

Beveiliging van netwerken en computers

CHAPTER 7 FUTURE EVOLUTIONS

PROF. DR. IR. ELI DE POORTER

eli.depoorter@ugent.be

GHENT UNIVERSITY – IMEC

IDLAB

<http://idlab.technology> | <http://idlab.ugent.be>



■ Overview

- **Cryptocurrency and block chains**
- Quantum computing

2



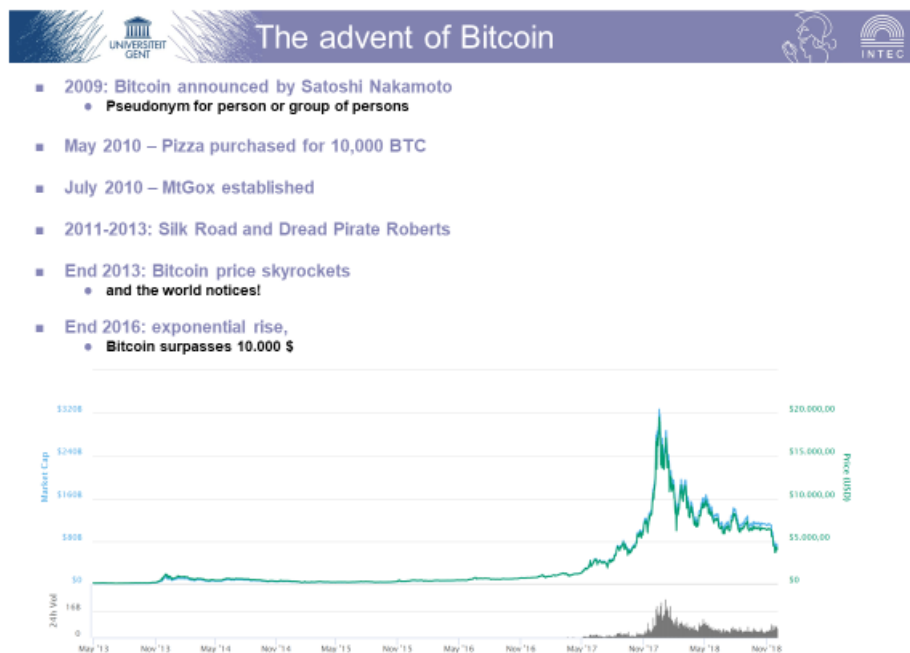
■ Virtual currencies

- **Unregulated, virtual money accepted in a virtual community**
 - ▶ Linden dollars (second life)
 - ▶ MMORPG: Massively multiplayer online role-playing game currencies
 - ▶ Facebook credits
 - ▶

■ Cryptocurrency

- **Utilizes cryptographic methods to**
 - ▶ Secure transactions
 - ▶ Create new currency units
- **Typically fully decentralized**

3



4

Bitcoin was created as a digital currency, by an entity only known as Satoshi Nakamoto. It has a fixed maximum supply of coins and rules on how it operated. It was created to solve the problem that banks can be manipulated by governments and bankers alike, and also to give people freedom of privacy in their transactions, although all transactions are public on the ledger, provided sending/receiving addresses are kept private and new ones used for different transactions a certain degree of privacy can be expected.

Bitcoin has experienced a surge in value. However, the surge in attention and value has also attracted a number of critics, including Vanguard founder Jack Bogle and Nobel Prize winner Professor Joseph E. Stiglitz from Columbia University. They have both attacked Bitcoin saying that it's a "bubble," comparing it to many Dotcom companies that were really shell companies offering little value and not "backed by anything." Stiglitz actually went so far to say Bitcoin should be outlawed and said it doesn't serve any useful social function.



- **Number of BitCoins in circulation 17 million**
 - **Total number of BitCoins generated cannot exceed 21 million**
- **Transactions per day (end 2017)**
 - **+/- 300.000 (still far less than VISA)**



In 2016, VisaNet processes an average of 150 million transaction each day, or around 1,667 transaction per second on average. “Based on rigorous testing, we estimate that VisaNet is capable of processing more than 56,000 transaction messages per second,” said Visa. PayPal processes around 193 transactions per second average, with up to 450 payments per second on Cyber Monday. Compared to these numbers, a theoretical maximum speed for Bitcoin that has been circulating online is seven transactions per second. However, in reality the Bitcoin network is achieving only maximums of 3 to 4 transactions per second. The much lower transactions per day for Bitcoin could be an indication that Bitcoin is still mostly seen as an investment vehicle, rather than a day-to-day currency, especially since the number of transactions remains fairly static even when the value of Bitcoin changes over time.



- **All virtual currency must address the following challenges:**
 - **Creation of a virtual coin/note**
 - ▶ How is it created in the first place?
 - ▶ How do you prevent inflation? (What prevents anyone from creating lots of coins?)
 - **Validation**
 - ▶ Is the coin legit? (proof-of-work)
 - ▶ How do you prevent a coin from double-spending?
- **BitCoin takes an infrastructure-less approach**
 - **Rely on proof instead of trust**
 - **No central bank or clearing house**

6

Buyer and Seller protection in traditional transactions (e.g. VISA) rely on a trusted 3th party. This party takes some of the risks of the transactions, manages fraud (e.g. by refunding) and in exchange is paid a fee. BitCoin gets rid of this trusted middleman, by being able to directly show the cryptographic proof that the money is transferred.



■ Security requirements of a currency

● Authentication

- ▶ Am I paying the right person? Not some other impersonator?
 - ✓ Through public key cryptography: Digital Signatures
- ▶ Is the coin legit
 - ✓ Through cryptographic hashes

● Integrity

- ▶ Is the coin double-spent?
 - ✓ Broadcasting transactions (signed)
- ▶ Can an attacker reverse or change transactions?
 - ✓ Ensured through a publicly disclosed linked ledger of transactions stored in a "blockchain"

● Availability

- ▶ Can I make a transaction anytime I want?

● Confidentiality

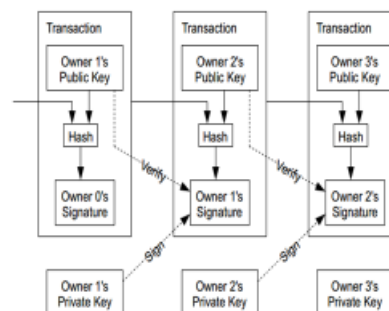
- ▶ Not very relevant(?). But privacy is important.

7



■ BitCoin transfer

- = $\text{Sign}(\text{Previous transaction} + \text{New owner's public key})$
- Anyone can verify (n-1)th owner transferred this to the n-th owner.
- Anyone can follow the history of a specific bitcoin



8

A coin owner transfers coins by digitally signing (via ECDSA) a hash digest of the previous transaction and the public key of the next owner. This signature is then appended to the end of the coin. Bitcoins do not need to be spent fully. Bitcoin has the ability to be split into many units, called a 'satoshi' at its smallest amount. As such, a Bitcoin can be broken down 100 million times if needed.

A transaction must have one or more inputs. For the transaction to be valid, every input must be an unspent output of a previous transaction. Every input must be digitally signed. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. A transaction can also have multiple outputs, allowing one to make multiple payments in one go. As in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such case, an additional output is

used, returning the change back to the payer. Any input that is not accounted for in the transaction outputs become the transaction fee.



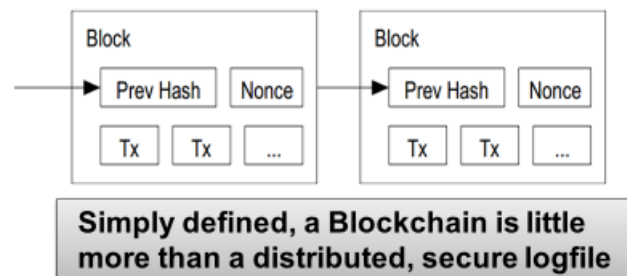
□ Record keeping

□ Collect transactions in a new “block”

- Block = list of previous transactions from many users, together with cryptographic relation to a previous block

□ Blocks are linked “chained” to the previous block through a difficult “proof-of-work” calculation

- Typically a hash function with a difficult to find nonce
- Verification is easy. But proof-of-work is hard.



9

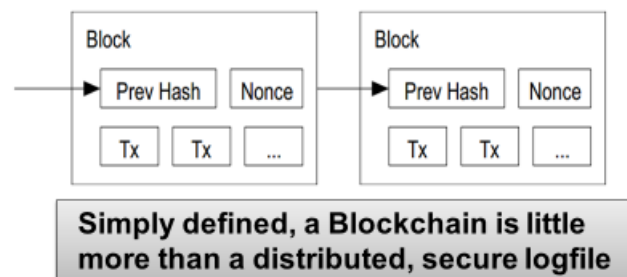
Tx = list of transactions

Unlike the traditional banking system, which can charge quite high transaction fees, bitcoin allows transactions globally with very little cost. Instead, miners are rewarded for verifying transactions by the possibility of earning bitcoins. The idea is that once all the bitcoins are minted, people donating computing power are still given an incentive to do so, while keeping the supply capped and well distributed.

The block chain is a public ledger that records and verifies bitcoin transactions. A novel solution accomplishes this without any trusted central authority: maintenance of the block chain is performed by a network of communicating nodes running bitcoin software. Transactions of the form payer X sends Y bitcoins to payee Z are broadcast to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The block chain is a distributed database; to achieve independent verification of the chain of ownership of any and every bitcoin (amount), each network node stores its own copy of the block chain. Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the block chain, and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent double-spending in an environment without central oversight.



- **Calculating the proof of work**
 - **Find a nonce such that $H(\text{prev hash, nonce, Tx}) < E$.**
 - E is a "difficulty" variable that the system specifies.
 - Basically, this amounts to finding a hash value whose leading bits are zero.



10

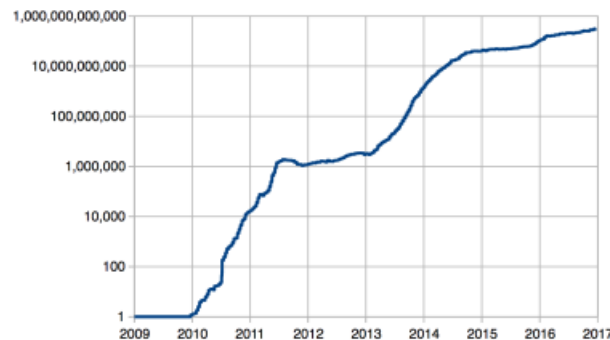
Mining is a record-keeping service. Miners keep the block chain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a block. A new block contains information that "chains" it to the previous block thus giving the block chain its name. It is a cryptographic hash of the previous block, using the SHA-256 hashing algorithm. In order to be accepted by the rest of the network, a new block must contain a so-called proof-of-work. The proof-of-work requires miners to find a number called a nonce, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target. This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash miners must try many different nonce before meeting the difficulty target.



□ Proof-of-work

- The work required is exponential in the number of zero bits required.
- Used for prevention of inflation: limit the creation rate of the BitCoins by lowering E over time
- Automatically adjusted so that a new block is found every 10 minutes

□ Difficulty increase over time (logarithmic):



11

Every 2016 blocks (approximately 14 days), the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. In this way the system automatically adapts to the total amount of mining power on the network. For example, between 1 March 2014 and 1 March 2015, the average number of nonces miners had to try before creating a new block increased from 16.4 quintillion to 200.5 quintillion.

Figure: relative mining difficulty from 9 January 2009 to 31 December 2017 (the difficulty scale is logarithmic). Relative mining difficulty is defined as the ratio between the difficulty target on 9 January 2009 and the current difficulty target.



■ Each node runs the following algorithm:

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a proof-of-work for its block.
(Hard to do. Probabilistic. The one to finish early will probably win.)
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
 - ▶ Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
 - ▶ Needs consensus (>50% of nodes agree)
 - ▶ Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

12



■ Having a transaction provisionally accepted into a candidate block signals that the network has verified that the inputs were viable

- Every new block accepted into the chain after the transaction was accepted is considered a confirmation
- Coins are not considered mature until there have been 6 confirmations (basically an hour assuming a 10 minute block cadence)
- New Coins created by the mining process are not valid until about 120 confirmations
- This is to assure that a node with more than 51% of the total hash-power does not pull off fraudulent transactions

13

Preventing Double-spending

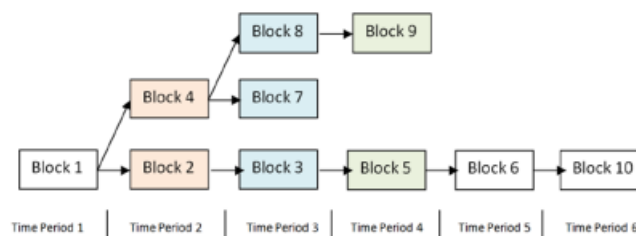
- **The only way is to be aware of all transactions.**
 - **Each node (miner) verifies that this is the first spending of the BitCoin by the payer.**
 - ▶ Only when it is verified it generates the proof-of-work and attaches it to the current chain.
 - **During the verification process (10 minutes) the coin can not be spent**
- **Subsequent blocks**
 - **Used for confirmation**
 - ▶ Make modifications to previous transactions more difficult over time

14

The proof-of-work system, alongside the chaining of blocks, makes modifications of the block chain extremely hard as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called confirmations of the given block) increases.

Arriving at Consensus

- **Although the accepted chain can be considered a list, the block chain is best represented with a tree.**
 - **The longest path represents the accepted chain.**
 - **A participant choosing to extend an existing path in the block chain indicates a vote towards consensus on that path.**
- **The longer the path, the more computation was expended building it.**

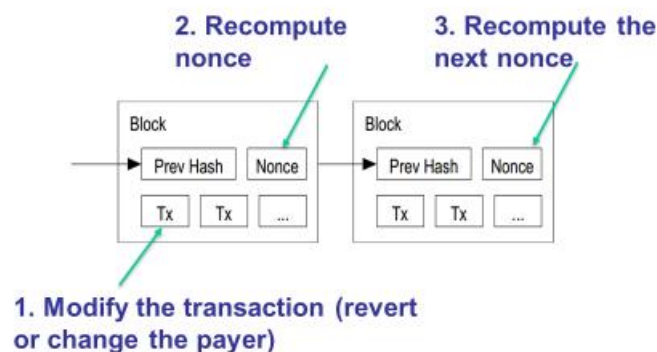


15

In case multiple competing solutions exist (e.g. two nodes find a correct block simultaneously by solving the proof-of-work), the reward is given to the solutions that includes the highest number of transactions. If two nodes offer a solution to the challenge and both have the same number of transactions, the reward will go to the node that found a lower NONCE that beat the challenge (the node that supplies a hash that has 5 zeros beats the node that only finds the minimum). Nevertheless, it still happens that multiple chains are temporarily coexisting. In case one chain grows significantly longer than the other, typically the longest chain is kept.



■ Reverting gets exponentially hard as the chain grows.



16



- **Payout**
 - The node that finds the best solution to the challenge is provisionally granted a reward (e.g. bitcoins)
- **Rate limiting on the creation of a new block**
 - Adapt to the “network’s capacity”
 - A block created every 10 mins (six blocks every hour)
 - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- **N new bitcoins per each new block: credited to the miner → incentives for miners**
 - N was 50 initially in 2008.
 - Halved every 210,000 blocks (+- every 4 years, next in 2020)
 - Thus, the total number of BitCoins will not exceed 21 million.

17

Finding a proof of work constitutes “mining” a new coin. This way, rewards are given to user to verify and keep the transaction histories up to date. As such, Bitcoins are introduced at a fixed rate every 10 minutes on average. When a miner solves the mathematical problem, they are awarded 12.5 bitcoins at the current writing. This originally started out at 50, halving in 2012, then in 2016, set to halve at every 4 years on average. In 2020, the expected bitcoins per block mined is expected to be 6.25. Unlike money which can be printed at will by the central banks and governments, bitcoins supply is capped at 21 million whole units. As such, 21 million bitcoins are the maximum amount that will be mined (although this could change in the future).



□ Transaction fees



18

Once all bitcoins are minted, the incentive to keep track of the transactions is lower. To remedy this, transaction fees give the miners an incentive to mine and record transactions on the blockchain. The sender of a transaction does include a ‘transaction fee’ or ‘miners fee’ with their transactions, typically 0.0001 of a bitcoin or similar, during high network load times this can go up slightly. You can send transactions without a fee and hope miners still include it in their blocks, which they may do at times of low network demand. The small fees add up when thousands of transactions are taking place. This fee goes to the miner who generates the next block. The fees are the incentive to mine when all the bitcoins have been minted.

Bitcoin has a fundamental problem which has come to light as demand for the currency has increased. Until recently, the Bitcoin network had a hard-coded 1 megabyte limit on the size of blocks on the blockchain, Bitcoin's shared transaction ledger. With a typical transaction size of around 500 bytes, the average block had fewer than 2,000 transactions. And with a block being generated once every 10 minutes, that works out to around 3.3 transactions per second.

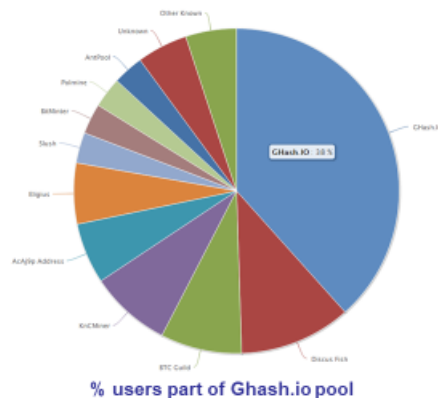
At times of peak demand, it can be recommended to increase your transaction fee to jump the queue for the limited block space. If there are more transactions than will fit into one block, miners can be expected to choose the transactions with the highest fees first. So the higher the fee you attach to a transaction, the more likely it is to make it into the next block. Of course, demand fluctuates over the course of the day. So if you have a non-urgent transaction, you're welcome to submit it with a below-average fee and let it sit around unconfirmed for a few hours. At some point, demand might slacken and you might get your transaction at a bargain price. The typical rates and their corresponding waiting time can be found at sites such as <https://bitcoinfees.info/> or <https://bitcoinfees.earn.com/>

A September 2017 upgrade called “segregated witness” allowed the cryptographic signatures associated with each transaction to be stored separately from the rest of the transaction. Under this scheme, the signatures no longer counted against the 1 megabyte blocksize limit, which should have roughly doubled the network's capacity. But only a small minority of transactions have taken advantage of this option as of 2017, so the network's average throughput has stayed below 2,500 transactions per block—around four transactions per second. Debate about how to cope with even further rising demand has split the Bitcoin community in two. On one side are “big block” advocates who argue that the network should simply raise the 1MB block limit. After more than two years of argument, some big blockers created Bitcoin Cash, a fork of the mainstream Bitcoin software that allows blocks to be up to 8MB. But others, including the main developers of the standard Bitcoin client, worry that larger blocks will make it too difficult for ordinary users to participate in Bitcoin's peer-to-peer process for validating transactions. They have instead pinned their hopes on Lightning, an experimental new payment network that routes payments using chains of payment channels. If Lightning works as supporters hope it will, it will allow most bitcoin transactions to occur off-chain, permitting a lot more transactions to occur without increasing the size of the blockchain.

- **At least 10 mins to verify a transaction.**
 - Agree to pay
 - Wait for one block (10 mins) for the transaction to go through.
 - But, for a large transactions wait longer. Because if you wait longer it becomes more secure. Typically, in this case you wait for six blocks (1 hour).
- **New Coins created by the mining process are not valid until about 120 confirmations**

19

- **BitCoin is becoming industrialized.**
 - Mining hardware becomes sophisticated
 - Miners form a pool
- **51% attack**
 - When a pool controls >50% of the miners
 - Full control over transaction
 - To date the network has voluntarily shifted its mining power around or faced Distributed Denial of Service attacks



20

See also <https://www.youtube.com/watch?v=6luEMwSASOI>

Mining bitcoins

- GPU: Radeon HD 6990 about 700 MH/s
- Butterfly Labs:
 - FPGA, ASIC



21

Interestingly, a paper published in 2014 by researchers from the Hamilton Institute at the National University of Ireland Maynooth considered the impact cryptocurrency mining has on electricity. The authors, Karl J. O'Dwyer and David Malone, concluded that “the cost of Bitcoin mining on commodity hardware now exceeds the value of the reward.” As a result, specialized firms now provide dedicated mining equipment based on FPGAs or ASICs.

Mining bitcoins

If the value represents anything it's this...\$1bn invested so far. Good or bad idea?



22

Mining bitcoins

Website Owners Are “Cryptojacking” Their Visitors’ Computers to Mine for Cash

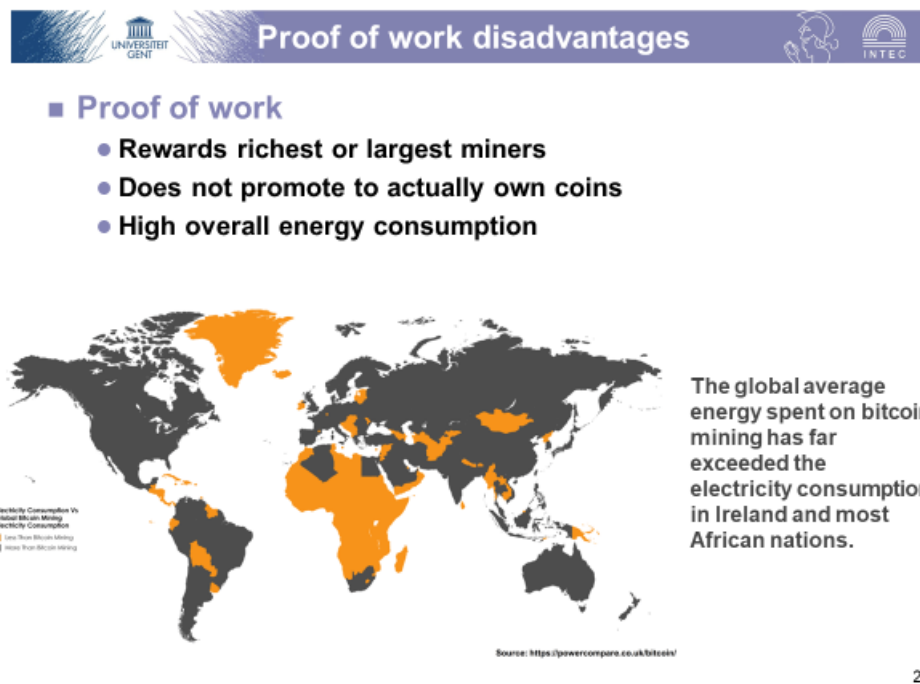
By Rafia Shaikh
Oct 10, 2017



23

Attackers are now increasingly using websites to mine for cryptocurrency using visitors of infected sites. Security firm Trend Micro reports that high-traffic sites – like file sharing websites – have been discovered infected with code that uses visitors’ machines for mining purposes without their consent. Hundreds of websites were found carrying this malicious code. Scanning the code behind a million of the most popular websites, security researchers found Coinhive – a popular, legitimate mining script – and a new JSE Coin script. These scripts are extremely easy to use by website owners or attackers since they offer a simple JavaScript file that website owners have to load on their sites to mine cryptocurrency using their site visitors’ CPU power. Coinhive suggests that a website that gets one million visitors in a month could make about \$116 worth of Monero.

According to security experts, it's not always criminal groups who infect hundreds of thousands of websites to generate quick cash as some websites deliberately use mining scripts to use their visitors' computers for mining cryptocurrency. However, this mining process is being adopted by many hackers. Popular, high-stream websites like The Pirate Bay have been found carrying the script, whether knowingly or not. On many websites that were running these scripts, researchers did say the script was concealed suggesting a surreptitious injection using attacks such as XSS.

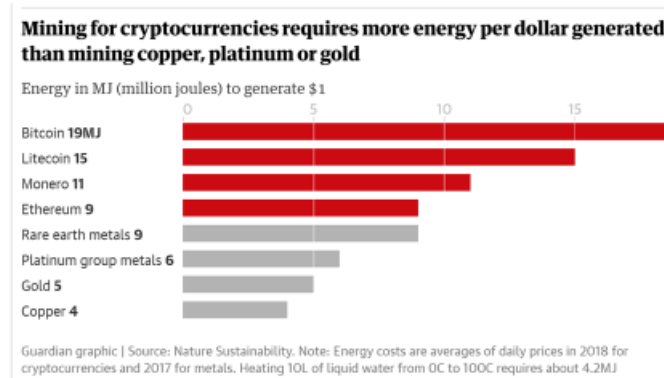


24

Proof of Work relies on energy use. According to a bitcoin mining-farm operator, energy consumption totaled 240kWh per bitcoin in 2014 (the equivalent of 16 gallons of gas). According to 2017 research conducted by a U.K.-based energy comparison tariff service called PowerCompare, the average electricity used to mine bitcoin this year has surpassed the annual energy usage of some 159 countries. Specifically, the global average energy spent on bitcoin mining has far exceeded the electricity consumption in Ireland and most African nations. The new research used data provided by Digiconomist, whose current estimate of electricity used to mine bitcoin is around 30.14 TWh annually. That's way above Ireland's 25 TWh yearly average electricity consumption. In fact, according to a recent paper from Dutch bank ING, a single bitcoin transaction consumes enough energy to power the average household for an entire month. Digiconomist also found that Ethereum, the second most popular cryptocurrency today, also uses more than a country's worth of electricity. Moreover, these energy costs are almost always paid in non-cryptocurrency, introducing constant downward pressure on the price.



■ Energy consumption per transaction (2018)



25

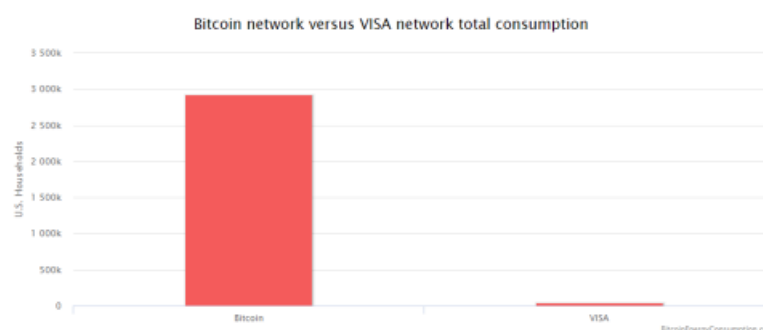
From <https://www.theguardian.com/technology/2018/nov/05/energy-cost-of-mining-bitcoin-more-than-twice-that-of-copper-or-gold>



■ Energy consumption per transaction

- “One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week”
- “Mining is responsible for 8,000 to 13,000 kg CO2 emissions per Bitcoin mined, and 24,000 - 40,000 kg of CO2 per hour”

■ Is it still ethically justifiable to use bitcoin?



26

To put the overall Bitcoin energy consumption in perspective, it is insightful to compare not just the overall energy consumption, but also the energy consumption per transaction. To this end, we can compare it to another payment system like VISA for example. Even though the available information on VISA's energy consumption is limited, we can establish that the data centers that process VISA's

transactions consume energy equal to that of 50,000 U.S. households. With the help of these numbers, it is possible to compare both networks and show that Bitcoin is extremely more energy intensive per transaction than VISA. On average, Bitcoin requires a shocking 215 kilowatt-hours (KWh) of juice used by miners for each Bitcoin transaction. Since the average American household consumes 901 KWh per month, each Bitcoin transfer represents enough energy to run a comfortable house, and everything in it, for more than a week! Of course, these estimations are far from perfect (e.g. energy consumption of VISA offices isn't included), but the differences are so extreme that they remain shocking regardless. It is questionable if Bitcoin is truly an ethical and sustainable way to perform transactions in the future... One could argue that this is simply the price of a transaction that doesn't require a trusted third party, but this price doesn't have to be so high as will be discussed hereafter.



■ Proof of Stake (PoS)

- **Make the coin generation process more democratic, less wasteful**
- **Selection options**
 - ▶ **Randomized**
 - ✓ E.g. Nxt, BlackCoin
 - ▶ **Coin age based selection**
 - ✓ Rewards saving coins
 - ✓ E.g. Peercoin
 - ▶ **Velocity based selection**
 - ✓ Rewards spending
 - ✓ E.g. Reddcoin
 - ▶ **Voting based selection**
 - ✓ Potentially through randomly selected delegates
 - ✓ E.g. Bitshares

27

Proof of Stake currencies can be several thousand times more cost effective. The incentives of the block-generator are also different. Under Proof-of-Work, the generator may potentially own none of the currency he is mining. The incentive of the miner is only to maximize his own profits. It is unclear whether this disparity lowers or raises security risks. In Proof-of-Stake, those "guarding" the coins are always those who own the coins (although several cryptocurrencies do allow or enforce lending the staking power to other nodes). Proof-of-stake must have a way of defining the next valid block in any blockchain. Selection by account balance would result in (undesirable) centralization, as the single richest member would have a permanent advantage. Instead, several different methods of selection have been devised.

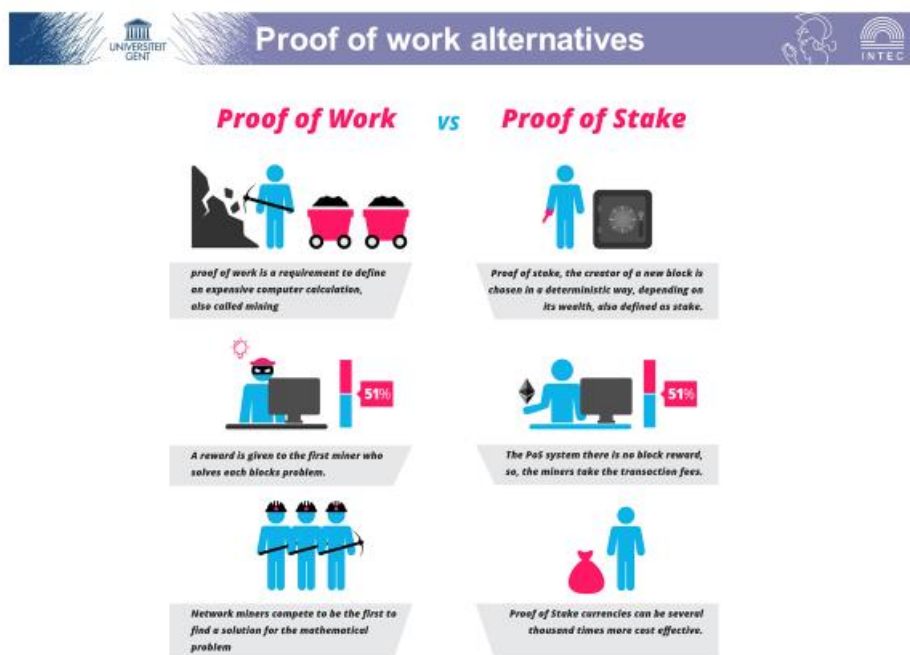
Randomized Block Selection. Nxt and BlackCoin use randomization to predict the following generator, by using a formula that looks for the lowest hash value in combination with the size of the stake. Since the stakes are public, each node can predict - with reasonable accuracy - which account will next win the right to forge a block.

Coin Age Based Selection. Peercoin's proof-of-stake system combines randomization with the concept of "coin age," a number derived from the product of the number of coins times the number of days the coins have been held. Coins that have been unspent for at least 30 days begin competing for the next block. Older and larger sets of coins have a greater probability of signing the next block. However, once a stake of coins has been used to sign a block, they must start over with zero "coin age" and thus wait at least 30 more days before signing another block. Also, the probability of finding the next block reaches a maximum after 90 days in order to prevent very old or very large collections of stakes from dominating the blockchain. This process secures the network and gradually produces new

coins over time without consuming significant computational power. Peercoin's developer claims that this makes a malicious attack on the network more difficult due to the lack of a need for centralized mining pools and the fact that purchasing more than half of the coins is likely more costly than acquiring 51% of proof-of-work hashing power.

Velocity Based Selection. Reddcoin's 'Proof of Stake Velocity' (PoSV) claims to encourage velocity i.e. movement of money between people, rather than hoarding.

Voting Based Selection. Instead of only using the stake size, the block generators can be selected by votes. BitShares uses a system where stake is used to elect a total of 101 delegates, who are then ordered at random. This has many of the advantages of shareholder voting (for example, the flexible accountability enhance the incentives of the generators to act responsibly), and yet it reintroduces the dangerous sybil attack - as in one case where one user posed as the top five delegates.



28

From <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

Implementation choices

■ Bitcoin signature

- ECDSA (Elliptic curve digital signature algorithm)
- Hash = SHA256
- Proof of work

■ Bitcoin variants

- Now well over 500 “alternate” coins to Bitcoin
- 99.999% of them are simply brands / clones
- Most tinker with:
 - ▶ the total coin supply
 - ▶ the hashing functions (SHA256, SCRYPT, X11 et al)
 - ▶ block emit time targets
 - ▶ Proof of Something (Proof of Work, Proof of Stake)
- Notable Alts: Ripple, Litecoin, Dogecoin

29

Bitcoin flavors

■ <http://coinmarketcap.com/>

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾		Exchanges ▾		Watchlist		USD ▾		Next 100 →	View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)		
1	Bitcoin	\$72,485,580,251	\$4,185.03	\$5,108,640,265	17,403,375 BTC	-0.64%			...
2	XRP	\$14,912,665,587	\$0.369790	\$345,626,988	40,327,341,704 XRP *	-0.68%			...
3	Ethereum	\$12,110,663,292	\$116.95	\$1,764,190,925	103,556,431 ETH	-0.98%			...
4	Stellar	\$3,114,789,870	\$0.162614	\$72,145,340	19,154,500,189 XLM *	-2.55%			...
5	Bitcoin Cash	\$3,028,709,460	\$173.18	\$72,117,282	17,488,988 BCH	-0.79%			...
6	EOS	\$2,665,599,063	\$2.94	\$759,463,378	906,245,118 EOS *	-1.00%			...
7	Litecoin	\$2,009,100,211	\$33.82	\$429,057,057	59,396,413 LTC	0.56%			...
8	Tether	\$1,846,250,162	\$0.994521	\$3,155,393,805	1,856,421,736 USD*	-0.36%			...
9	Bitcoin SV	\$1,756,475,657	\$100.50	\$101,550,357	17,477,861 BSV	5.80%			...

30



■ Bitcoin has had its fair share of “bad press”

- **Silk Road**
 - ▶ An online anonymous marketplace for “censorship-free” commerce
- **Bitinstant**
 - ▶ Charlie Shrem plead guilty to aiding money laundering
- **MT-GOX**
 - ▶ aka “Magic The Gathering Online eXchange”
 - ▶ 700,000 coins “missing”
- **Bitstamp**
 - ▶ Hacked and lost 19.000 bitcoins
-

31



■ Advantages

- **Low inflation risks**
- **Freedom in payment**
 - ▶ No unexpected fees, limitations, ...
- **No personal information divulged**
- **Transparent**
 - ▶ No external manipulation, fraud detection, etc.
- **Can not go bankrupt (?)**
 - ▶ Resilient to government collapse or bank crisis

■ Disadvantages

- **Risk and volatility**
- **Not generally accepted**
- **Bad reputation due to incidents**
- **Easy to loose**
- **Energy costs (for proof of work)**

32



■ Similar ideas have already been applied for

- **Asset & supply chain management**
 - ▶ E.g. Ethereum, Skuchain, Factom
- **Cloud storage**
 - ▶ E.g. Storj.io
- **Insurance & smart contracts**
 - ▶ E.g. ethereum, mastercoin.org
- **Voting**
- **Identity & Reputation Systems**
 - ▶ <http://bit.ly/idcoins>
- **Government resilient DNS system**
 - ▶ E.g. NameCoin
- **News sharing, Taxes, p2p payments, microfinance, etc.**

33

The technology underlying blockchains has several potential non-cryptocurrency applications. Blockchain is mostly useful when it eliminates a third party whose main responsibility is maintaining trust (e.g. banks). On the application level, companies who help businesses and consumers trace and authenticate a product and its source are the most valuable. Some examples include the following.

- **Asset management.** The block chain ledger can be used to keep track of the location and ownership of assets, replacing ownership and lending contracts especially for markets with very mobile goods. Blockchain's immutable ledger makes it well suited to tasks such as tracking goods as they move and change hands in the supply chain. Using a blockchain opens up several options for companies transporting these goods. Entries on a blockchain can be used to queue up events with a supply chain (allocating goods newly arrived at a port to different shipping containers, for example). Blockchain provides a new and dynamic means of organizing tracking data and putting it to use. Companies like Skuchain and Factom offer solutions that utilize blockchain in supply chain management solutions.
- **Cloud storage.** Storj is beta-testing cloud storage using a Blockchain-powered network to improve security and decrease dependency. Users (you) can rent out their excess storage capacity, Airbnb-style, creating new marketplaces. Anyone on the internet can store your data at a pre-agreed price. Hashing and having the data in multiple locations are the keys to securing it. After encrypting your data, blockchains track the availability, access rights and storage location of your data.
- **Insurance.** Arguably the greatest blockchain application for insurance is through smart contracts. Such contracts powered by blockchain could allow customers and insurers to manage claims in a truly transparent and secure manner, according to Deloitte. All contracts and claims could be recorded on the blockchain and validated by the network, which would eliminate invalid claims. For example, the blockchain would reject multiple claims on the same accident.
- **Voting.** Pete Martin, the CEO of mobile voting platform Votem, said the following to Government Technology about blockchain's application in voting: "Blockchain technology provides all of the characteristics you would want in a platform that is arguably the most important part of a democratic society; it's fault-tolerant, you cannot change the past, you cannot hack the present, you cannot alter the access to the system, every node with access can see the exact same results, and every vote can be irrefutably traced to its source without sacrificing a voter's vote anonymity. End to end verifiable voting systems will give the voter the ability to verify if their

vote is correctly recorded and correctly counted, for instance, if a ballot is missing, in transit or modified, it can even be detected by the voter and caught before the election is over.“



■ Overview

- Cryptocurrency and block chains
- Quantum computing

34



Quantum computers differ in the way information is stored and processed.

- In **classical computers**, information is represented on **macroscopic level** by **bits**, which can take one of the two values

0 or 1

- In **quantum computers**, information is represented on **microscopic level** using **qubits**, (quantum bits) which can take on any from the following uncountable many values

$$\alpha | 0 \rangle + \beta | 1 \rangle$$

where α, β are arbitrary complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1.$$

35



- In 1994 Peter Shor from the AT&T Bell Laboratory showed that in principle a quantum computer could factor a very long product of primes in seconds.
 - RSA & ElGamal would no longer be safe!
 - Although some other protocols likely won't be compromised
- Quantum computing *might* also render other unproven mathematical assumptions moot
 - Although this remains to be seen...

36

In 1994, Peter Shor, the Morss Professor of Applied Mathematics at MIT, came up with a quantum algorithm that calculates the prime factors of a large number, vastly more efficiently than a classical computer. However, the algorithm's success depends on a computer with a large number of quantum bits. While others have attempted to implement Shor's algorithm in various quantum systems, none have been yet been able to do so with more than a few quantum bits, in a scalable way.



■ Based on physical properties

- **Qubit or quantum bit**
 - ▶ Unit of quantum information
 - ▶ Can be in a 'superposition' of 0 and 1 simultaneously
- **Impossible to copy data encoded in a quantum state**
 - ▶ Reading data encoded in a quantum state changes the state
 - ▶ Used to detect eavesdropping in quantum key distribution.

37



■ Quantum Key Distribution (QKD)

- **Utilizes polarized photons (qubits) with quantum properties**

■ Photons

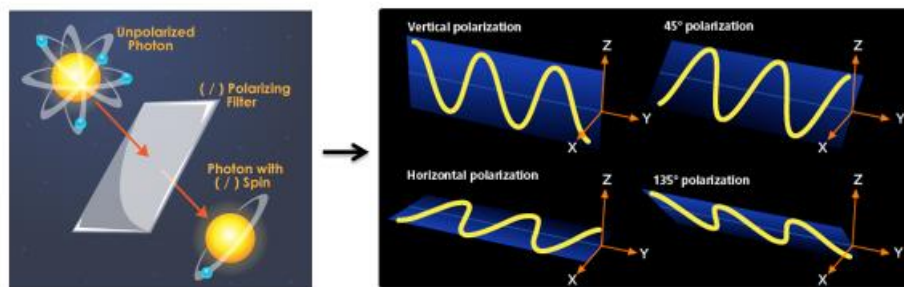
- **No mass**
- **Exists in all states at once (the "wave" function)**
 - ▶ Heisenberg's Uncertainty Principle
 - ▶ Photons spin in all directions at once

38



■ Photons

- Can be polarized through polarization filters

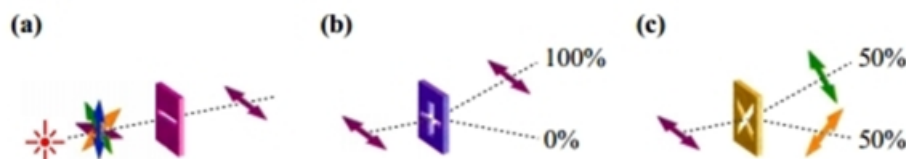


39



■ Photons

- Once polarized, can only be observed through similar oriented filters.
 - Using a different oriented filter will modify the photon behavior
 - ✓ Diagonal filters vs rectilinear filters
 - Only 1 filter can be used simultaneously
 - Combining the two types of filters randomizes the spin of the photons



40

- To create a photon, quantum cryptographers use LEDs -- light emitting diodes, a source of unpolarized light. LEDs are capable of creating just one photon at a time, which is how a string of photons can be created, rather than a wild burst. Through the use of linear polarization filters, we can force the photon to take one state or another -- or polarize it. If we use a horizontal polarizing filter situated beyond a LED, we can polarize the photons that emerge: the photons that aren't absorbed will emerge on the other side with a horizontal spin (-). That process creates a qubit with horizontal polarization.
- Once photons are polarized, they can't be accurately measured again, except by a filter like the one that initially produced their current spin. As such, when the horizontally-polarized photon

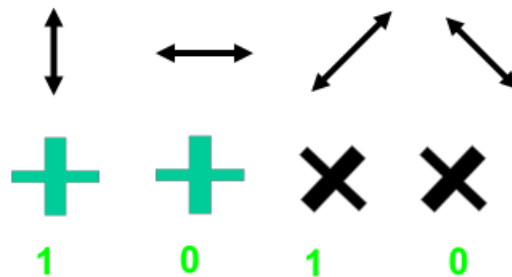
passes through a horizontally/vertically-oriented polarizing beamsplitter, it retains its horizontal polarization.

- (c) However, if a photon with a horizontal spin is measured through a diagonal diagonally-oriented polarizing beamsplitter, either the photon won't pass through the filter or the filter will affect the photon's behavior, causing it to take a diagonal spin. In fact, when the horizontally-polarized photon passes through a diagonally-oriented polarizing beamsplitter, there is a 50% probability of finding the photon at one (and only one) of the exits. The polarization of the photon will have changed to one of the corresponding diagonal polarization. In this sense, the information on the photon's original polarization is lost, and so, too, is any information attached to the photon's spin



■ Quantum Key Distribution (QKD)

- Two distinct polarized photon coding schemes are used
 - ▶ Horizontal (+) and diagonal (x)

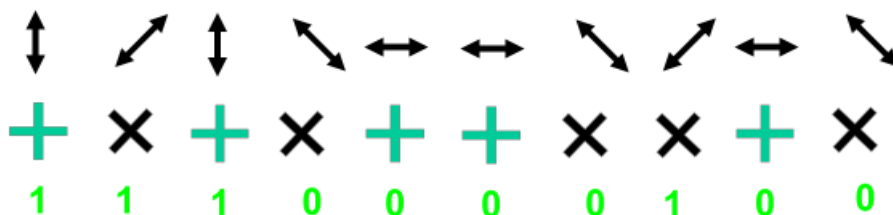


41



■ Quantum Key Distribution (QKD)





























































- Two distinct polarized photon coding schemes are used
 - ▶ Horizontal (+) and diagonal (x)
- Alice randomly switches between + and x schemes, and sends a random string of 1's and 0's to Bob.
 - ▶ Alice keeps track of the coding schemes she used and the bits she sent.



42

■ Quantum Key Distribution (QKD)

- **Bob measures these photons with his own random choice of scheme (he does not know what Alice has done).**
 - Sometimes he gets it right, sometimes he gets it wrong

  	  	  	  	  	  	  	  	  	  	Alice's message
  	  	  	  	  	  	  	  	  	  	Bob measures

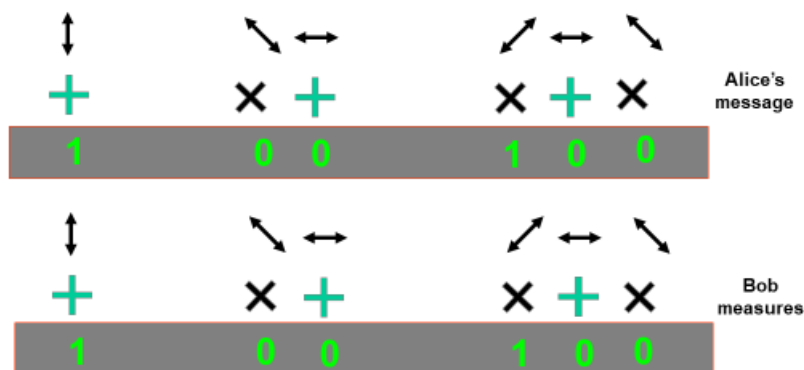
43

- Alice uses a light source to create a photon.
- The photon is sent through a polarizer and randomly given one of four possible polarization and bit designations — Vertical (One bit), Horizontal (Zero bit), 45 degree right (One bit), or 45 degree left (Zero bit).
- The photon travels to Bob's location.
- Bob has two beamsplitters — a diagonal and vertical/horizontal - and two photon detectors.
- For each incoming photon, Bob randomly chooses one of the two beamsplitters and checks the photon detectors.
- The process is repeated until the entire key has been transmitted to Bob.
- Bob then tells Alice in sequence which beamsplitter he used.
- Alice compares this information with the sequence of polarizers she used to send the key.
- Alice tells Bob where in the sequence of sent photons he used the right beamsplitter.
- Now both Alice and Bob have a sequence of bits (sifted key) they both know.



■ Quantum Key Distribution (QKD)

- Bob tells Alice which filters he used
- Alice informs Bob which bits were rightly decoded
 - ▶ These bits form a shared key



44



■ Quantum Key Distribution (QKD)

- Someone overhearing only knows which filter schemes were used, but not what the exchanged bits were
 - ▶ Even knowing the filter, the bit can still be
 - ✓ "—" or "|" (for rectilinear filters)
 - ✓ "/" or "\" (for diagonal filters)
- Any attempt to intercept photons will alter their state
 - ▶ Alice and Bob can detect this by comparing some of their bits to make sure they agree (and discarding these)
 - ▶ Safeguard against passive interception



45



Quantum cryptology is the first cryptology that safeguards against passive interception. Since we can't measure a photon without affecting its behavior, Heisenberg's Uncertainty Principle emerges when Eve makes her own eavesdrop measurements.

Here's an example. If Alice sends Bob a series of polarized photons, and Eve has set up a filter of her own to intercept the photons, Eve is in the same boat as Bob: Neither has any idea what the polarizations of the photons Alice sent are. Like Bob, Eve can only guess which filter orientation (for example an X filter or a + filter) she should use to measure the photons. After Eve has measured the photons by randomly selecting filters to determine their spin, she will pass them down the line to Bob using her own LED with a filter set to the alignment she chose to measure the original photon. She does

so to cover up her presence and the fact that she intercepted the photon message. But due to the Heisenberg Uncertainty Principle, Eve's presence will be detected. By measuring the photons, Eve inevitably altered some of them.

Say Alice sent to Bob one photon polarized to a (--) spin, and Eve intercepts the photon. But Eve has incorrectly chosen to use an X filter to measure the photon. If Bob randomly (and correctly) chooses to use a + filter to measure the original photon, he will find it's polarized in either a (/) or (\) position. Bob will believe he chose incorrectly until he has his conversation with Alice about the filter choice. After all of the photons are received by Bob, and he and Alice have their conversation about the filters used to determine the polarizations, discrepancies will emerge if Eve has intercepted the message. In the example of the (--) photon that Alice sent, Bob will tell her that he used a + filter. Alice will tell him this is correct, but Bob will know that the photon he received didn't measure as (--) or (|). Due to this discrepancy, Bob and Alice will know that their photon has been measured by a third party, who inadvertently altered it.

Alice and Bob can further protect their transmission by discussing some of the exact correct results after they've discarded the incorrect measurements. This is called a **parity check**. If the chosen examples of Bob's measurements are all correct -- meaning the pairs of Alice's transmitted photons and Bob's received photons all match up -- then their message is secure. Bob and Alice can then discard these discussed measurements and use the remaining secret measurements as their key. If discrepancies are found, they should occur in 50 percent of the parity checks. Since Eve will have altered about 25 percent of the photons through her measurements, Bob and Alice can reduce the likelihood that Eve has the remaining correct information down to a one-in-a-million chance by conducting 20 parity checks (<http://www.csa.com/discoveryguides/crypt/overview.php>).


Quantum cryptography


■ **Quantum Key Distribution (QKD)**

- **Disadvantages**
 - ▶ **Short range due to interference**
 - ✓ Photon spin can change when bouncing off other particles
 - ✓ Partly solved by applying quantum entanglement
 - ▶ **Practical ranges**
 - ✓ 36 cm in 1989
 - ✓ Nowadays up to 400+ km (optical cable)

46

The original quantum cryptography system, built in 1989 by Charles Bennett, Gilles Brassard and John Smolin, sent a key over a distance of 36 centimeters. The reason why the length of quantum cryptography capability is so short is because of interference. A photon's spin can be changed when it bounces off other particles, and so when it's received, it may no longer be polarized the way it was originally intended to be. This means that a 1 may come through as a 0 -- this is the probability factor at work in quantum physics. As the distance a photon must travel to carry its binary message is increased, so, too, is the chance that it will meet other particles and be influenced by them.

One group of Austrian researchers may have solved this problem. This team used what Albert Einstein called “spooky action at a distance.” This observation of quantum physics is based on the entanglement of photons. At the quantum level, photons can come to depend on one another after undergoing some particle reactions, and their states become entangled. This entanglement doesn’t mean that the two photons are physically connected, but they become connected in a way that physicists still don’t understand. In entangled pairs, each photon has the opposite spin of the other -- for example, (/) and (\). If the spin of one is measured, the spin of the other can be deduced. What’s strange (or “spooky”) about the entangled pairs is that they remain entangled, even when they’re separated at a distance. The Austrian team put a photon from an entangled pair at each end of a fiber optic cable. When one photon was measured in one polarization, its entangled counterpart took the opposite polarization, meaning the polarization the other photon would take could be predicted. It transmitted its information to its entangled partner. This could solve the distance problem of quantum cryptography, since there is now a method to help predict the actions of entangled photons.

Even though it’s existed just a few years so far, quantum cryptography already includes a number of potential attacks. A group of researchers from Massachusetts Institute of Technology took advantage of another property of entanglement. In this form, two states of a single photon become related, rather than the properties of two separate photons. By entangling the photons the team intercepted, they were able to measure one property of the photon and make an educated guess of what the measurement of another property -- like its spin -- would be. By not measuring the photon’s spin, they were able to identify its direction without affecting it. So the photon traveled down the line to its intended recipient none the wiser. The MIT researchers admit that their eavesdropping method may not hold up to other systems, but that with a little more research, it could be perfected. Hopefully, quantum cryptology will be able to stay one step ahead as decoding methods continue to advance. Since then, newer models have reached a distance of 400+ kilometers, bringing the techniques within the communication ranges for wireless communication.



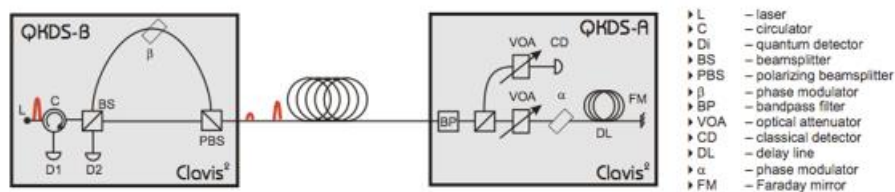
■ QKD protocols

- **BB84**
- **E91**
- **SARG04**
- **B92**
- **SSP**

An overview of differences and improvements made over the years can be found in <http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/>



■ Commercial quantum key distribution products exist



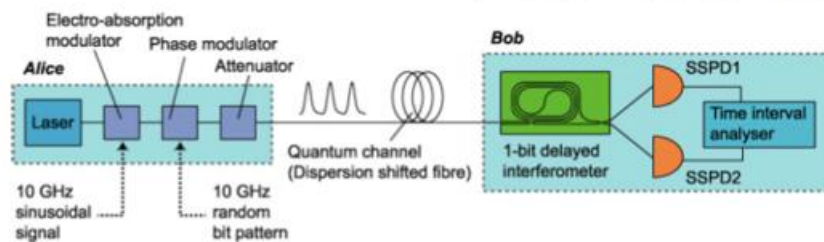
48

There are currently four companies offering commercial quantum key distribution systems; ID Quantique (Geneva), MagiQ Technologies (New York), QuintessenceLabs (Australia) and SeQureNet (Paris). Several other companies also have active research programs, including Toshiba, HP, IBM, Mitsubishi, NEC and NTT.

In 2004, the world's first bank transfer using quantum key distribution was carried in Vienna, Austria. Quantum encryption technology provided by the Swiss company ID Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capital in the national election occurring on 21 October 2007. In 2013, Battelle Memorial Institute installed a QKD system built by ID Quantique between their main campus in Columbus, Ohio and their manufacturing facility in nearby Dublin. Field tests of Tokyo QKD network have been underway for some time.

Current State of Affairs

■ Current fiber-based distance record: 307 km (University of Geneva)



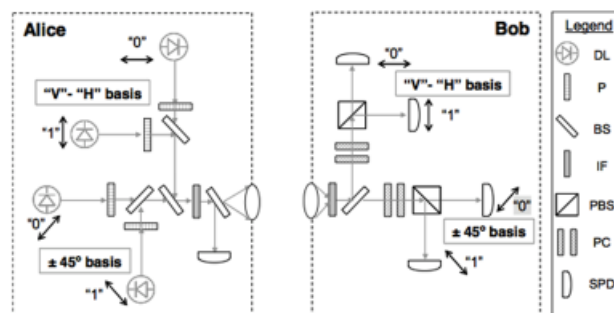
49

Current State of Affairs

■ Highest secure key exchange speed

- 1 Mbit/sec (20 km optical cable)
- 12.7 kbps (100 km optical cable)

■ Demonstrated free-space link: 10 km



50

Future Prospects

- **Ground-to-satellite, satellite-to-satellite links**
 - Possible due to lower atmospheric attenuation
 - Currently successful quantum entangled photons 1200 km apart

- **General improvement with evolving qubit-handling techniques, new detector technologies**

Tuesday
16 August
2016

51

QUESS (Quantum Experiments at Space Scale) is a proof-of-concept satellite mission designed to facilitate quantum optics experiments over long distances to allow the development of quantum encryption and quantum teleportation technology. The project uses the principle of entanglement to facilitate communication that is totally safe against eavesdropping, let alone decryption, by a third party. By producing pairs of entangled photons, QUESS will allow ground stations separated by many thousands of kilometres to establish secure quantum channels. QUESS itself has limited communication capabilities: it needs line-of-sight, and can only operate when not in sunlight. If QUESS is successful, further Micius satellites will follow, allowing a European–Asian quantum-encrypted network by 2020, and a global network by 2030.

The initial experiment will attempt to demonstrate quantum key distribution (QKD) between Xinjiang Astronomical Observatory near Ürümqi and Xinglong Observatory near Beijing – a great-circle distance of approximately 2,500 kilometers (1,600 mi). In addition, QUESS will test Bell's inequality at a distance of 1,200 km – further than any experiment to date – and teleport a photon state between Ali, Tibet Autonomous Region, and the satellite. This requires very accurate orbital maneuvering and satellite tracking so the base stations can keep line-of-sight with the craft.