International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

Cryptocurrency and Cybersecurity

Shweta Tewari

S.P Jain School of Global Management, India, shweta.dbaff01031[at]spjain.org

1. Cryptocurrency and Cybersecurity

Bitcoin is a digital currency created in 2009. Bitcoin is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency, as the system works without a central bank or single administrator.

Bitcoin offers the promise of lower transaction fees than traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies. Today's market cap for all bitcoin (abbreviated BTC or, less frequently, XBT) in circulation exceeds $7 billion.The different types of cryptocurrency are – Litecoin, Ethereum, Zcash, Dash, Ripple, Monero etc.

2. How Bitcoin Works

The independent individuals and companies who own the governing computing power and participate in the Bitcoin network, also known as "miners," are motivated by rewards (the release of new bitcoin) and transaction fees paid in bitcoin. One bitcoin is divisible to eight decimal places (100 millionth of one bitcoin), and this smallest unit is referred to as a Satoshi. If necessary, and if the participating miners accept the change, Bitcoin could eventually be made divisible to even more decimal places.

3. Why Use Digital Currency?

In addition to things like better fraud protection and lower fees, the biggest benefit of digital currency is inherent in its existence; digital currency allows disenfranchised groups to store and exchange value. Digital currency is the economic means of that future.

Security Risk

Bitcoin exchanges are entirely digital and, as with any virtual system, are at risk from hackers, malware and operational glitches. If a thief gains access to a Bitcoin owner's computer hard drive and steals his private encryption key, he could transfer the stolen Bitcoins to another account. Hackers can also target Bitcoin exchanges, gaining access to thousands of accounts and digital wallets where bitcoins are stored.

In 2014, when Mt. Gox, a Bitcoin exchange in Japan, was forced to close down after millions of dollars worth of bitcoins were stolen.

Nearly $64m in bitcoin has been stolen by hackers of NiceHash.

Around $72 million worth of bitcoins were stolen from the South Korean exchange Youbit.

4. Continued Vulnerability

Hackers often use the same tactics to target multiple victims, driving down the cost of an attack while expanding the potential rewards.

The future looks bright for blockchain-based security platforms

The anonymity of the bitcoin wallets, and the ease and security in which users can transfer currency from one user to the next, opens the gateway for cyber criminals.

Blockchain technologies are here to stay. These days, the common method of adding users to any system is by using a centralized approach with logins and passwords. REMME, a new startup which aims at using blockchain to recognize devices and users, is trying to change that. Obsidian messenger is going to secure metadata of users by using blockchain. The user will not have to use email or any other authentication information in order to use the messenger. The metadata will be randomly distributed throughout a ledger and thus will not be available for gathering in one single point, from which it could then be hacked.