{tag} {/tag}
IJCA Proceedings on National Conference cum Workshop on Bioinformatics and Computational Biology

NCWBCB - Number 2

Year of Publication: 2014

Authors:
Chinmay A. Vyas

Munindra Lunagaria

{bibtex}ncwbcb1414.bib{/bibtex}

Abstract

This paper focuses on the unique characteristics of Bitcoin as a cryptocurrency and the major security issues regarding the mining process and transaction process of Bitcoin. Nowadays, Bitcoin is emerging as the most successful implementation of the concept known as cryptocurrency. The Bitcoin records its transactions in a public log called the blockchain. The distributed protocols that maintain the blockchain are responsible for the security of the Bitcoin. The blockchain is run by participants known as the miners. The Bitcoin technology - the protocol and the cryptography - has a strong security track record, and the Bitcoin network is known as one of the largest distributed computing project in the world. The security aspect of

the Bitcoin is the major area of research. This currency may be vulnerable during the transactions or it can be also attacked on its online storage pools or exchanges. The recent researches, mainly focused on the protocol of the Bitcoin, shows that the currency is not fully secure against the colluding groups of users that uses different attacks to fraud the 'Honest' miners of the Bitcoin.

Refer ences

- Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" (2008).
- Ittay Eyal and Emin Gün Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," unpublished.
- Yogesh Malhotra, "Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System", December 4, 2013.
- Ghassan O. Karame, Elli Androulaki and Srdjan Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," In Proceedings of the ACM Conference on Computer and Communications Security (CCS), Chicago, IL, USA, pp. 1-17, 2012.
- M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On Bitcoin and Red Balloons," in ACM Conference on Electronic Commerce (EC'12), ACM,. pp. 1-18, June 2012.
- Proof of work (online available at: https://en. bitcoin. it/wiki/ Proof _of _stake).

Index Terms

Computer Science Security

Keywords

Bitcoin; Cryptocurrency; Security; Blockchain; Miners;