Shuai Yuan, Pang-Ning Tan, Kendra Spence Cheruvelil, Sarah M Collins, and Patricia A Soranno. Constrained spectral clustering for regionalization: exploring the trade-off between spatial contiguity and landscape homogeneity. In *Data Science and Advanced Analytics (DSAA), 2015. 36678 2015. IEEE International Conference on*, pages 1–10. IEEE, 2015.

[17] Dániel Kondor, Márton Pósfai, István Csabai, and Gábor Vattay. Do the rich get richer? an empirical analysis of the bitcoin transaction network. *PloS one*, 9(2):e86197, 2014.

[18] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151:1–32, 2014.

[19] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In *International Conference on Principles of Security and Trust*, pages 164–186. Springer, 2017.

[20] Shuai Yuan, Pang-Ning Tan, Kendra S Cheruvelil, C Emi Fergus, Nicholas K Skaff, and Patricia A Soranno. Hash-based feature learning for incomplete continuous-valued data. In *Proceedings of the 2017 SIAM International Conference on Data Mining*, pages 678–686. SIAM, 2017.

[21] Shuai Yuan, Jiayu Zhou, Pang-Ning Tan, Emi Fergus, Tyler Wagner, and Patricia Soranno. Multi-level multi-task learning for modeling cross-scale interactions in nested geospatial data. In *Data Mining (ICDM), 2017 IEEE International Conference on*, pages 1153–1158. IEEE, 2017.

[22] Noah R Lottig, Pang-Ning Tan, Tyler Wagner, Kendra Spence Cheruvelil, Patricia A Soranno, Emily H Stanley, Caren E Scott, Craig A Stow, and Shuai Yuan. Macroscale patterns of synchrony identify complex relationships among spatial and temporal ecosystem drivers. *Ecosphere*, 8(12), 2017.

[23] Kendra Spence Cheruvelil, Shuai Yuan, Katherine E Webster, Pang-Ning Tan, Jean-François Lapierre, Sarah M Collins, C Emi Fergus, Caren E Scott, Emily Norton Henry, Patricia A Soranno, et al. Creating multithemed ecological regions for macroscale ecology: testing a flexible, repeatable, and accessible clustering method. *Ecology and evolution*, 7(9):3046–3058, 2017.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26911v1 | CC BY 4.0 Open Access | rec: 3 May 2018, publ: 3 May 2018

[24] Patricia A Soranno, Edward G Bissell, Kendra S Cheruvelil, Samuel T Christel, Sarah M Collins, C Emi Fergus, Christopher T Filstrup, Jean-Francois Lapierre, Noah R Lottig, Samantha K Oliver, et al. Building a multi-scaled geospatial temporal ecology database from disparate data sources: fostering open science and data reuse. *GigaScience*, 4(1):28, 2015.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26911v1 | CC BY 4.0 Open Access | rec: 3 May 2018, publ: 3 May 2018