CSE300_Assignment1
Introduction to LaTeX
Bitcoin

Sanjay Malakar
Student Id : 1505057

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology
(BUET)
Dhaka 1000

April 22, 2018

Contents

1 Introduction **3**

1.1 What is Bitcoin? 3

1.2 Who created Bitcoin? 3

2 How does Bitcoin work? **3**

2.1 What is block chain? 3

3 Acquiring and owning bitcoins **4**

3.1 Acquiring 4

3.2 Owning 4

4 Bitcoin and the Law **5**

5 The Mathematics Behind Bitcoin **5**

5.1 First Result 5

5.2 Other results 6

6 What does future hold for Bitcoin? **7**

1 Introduction

1.1 What is Bitcoin?

With the Bitcoin price so volatile everyone is curious. Bitcoin, the category creator of **blockchain technology**, is the **World Wide Ledger** yet extremely complicated and no one definition fully encapsulates it. By analogy it is like being able to send a gold coin via email. It is a consensus network that enables a new payment system and a completely digital money.
It is the first decentralized peer-to-peer***(P2P)*** payment network that is powered by its users with no central authority or middlemen. Bitcoin was the first practical implementation and is currently the most prominent triple entry bookkeeping system in existence.

1.2 Who created Bitcoin?

The first Bitcoin specification and proof of concept was published in 2009 by an unknown individual under the pseudonym Satoshi Nakamoto who revealed little about himself and left the project in late 2010. The Bitcoin community has since grown exponentially.
Satoshi's anonymity often raises unjustified concerns because of a misunderstanding of Bitcoin's open-source nature. Everyone has access to all of the source code all of the time and any developer can review or modify the software code. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper.

2 How does Bitcoin work?

From a user perspective, Bitcoin is nothing more than a mobile app or computer program that provides a personal Bitcoin wallet and enables a user to send and receive bitcoins.

Behind the scenes, the Bitcoin network is sharing a massive public ledger called the ”block chain”. This ledger contains every transaction ever processed which enables a user's computer to verify the validity of each transaction. The authenticity of each transaction is protected by digital signatures corresponding to the sending addresses therefore allowing all users to have full control over sending bitcoins.

2.1 What is block chain?

A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions. Constantly growing as completed blocks (the most recent transactions) are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the blockchain, which is downloaded automatically.

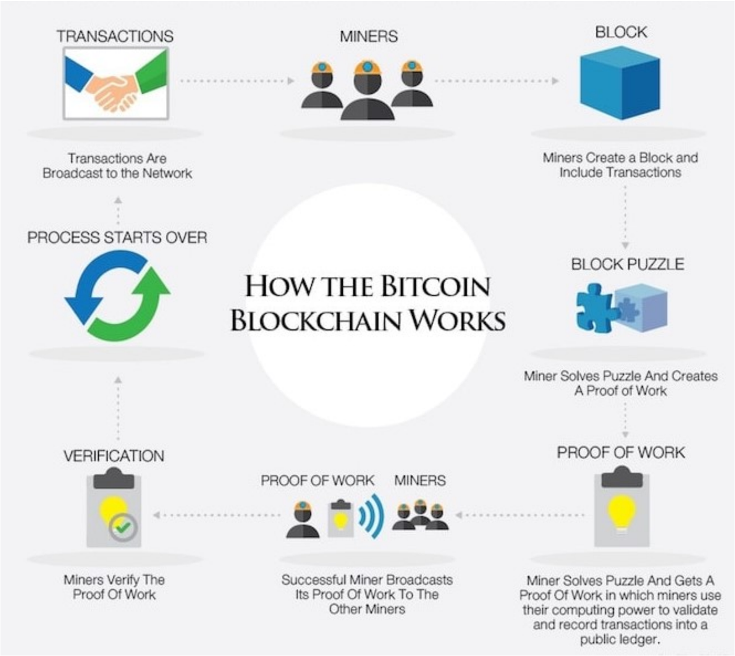

TRANSACTIONS
MINERS
BLOCK
Transactions Are Broadcast to the Network
Miners Create a Block and Include Transactions
PROCESS STARTS OVER
HOW THE BITCOIN BLOCKCHAIN WORKS
BLOCK PUZZLE
Miner Solves Puzzle And Creates A Proof of Work
VERIFICATION
PROOF OF WORK
MINERS
PROOF OF WORK
Miners Verify The Proof Of Work
Successful Miner Broadcasts Its Proof Of Work To The Other Miners
Miner Solves Puzzle And Gets A Proof Of Work in which miners use their computing power to validate and record transactions into a public ledger.

Figure 1: How bitcoin blockchain work

3 Acquiring and owning bitcoins

3.1 Acquiring

Some most popular ways are :

Buy on an Exchange Many marketplaces called bitcoin exchanges allow people to buy or sell bitcoins using different currencies.

Transfers People can send bitcoins to each other using mobile apps or their computers.

Mining People compete to mine bitcoins using computers to solve complex math puzzles.

3.2 Owning

Bitcoins are stored in a digital wallet, which exists either in the cloud or on a users computer. The wallet is a kind of virtual bank account that allows users to send or receive bitcoins, pay for goods or save their money.

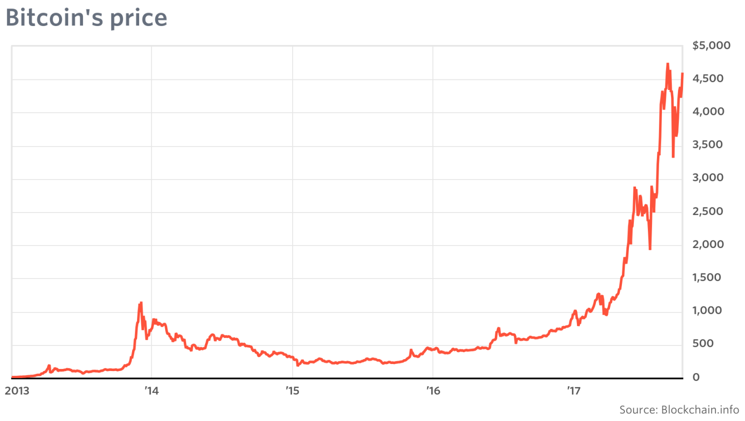
1. Wallet in cloud
2. Wallet on computer

4 Bitcoin and the Law

Mostly all governments will follow regulations such as Canada national law on digital currencies but always somewhere in the world criminals will find financial products free of any intervention in the e-currency, government-backed or otherwise.

- Bitcoin and Taxes : Bitcoin can be considered money as it fulfils the functions of money but it is doubtful that Bitcoin would pass as money in many Countries under the Nation-al Currency Law.

- National digital currency law : Parliament of Canada approved this June the worlds first national law on digital currencies in order check all transactions under national anti-money laundering law.


Bitcoin's price

Source: Blockchain.info

Figure 2: Bitcoins price over years

5 The Mathematics Behind Bitcoin

Why should we trust Bitcoin :

5.1 First Result

- Underestimation of double spend success probability

- **Existence of closed form formulas**

- Mathematical foundation of bitcoin

- Bitcoin and gamma functions

Notation 1. *Let* $0 < q < \frac{1}{2}(resp.\ p = 1 - q)$, the relative hash power of the group of attackers (resp. of honest miners).

Theorem 2. *After z blocks have been validated by honest miners, the probability of success of the attackers is*

$$P(z) = I_{4pq}\Big(z, \frac{1}{2}\Big)$$

where $I_x(a, b)$ *is the regularized imcomplete beta function*

$$I_x(a, b) := \frac{\Gamma(a + b)}{\Gamma(a)\Gamma(b)} \int_0^x t^{a-1}(1 - t)^{b-1} dt \tag{1}$$

Corolarry 3. *Let* $s = 4pq < 1$. *When* $z \to \infty$, *we have*

$$P(z) \ \sim \ \frac{s^z}{\sqrt{\pi(1 - z)s}} \tag{2}$$

5.2 Other results

Given $z \in \mathbb{N}$, block generation time t for mining z block(s) is publicly known.

Defination 4. *We denote by P(z,t) the probability of success of a double spend attack when z blocks have been validated within a period of time t.*

What we'll obtain also:

1. Closed form formula for $P(z, t)$
2. Asymtotics formulas for $P_{SN}(z)$ and $P(z, t)$
3. Explicit rank z_0 such that $P(z) < P_{SN}(z)$

In particular,

$$P_{SN}(z) \ \sim \ \frac{e^{-z\left(\frac{q}{p} - 1 - \ln\frac{q}{p}\right)}}{2} \tag{3}$$

6 What does future hold for Bitcoin?

So whats next for Bitcoin? As outlined previously, it has many advantages and for this reason it will remain relevant as a currency. The vast majority of BTC transactions by volume are made in China so the two will remain interlinked.

We see the biggest risk to Bitcoin being its substitution and/or parallel use by other crypto currencies. Bitcoin die-hard fans claim that this is never going to be an issue since Bitcoin was the pioneer and as such enjoys first-mover privilege. This argument is probably flawed because although the BTC is used for payments, this is only a relatively small % of all Bitcoins. One of its primary uses is being a store of value and for this reason other crypto currencies can always step in and enjoy similar status if aggregate demand requires it.

Is Bitcoin simply a 21st century version of gold, only without the storage issues? Or is it just a short-lived popular fad that may soon evolve into something quite different? Only time will tell. The only certainty is that its price will remain very volatile in the future.

The End