Seminar on

Bitcoin As a New Digital currency: Infiltrating the Financial System Bit by Bit

Twana T. Sulaiman
ttahsen@cihanuniveristy.edu.iq

Asst. Lecturer in Financial and Banking Sciences Department
College of Financial and Administrative Sciences, Cihan University

10th Seminar of Finance and Banking Science Department
Cihan University Campus, Cihan Academy Hall
11th January 2018

FOLLOWING ARE THE CONTENTS OF THE SEMINAR

- Meaning of Bitcoin
- Characteristic of Bitcoin
- Why some people use Bitcoin
- How dose the Bitcoin work
- Bitcoin Mining
- What are the Risks?
- What are the Benefits?
- What are the Possibilities?
- Alternatives

by: Twana T. Sulaiman

What is Bitcoin?

Bitcoin is a software-based payment system described by Satoshi Nakamoto in 2008, and introduced as open-source software in 2009. Payments are recorded in a public ledger using its own unit of account, which is also called bitcoin. Payments work peer-to-peer without a central repository or single administrator, which has led the US Treasury to call bitcoin a decentralized virtual currency. Although its status as a currency is disputed, media reports often refer to bitcoin as a cryptocurrency or digital currency.

-Wikipedia

BitCoin

- It is simply a means of sending and receiving numbers to and from "addresses"
- An Open-Source Peer-To-Peer Payment Network
  - Using Digital Signatures & Encryption
    - decentralization is the basis for Bitcoin's security and freedom
- Public –Private Key Encryption
  - Alice & Bob Illustration
  - Digital Certificate Blocking Chain

Why Bitcoins?

- Bitcoin can be used to buy merchandise anonymously
- Bitcoin is not tied to any country or subject to regulation
- Small businesses like bitcoin because there are no credit card fees or chargebacks
- Some people buy bitcoins as an investment, hoping that they'll go up in value.
  - This is one of the reasons for it's price instability

Bitcoin

- **Governance** - an open source community of developers backed by the Bitcoin Foundation.
- **Democratic** - if you don't like one of the changes, you are more than welcome to fork the chain and implement your own rules
- **Money Creation** - is given to the people, not to the central bankers.
- **Deflationary** by design - money supply cannot be manipulated and is fixed at 21 million coins, each divisible up to 8 decimal

How does it work?

There are no bitcoins, only records of bitcoin transactions

Here's the funny thing about bitcoins: they don't exist anywhere, even on a hard drive. We talk about someone having bitcoins, but when you look at a particular bitcoin address, there are no digital bitcoins held in it, in the same way that you might hold pounds or dollars in a bank account. You cannot point to a physical object, or even a digital file, and say "this is a bitcoin".

Instead, there are only records of transactions between different addresses, with balances that increase and decrease. Every transaction that ever took place is stored in a vast general ledger called the block chain. If you want to work out the balance of any bitcoin address, the information isn't held at that address; you must reconstruct it by looking at the block chain.

How it works

- The block chain is the fundamental data structure of the **Bitcoin protocol**.
- It's a single data file participants pass around to each other.
- It allows them to know who owns what.
  - Anyone can change it to send money to someone else.
- Other users mathematically verify the transaction to ensure it's validity.

How It Works

- It's essentially an accounting ledger:
  1. 3/3/13 Sally found : $15.00
  2. 3/3/13 Sally -> Bob : $10.00
  3. 3/4/13 Bob -> Jimmy : $4.00
  4. 3/4/13 Sally -> Barb : $4.00
  5. 3/4/13 Jimmy -> Sally : $2.00
- How much money does Sally have in her wallet?
  - Sally had $15, then gave $10 to Bob, then $4 to Barb, then was given $2 from Jimmy. Sally has $3 as of right now.

Bitcoin Mining

1. Collects transactions from the network
2. Validates them, and doesn't allow conflicting ones
3. Puts them into large bundles called blocks
4. Computes cryptographic hashes over and over until if finds one "good enough to count"
5. Then submits the block to the network, adding it to the block chain and earning a reward in return

Risks

- Theft
- Lost keys
- Lost memory
- EMP Bomb
- Exchange Collapse
- Value collapse
- Hacking

What are the benefits?

- Low or non-existent fees
- No chargebacks
- Every time a customer swipes a credit card at the grocery store, banks and credit card companies collect up to 4 percent of the total bill.
- Hedge against inflation
- Safe haven for currency collapse
  - For every Trillion dollars that enter, each bitcoin will increase $75,000
- You can email money
- You can send money to anyone in the world who needs quick cash
- Profit
- Can not be deflated due to printing

What are the Possibilities?

- End of national currencies
- End of Banks
- A new notary system
- The end of Western Union/Money Orders
- Anyone with a cellphone is a bank

Alternatives

- Litecoin (LTC)
  - transaction confirmation in 2.5 min
  - prevent ASICs
- PPCoin (PPC)
  - proof-of-stake
  - energy efficient
- NameCoin (NMC)
  - Decentralized DNS
  - .bit domain

Alternatives

- Dogecouin (DOGE)
- Auroracoin (AUR)
- Quarkcoin (QRK)
- Feathercoin (FTC)
- Vertcoin (VTC)
- Novacoin (NVC)

As of Apr 17, 2014

Currency	BTC	LTC	PPC	**DOGE**	**NMC**	**AUR**	QRK	FTC	VTC	NVC
Value	$499.6	$12.5	$2.7	$0.0006	$3.0	$0.98	$0.027	$0.12	$1	$4.3
Total	12.6 m	27.6 m	21.3 m	71 b	8.5 m	10.7 m	248 m	40 m	3.5 m	0.8 m
Capitalization	6.3 b	344 m	58.3 m	44.8 m	26 m	10.4 m	6.6 m	4.8 m	3.5 m	3.3 m

THANK YOU

by: Twana T. Sulaiman