Custodianship of Cryptocurrencies

Seyedehmahsa Moosavi

Concordia University

Abstract.

The paper will include following parts:

1 Philosophy of Cryptocurrency Ownership and Control

First say Bitcoin (and all other cryptocurrency) and custodianship are mutually exclusive. Talk about the philosophy of ownership of cryptocurrency in the crypto space. Bitcoin holders believe that once they have the private key they have full ownership and control over those coins.

2 Why do we need a Custodian

However, auditors do not accept this philosophy, in case of a financial audit, an auditor wants to audit and they need to be equipped with some tools/things to make sure cryptocurrency holders actually own the coins. That is the reason custodianship for cryptocurrencies is significant. In the real world this is so simple, Alice gives her Bitcoins to Bob, who is certifies by some trusted parties to act as a custodian, however, there is no such service in the crypto space. The other use-case is the law enforcement when they want to freeze some illegal cryptocurrencies (Look at the references and docs you prepared before)

3 Custodianship of Non-crypto Assets

There is an standard of what it means to be a custodian: SOC 1 (or 2 not sure yet) Need to Be Paraphrased: A reporting framework through which organizations can communicate relevant useful information about the effectiveness of their cybersecurity risk management program and CPAs can report on such information to meet the cybersecurity information needs of a broad range of stakeholders.

If your company provides services to other companies, those services may have an impact on your customers' financial reporting. As a result, your customers' auditors may need assurance that the controls surrounding your services are designed effectively, and in some cases, operating effectively. A way to provide that assurance is by undergoing a Service Organization Control (SOC)

audit. SOC 1 and SOC 2 audit reports have distinct differences. In order to determine which one is right for your organization, you must know how they work.

System and Organization Controls (SOC) Reporting. SOC reports can help clients, prospects, stakeholders and other interested parties understand and gain confidence in the internal control environment of the service organization. Obtaining a SOC report can help service organizations: Meet client expectations, contractual commitments and regulatory requirements.

https://linfordco.com/blog/soc-1-vs-soc-2-audit-reports/ Difference between ISO 27001 and SOC 2: https://linfordco.com/blog/soc-2-security-vs-iso-27001-certification/

Soc 1: Do you need to report to regulators on controls over financial reporting? By certifying SOC 1 compliance of service organizations, clients, prospects and other stakeholders of the service organization are provided with reasonable confidence in its internal controls. There are two types of SOC 1 reports:

Soc 2: Does your company rely on vendors to process and safeguard your sensitive data—or are you a vendor entrusted with sensitive data? SOC 2 reports cover controls such as security and privacy and may be used by leaders in internal audit, risk management, operations, business lines and IT, as well as regulators.

The SOC 2 report addresses a service organization's controls that relate to operations and compliance, as outlined by the AICPA's Trust Services criteria in relation to availability, security, processing integrity, confidentiality and privacy. A service organization may choose a SOC 2 report that focuses on any one or all five Trust Service principles and may choose either a Type I or a Type II audit. A SOC 2 report includes a detailed description of the service auditor's test of controls and results. The use of this report is generally restricted. Why was the SOC 2 report created? The SOC 2 report was created in part because of the rise of cloud computing and business outsourcing of functions to service organizations. These are called user entities in the SOC reports. **Liability concerns have caused a demand in assurance of confidentiality and privacy of information processed by the system.**

In order for a firm to be able to serve as a custodianship service for currencies, it has to be SOC 1 certified (compliant). **Importnat**: When a service organization completes a SOC 2 report, the report contains an opinion from a CPA firm that states whether the CPA firm agrees with management's assertion. The opinion states that the appropriate controls are in place to address the selected TSCs and the controls are designed (Type I report) or designed and operating effectively (Type II report). In many cases, the opinion is positive and the CPA firm agrees with management's assertion. In other cases, the CPA firm does not agree with management's assertion and provides a qualified or adverse opinion. Very Good link (https://linfordco.com/blog/what-is-soc-2/)

My Own Words: If you (as a company) are hosting/processing information for your clients that is not affecting the financial reports, you might be just generally concerned that if you're handling their information in a secure way, or will this information be available to the clients as it's been agreed upon in the

	Custodianship	**Self Custodianship**
Currencies	1	2
Crypto-Currencies	3	4

Table 1:

contract, then you'll need a SOC 2 report/certification. (a CPA firm that has auditors can provide yo with this certification)

4 table

: cell 1,2,4: already exist. cell 3 does not exist and that's why we see a research gap here to be filled. You can have examples too: self custodianship of cryptocurrencies (cell 4): wallet, air-gap

References

1. Audit considerations related to cryptocurrency assets and transactions. `https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations`. (Accessed on 01/23/2019).
2. Auditing in the crypto-asset sector.pdf. `http://www.cpab-ccrc.ca/Documents/News%20and%20Publications/Auditing%20in%20the%20Crypto-Asset%20Sector.pdf`. (Accessed on 01/23/2019).
3. Bitcoins transferred at request of amf — amf. `https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/transfert-de-bitcoins-obtenu-a-la-demande-de-lautorite-des-marches-financiers/`. (Accessed on 01/22/2019).
4. Custodypaper.pdf. `https://www.iapf.ie/_files/list/CustodyPaper.pdf`. (Accessed on 01/23/2019).
5. Sec.gov — investor bulletin: Initial coin offerings. `https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings`. (Accessed on 01/22/2019).
6. www.iacpcybercenter.org/wp-content/uploads/2018/03/bitcoin.pdf. `http://www.iacpcybercenter.org/wp-content/uploads/2018/03/Bitcoin.pdf`. (Accessed on 01/22/2019).
7. J. B. A. M. J. Clark, A. N. J. A. K. Edward, and W. Felten. Research perspectives and challenges for bitcoin and cryptocurrencies. *url: https://eprint. iacr. org/2015/261. pdf*, 2015.
8. G. G. Dagher, B. Bünz, J. Bonneau, J. Clark, and D. Boneh. Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 720–731. ACM, 2015.
9. S. Eskandari, J. Clark, D. Barrera, and E. Stobert. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*, 2018.
10. T. Moore and N. Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In A.-R. Sadeghi, editor, *Financial Cryptography and Data Security*, pages 25–33, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

11. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
12. E. Pimentel, E. Boulianne, S. Eskandari, and J. Clark. A first look at auditing in a blockchain world. 2019.
13. C.-P. Schnorr. Efficient signature generation by smart cards. *Journal of cryptology*, 4(3):161–174, 1991.
14. H. Wang, D. He, and Y. Ji. Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. *Future Generation Computer Systems*, 2017.