CS6290: Reading Summary III

Yang Ji
Dept. of Computer Science
ID: 56064832

I. Summary of Paper [1]

A. Problem Statement

This survey paper targets at a systematic summary of privacy and security issues in Bitcoin. To be more specific, the authors firstly present a overview of its workflow and protocols. From the perspective of system security and privacy, they then discuss the existing vulnerabilities and countermeasures elaborately. By analyzing pros and cons of these possible solutions, they summarize remaining questions and latent research directions of blockchain.

B. Problem Significance

Compared to other general survey papers, this paper focuses on the privacy and security issues in Bitcoin, which renders an detailed security analysis to us.

C. State of the Art

Apart from double spending, there are also many other types of attacks on Bitcoin like mining pool attacks, cryptography tool attacks and so on. According to the tutorials taught by TA and the descriptions in paper, I conclude these attacks as follows:

(i) **Double Spending.** Satoshi Nakamoto claimed that double spending problems can be avoided with a high probability [2] based on the assumption of majority honest nodes. However, this classical problem in cryptocurrency could still happen possibly by following some specific workflows. For example, two partial confirmations on the same unspent money might lead to a successful double spending.
Therefore, it is very necessary for recipients to wait for seven blocks to get a global confirmation. (But if the computational power of adversaries takes up a large proportion, waiting for multiple confirmations could still fail.) Except for the power of CPU, some other factors like network propagation delay, exchange service connectivity and node position in network could also bring about a double-spending.

(ii) **Mining Pool Attacks.** Due to the highly concentrated power, mining pools could easily launch a selfish mining or 51% attack. Another scenario is called Pool Hopping attack. Adversaries might collect the submitted shares from fellow miners and avoid these invalid attempts. What's more, bribery attacks would involve multi-party game.

(iii) **Client-side Threats.** Threat model in this part is related to key management and cryptographic schemes. In particular, Bitcoin adopts elliptic curve digital signature algorithm (ECDSA) to ensure the security of transactions. However, this signature scheme has some potential treats (e.g. collision attack) and current system has no migration plans for broken cryptographic scheme. And there are many third-party wallets targeting to address the tension between usability and security at the Bitcoin client.

(iv) **Attacks on Bitcoin and Networking Infrastructure.** This section lists a number of attacks on distributed network, including DDoS attacks, Malleability attacks, Refund attacks and Time jacking attack.

After rendering the above four kinds of security problems, the authors also provide several possible solutions. The key problem lies in its consensus protocol called Proof-of-Work (PoW). Therefore, many variants of PoW are proposed to address security issues in a new way of generating and verifying a new block. Despite these schemes solve specific problems in Bitcoin, they usually rely on some strong assumptions or bring about new troubles. For example, although Proof-of-Elapsed-Time avoids resources waste successfully, it incurs stale and broken chip problems.

Apart from security problems, privacy issues are also concerned by the public. In fact, Bitcoin provides the unlinkability in some degree. Users could hide their true identities in a high possibility by generating a fresh blockchain address for each transaction. However, some adversaries might utilize graph analysis of transactions, addresses or entities to deduce the relationships among different transactions. This heuristic method works well especially on the publicly known addresses. What's more, IP address leakage could also lead to a successful deanonymization attack.

As a countermeasure, mixing protocol could solve external unlinkability effectively. However, it also incurs other problems like limited scalability and internal privacy leakage. Another solution, like ZeroCash and ZeroCoin, is to realize a total privacy-preserving transaction by utilizing a trusted hardware called zk-SNARKs.

D. Contributions

This paper mainly focuses on the privacy and security issues of Bitcoin and conduct many detailed analyses on state-of-the-art approaches.

E. Remaining Questions

The domain of this paper is only limited to the security and privacy perspective of Bitcoin. Other cryptocurrency like Ethereum, which firstly introduces the smart contract in

TABLE I
COMPARISON OF THE MOST POPULAR ZKP SYSTEMS

Case	SNARKs	STARKs	Bulletproofs
Proving Algorithm	O($N\times log(N)$)	O($N\times poly-log(N)$)	O($N\times log(N)$)
Verifying Algorithm	O(1)	O($poly-log(N)$)	O(N)
Proof Size	O(1)	O($poly-log(N)$)	O($log(N)$)
Trusted Setup Required	Yes	No	No
Post-quantum secure	No	Yes	No
Crypto assumption	Strong	Collision resistant	Discrete Log

blockchain systems, has many distinct threats and challenges. And how to effectively balance the tensions in these cryptocurrencies still remains an open question.

II. SUMMARY OF PAPER [3]

A. Problem Statement

This paper presents a zero-knowledge (ZK) proof system which enables verifiable computation with strong confidentiality. Compared to ZK-SNARK system [4], ZK-STARK has no reliance on a trusted third party to generate its initial proving key. What's more, with assumptions on collision-based hash functions, this solution isn't vulnerable to post-quantum attacks. For cryptocurrencies, ZK-STARK has great practical value to scaling transaction throughput and achieving privacy-preserving transactions.

B. Problem Significance

Zero-knowledge proof could be used to address many trust issues in our daily life. In this paper, authors utilize a DNA profile match (DPM) example as a special case. Nowadays, governments usually play a role of a trusted third party to claim some statements or survey results are true. However, due to the lack of enough convincing evidence (these materials might be related to privacy issues), the public might question the validation of results. In this scenario, zero-knowledge proof could be viewed as a powerful tool to persuade the public of those issues with confidentiality requirement.

C. State of the Art

Summarizing, systems for ensuring computational integrity over confidential data possess the following six core virtues:

- **Transparency** It means proving process doesn't need any trusted third party.
- **Universality** The system could be applied to any efficient computation.
- **Confidentiality** The proof doesn't leak any other information except for witnesses.
- **Post-quantum Security** Many cryptographic assumptions start to crumble once quantum computers become scalable.
- **Proof/Argument of Knowledge** The proof could valid the statements efficiently.
- **Scalable Verification** Verifier could valid the witnesses in a short time.

From the perspective of the above six properties, the existing solutions can be summarized as follows:

- **Homomorphic public-key cryptography (hPKC):** ZK-SNARK is a classical zk system based on this theorem, which serves in ZeroCoin [5] and ZeroCash [6] system for privacy-preserving transactions. In general, hPKC methods lack transparency and post-quantum security. But in comparison with zk-STARK, verification time in hPKC is scalable.
- **Discrete logarithm problem (DLP):** The approach based on DLP has advantages on its succinct proof size and no trusted setup phase. However, due to broken DLP under quantum factoring algorithms, this method is actually quantum-susceptible. And verifier needs massive of resources to valid the proof.
- **Interactive Proofs (IP) based:** Like BulletProofs, these IP-based solutions are also quantum-susceptible and overlong verification time.
- **Secure multi-party computation (MPC):** Although MPC-based approaches are posy-quantum secure, transparent and have quasi-linear proving time, it can not render a scalable verification algorithm and a succinct proof.
- **Incrementally verifiable computaion (IVC):** This scheme could build on top of other proof systems and hence inherit internal properties of these systems.

D. Contributions

As for verifying computational integrity, the naive solution is to let verifiers re-execute programs again which is time-consuming and impractical. Especially, when the database involves some sensitive information (e.g. DNA profiles, personal particulars), this naive method won't work any more. Under this circumstance, a trusted third party is introduced to play a role as a warranter. However, due to unexpected attacks or corruption, this third party can't work well all the time. Therefore, zkp systems are proposed to balance the tension between data privacy and computational integrity.

ZK-STARK is a novel zero-knowledge system which renders scalable proving and verifying algorithms without any trusted setup phase. In particular, provers need to execute O($t\times log(t)$) steps to generate a proof and verifiers would cost the time of O($log^2(t)$) steps to validate the proof.

Despite the details of the whole system are obscure and complicated, the general idea is to convince verifiers just checking relatively low degree polynomial instead of the whole structure by employing FRI scheme.

E. Remaining Questions

Compared to ZK-SNARK, the short coming of ZK-STARK is long proof size and verification time. Whether this ideal approach could be improved further still remains an open question.

References

[1] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[2] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity." *IACR Cryptology ePrint Archive*, vol. 2018, p. 46, 2018.

[4] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, "Snarks for c: Verifying program executions succinctly and in zero knowledge," in *Advances in Cryptology–CRYPTO 2013*. Springer, 2013, pp. 90–108.

[5] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 397–411.

[6] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*. IEEE, 2014, pp. 459–474.