Review of: "CryptoAudit and its inherent challenges"

Larry Shi[1]

1 University of Houston

In this article, the author conducts a brief literature survey of cryptocurrency audit and then discusses challenges of cryptocurrency audit.

[] Strengths

The article is short and easy to understand. The information may be useful for the readers who want to get familiar with this topic area, in particular the challenges of cryptocurrency audit.

The article includes a brief survey of previously published work in cryptocurrency audit.

[] Comments

In introduction, the author appears to treat technologies such as electronic cash, digital currency, and cryptocurrency the same. In fact, these technologies are quite different.

Certain terms are mentioned in the article without definition, like triple entry book keeping, consensual accounting record.

Blockchain often involves both on-chain and off-chain data, which creates audit challenge because off-chain data is sometimes hidden from the public or auditor. Although mentioned at high level, the article does not explicitly describe the differences between on-chain data and off-chain data from audit perspective.

A subtle aspect is that blockchain validators are "auditors" who verify the blockchain ledger. The article does not explicitly define what additional and/or separate audit requirements are from accounting perspective.

Two specific reasons not sufficiently discussed causing audit challenges are: lack of digital identity in blockchain that connects digital wallets to legal person; and heterogeneous environment where digital assets are managed by both centralized (like centralized exchanges often located in different jurisdictions) and decentralized components. Services like mixers also make audit a difficult job.

No discussion of impact from emerging technologies such as ZK proof and audit based on general purpose ZK protocols.

[] Suggestions

Clarify the differences like electronic cash, cryptocurrency, and digital currency.

Define terms when they are introduced.

Elaborate the requirements of accounting audit and how these requirements can or cannot be met by the records of a distributed ledger.

Discuss emerging trend like impact of ZK based audit.