Presentation By:

- Ahmed Sayed Ahmed
- Kirusanth Thiruchelvam
- Amro Bahri

What is BitCoin?

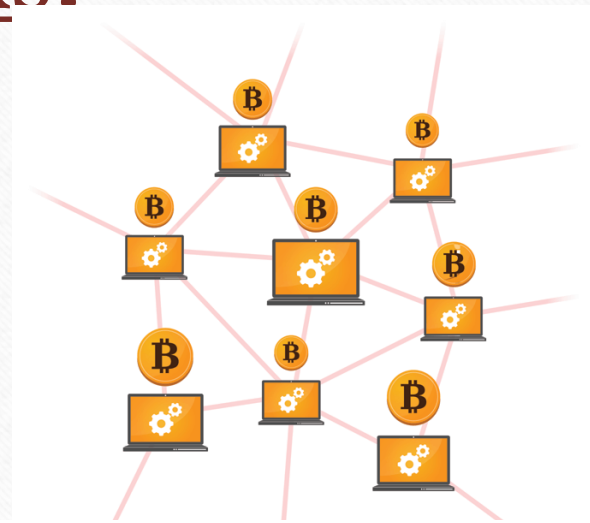
Background:

- Bitcoin is a digital currency created and held electronically.
- Created in 2008 by Satoshi Nakamoto.
- Bitcoin is decentralized, not controlled by a central bank nor anyone else.
- It allows us to operate independently from the government, which is beneficial when the government is being irresponsible.
- No one, not the bank nor the government can freeze your bitcoin account.

How it Works?

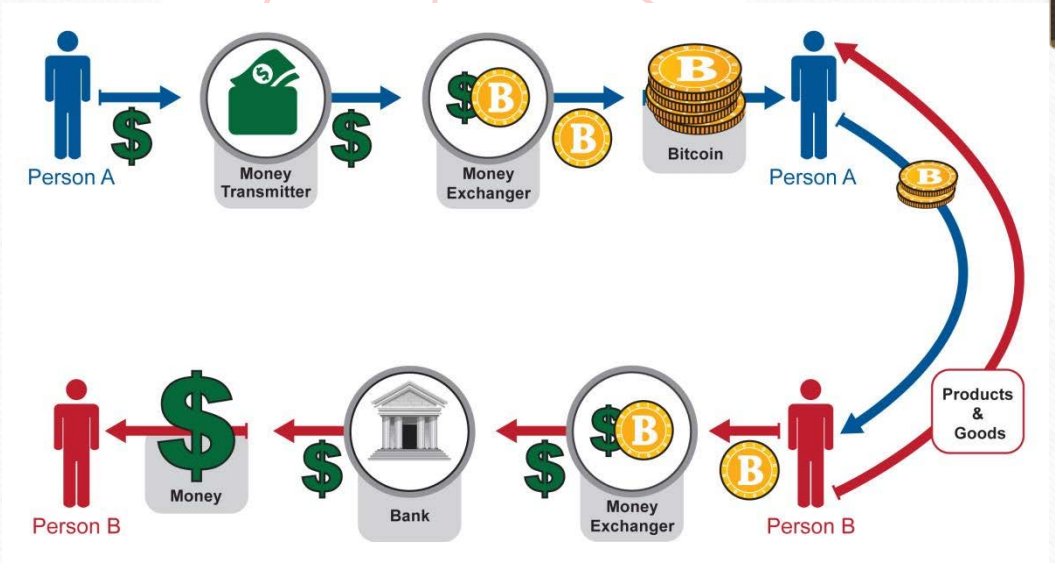
Peer-To-Peer:

- Bitcoin travels on peer to peer networks world wide.
- Bitcoins are produced by people and business around the world running computers using a software to solve mathematical problems.
- Transfer occurs directly from one person to another.



Bitcoin Transactions:

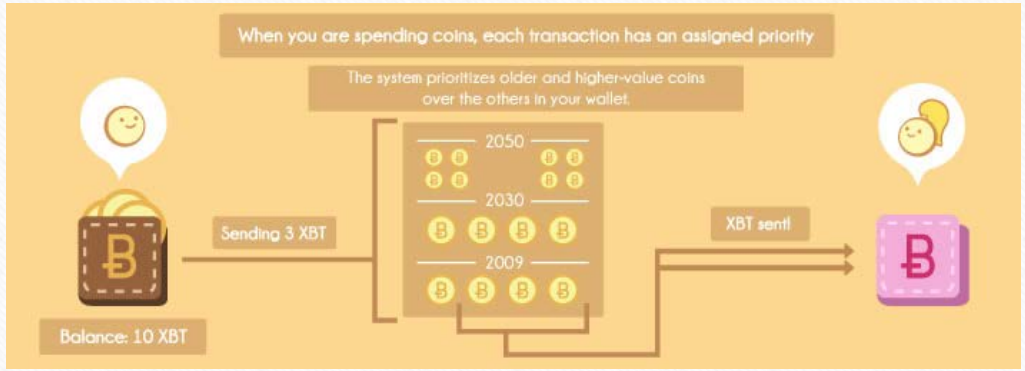
- Miners use special hardware to “mine” bitcoins by solving complicated mathematical operations that are used to validate transactions.
- Transactions are processed by other users in a service knows as mining.
- Operations that miners perform are required for the protection of the network



How it Works? Cont…

Mining:

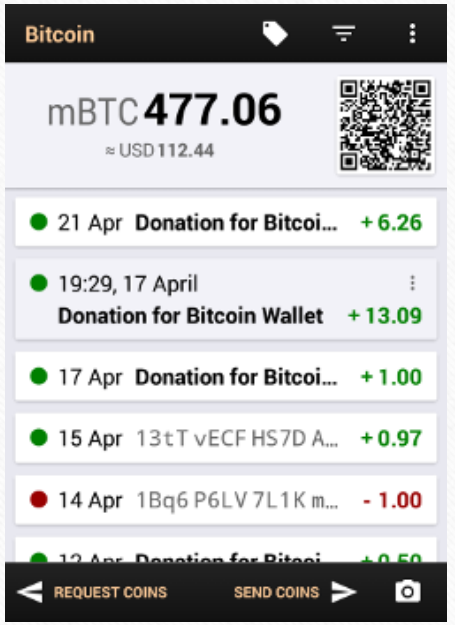
- There are only 25 new BTC produced every 10 minutes.
- The miner that solves the mathematical equation first gets awarded 25 bitcoins.
- Bitcoin miners generate more bitcoins through a series of de-encryption of public hashes. Bitcoins use what is called “sha256” which is a set of cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm.
- This hashing on the network also provides payment verification and is the means of transferring bitcoins from one user to another.



How it Works? Cont…

Bitcoin Wallet:

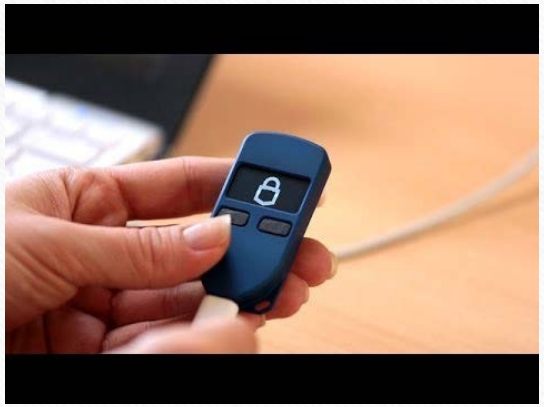
- A "wallet" is basically the Bitcoin equivalent of a bank account.
- It allows you to receive bitcoins, store them, and then send them to others.
- Bitcoin wallets store the private keys that you need to access a bitcoin address that allows you tospend your funds.
- There are two main types of wallets. A software wallet is one that you install on your own computer or mobile device.
- You are in complete control over the security of your coins, but they can sometimes be tricky to install and maintain.
- A web wallet or hosted wallet is one that is hosted by a third party. They are often much easier to use, but you have to trust the provider to maintain high levels of security to protect your coins.



Is It Safe?

Safety:

- Bitcoin uses cryptography to secure all its transactions.
- No central bank backing your bitcoins, there is no possible way to recoup your lose.
- If you lose your private keys you lose your bitcoins and can never get them back
- Don't need a login/password (No identity tracking) to access your account, just need your keys.
- It is not possible to create money out of thin air.
- This doesn't mean that it is 100% secure.



Security Attacks

Presented By: Kirusanth Thiruchelvam

Is It Secure?

Security:

- The currency is unstable and impractical.
- Security is a problem as theft can occur.
- Recently there has been thefts of values equal to hundreds to millions of dollars.
- Mt. Gox was a bitcoin exchange based in Tokyo, Japan. It was launched in July 2010, and by 2013 was handling 70% of all bitcoin transactions.
- In 2014 Mt. Gox filed for bankruptcy as around 850,000 bitcoins belonging to customers and the company were stolen.
- There is no way to return stolen money if hacked since nothing is tracked.
- Buyers are not well protected.
- Since there is no central power controlling or limiting the amount of transactions then there is also no grantees.

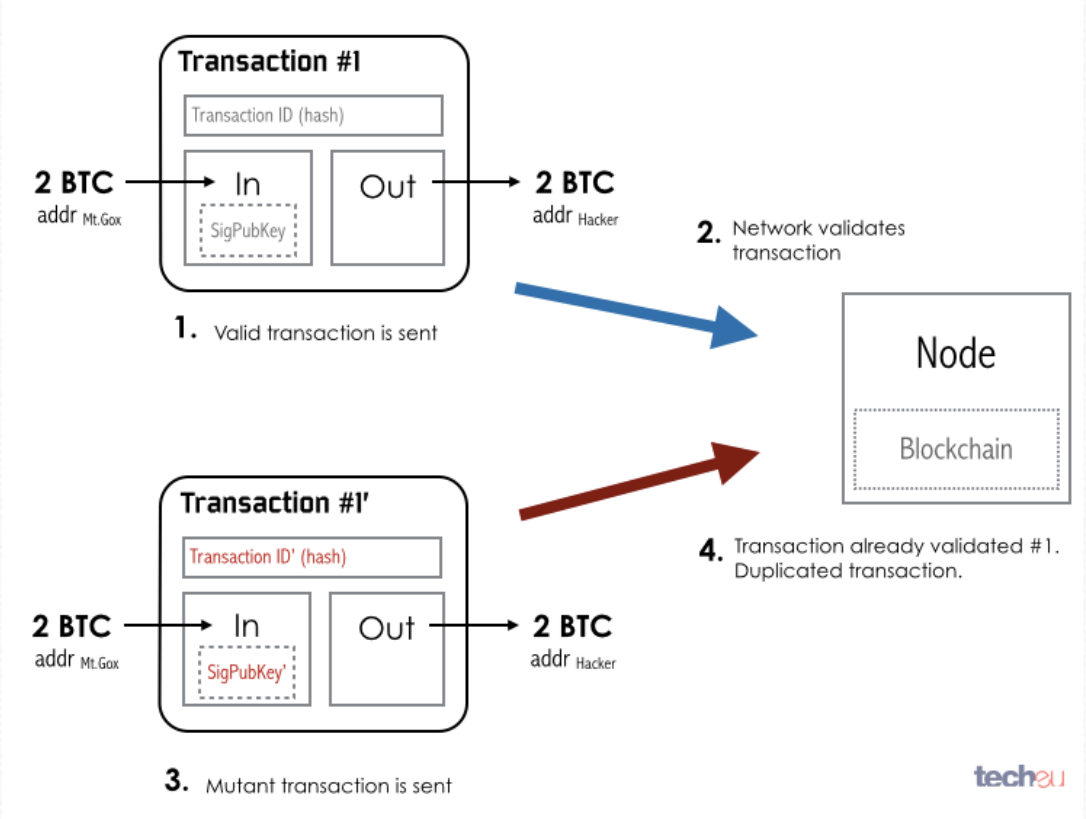
Bitcoin Security Attacks

What is transaction malleability?

- It's an attack that lets someone change the unique ID of a bitcoin transaction before it is confirmed on the bitcoin network.
- The change makes it possible for someone to pretend that a transaction didn't happen, if all the right conditions are in place.

Is it the same as double spending?

- No. Double spending involves spending coins once, then creating a different transaction with those same coins before the first transaction is confirmed. The trick is then to get the fraudulent transaction confirmed on the bitcoin network first, so that the first transaction didn't happen. That effectively means that you get to spend them twice.



Secret Bitcoin Mining?

So you use Torrents to download games for FREE?

- Programmers have found a way to embed their own miners into some of the latest games such as GTA, Counter Strike and other multiplayer games.
- The idea to hide their miners inside games on bittorent networks where they know that a lot of people will be downloading for free, and once the game starts, their miner gets to work and starts to earn them money.
- Imagine a game like GTA which in 3 days has earned over 1 billions dollars in sales, and that's based on those who bought it, now think about the amount of people downloaded it for free, with that many miners, the programmer can earn thousands of dollars.

Secret Bitcoin Mining?

Rogue Employee Fired for Turning Game Network Into Bitcoin Mining Colony

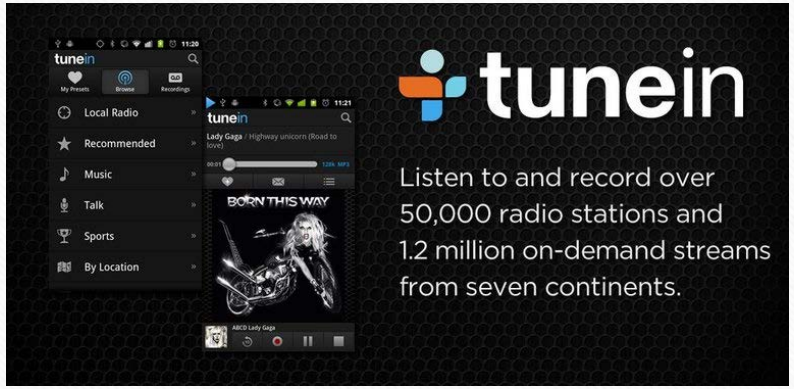
- An unidentified staffer at the ESEA gaming network has been fired for allegedly turning the company's software into a secret Bitcoin-mining Trojan.
- ESEA (the E-Sports Entertainment Association) admitted that its software — which serious Counter-Strike players use to play each other in anti-cheating modes — had been altered to secretly mine Bitcoins.
- So far the company has resolved 275 claims from customers who say they were damaged by the mining software.
- The Bitcoin-mining update may have been installed on as many as 14,000 computers.
- In just a few weeks ESEA's employee earned himself BTC30, or about $2,400 at today's exchange rates.

ESEA
ESPORTS ENTERTAINMENT

Secret Bitcoin Mining?

Code in two Android apps turned phones into a secret army of Bitcoin miners

- Trend Micro has discovered a pair of apps that turned smartphones into tiny, secret Bitcoin mining machines when they weren't in use. Unfortunately, these apps weren't mining Bitcoins for their owners.
- Two apps that were repackaged copies of existing popular apps — Songs (which copied TuneIn Radio) and Prized (Football Manager Handheld) — are guilty of doing a lot more than just getting stuck in a loop and eating up resources.
- Whenever the phone was connected to power and inactive for a few minutes app would activate and would start mining Bitcoin, Litecoin, and Dogecoin.
- While a single smartphone lacks sufficient power to pull in any real amount of Bitcoin, while installed a million times it adds up quite a bit.



Security Solutions

Presented By: Amro Bahri

Bitcoin Security Solutions

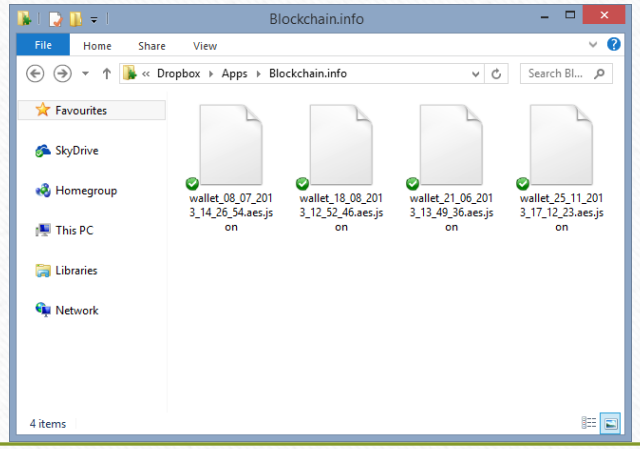
Securing your wallet:

- Be careful with online services.
- You should be wary of any service designed to store your money online.
- Many exchanges and online wallets suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank.
- Small amounts for everyday uses.
- A Bitcoin wallet is like a wallet with cash. If you wouldn't keep a thousand dollars in your pocket, you might want to have the same consideration for your Bitcoin wallet.
- In general, it is a good practice to keep only small amounts of bitcoins on your computer, mobile, or server for everyday uses and to keep the remaining part of your funds in a safer environment.

Bitcoin Security Solutions

Backup your wallet:

- Stored in a safe place, a backup of your wallet can protect you against computer failures and many human mistakes.
- It can also allow you to recover your wallet after your mobile or computer was stolen if you keep your wallet encrypted.
- Backup your entire wallet: Some wallets use many hidden private keys internally. If you only have a backup of the private keys for your visible Bitcoin addresses, you might not be able to recover a great part of your funds with your backup.
- Encrypt online backups: encrypting any backup that is exposed to the network is a good security practice.
- Use many secure locations: consider using different medias like USB keys, papers and CDs to backup your wallet.



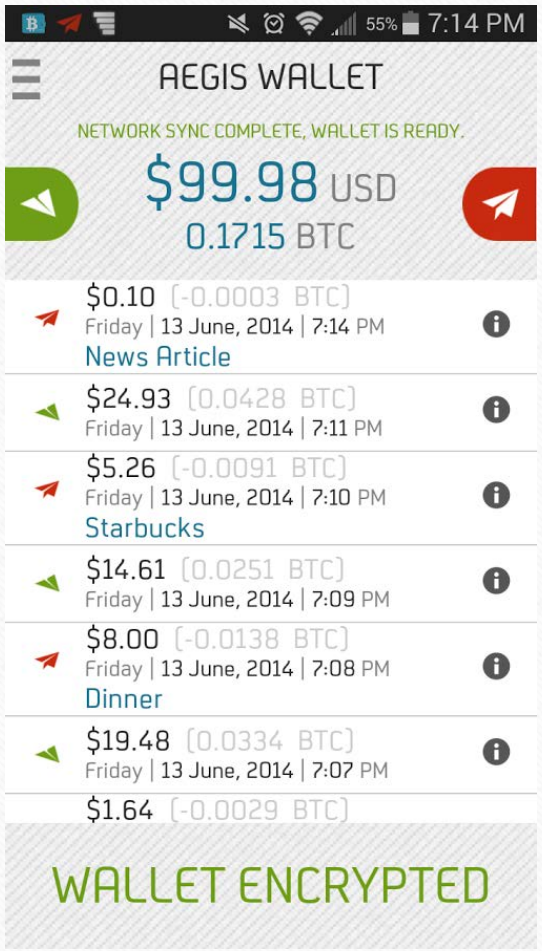
Bitcoin Security Solutions

Encrypt your wallet:

- Encrypting your wallet or your smartphone allows you to set a password for anyone trying to withdraw any funds. This helps protect against thieves, though it cannot protect against keylogging hardware or software.

- Use a strong password: A strong password must contain letters, numbers, punctuation marks and must be at least 16 characters long.
- The most secure passwords are those generated by programs designed specifically for that purpose

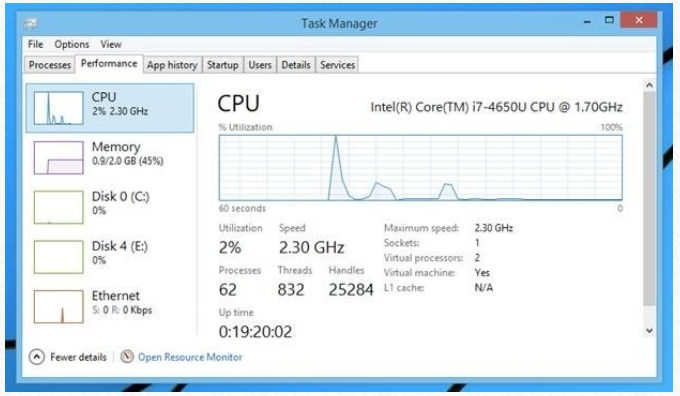
- Offline wallet for savings: An offline wallet, also known as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network.

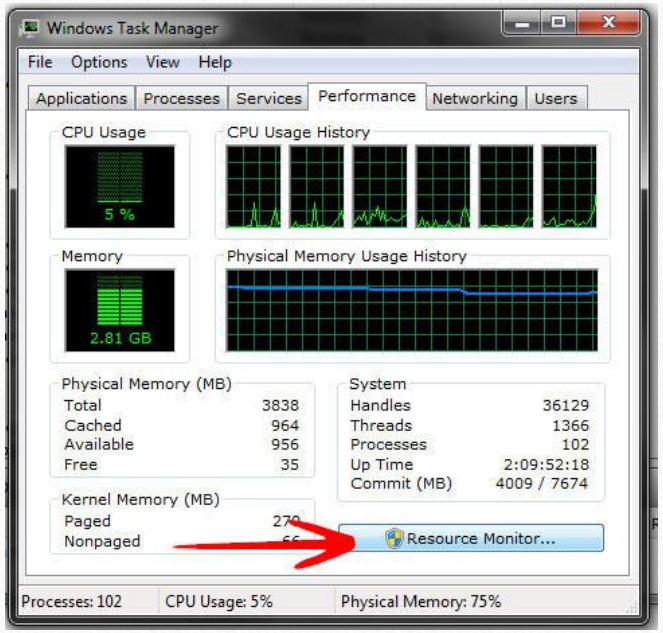


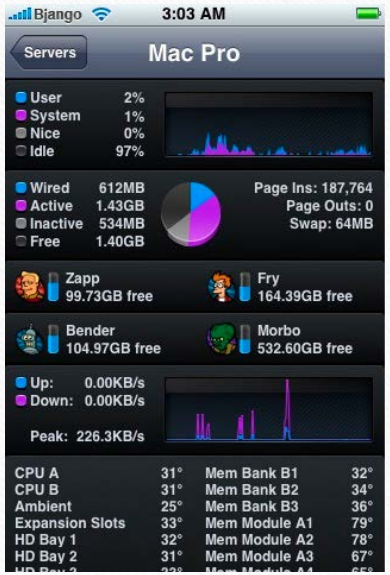
Bitcoin Security Solutions

Monitor your computer Resrouces:

- When it comes to embedded miners into games and applications, it can be very difficult to determine whether or not the application or game you downloaded is infected.
- If you notice that your computer is slowing down more than usual once you open a certain application or game then it is likely that it contains a bitcoin miner running in the background and eating up your resources.
- Fastest way to check it by hitting Ctrl + Alt + Del and checking your CPU usage under task manager to see if it is under a heavy load or not.
- Another way to check is by installing software for system monitoring such as "Performance Monitor" which places four system monitoring graphs on your desktop and check when your resources spike.







Bitcoin Final Thoughts

The Good	The Bad
• Freedom in Payment	• Lack of Awareness & Understanding
• Control and Security	• Risk and Volatility
• Information is Transparent	• Unpredictable
• Very Low Fees	• Unconfirmed transactions are not secure within the initial 10-minute window of the transaction process
• Fewer Risks for Merchants	• No refunds
• Mining rigs pay for themselves over time	• Can be run hidden from view
• 25 BitCoin lottery created every 10 min	• Can destroy your desktop PC, needs special hardware.

Questions and Answers

What are the two types of wallets used in bitcoin?:

- Software wallet.
- Web (hosted) wallet.

Is Bitcoin backed by a central bank?

- No central bank backing your bitcoins, there is no possible way to recoup your lose.

How many bitcoins produced every 10 minutes?

- There are only 25 new BTC produced every 10 minutes.

Thanks For Watching