Title of the project:

Bitcoin- An Innovation

Members in the team:

Ravali Chennamneni

Rajitha Devabhaktuni

Introduction and Motivation:

Bitcoin is a peer-to-peer (P2P) payment system which eliminates the need of a trusted third party to carry out transactions among the users in the network. It is referred to as the first digital crypto-currency though there were such inventions prior to this technology. The system is designed such that the users can take the advantage of its decentralized nature of operation without the need for a central authority and without overhead charges during transactions except for a samll transaction fee in some cases. It is one of the emerging technologies which has been invented in 2009 and has gained enough popularity all over the world within a short period. It has been invented by an unknown user with the pseudonym "Sathoshi Nakamoto". It is a virtual currency with the unit of account named 'bitcoin'. The users must download a web application in order to join the network and use the bitcoins. The transactions of bitcoins can be carried out through a computer or mobile apps. The bitcoins are stored in a digital wallet which is securing stored over a cloud or on the user's computer. The peers involving in transactions need not reveal their identities, instead they use wallet IDs for a secure transaction. The technology is based on public key infrastructure where in the user who is paying signs the transaction using his public key and the network verifies the signature with the corresponding public key of the user. Users are even rewarded bitcoins for solving complex math puzzles. In the present scenario, users are rewarded with 25 bitcoins every ten minutes approximately. This is how bitcoins are created. Through our case study, we will analyze on the security of bitcoin technology and a detailed explanation of different types of attacks possible and the corresponding improvements that can be made.

Protocols/ Algorithms / Implementations / Problems we are planning to explore:

1. SHA 256 hashing algorithm.

2. The bitcoin block chain technology used for bitcoin mining.

3. ECDSA (Elliptical curve digital signature Algorithm).

4. Multibit application.

Procedures for verifying the results of our investigation:

1. Examine the protocols and algorithms used in the transaction process.

2. Various types of attacks possible and improvements made.

3. Keeping track of all the improvements made and problems occurred since the invention of bitcoin technology till date.

4. Successful case studies of bitcoin users.

A Tentative list of questions we will be seeking an answer to:

1. How safe are the transactions under this technology?

2. How to analyze illegal activities of users who misuses the advantage of concealing the identity of the peers undergoing the transaction?

3. Is bitcoin the best available crypto-currency?

4. What are the possible attacks and solutions on bitcoin.

5. Is bitcoin vulnerable to quantum computing and does it have any security flaws.

6. Is bitcoin mining a waste of energy?

Work we're planning to do differently in comparison to the work done previously:

1. Considering different case studies of Bitcoin users, both who succeeded and who did not succeeded through the Technology (for a better understanding of the technology).

2. Bitcoin Improvement protocol (BIP).

3. Some vulnerabilities that may pose a threat to bitcoin like quantum computing and best solution so far to be safe from the threat, the Selfish-Mine Strategy (a mining strategy that enables pools of colluding miners that adopt it to earn revenues in excess of their mining power).

Tentative table of contents of your final report :

1. Introduction and Motivation.

2. Overview of Bitcoin.

3. Bitcoin Mining process.

4. Cryptography and Bitcoin.

5. Bitcoin Transactions and verification.

6. Attacks and possible alternative solutions.

7. Improvements made during the course of invention.

8. Conclusion.

9. References.

Time Schedule :

Oct 27-28: The basic working of bitcoin, detail analysis on bitcoin and its cryptographic sideand the security services that are compromised due to attacks.

Nov 3-4: the security services that are compromised due to attacks, and the examination of bitcoin in comparison to top 10 crypto-currencies available (such as Blackcoin, dogecoin, litecoin, namecoinetc). The comparison criteria seem to vary for each comparison.

Nov 17-18: First draft of the report .Working on the proposed improvements from the first meet.

Dec 1-2:Evaluation of results and final report. Also, make possible improvements if suggested.

Dec 8-9: Final presentation and Written report.

References:

[1] Eric Rykwalder , "The Math Behind Bitcoin" Internet: http://www.coindesk.com/math-behind-bitcoin/ , October 19, 1024.

[2] Morgen E. Peck , " The Future of the Web Looks a Lot Like Bitcoin" , Internet: http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin , July 1,2015 .

[3] Bitcoin. (2015, Sept 29). Wikipedia. Available: https://en.wikipedia.org/wiki/Bitcoin. Accessed: Oct 5,2015.

[4] What is Bitcoin? (n.d) CNN Money. [Online]. Available: http://money.cnn.com/infographic/technology/what-is-bitcoin/ . Accessed Oct. 3 , 2015.

[5] Josua Davis," THECRYPTO-CURRENCY" Internet: http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency , Oct 12, 2011.

[6] Andreas M. Antonopoulos. (2014) . Mastering Bitcoin: Unlocking Digital Cryptocurrencies . [Online]. Available: http://chimera.labs.oreilly.com/books/1234000001802/ch01.html

[7] Bitcoin . (n.d) . bitcoinwiki. [online]. Available: https://en.bitcoin.it/wiki/Main_Page. Accessed : Oct. 5, 2015.

[8] How do Bitcoin Transactions Work?. (2015, March 20). *Coin Desk* [Online]. Available: http://www.coindesk.com/information/how-do-bitcoin-transactions-work/

[9]Duncan Hood, "Bitcoin has flaws, but it will change the world" , Internet: http://www.canadianbusiness.com/economy/bitcoin-will-change-the-world/ , 7 Nov, 2013

[10] Max Raskin. (2013, April 10). Meet the Bitcoin Millionaires. *Bloomberg Business* [Online]. Available: http://www.bloomberg.com/bw/articles/2013-04-10/meet-the-bitcoin-millionaires.