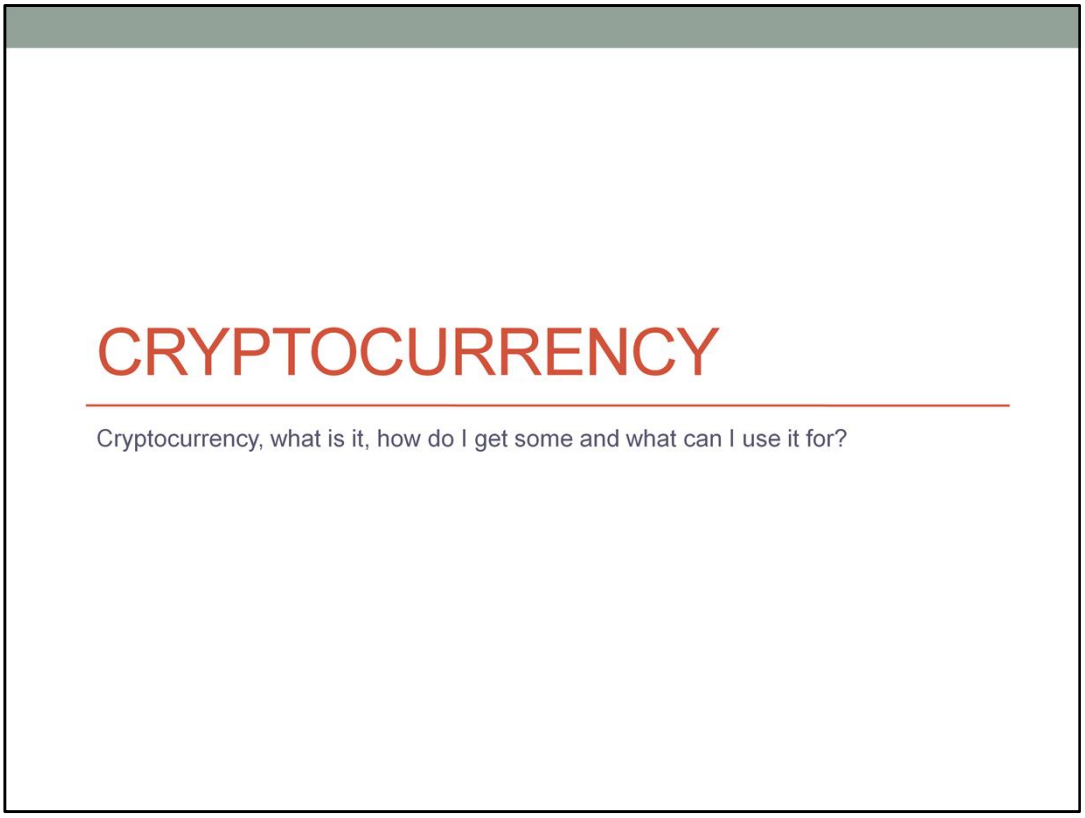
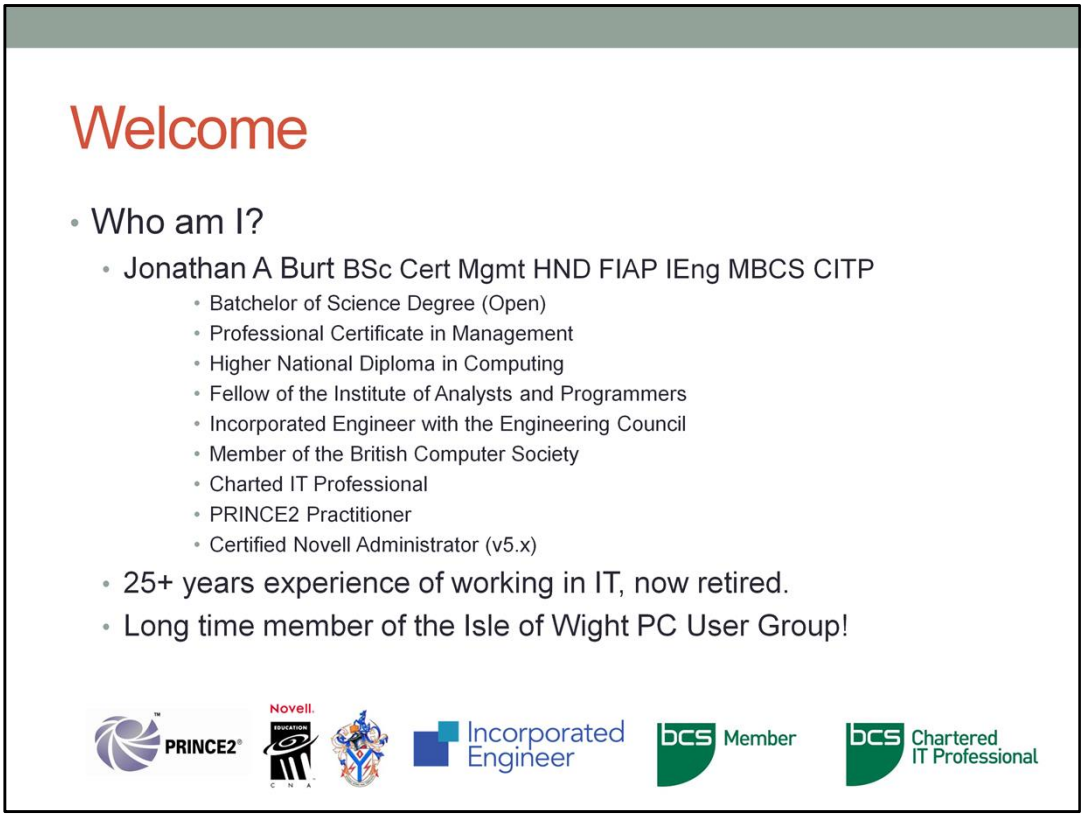


https://mymonero.com/#/
https://www.coinbase.com/
https://coinsquare.com/
https://cex.io/
https://www.kraken.com/



1. Explain about me, my background and experience.

Warning!

- As with all my talks, I recommend that you do you own research before making any changes to your PC.
- Also, please ensure you have backed up all of your data before you make changes to your PC.
- Cryptocurrencies are unregulated! No guarantee of getting your investment back.

1. Warning notice.
2. Apologies if “boring”…

What is Cryptocurrency?

- A cryptocurrency is digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.
- Cryptocurrency is a digital (or virtual) currency.
- Cryptocurrencies use decentralised control as opposed to centralised electronic money and central banking systems.
- The decentralised control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

1. So generally there is no physical representation of the currency, i.e. coins/notes. However, as some cryptocurrencies have created physical coins – unsure of their use though as could easily make fakes.

Formal Definition

- A cryptocurrency is a system that meets six conditions:

1. The system does not require a central authority.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

So how many are there?

- Bitcoin, first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency.
- Since then, over 4,000 different cryptocurrencies have been created (often referred to as ‘altcoin’).
- Some of these are ‘forks’, i.e. copies/alterations of the original Bitcoin code and some are new or independently created.

Legality

- The legal status of cryptocurrencies varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed their use and trade, others have banned or restricted it.
- Bangladesh , Bolivia, Ecuador, Nepal, Lebanon, and Indonesia have all banned the buying and selling of cryptocurrencies.
- They are currently legal in the UK, however, with conditions…

1. Note: Even if they are “legal” you are limited with you can use them for.

Legality - UK

- As of 2017, the government has stated that bitcoin (and other cryptocurrencies) is unregulated and that it is treated as a 'foreign currency' for most purposes, including VAT/GST.
- Bitcoin is treated as 'private money'. When bitcoin is exchanged for sterling or for foreign currencies, such as euro or dollar, no VAT will be due on the value of the bitcoins themselves. However, in all instances, VAT will be due in the normal way from suppliers of any goods or services sold in exchange for bitcoin or other similar cryptocurrency. Profits and losses on cryptocurrencies are subject to capital gains tax.

1. VAT (Value Added Tax) and GST (Goods and Services Tax)

How do they work?

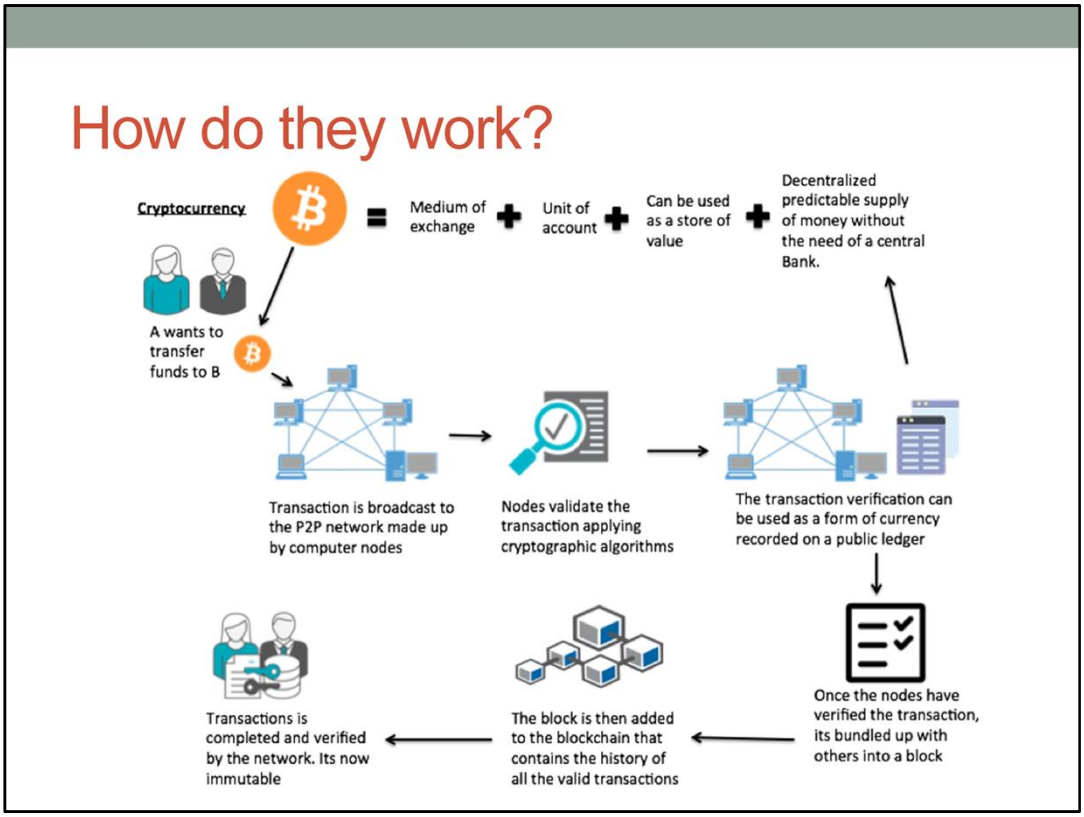
- Transactions are sent between peers using software wallets. The person creating the transaction uses the software to transfer balances from one account (a public address) to another.
- To transfer funds, the sender needs to know the password (a private key) associated with their wallet.
- Transactions made between peers are encrypted and then broadcast (utilising a peer-2-peer network) to the cryptocurrency's network and queued up to be added to the public ledger.
- Transactions are then recorded on the public ledger via a process called "mining".

1. Cryptocurrency "coins" are only generated via the mining algorithm – so people need to mine them before they start to enter use!
2. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

How do they work?

- All users of a given cryptocurrency have access to the ledger if they choose to download a "full node" wallet (as opposed to holding their coins in a third party wallet like Coinbase). For Bitcoin, the transaction amounts are public, but who sent the transaction is encrypted (it is pseudo anonymous).
- Each transaction leads back to a unique set of keys. Whoever owns a set of keys, owns the amount of cryptocurrency associated with those keys (just like whoever owns a bank account owns the money in it).
- Many transactions are added to a ledger at once. These "blocks" of transactions are added sequentially by miners.

1. That is why the ledger and the technology behind it are called "block" "chain." It is a "chain" of "blocks" of transactions.



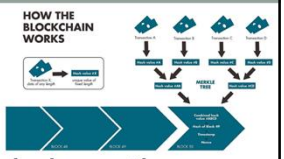
A picture speaks a thousand words!

Blockchain

- The blockchain is like a decentralized bank ledger, in both cases the ledger is a record of transactions and balances.
- When a cryptocurrency transaction is made, that transaction is sent out to all users hosting a copy of the blockchain. Specific types of users called miners then try to solve a cryptographic puzzle (using software) which lets them add a "block" of transactions to the ledger.
- Whoever solves the puzzle first gets a few "newly mined" coins as a reward (they also get transaction fees paid by those who created the transactions).

1. Blockchains have uses outside of cryptocurrency, and are being looked at and used by different companies as alternative ways of holding transaction/ledger/record details.

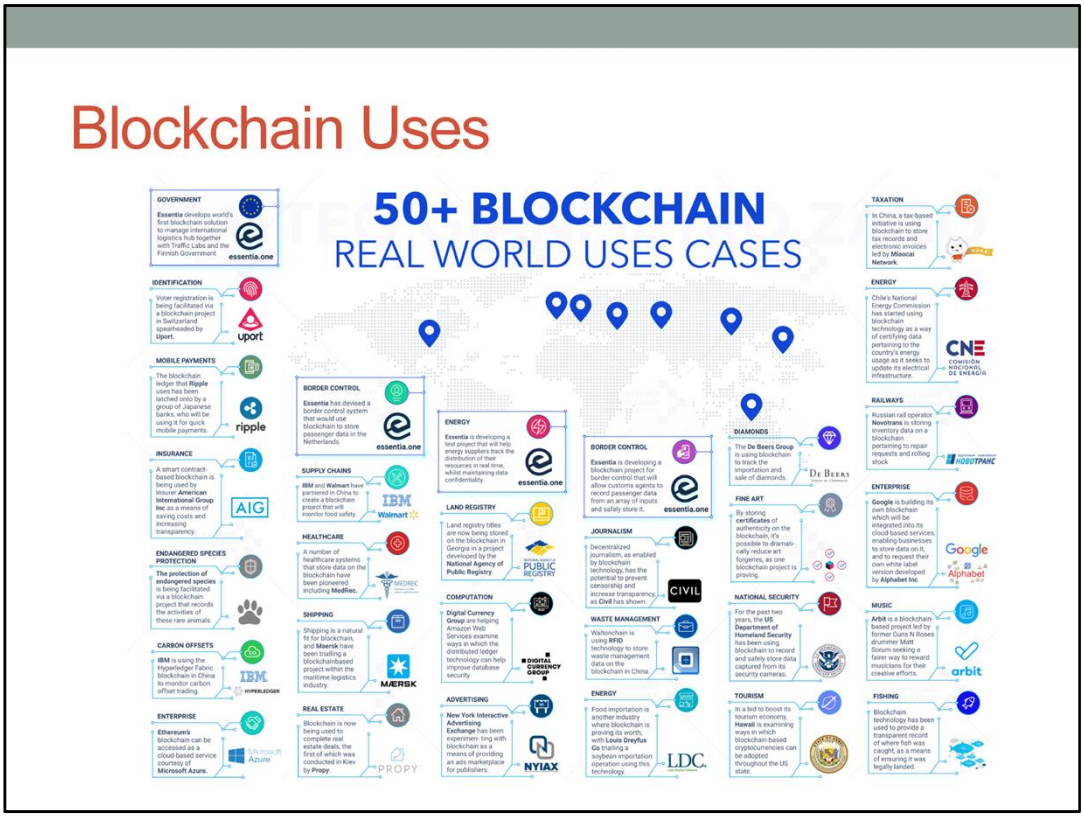
Blockchain



- Sometimes miners pool computing power and share the new coins. The algorithm relies on consensus. If the majority of users trying to solve the puzzle all submit the same transaction data, then it confirms that the transactions are correct.
- Further, the security of the blockchain relies on cryptography. Each block is connected to the data in the last block via one-way cryptographic codes called hashes which are designed to make tampering with the blockchain very difficult.
- The difficulty of cracking the cryptographic puzzles, and the amount of effort it would take to add incorrect data to the blockchain by faking consensus or tampering with the blockchain helps to ensure the integrity of the blockchain.

1. This helps to ensure the integrity of the blockchain/transactions against malicious users (hacking, etc.).
2. The Bitcoin Blockchain is currently 163GB in size, and growing daily – remember it holds all transactions since transaction #1!
3. **Cryptographic hash** functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. For example, computing the hash of a downloaded file and comparing the result to a previously published hash result can show whether the download has been modified or tampered with. A key aspect of cryptographic hash functions is their collision resistance: nobody should be able to find two different input values that result in the same hash output.

Blockchain Uses



1. As you can see, blockchain technology has many uses.
2. Blockchain technology was created by the author(s) of Bitcoin.

Mining

- People who are running software and hardware aimed at confirming transactions to the digital ledger are cryptocurrency miners.
- Solving cryptographic puzzles (via software), by generating hashes, to add transactions to the ledger (the blockchain) in the hope of getting coins as a reward is cryptocurrency mining.
- The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines running complex hashing algorithms like SHA-256 and Scrypt.

1. **SHA-2 (Secure Hash Algorithm 2)** is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). They are built using the Merkle–Damgård structure, from a one-way compression function itself built using the Davies-Meyer structure from a (classified) specialized block cipher.
2. SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224,56, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.
3. In cryptography, **scrypt** (pronounced "ess crypt") is a password-based key derivation function created by Colin Percival, originally for the Tarsnap online backup service. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2016, the scrypt algorithm was published by IETF as RFC 7914. A simplified version of scrypt is used as a proof-of-work scheme by a number of cryptocurrencies, first implemented by an anonymous programmer called ArtForz in Tenebrix and followed by Fairbrix and Litecoin soon after.

Mining

- This arms race for cheaper-yet-efficient machines has been on since the day the first cryptocurrency, bitcoin, was introduced in 2009.
- With more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest large sums of money on employing multiple high performance ASICs and GPUs.
- Thus the value of the currency obtained for finding a hash often does not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the enormous amount of heat they produce, and the electricity required to run them.

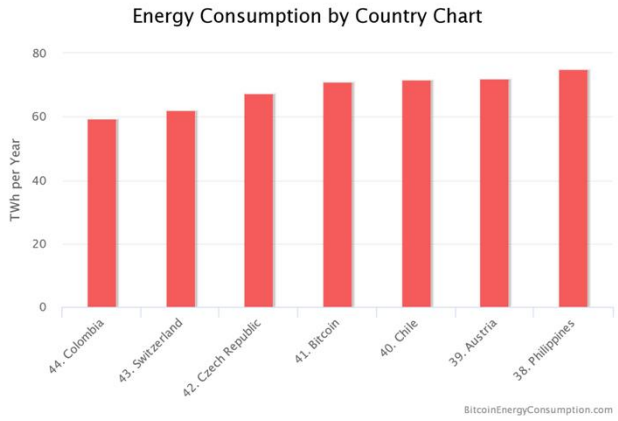
1. An Application-Specific Integrated Circuit (ASIC) /ˈeɪsɪk/, is an integrated circuit (IC) customized for a particular use, rather than intended for general-purpose use. For example, a chip designed to run in a digital voice recorder or a high-efficiency Bitcoin miner is an ASIC. Application-specific standard products (ASSPs) are intermediate between ASICs and industry standard integrated circuits like the 7400 series or the 4000 series.
2. It has also led to a shortage of GPU's thus affecting the price of Graphic Cards (i.e. prices have gone up – doubled and even tripled in price!).
3. Basically as the cryptocurrency ages, the "freebies" from mining become harder to obtain.

Extreme Mining

Extreme Mining

Electricity Use

- The entire Bitcoin network now consumes more energy than a number of countries, based on a report published by the International Energy Agency. If Bitcoin was a country, it would rank as shown below:



1. Megawatt hours (MWh), gigawatt hours (GWh), and terawatt hours (**TWh**) are often used for metering larger amounts of electrical energy to industrial customers and in power generation.
2. It's why a lot of "farms" are moving to Iceland due to their cheap Electricity.
3. All this for something which doesn't exist… and just for people to make a "cheap buck".

Wallets

- A cryptocurrency wallet stores the public and private keys which can be used to receive or spend the cryptocurrency.
- A wallet can contain multiple public and private key pairs.
- The cryptocurrency itself is not in the wallet. In case of bitcoin and cryptocurrencies derived from it, the cryptocurrency is decentrally stored and maintained in a publicly available ledger.
- Every piece of cryptocurrency has a private key. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency.

1. You can get wallets which hold multiple types of cryptocurrencies.

Wallets

- When choosing a wallet, you must keep in mind who is supposed to have access to the private keys and thus has potentially access to the cryptocurrency.
- Just like with a bank, you need to trust the provider to keep the cryptocurrency safe. Trust was misplaced in the case of the Mt. Gox exchange, who 'lost' most of their clients' bitcoins.
- Downloading a cryptocurrency wallet from a wallet provider to a computer or phone does not automatically mean that you are the only one who has a copy of the private keys. For example with Coinbase, it is possible to install a wallet on a phone and to also have access to the same wallet through their website.
- For receiving cryptocurrency, access to the receiving wallet is not needed. The sending party only needs to know the destination address. Anyone can send cryptocurrency to an address. Only the one who has the private key of the corresponding address can use it.

1. Mt. Gox lose was 850,000 bitcoins at a value of $450million (at the time).
2. A wallet can also have known or unknown vulnerabilities.

Wallets (Software)

- An application installed locally on a computer, phone or tablet.
- When using a web wallet the private keys are managed by a trusted third party. Some web-based wallet providers use two-factor (like Google Authenticator) for extra security.
- Cryptocurrency exchanges link the user's wallet to their centrally managed wallet(s).
  - For example: When trading bitcoins between users on the Kraken exchange, the trades are written in their private ledger (off-chain transaction). Only when a user wants to enter his cryptocurrency into the exchange or when he wants to take his cryptocurrency out of the exchange, the transaction is written onto the public bitcoin blockchain (on-chain transaction).
- In order to initiate or verify a transaction, the cryptocurrency wallet connects to a client or node on the network to process the request.

1. Benefit of two-faction: A key-logger is not enough for a hacker to steal the credentials and get access to the wallet.

Wallets (Hardware)

- When the user of a hardware wallet requests a payment, the wallet's API creates the transaction. Then the wallet's hardware signs the transaction and provides a public key, which is sent to the network by the API. That way, the signing keys never leave the hardware wallet.
- If a hardware wallet uses a mnemonic sentence for backup, then the users should not electronically store the mnemonic sentence, but write it down and store in a separate physical location.
- Storing the backup electronically lowers the security level to a software wallet level. Hardware wallets like LedgerWallet and Trezor have models that require the user to physically press or touch the wallet in order to sign a transaction, the destination address and the amount of coins.
- The private keys remain safe inside the hardware wallet. Without the private key a signed transaction cannot be altered successfully. Some hardware wallets have a display where the user can enter a pin to open the wallet and where the transaction can be verified before being signed.

1. When reading a mnemonic sentence from the physical display of the hardware wallet a screencapture of an infected computer will not reveal the mnemonic sentence

Wallets - Backups

- A backup of a wallet can come in different forms like:
  - A (encrypted) file like wallet.dat or wallet.bin which contains all the private keys.
  - A mnemonic sentence from which the root key can be generated, from which all the private keys can be recreated. Preferably these words could be remembered or written down and stored on other physical locations.
- When the private keys and the backup are lost then that cryptocurrency is lost forever. When using a webwallet, the private keys are managed by the provider. When owning cryptocurrency, those trusted with managing the private keys should be carefully selected.
- An (encrypted) copy of the wallet should be kept in a trusted place. Preferably off-line. Some people 'write' their mnemonic sentence or private key on metal, because it is robust!

1. mnemonic sentence : https://mymonero.com/#/

Exchanges

- Exchanges are businesses (generally online) that lets you sell and buy cryptocurrencies for “cash” or other cryptocurrencies.
- Exchanges often operate as online software wallets for your cryptocurrencies.
- Exchanges charge a transaction fee.

- Remember that a lot of these exchanges are unregulated, however some countries (Japan, US SEC and the EU) are insisting on a formal licence process to become an exchange. So check before you use an exchange!

1. “cash” generally to bank accounts, or sometime pre-paid anonymous ATM cards!
2. Very much like a Bureau de change!
3. Buying/selling – many credit cards wont let you use them to buy cryptocurrenies (to protect the users from big debts), after the big Bitcoin Hype/crash in 2017!
4. Exchange examples: https://www.coinbase.com/ - https://coinsquare.com/ - https://cex.io/ - https://www.kraken.com/

Anonymity

- Bitcoin is pseudonymous rather than anonymous in that the cryptocurrency within a wallet is not tied to people, but rather to one or more specific keys (or "addresses").
  - Thereby, bitcoin owners are not identifiable, but all transactions are publicly available in the blockchain.
- Additions such as Zerocoin have been suggested, which would allow for true anonymity. In recent years, anonymizing technologies like zero-knowledge proofs and ring signatures have been employed in the cryptocurrencies Zcash and Monero, respectively.
- Note: Some cryptocurrency exchanges are required by law to collect the personal information of their users.

1. In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover Peggy) can prove to another party (the verifier Victor) that she knows a value x, without conveying any information apart from the fact that she knows the value x.
2. In cryptography, a ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group members' keys was used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup. Ring signatures were invented by Ron Rivest, Adi Shamir, and Yael Tauman, and introduced at ASIACRYPT in 2001. The name, ring signature, comes from the ring-like structure of the signature algorithm.

Negative Uses

- Due to the anonymous nature of cryptocurrencies, their use has been “hijack” into the darker side of the Internet.
- As mentioned in my Dark Net talk, the majority of the sites selling illegal goods and services use cryptocurrencies to pay for the them.
- They are also targets for criminals with regard to hacking and Malware to obtain them for free.
- They are also being used by some “rogue states” to get around UN sanctions.

Hacking

- Unfortunately quite a few exchanges have been hacked over the years:

Exchange	Details
Bitstamp	in 2015 cryptocurrencies worth $5 million were stolen
Mt. Gox	between 2011 and 2014, $450 million worth of bitcoin were stolen
Bitfinexb	In 2016, $72 million were stolen through exploiting the exchange wallet, users were refunded
NiceHash	in 2017 more than $60 million worth of cryptocurrency was stolen
Coincheck	NEM tokens worth $400 million were stolen in 2018

1. As you can see, there is big money for hackers, criminals, rogue states and government agencies to make by “simply hacking” weak exchanges.

Hacking

- Then there is the simple case of computers and phones being hacked to gain access to wallets and passwords!

1. Malware, Keyloggers, phishing websites, etc.

RansomWare

- Many types of ransomware demand payment in bitcoin.
- One program called CryptoLocker, typically spread through legitimate-looking email attachments, encrypts the hard drive of an infected computer, then displays a countdown timer and demands a ransom in bitcoin, to decrypt it.
  - Massachusetts (USA) police said they paid a 2 bitcoin ransom in November 2013, worth more than $1,300 at the time, to decrypt one of their hard drives.
- Bitcoin was used as the ransom medium in the WannaCry RansomWare. One RansomWare variant disables internet access and demands credit card information to restore it, while secretly mining bitcoins.

1. WannaCry is the one that “shutdown” the NHS last year!

RansomWare


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
1/4/1970 01:00:00
Time Left
00: 00: 00: 00
Your files will be lost on
1/8/1970 01:00:00
Time Left
00: 00: 00: 00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt

Malware

- In June 2011, Symantec warned about the possibility that botnets could mine covertly for bitcoins. Malware used the parallel processing capabilities of GPUs built into many modern video cards. Although the average PC with an integrated graphics processor is virtually useless for bitcoin mining, tens of thousands of PCs laden with mining malware could produce some results.

- Since then this has become a reality:
  - Linux.Lady – Mal/Miner-C – CoinKrypt
  - BadLepricon – Proteus – F0xy

1. Much easier to infect a PC with Malware to doing some unauthorised mining, than using RansomWare! And easier to infect than do it mine yourself!

Malware

- In mid-August 2011, bitcoin mining botnets were detected, and less than three months later, bitcoin mining Trojans had infected Mac OS X.
- German police arrested two people in December 2013 who customized existing botnet software to perform bitcoin mining, which police said had been used to mine at least 1,155 bitcoins (at approx. $900 ea.).
- For four days in December 2013 and January 2014, Yahoo! Europe hosted an ad containing bitcoin mining malware that infected an estimated two million computers. The software, called Sefnit, was first detected in mid-2013 and has been bundled with many software packages.

Malicious Use Of Facilities

- Several reports of employees or students using university, business, or research computers to mine bitcoins have been published.
  - On February 20, 2014, a member of the Harvard community was stripped of their access to the University's research computing facilities after setting up a "dogecoin" mining operation using a Harvard research network, according to an internal email circulated by Faculty of Arts and Sciences Research Computing officials.
  - In June 2014 the National Science Foundation banned a researcher for using supercomputer resources to generate Bitcoin. The mining took up about $150,000 worth of NSF-supported computer use to generate approximately 15 bitcoins worth about $654 ea. (at the time).

Malicious Use Of Facilities

- In February 2018, several Russian scientist working at the Federal Nuclear Center in Sarov, decided to use their supercomputer to do some bitcoin mining!

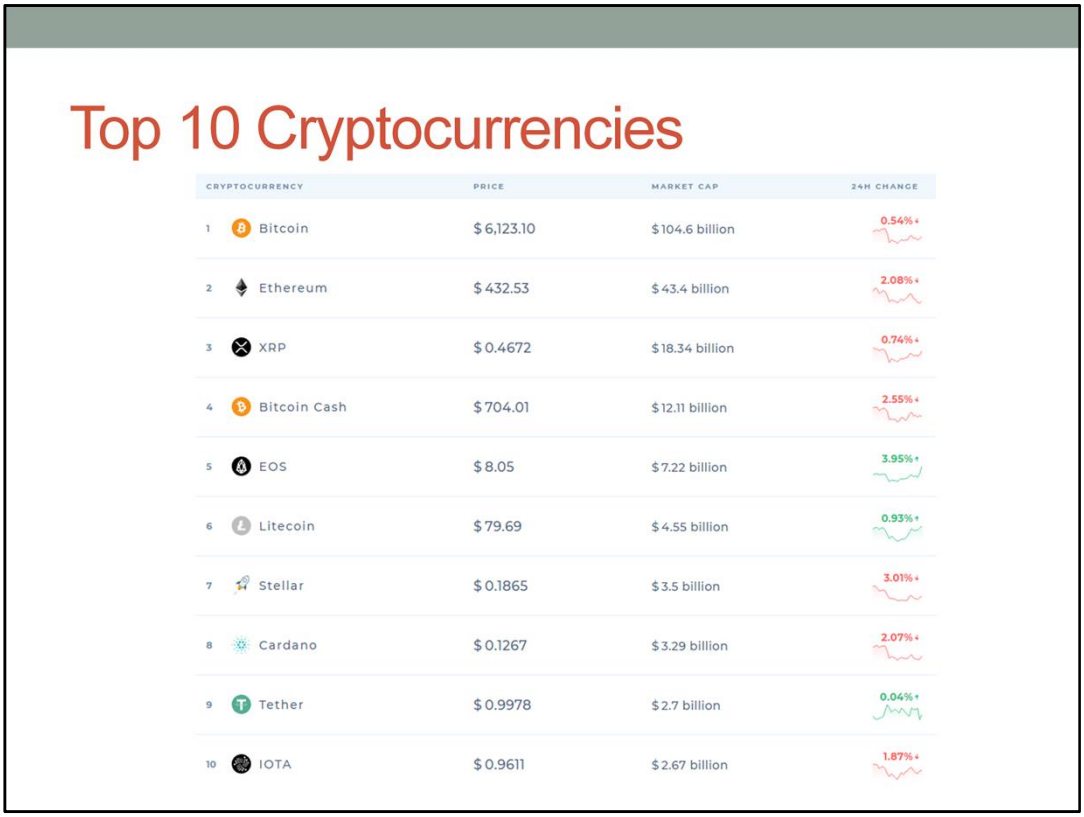
	floating point operations per second
Intel 8087 Maths co-processor (1980)	50,000
Intel 80486 (1989)	50,000,000
IBM Roadrunner (2008)	1,026,000,000,000,000
Russian Supercomputer (2011)	1,000,000,000,000,000
Chinas Sunway TaihuLight (2016)	93,000,000,000,000,000
IBM Summit (2018)	122,300,000,000,000,000
Intel i7-7800X @ 3.5Ghz (2017)	672,000,000,000
Human Brain (estimated)	1,000,000,000,000,000,000

1. Federal Nuclear Center – this is one of Russia's "closed cities" where only authorized personnel are permitted. (12th most powerful in the world at the time 2011), it has been upgraded since but the specs are secret.
2. They were caught when they connected the super computer to the Internet!
3. Petaflop = A quadrillion (thousand trillion) floating point operations per second
4. IBM Summit is 181,994 times faster than my home PC!

Website Mining Software

- In 2017 a new website appeared called coinhive.com, which offered you the opportunity to use a Java based mining software (on Monero) on your website.
- This meant that visitors to your website would be mining the Monero altcoin for you – an alternative to having Ads!
- The site is still there, but many Internet Security packages will now by default warn you and block the code from running, as many sites where using it without informing visitors or unaware that their site had been hacked to run the code.

1. Multiple security firms recently identified cryptocurrency mining service Coinhive as the top malicious threat to Web users, thanks to the tendency for Coinhive's computer code to be used on hacked Web sites to steal the processing power of its visitors' devices.
2. Even the UK ICO website got hacked!
3. Nice idea in principle, implement badly with lack of security = blocked by most things now.



1. Top 10 cryptocurrencies with “market valuation” as at 27 June 2018.

Bitcoin – Value History

- When Bitcoin started in 2009 it had a value of Zero, and no-one was really interested in it (just geek value), for example:
  - In March 2010, user "SmokeTooMuch" auctioned 10,000 BTC for $50 (cumulatively), but no buyer was found.
  - On 22 May 2010, Laszlo Hanyecz made the first real-world transaction by buying two pizzas in Jacksonville, Florida for 10,000 Bitcoins.
  - In March 2010 the first exchange starts operating – Bitcoin has a nominal value of $0.003.
  - In April 2011 one Bitcoin was worth $1.
  - By July 2011 it had raised to $31 then the “bubble burst” and it dropped back to $2 by December 2011.

1. 10,000 for two Pizzas – remember that!

Bitcoin – Value History

- Bitcoin was now becoming more widely known, and more people started “playing” with it:
  - The price rose steadily from $2 to $13 by December 2012.
  - In April 2013 the price had a new price-rally, with increases of 5-10% daily, topping $266 by 11 April.
  - In May 2013 the price dropped to $130, and then to $70 in June and backup to $100 by July.
  - In October 2013 the price started to sky-rocket, going from $150 to $1,242 in November 2013.
  - In December 2013 the price crashed to $600, then rebound to $1,000, crashed again to $500 and stabilised in the $650-$800 range.

Bitcoin – Value History

- Now Bitcoin was becoming popular, and the price started to fluctuate widely:
  - In 2014 the price went up and down like a Yo-Yo! January $750-$1,000, February $550-$750 (dropped due to Mt. Gox hack), March $450-700 (price fell due to a false report that Bitcoins were banned in China), April saw another drop $340-$530, with May increasing to $630.
  - It stayed around the $500-$600 until a drop in May 2015 saw the value reduced to $200. By the end of 2015 the value had increased to $500.
  - 2016 was a “steady year”, with the price fluctuating in the $450-$750 range.

Bitcoin – Value History

- 2017… now it just went silly – all thanks to Press Hype!:
  - Bitcoin started with a value of $950, and dropped in a low of $750 in January, then it just went up, up, up!
  - March $1,290, April $1,250, May $2,000, June $3,200, August $4,400, September $5,000.
  - Then on the 12 September the price crashed to $2,900 due to improper practices in Chinese exchanges.
  - It soon recovered, and in October went from $5,600 to $8,100 by the end of November,
  - In December it went mad! By the 17 December 2017 it reached an all-time high of $19,189.30.
  - Then the inevitable happened, it crashed!

1. $19,189.30 on 17/12/2017 from $993.59 on the 01/01/17 – 1,831.31% increase!
2. 10,000 Bitcoins at the peak in December 2017 = $191,893,000…

Bitcoin – Value History

- The crash:
  - After reaching the all-time high of $19,189.30 on the 17 December 2017, the crash happened, by the 23 December it was down to $14,000 briefly increased to $16,000 and the dropped to $12,000 by the 30 December.
  - Then in January 2018 it recovered back to $16,000, but within a couple of days dropped to $13,000 then $11,000 by the 18 January.
  - Despite a couple of recoveries, and small increases, the price dropped again in February to $7,000.
  - Then the price sharply jumped around a bit between $7,000 and $11,000 before setting at $6,000 in March 2018.
  - During April and May the price increased to $9,500 before a steady drop to $6,000 (today's value)

1. 10,000 Bitcoins at todays value of approx. $6,000 = $60,000,000...

A Final Word of Advice

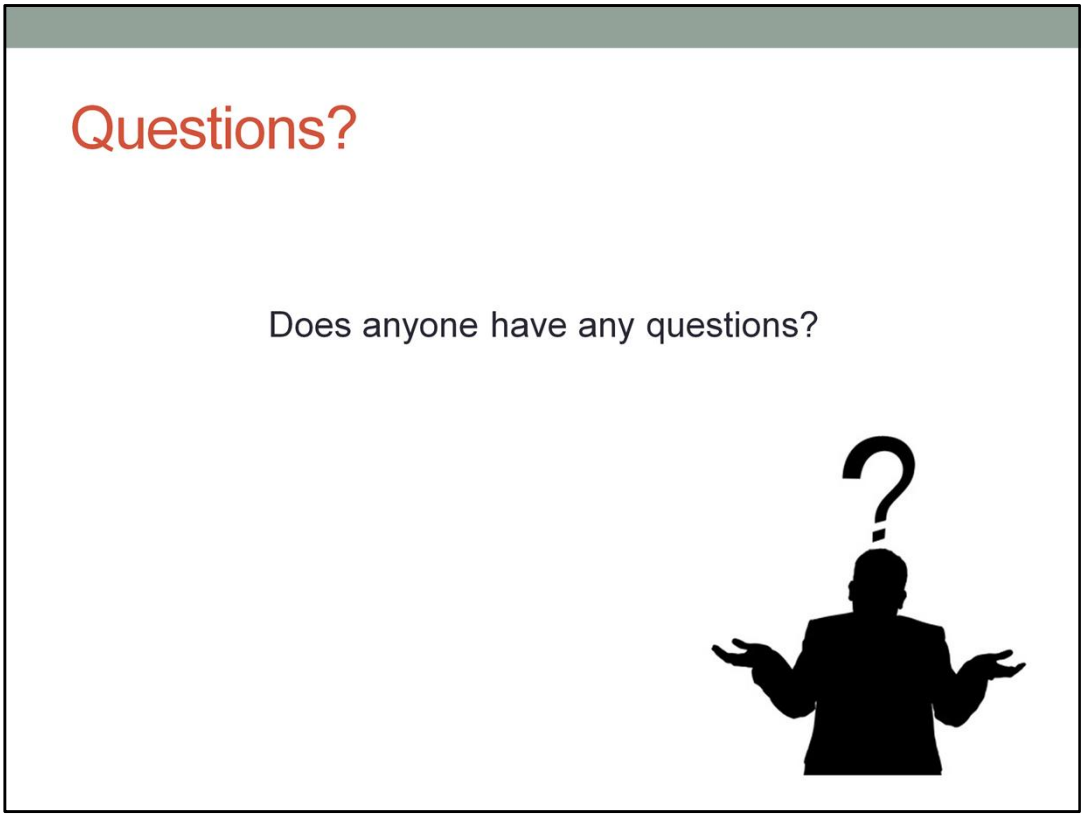
- With so many cryptocurrencies available, it's a gamble on choosing which one to use/mine, and which one you may "make a profit" on.
- The cost of "mining" can outweigh the return you get.
- Personally, I recommend you avoid cryptocurrencies, in my view they are just too risky!

1. Play with them for fun, to understand and see how they work.
2. Really, only the early adopters make any profit. Be wary of the "press hype".

Further Information

- Wikipedia
  - https://en.wikipedia.org/
- Lots of useful tutorials
  - http://www.howtogeek.com/
- TechRadar has a good selection of reviews.
  - http://www.techradar.com/

1. Further Information.



1. Questions?