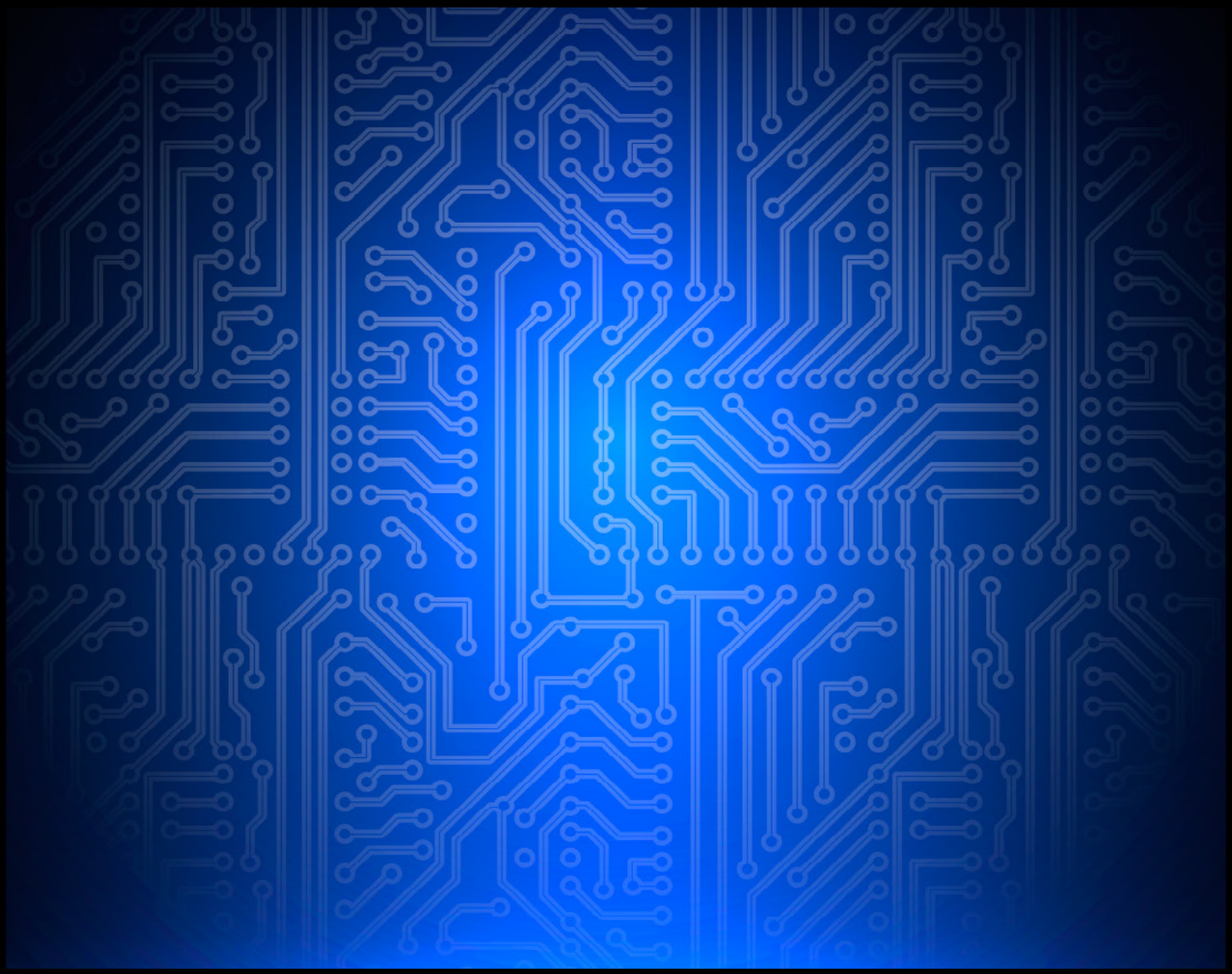
CYB3R

Vol.1 No.1 Issue 1/2013 (01)



SECURITY AWARENESS
CLOUD COMPUTING - POLITICS
INDUSTRIAL CONTROL SYSTEMS

Digital Currency: Future of Bitcoin's

by V P Prabhakaran

Its very important to understand the future of Digital Currency that is bitcoin. What is Bitcoint. Bitcoin is Networked Crypto-Currency. Networked Crypto-Currency Crypt " refer to the fact that the technology is based on the "Cryptography" branch of Mathematics

Bitcoins are transmitted from one bitcoin address to next in any amount desired.

Addresses are identified by a string of 32 random number and letters similar to a bank account number. User can have one or many Bitcoin address to send from and received it. If you want to learn how to use bitcoin's there are some website such as *weusecoins.com* and *tryBTC.com*.

Bitcoin is a software

In order to participate in Bitcoin people download Bitcoin software designed and written by public known developers from around the world. Changes are made to the software over time based on fixes and features that are in demand by consensus of users. No one person or authority can enforce changes.

- Because of this consensus based approach, many qualities that currencies would want to have in the free market are found in Bitcoin.
- Likewise many qualities that government regulations would like to a currency to have are extremely unlikely to be added Bitcoin.

Bitcoin Mining

Bitcoin Comes into existence when it is "mined" by a participant Bitcoin miners use special software and hardware to solve mathematical equations.

Many permutations of these equations have to be solved to find the right solutions and this servers as "Proof of work" performed by the miner the process is somewhat analogous to working to dig into the ground and mine gold, hence the term "mining".

Processing power of computers mining for Bitcoins is estimated to be 6-8x greater than the top 500 supercomputers combined as of july 2012. 3rd party website such a coinbase and Bitpay Server to make merchant transactions simpler and link Bitcoin account to legacy bank accounts.

Transactions

Bitcoin transactions are irreversible, so there is less risk to senders of fraud or "charge-back".

Escrow service can be used to help protect revivers as well.

Transaction anywhere in the world are generally confirmed with in 10 minutes, regardless of the size of the transactions. It is possible to have confirmed transactions within moments by introducing trusted intermediates amd "of-chain transactions" that are validated by 3rd parties rather than by Bitcoin network where highly regulated money servies like paypal have been unable to connect foreign market places, Bitcoin permits those previously isolated areas of the world to send and receive wealth, creating truly global marketplace. Bitcoin is often described as "frictionless" because of the lack of need for intermediate, low fees and speed. Authenticity of the transactions are double checked and assured by the rest of the network.

In order to protect privacy against incredibly powerful actor like the NSA, if it is possible to do so at all, a variety of seem-obscure tools must be utilized in very particular ways, any small mistake can leak information about the participants of bitcoin transactions. The notion that bitcoin is anonymous out of the box is a myth and few users are sufficiently educated to use bitcoin as anonymously as possible.

About the Author

V P Prabhakaran is an Information Security Consultant at Koenig Solutions Ltd and an industry certified professional who provides consultancy and trains candidates for Computer Hacking Forensic Security and Firewalls. He is certified in CEH, ECSA, ECSS, CHFI, OWASP, OSSTMM, OPSA OPST. Taking Session of CEH, ECSA, CHFI, ECSS, ENSA, ECIH, SSCP, OPSA, OPST, Backtrack, Metasploit of Overseas Clients.