

BIT COIN - 2

Reference

Bitcoin and Cryptocurrency Technologies

**By Arvind Narayanan, Joseph Bonneau, Edward Felten,
Andrew Miller, Steven Goldfeder**

References

- Main reference: *Bitcoin and Cryptocurrency Technologies*, By Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder
- Slides are mainly taken (or adapted) from slides of the authors of the text

BITCOIN protocol: Conclusions

Protection against invalid transactions is based on cryptography and it is enforced by consensus

- if a node does attempt to include a cryptographically invalid transaction, then the transaction won't end up in the long-term consensus chain because a majority of the nodes are honest and won't include an invalid transaction in the block chain.

Protection against double-spending is by consensus (no crypto): two transactions that represent a double-spending attempts are both valid from a cryptographic perspective; consensus determines which one will end up on the long-term consensus chain.

- you're never 100 percent sure that a transaction you're interested in is on consensus branch.
- the exponential probability guarantee is rather good. After about six transactions, there's virtually no chance that you're going to go wrong

Consensus is based on incentives for miners

Mechanics of Bitcoin

Transactions are not indicating transfer but ownership of coins

Recall: a block includes many transactions

Website: blockchain.info

Create 25 coins and credit to Alice	ASSERTED BY MINERS
Transfer 17 coins from Alice to Bob	SIGNED(Alice)
Transfer 8 coins from Bob to Carol	SIGNED(Bob)
Transfer 5 coins from Carol to Alice	SIGNED(Carol)
Transfer 15 coins from Alice to David	SIGNED(Alice)

Figure 3.1 an account-based ledger

Mechanics of Bitcoin

Example

Alice receives 25 and splits it in 17 (to Bob) and 8 (to herself); then transfers these 8 later in time

1	Inputs: \emptyset Outputs: 25.0 → Alice
2	Inputs: 1[0] Outputs: 17.0 → Bob, 8.0 → Alice SIGNED(Alice)
3	Inputs: 2[0] Outputs: 8.0 → Carol, 7.0 → Bob SIGNED(Bob)
4	Inputs: 2[1] Outputs: 6.0 → David, 2.0 → Alice SIGNED(Alice)

Figure 3.2 a transaction-based ledger, which is very close to Bitcoin

The negative aspect is that anyone who wants to determine if a transaction is valid will have to keep track of these account balances.

Mechanics of Bitcoin

Example: In the last transaction Alice transfers 15 Bitcoin to David

- To verify that she has the 15 Bitcoins we need to go backwards in time forever to see every transaction affecting Alice, and whether or not her net balance at the time that she tries to transfer 15 coins to David is greater than 15 coins
- Clearly we can make this a little bit more efficient with some data structures that track Alice's balance after each transaction (as it is done in bank accounts)
- Problem: this requires a lot of extra housekeeping besides the ledger itself

Conclusions Bitcoin doesn't use an account-based model but a ledger that just keeps track of all transactions similar to ScroogeCoin

Mechanics of Bitcoin

The first transaction is the one that creates the coin

Advantages

- Efficient verification of ownership
- Splitting Bitcoins
- Possibility of consolidating funds
 - Assume Bob has 2 BTC from one trans. and 5 from another trans. He can transfer 7 BTC in a single transaction to an address he owns
- Joint payments in one transaction
- **Escrow transactions:** The funds will be held in deposit till the case is settled.

Blockchain.info

Altezza	Età	Le transazioni	Totale Inviati	Rilasciato da	Dimensione (kB)
515274	21 minutes	2376	8,689.55 BTC	BTC.com	1,120.35
515273	45 minutes	640	767.09 BTC	AntPool	1,025.94
515272	47 minutes	241	749.11 BTC	58COIN	124.24
515271	48 minutes	1503	1,949.47 BTC	ViaBTC	1,068.72

Blockchain.info

Sommario		Hashes	
Numero delle Transazioni	611	hash	0000000000000000000028d76757be8eb798cc29545236b6d39a42824ef257a483
Totale Output	862.6764608 BTC	Blocco Precedente	00000000000000000000331647437fc2771f349336ad4f6997f97d11a25bb0d0a6
Volume stimato della Transazione	501.33305984 BTC	Blocco(chi) Successivo(i)	0000000000000000000028bfaa550759f52d2da362aa535f5bf353a79d92b71400
Commissioni di Transazione	0.06593639 BTC	Merkle Root	ff3f864534b264a2fc7742a3e3f3873a8dbfee101a60ada8246ef12e6167ae08
Altezza	515279 (Catena Principale)		
timestamp	2018-03-26 19:16:25		
Orario di Ricezione	2018-03-26 19:16:25		
Inoltrato da	BTC.com		
Difficoltà	3,462,542,391,191.56		
bits	391203401		
Dimensione	1029.234 kB		

Mechanics of Bitcoin

Change addresses. Why does Alice have to send money to herself?

- Bitcoins are immutable, hence the entirety of a transaction output must be consumed by another transaction. So she needs to create a new output where 8 bitcoins are sent back to herself

Efficient verification. When a new transaction is added to the ledger, how easy is it to check if it is valid?

- We need to look up the transaction output that Alice referenced, make sure that it has a value of 25 bitcoins, and that it hasn't already been spent. Looking up the transaction output is easy since we're using hash pointers.
- To ensure it hasn't been spent, we need to scan the block chain between the referenced transaction and the latest block. We don't need to go all the way back to the beginning of the block chain, and it doesn't require keeping any additional data structures (although, as we'll see, additional data structures will speed things up)

Mechanics of Bitcoin

Consolidating funds.

- For example, if Bob received money in two different transactions — 17 bitcoins in one, and 2 in another. If Bob wants to spend all 19 bitcoins in a transaction he creates a transaction with the two inputs and one output, with the output address being one that he owns. That lets him consolidate those two transactions.

Joint payments (by two or more people)

- Say Carol and Bob both want to pay David in a single transaction. They can create a transaction with two inputs and one output, but with the two inputs owned by two different people.
- The only difference from the previous example is that since the two outputs from prior transactions that are being claimed here are from different addresses, the transaction will need two separate signatures — one by Carol and one by Bob.

Mechanics of Bitcoin

Escrow Transactions

- Alice buys something but she does not want to pay until she is sure to receive the object: she doesn't send the money directly to Bob,
- She creates a MULTISIG transaction that requires two of three people to sign in order to redeem the coins: Alice, Bob, and some third party arbitrator, Judy, who will come into play.

A 2-of-3 MULTISIG transaction that sends some specifies that they can be spent if any two among Alice, Bob, and Judy sign.
The money is kept in deposit

- If there is no problem Alice and Bob sign an Bob can use the coins
- If there is dispute they call Judy as a judge to settle the issue

Mechanics of Bitcoin

Green addresses Alice wants to pay Bob, and Bob is offline so cannot check if a transaction that Alice is sending is actually there.

We introduce a third party (bank or an intermediate)

- Alice asks the bank to send the money to Bob
- The bank takes money from Alice and gives to Bob
- The bank should be trusted also for checking double spending

Note: this is not a Bitcoin-enforced guarantee but a real world; both Alice and Bob should trust the bank

Bitcoin transaction

- **Metadata** the size of the transaction, the number of inputs, and the number of outputs. There's the hash of the entire transaction which serves as a unique ID for the transaction. Finally there's a “lock_time” field (later)
- **Inputs** An array of inputs; each input specifies a previous transaction (so it contains a hash of that transaction). The input also contains the index of the previous transaction's outputs that's being claimed. And then there's a signature.
- **Outputs**. The outputs are again an array. Each output has just two fields. They each have a value, and the sum of all the output values has to be less than or equal to the sum of all the input values. You may be wondering why the output value would ever be less than the input value (later)

Bitcoin block

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Bitcoin header

Size bytes	Field	Description
4	version	A version number to track software/protocol upgrades
32	Previous block hash	A reference to the hash of the previous (parent) block in the chain
32	Merkle root	Merkle Root A hash of the root of the merkle tree of this block's transactions
4	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4	Difficulty	The proof-of-work algorithm difficulty target for this block
4	Nonce	A counter used for the proof-of-work algorithm

Bitcoin script language

Script: the scripting language built for Bitcoin

- small: 256 instructions, one instruct. is represented by one byte; Stack based (no loop) with “if..then”
- Script lets to specify arbitrary conditions that must be met in order to spend coins. But, as of today, this flexibility isn't used very heavily: 99.9 percent, are exactly the same script: it specifies one public key and requires a signature for that public key in order to spend the coins.
- USED: Multi SIG that involves third parties in signing

Bitcoin script language

```
{  
    "hash": "5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",  
    "ver": 1,  
    "vin_sz": 2,  
    "vout_sz": 1,  
    "lock_time": 0,  
    "size": 404,  
    "in": [  
        {  
            "prev_out": {  
                "hash": "3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",  
                "n": 0  
            },  
            "scriptSig": "30440..."  
        },  
        {  
            "prev_out": {  
                "hash": "7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",  
                "n": 0  
            },  
            "scriptSig": "3f3a4ce81..."  
        }  
    ],  
    "out": [  
        {  
            "value": "10.12287097",  
            "scriptPubKey": "OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"  
        }  
    ]  
}
```

metadata

input(s)

output(s)

2 inputs

1 output

Bitcoin blocks

Transactions are grouped in blocks for optimization

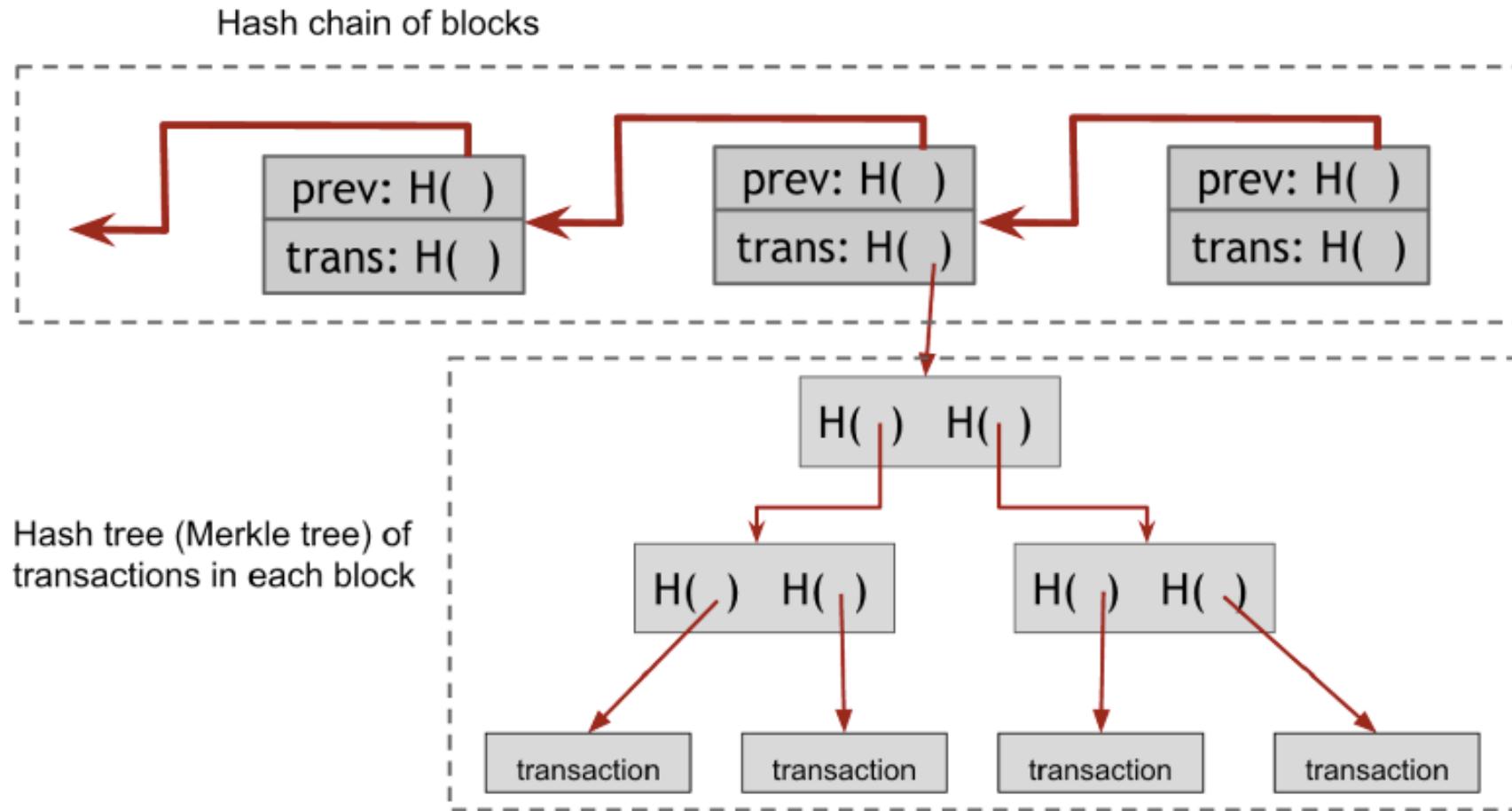
- If miners had to come to consensus on each transaction individually, the rate at which new transactions could be accepted by the system would be much lower.
- A hash chain of blocks is much shorter than a hash chain of transactions (many transactions can be put into a block). This allows to verify the block chain data structure faster.

Hash blocks

Bitcoin hashes many transactions in one block, why?

- Optimization
 - If we ask one transaction per block the process of accepting transactions is slow
 - Also to check validity of a block is faster than separately checking the validity of many transactions
- If transactions are grouped how do we check validity of each single transaction?
 - A transaction does NOT know which block it belongs; blockexplorer maintain index of transactions; you give the transaction and you get the block
 - Merkle Trees are used to check a transation is in a block

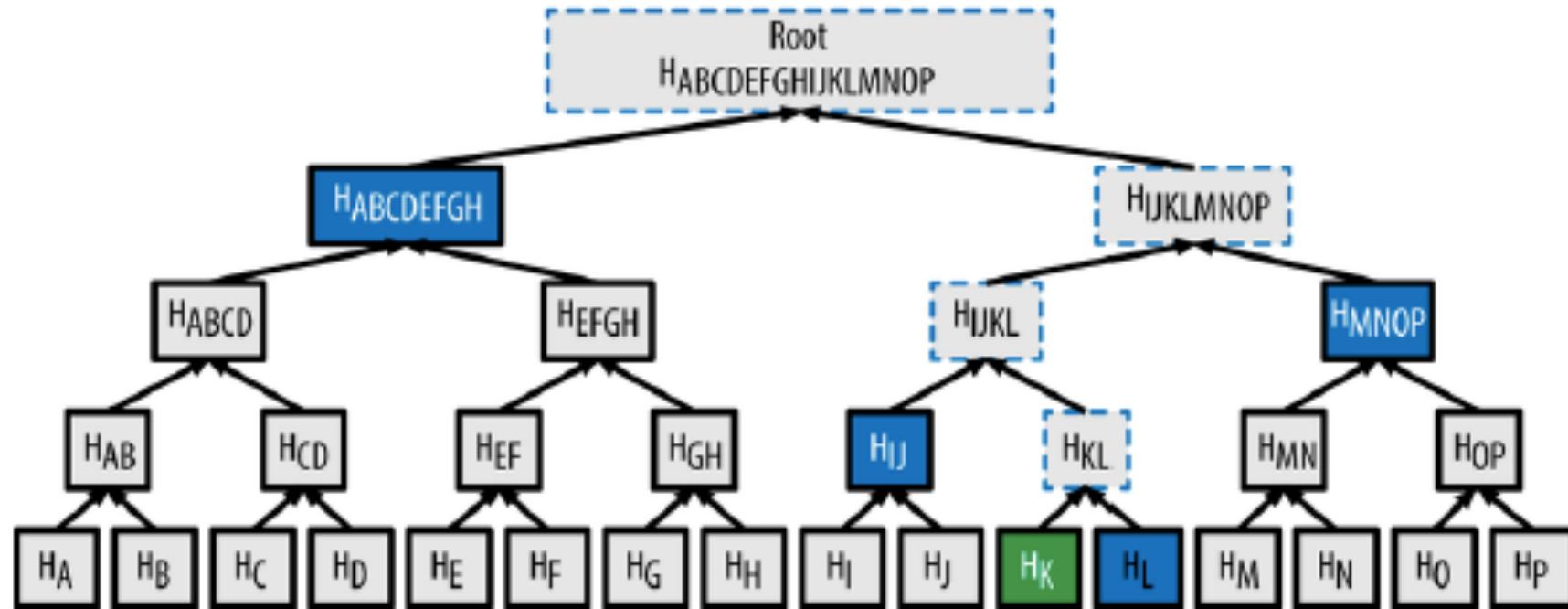
Hash blocks



Top: a hash chain of blocks linking the different blocks

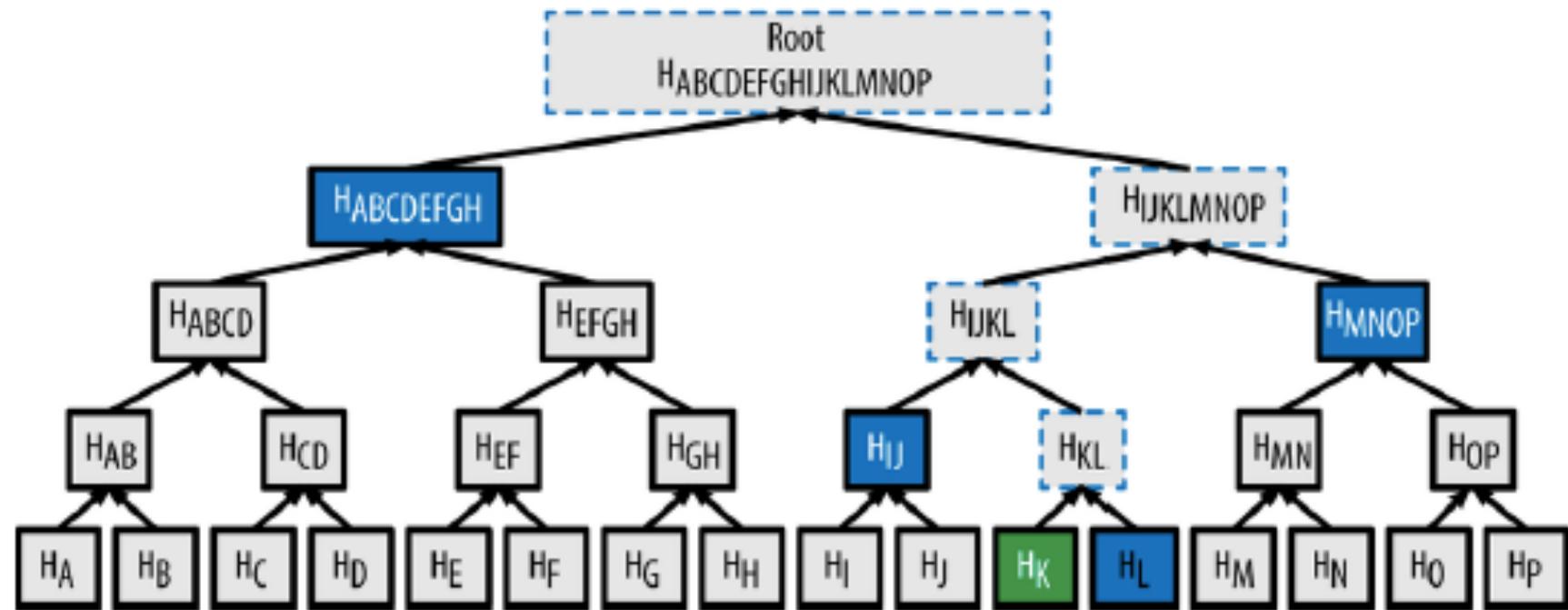
Bottom: internal to each block there is a Merkle Tree of transactions within the blocks

Hash blocks



A node can prove that a **transaction K** is included in the block by producing a merkle path that is only four 32-byte hashes long (128 bytes total). The path consists of the four hashes (in blue) HL, HIJ, HMNOP and HABCDEFGH.

Hash blocks



The path consists of the four hashes (in blue) HL , HIJ , $HMNOP$ and $HABCDEFGH$.

With those four hashes and computing four additional pair-wise hashes HKL , $HIJKL$, $HJKLMNOP$, and the merkle tree root, any node can prove that HK (noted in green in the diagram) is included in the merkle root

Bitcoin network

A peer-to-peer network

- all nodes are equal. There is no hierarchy, and there are no special nodes
- It runs over TCP and has a random topology, where each node peers with other random nodes.
- New nodes can join at any time.
 - you can download a Bitcoin client today, spin up your computer up as a node, and it will have equal rights and capabilities as every other node
 - You start sending a message to one node that you know: “Tell me the addresses of all the other nodes in the network that you know” You repeat the process with the new and then you can choose which ones to peer with
- Nodes can leave
 - if a node hasn’t been heard from in a while — about three hours — other nodes start to forget it. In this way, the network gracefully handles nodes going offline.

Bitcoin network

A simple flooding algorithm is used to publish a new transaction

- Alice wants to pay Bob some money: she sends this transaction to all the nodes it's peered with. Each of those nodes executes a series of checks to determine validity
- If the checks pass, the node in turn sends it to all of its peer nodes.
- Nodes that hear about a transaction put them in a pool of transactions that they've heard about but aren't on the block chain yet
- Remember that every transaction is identified uniquely by its hash, so it's easy to look up a transaction in the pool.

Bitcoin network: validating transaction

- When you join the netork you should know one node (seed node); then asking the seed you know more of the network
- When you receiv a transaction you check validity
 - Transaction validation: transaction must be valid in the current blcok chain: you run the script and check validity
 - Check outputs are not already being spent
 - Do not relay a trnsaction you have already processed
 - Script are restricted (only few possibilities are allowed)
- In case of double spending: one node can receive two transactions using the same coin; only the first one is processed (and transmitted)
- So nodes can have different views

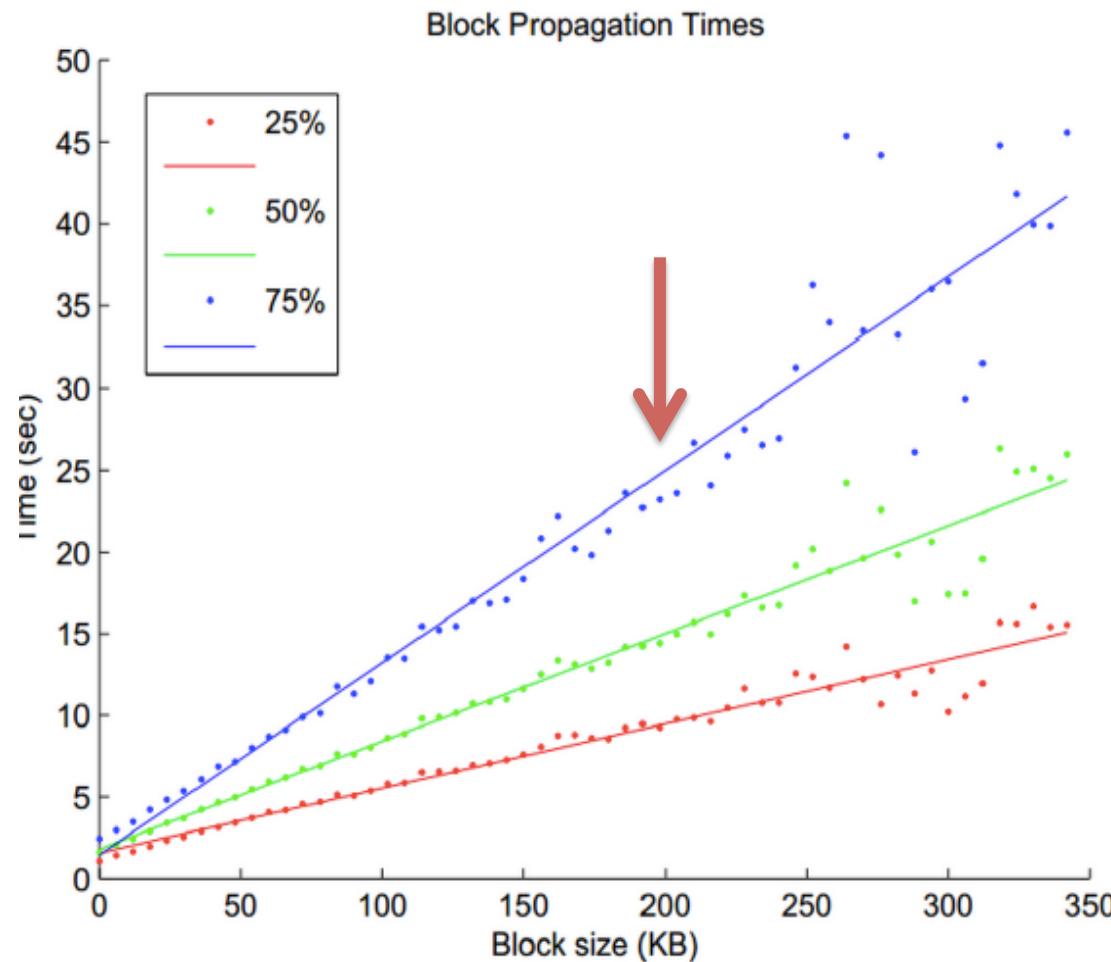
Bitcoin network: validating block

- Miner to validate a block must
- Validate all transactions contained in the block
- Make sure the hash of the block is in the admissible range
- Transmit only if this is in the longest branch of the block chain they see (remember there can be bifurcations)
- When you receive a transaction you check validity

Bitcoin network

- **Some claim that over a million IP addresses** in a given month will, at some point, act as Bitcoin nodes (at least temporarily)
- **Fully validating nodes (miners)** store the entire block chain,
 - which at March 2016 is over 100 gigabytes
 - Also they should keep unspent bitcoins (why?): about 50 millions trans. (size less than 1 GB)
 - There seem to be only about 5,000 to 10,000 nodes that are permanently connected and fully validate every transaction they hear
- **Lightweight nodes** (Simple Payment Verification (SPV)) clients.
 - vast majority of nodes on the Bitcoin network are lightweight nodes.
 - They don't store the entire block chain. They only store the pieces that they need to verify specific transactions that they care
 - They trust miners
- **Size of ledger could be a problem soon**

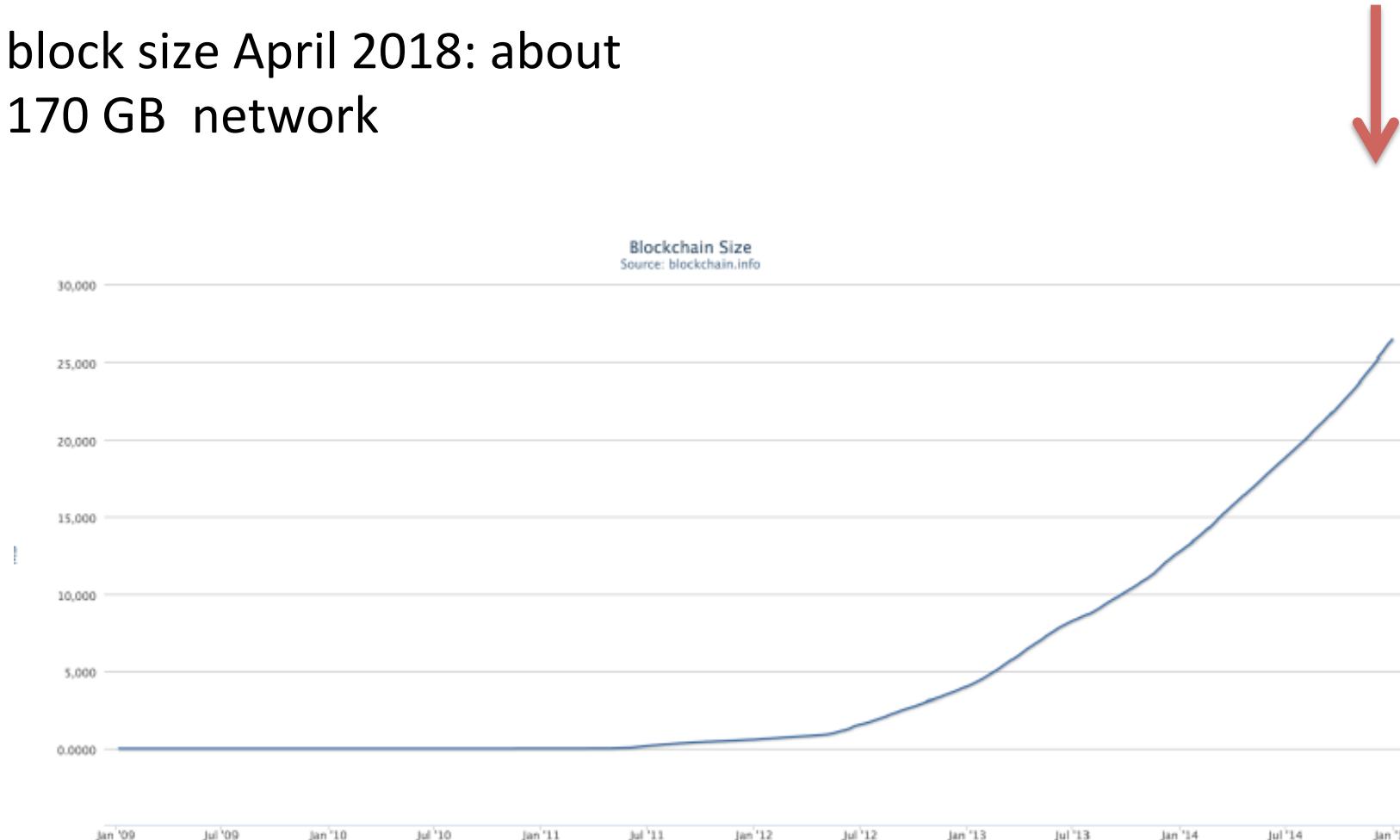
Bitcoin network: time propagation



If block size is 200KB then it takes less than 30 sec. To reach 75% of the network

Bitcoin network: size of block chain

block size April 2018: about
170 GB network



51-percent attack

What happen if there is an attacker who controls 51 percent or more of the mining power in the Bitcoin network?

- can this attacker steal coins from an existing address?
 - the 51 percent attacker creates an invalid block that contains an invalid transaction from an existing address of someone and transferring to his own address.
- NO, unless the attacker breaks the cryptography
 - the attacker can publish the block, can make the block the longest one; but the block contains an invalid transaction (not signed) so it will not be accepted by other users.

51-percent attack

Can the 51-percent attacker suppress any transactions?

- Assume that the attacker doesn't like Carol and wants to block all her transactions; so Carol cannot spend her Bitcoin.
 - he controls the consensus process of the block chain, so he can simply refuse to create any new blocks that contain transactions from one of Carol's addresses.
- But, he can't prevent these transactions from being broadcast to the peer-to-peer network
 - the network doesn't depend on the block chain, or on consensus, and we're assuming that the attacker doesn't fully control the network.
 - The attacker cannot stop the transactions from reaching the majority of nodes, so even if the attack succeeds, it will at least be apparent that the attack is happening.

51-percent attack

Can the attacker destroy confidence in Bitcoin?

- Assume that there are many double-spend attempts, and other attempted attacks, then people might decide that Bitcoin is no longer acting as a decentralized ledger that they can trust
 - People will lose confidence in the currency, and we might expect that the exchange rate of Bitcoin will go down.
- So it is not possible, but in fact likely, that a 51 percent attacker of any sort will destroy confidence in the currency.
 - Indeed, this is the main practical threat if a 51 percent attack were ever to materialize.
- However the **cost of achieving a 51 percent majority**, really make sense from a financial point of view.

Reward for miners: transaction fees

Whenever a transaction is put into the Bitcoin block chain, that transaction might include a **transaction fee** that is defined to be the

- **difference** between the total value of coins that go into a transaction minus the total value of coins that come out.
- The inputs always have to be at least as big as the outputs because a regular transaction can't create coins, but if the inputs are bigger than the outputs then the difference is a transaction fee, and that **fee goes to the miner who makes the block that includes this transaction**.
- The idea of a transaction fee is to compensate miners for those costs they incur to process your transaction.

Bitcoin Mining: task of a miner

1. **Listen for transactions on the network** and validate them by checking that signatures are correct and that the outputs being spent haven't been spent before.
2. **Maintain block chain and listen for new blocks.** You must maintain the block chain. You start by asking other nodes to give you all of the historical blocks that are already part of the block chain before you joined the network. You then listen for new blocks that are being broadcast to the network. You must validate each block that you receive — by validating each transaction in the block and checking that the block contains a valid nonce
3. **Assemble a candidate block.** Once you have an up-to-date copy of the block chain, you can begin building your own blocks. To do this, you group transactions that you heard about into a new block that extends the latest block you know about. You must make sure that each transaction included in your block is valid.
4. **Find a nonce that makes your block valid.** This step requires the most work and it's where all the real difficulty happens for miners.

Bitcoin Mining: reward for a miner

4. Once you have found a nonce and proposed anew valid block
 - Hope your block is accepted. Even if you find a block, there's no guarantee that your block will become part of the consensus chain. There's bit of luck here; you have to hope that other miners accept your block and start mining on top of it, instead of some competitor's block.
5. Profit. If all other miners do accept your block, then you profit!
 - Today the block reward is 12.5 bitcoins (June 2016 was 25 BTC, in 2020 the reward will be halved to 6.25) .
 - In addition collect transactions fees of the transactions in the block contained transaction fees
 - So far transaction fees have been a modest source of additional income, only about 1% of block rewards.

Reward for miners: transaction fees

The current transaction fees that most miners expect are

- no fee is charged if a transaction verifies three conditions:
 1. the transaction is less than 1000 bytes in size,
 2. all outputs are 0.01 BTC or larger
 3. priority is large enough (increases with time)
- Otherwise a fee is charged and that fee is about
 1. 0.0001 BTC per 1000 bytes, that's a fraction of a U.S. penny per 1000 bytes. (The approximate size of a transaction is 148 bytes for each input plus, 34 bytes for each output and ten bytes for other information. So a transaction with two inputs and two outputs would be about 400 bytes)

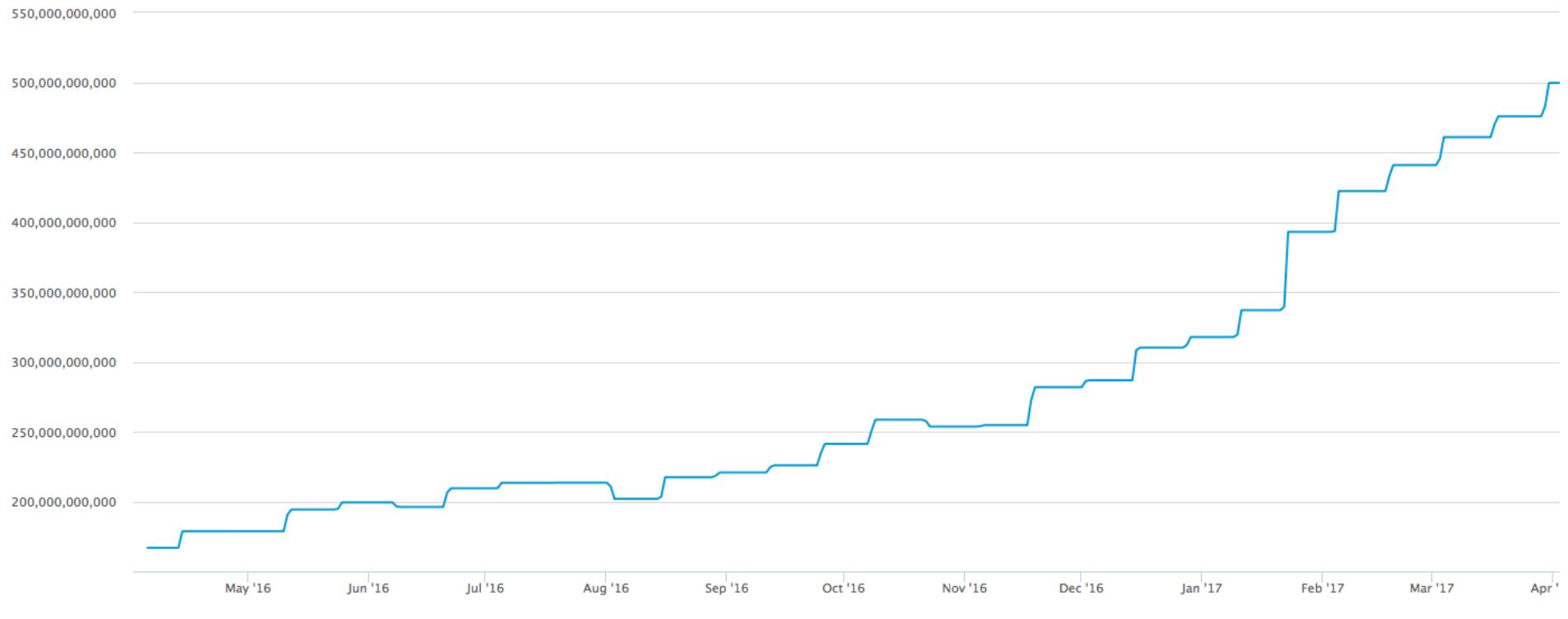
Transaction fees: conclusions

Today most miners would like to enforce the above fee structure,

1. Miners will either not service or will service last transact. that don't provide the necessary transaction fees.
2. But there are other miners who don't enforce these rules, and who will record and operate on a transaction even if it pays a smaller fee or no fee at all.
3. If you make a transaction that doesn't meet the fee requirements it will probably find its way into the block chain anyway,
4. but the way to get your transaction recorded more quickly and more reliably is to pay the standard fee, and that's why most wallet software and most payment services include the standard fee structure in the payments that go on,

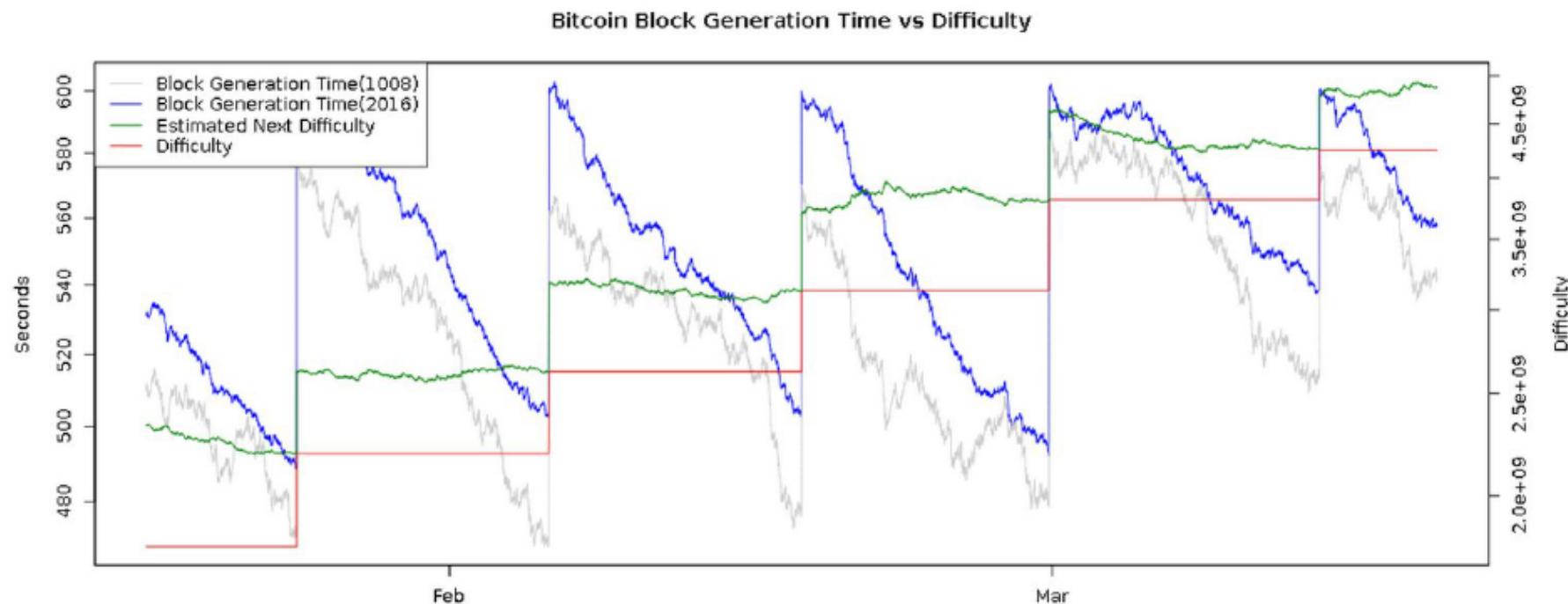
Bitcoin mining: difficulty

- Difficulty changes every 2016 blocks to maintain the time for finding a block to be about 10 minutes (more hash power more difficult, less hash power less difficult. Today about 500×10^9 hash)



Bitcoin mining: difficulty

- Difficulty changes every 2016 blocks to maintain the time for finding a block to be about 10 minutes. Why we observe up and down in the picture Bitcoin block generation time vs difficulty?



Bitcoin mining: hardware

- First generation mining: your personal computer
- difficulty increases so you need specialised HW (if you use your PC for mining the expected time to find a block about 1 million year with the current difficulty).
- Second generation: Home built rack with FPGAs



Bitcoin mining: hardware

- Today: there is no space for small miners
- Professional miners:
- BitFury (Georgia)



Bitcoin mining: hardware

Professional miners

Use ASICs, Application-Specific Integrated Circuits .

- These are chips that were designed, built, and optimized for the sole purpose of mining Bitcoins.
- There are a few big vendors that sell these to consumers with a good deal of variety: you can choose between slightly bigger and more expensive models, more compact models, as well as models with varying performance and energy consumption claims.

where to put a mining center?

- Cost of electricity
- Cold climate
- Network speed

Evolution of miners/ bitcoin miners



CPU



GPU



FPGA



ASIC



hand pan



sluice box



placer mining



pit mining

Bitcoin mining: mining pool

If you start the mining business and you are small the variance of having one block accepted is very high

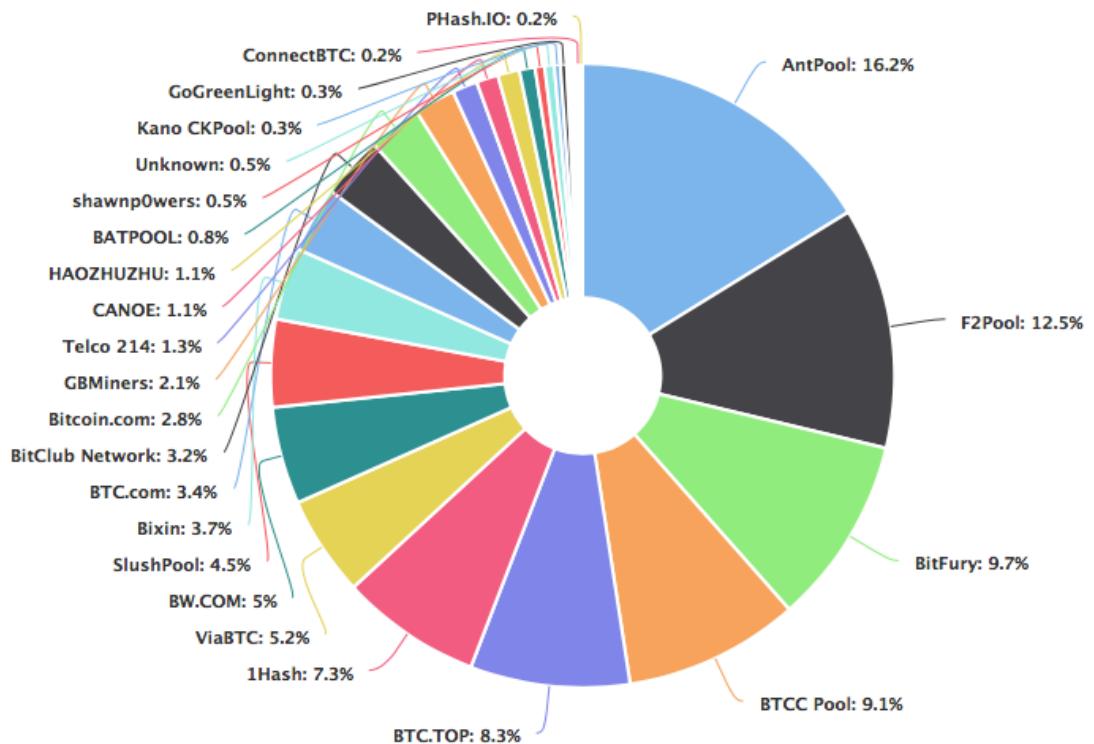
To decrease risk: mining pool that is mutual insurance for Bitcoin miners. A group of miners will form a

- pool and all attempt to mine a block with a designated coinbase recipient. That recipient is called the
- pool manager. So, no matter who actually finds the block, the pool manager will receive the rewards.
- The pool manager will take that revenue and distribute it to all the participants in the pool based on
- how much work each participant actually performed.

Bitcoin mining: mining pool

Mining pool: today

Note that a large organization might be part of several pools



Getting a cryptocurrency

Relations among three different ideas in Bitcoin:

1. the security of the block chain, 2. the health of the mining ecosystem, and 3. the value of the currency
1. We obviously want the block chain to be secure for Bitcoin to be used (we must trust Bitcoin)
2. For the block chain to be secure, an adversary must not be able to overwhelm the consensus process; we pay miners to be honest (health of mining ecosystem)
3. Miners are paid in Bitcoin: the incentive to be honest depends on Bitcoin's exchange rate at any given time.

Getting a cryptocurrency

What ensures a high and stable value of Bitcoin?

- If users believe that the network could be attacked then Bitcoin is not going to have value as a currency.
- When Bitcoin was first created, properties 1,2,3 did not hold. At the very begin: 1 miner (Nakamoto)
 - Bitcoin didn't have a lot of value as a currency. For some time the block chain was insecure because there was very few miners.
- There's no simple explanation for how Bitcoin went from now having properties 1,2,3 to having all three of them.
 - Media attention: the more people hear about Bitcoin, the more they're going to get interested in mining. And the more they get interested in mining, the more confidence people will have in the security of the block chain because there's now more mining activity going on, and so forth.

How to Store and Use Bitcoins

- Simplest way: putting them on a local device (phone, laptop)
- Storing bitcoins implies managing Bitcoin secret keys
 - public information on the block chain: identity of the coin (QR code)
 - secret information: secret key of the owner of the bitcoin
 - if you lose the device, if the device crashes, or if your file gets corrupted, your keys are lost, and so are your coins
 - if someone steals or breaks into your device, or it gets infected with malware, they can copy your keys and then they can then send all your coins to themselves

How to Store and Use Bitcoins

- Storing bitcoins on your computer is like carrying around money in your wallet
 - It's useful to have some spending money, but you don't want to carry around your life savings because you might lose it, or somebody might steal it.
 - James Howell: summer 2013, by mistake he threw out a computer hard drive containing more than \$9 million in bitcoin. He did not find (NO back-up); he lost everything

Hot and Cold Storage

- **Hot storage:** storing bitcoins on your computer is like carrying money around in your wallet - convenient but also risky.
- **Cold storage** is offline. It's locked away somewhere and It's not connected to the internet, and it's archival
 - it's safer and more secure, but of course, not as convenient.
- To have separate hot and cold storage, you need to have separate secret keys
 - otherwise the coins in cold storage would be vulnerable if the hot storage is compromised.
 - You'll want to move coins back and forth between the hot side and the cold side, so each side will need to know the other's addresses, or public keys.

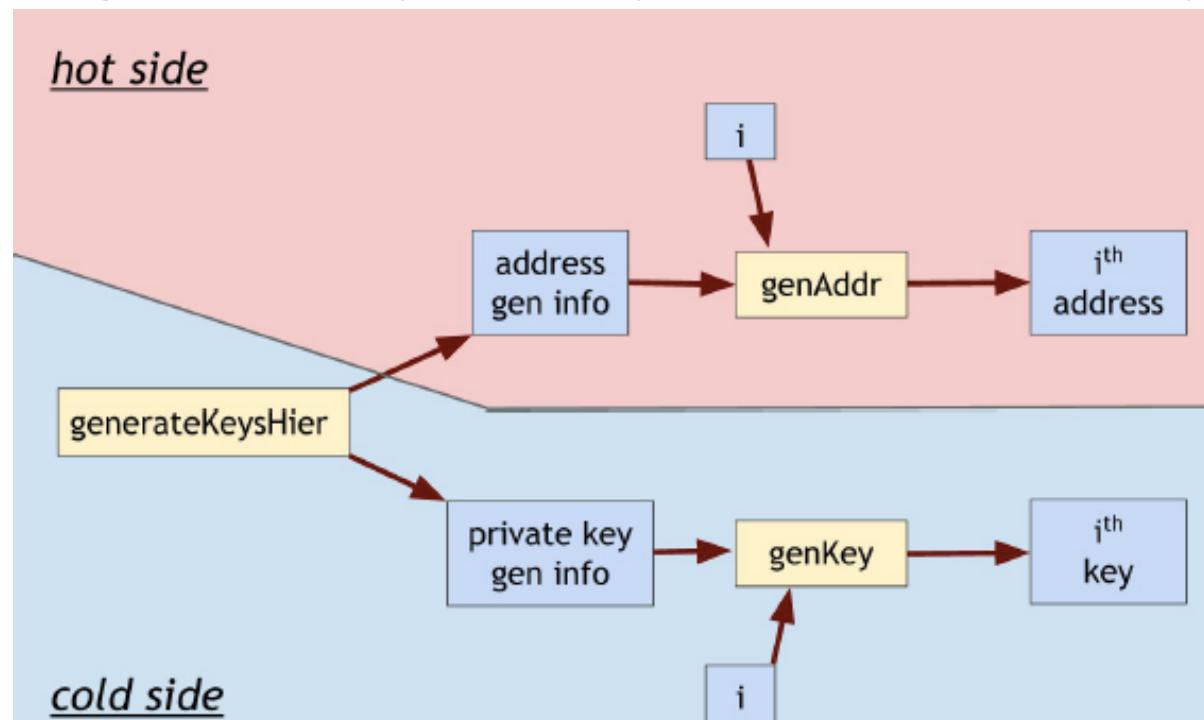
Hierarchical wallet

- Whenever we transfer a coin from the hot side to the cold side we'd like to use a fresh cold address for that purpose.
 - Since the cold side is not online we have to must find out about those addresses.
 - generate a big batch of addresses all at once and those over to the hot side, and the hot side uses them up one by one.
- A more effective solution is to use a hierarchical wallet. It allows the cold side to use an essentially unbounded number of addresses and the hot side to know about these addresses,
 - but with only a short, one-time communication between the two sides. But it requires a little bit of cryptographic trick

Hierarchical wallet

Given an initial address generation info, there is a function that generates a **sequence of public and private keys**

- For any integer i the function generates the i -th address
- and the i -secret key in the sequence
- Knowing the list of public keys does not reveal any secret key



Wallet: conclusions

- ownership of BTC is given by knowing keys; you must be sure that getting keys is difficult
- There are other possibilites
 - Tamper resistant card
 - Online wallet: you give your keys to a trust entity (that acts as a Bank and stores your Bitcoin); you give your money but you trust that they are expert in security
 - August 2016: a cyber attack to Bitfinex has stolen BTC about the equivalent of 65 M \$ from clients' wallets. As a consequence Bitcoin value dropped by 22% in a day.
 - Secret sharing mechanism: you divide the secret in pieces

Secret sharing

we want to divide our secret key into some number N of pieces.

We want to do it in such a way that

- if we're given any K of those pieces then we'll be able to reconstruct the original secret,
- but if we're given fewer than K pieces then we won't be able to learn anything about the original secret.

Secret sharing

Let's say we have $N=2$ and $K=2$. That means we're generating 2 shares based on the secret, and we need both shares to be able to reconstruct the secret.

- Let's call our secret S , which is just a big (say 128-bit) number. We could generate a 128-bit random number R and make the two shares be R and $S \oplus R$. (\oplus represents bitwise XOR).
- Essentially, we've “encrypted” S with a one-time pad, and we store the key (R) and the ciphertext ($S \oplus R$) in separate places.
- Neither the key nor the ciphertext by itself tells us anything about the secret. But given the two shares, we simply XOR them together to reconstruct the secret.

Secret sharing

This trick works as long as N and K are the same we'd just need to generate N-1 different random numbers for the first N-1 shares, and the final share would be the secret XOR'd with all other N-1 shares.

But if N is more than K, this doesn't work any more, and we need some algebra.

Secret sharing

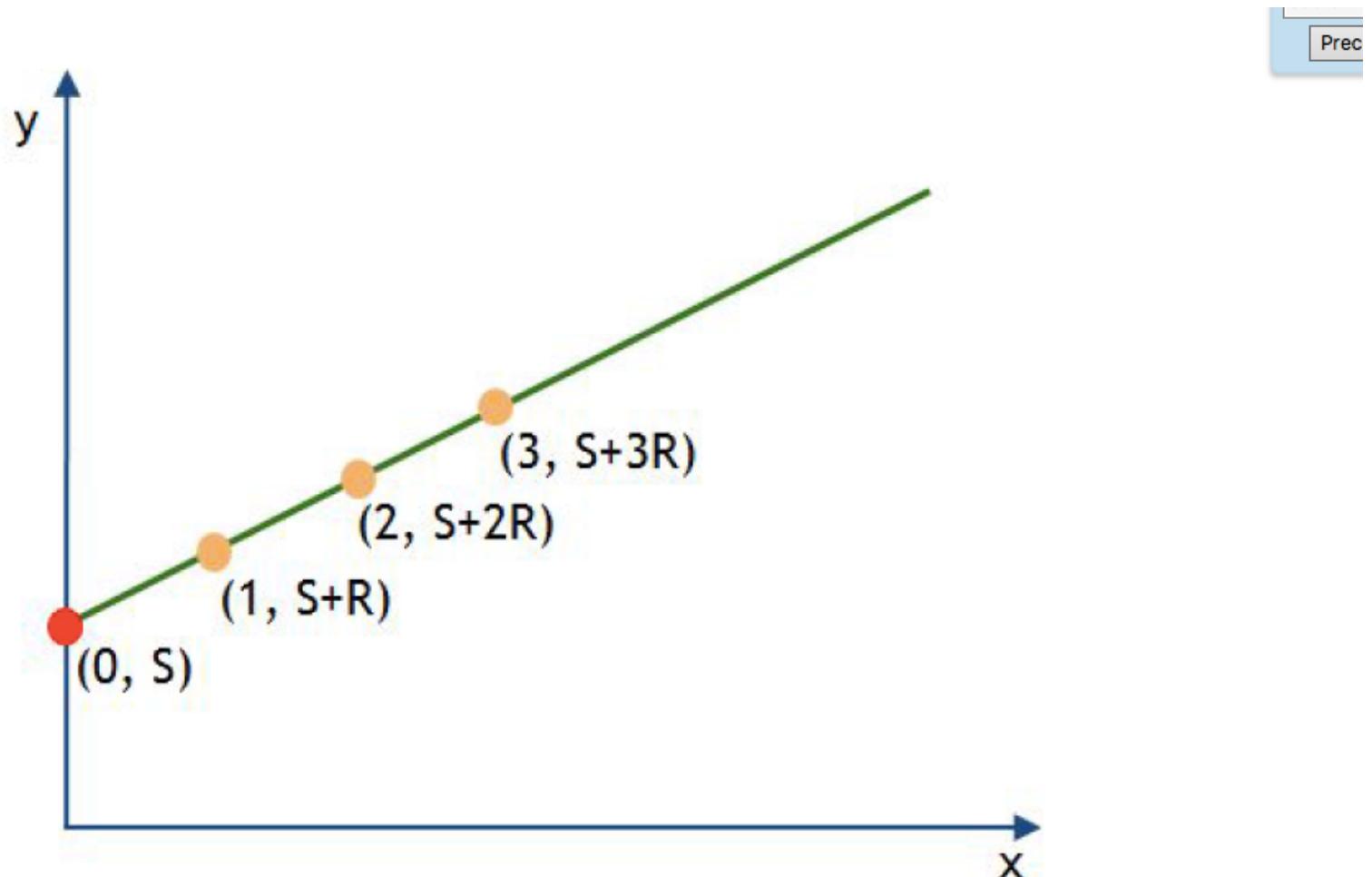


Figure 4.4: Geometric illustration of 2-out-of-N secret sharing. S represents the secret, encoded as a (large) integer. The green line has a slope chosen at random. The orange points (specifically, their y-coordinates $S+R$, $S+2R$, $S+3R$) are known to share the same secret S .

Bitcoin currency exchange

Currency exchange: trading bitcoins against flat currency like dollars and euros. Several possibilities

- marketUsers: I want to use BTC for privacy reasons
 - I need to buy BTC, do my transaction and then sell my BTC
- Investors: I want to make money with BTC
 - I buy BTC and I hope their value will increase and then I sell
- BTC intermediaries: sell and buy BTC
 - Exchange fee

Buying and selling BTC

- Alice wants to pay Bob in BTC for not being traced
 - She goes to a bank pays in Euro and buys BTC
 - She pays in BTC and get the service from Bob
 - Bob goes to another bank and gets Euros
- Cost: exchanges Euro → BTC → Euro
- Advantages: anonymity
 - 2014: Russian hakers block the information systems of few small cities in Italy; they asked to be paid in BTC to unlock the data; they were paid

Buying and selling BTC

- Intermediairies act as a Bank
 - Regulations concerning their reliability
 - Minimum reserve
 - Problem: show that you have minimum reserve without revealing exactly what you have
- Cost: exchanges Euro → BTC → Euro
- There is lot of activity
 - Many companies trade and maintain Bitcoin wallets
 - Meets-up people: people meet and exchange BTC

Buying and selling BTC

- Bitfinex: the world's biggest Bitcoin exchange by volume: 5.77 million bitcoins traded through Bitfinex from mid-April to mid-October 2017—nearly twice the volume of Bitfinex's nearest competitors,
- High volume is important for traders as it ensures a low spread, which is the difference between the best bid and ask prices.
- April 2016 theft of nearly 120,000 BTC from Bitfinex stands as the second-largest Bitcoin heist in history

Buying and selling BTC

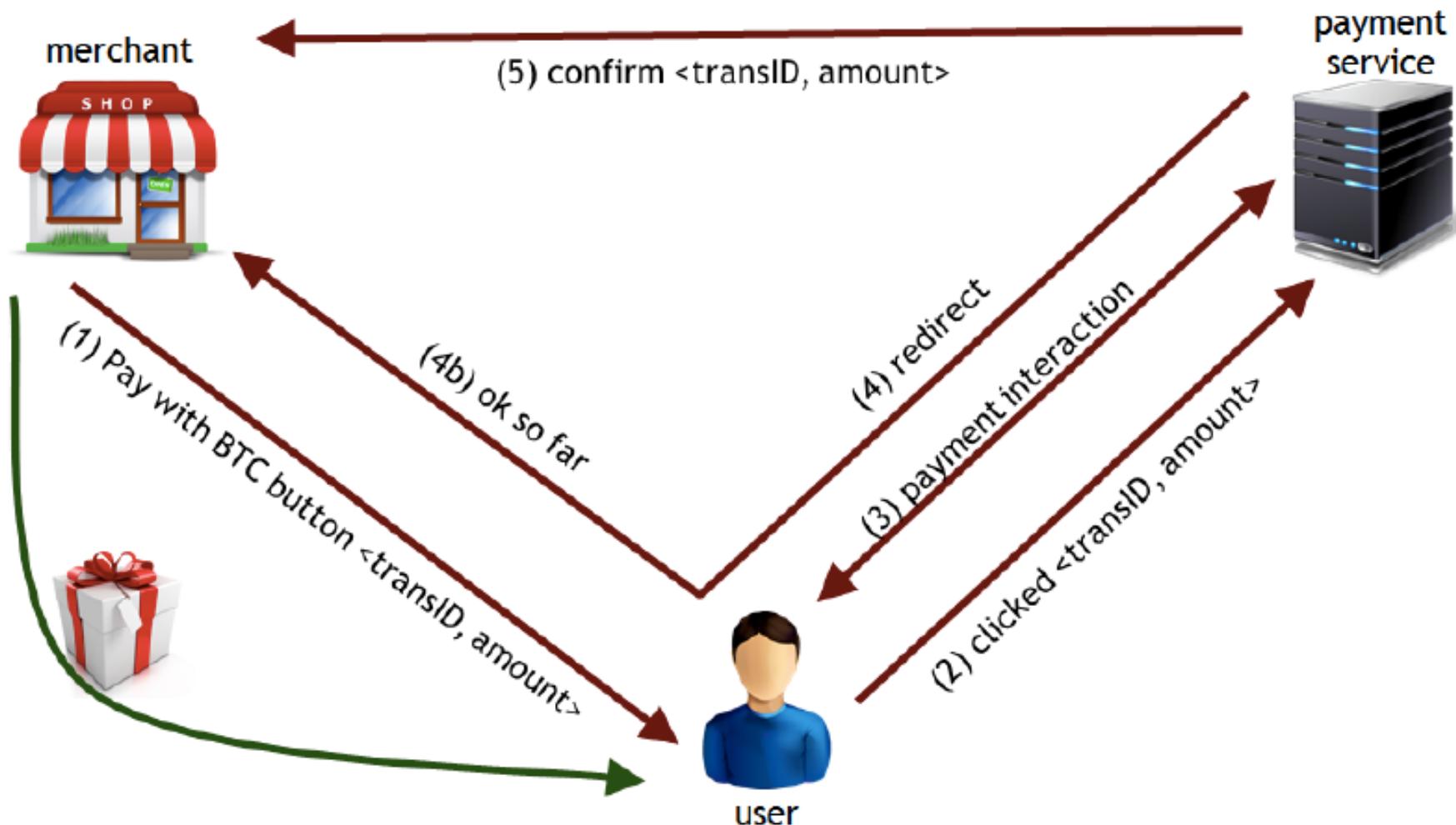


Figure 4.7: Payment process involving a user, merchant, and payment service.

Bitcoin numbers: rate, value etc.

The **price of Bitcoin**, like the price of anything in a liquid market, will be set by **supply and demand**. By that we mean

- the supply of bitcoins that might potentially be sold and the
- demand for bitcoins by people who have dollars/euros. The price through this market mechanism will be set to the level that matches supply and demand.

Bitcoin numbers: rate, value etc.

- Similar to the exchange rate between euro and dollars
 - The BTC exchange matches buyers and sellers of BTC: many people want BTC price goes up
 - Supply of BTC is limited: now ~ 15 Million, max 21 Million
 - If you a deposit BTC (hoping the price will raise) less BTC available for trading (BTC as an investment)

Bitcoin numbers: rate, value etc.

Demand for bitcoins as a way of mediating currency transactions

- Alice sells something to Bob; Bob pays in BTC; Alice waits few days before converting in euros (just to be sure everything is ok)
- Alice thinks the price of BTC will raise; she buys BTC to as an investment
- BTC are out of the market for some time
- Simple economic models show that the price is depends on **supply of BTC** (slowly changing) and the **demand of BTC** as measured in dollars/euros (more requests of BTC the amount is fixed, price goes up)

Bitcoin numbers: value 2013-today

from bitcoincharts.com

Yesterday (oct 2019) euro 7.300

Maximum about 17000 euro

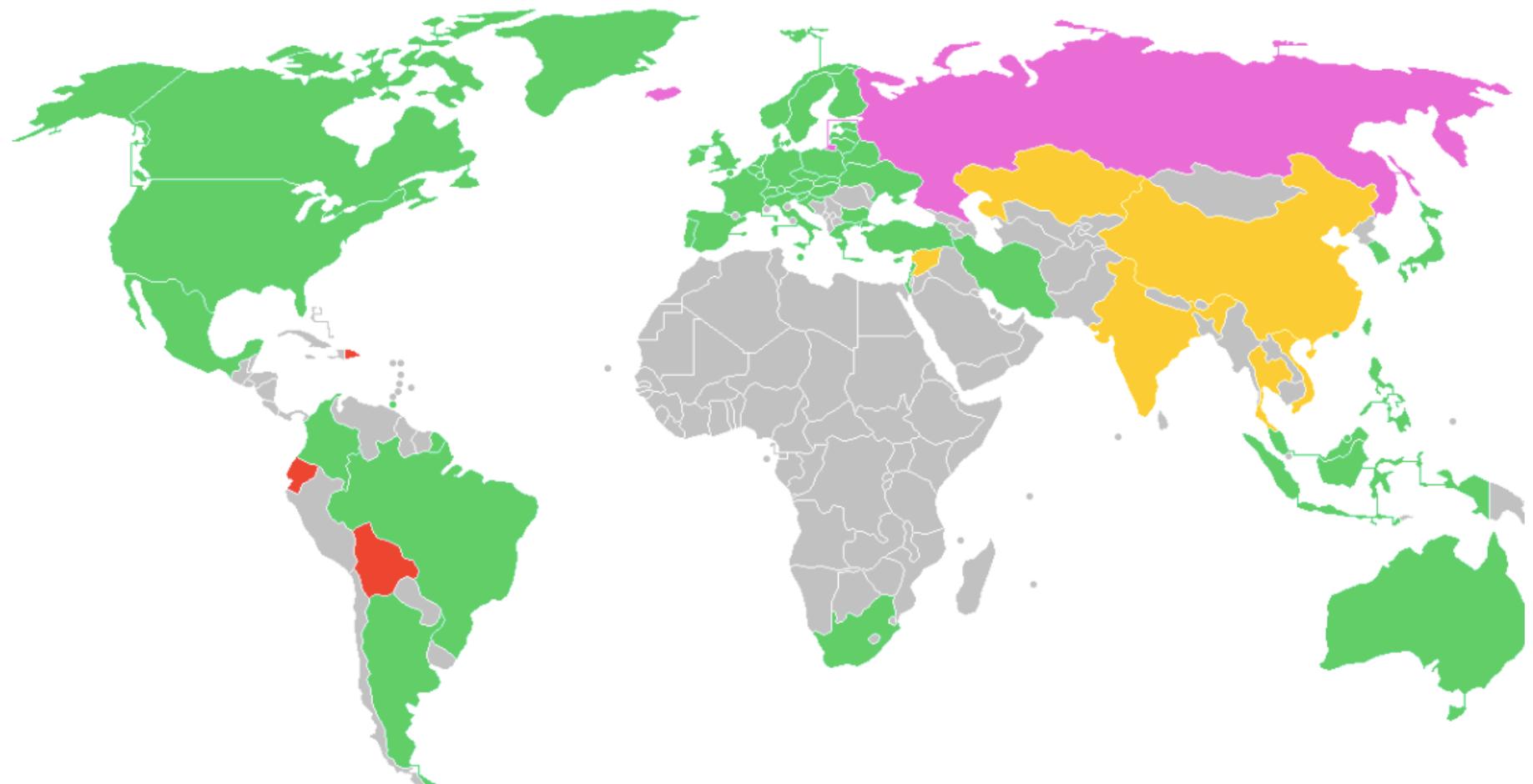


The number of transactions is ~ 300000 per day (max about 7 per second)

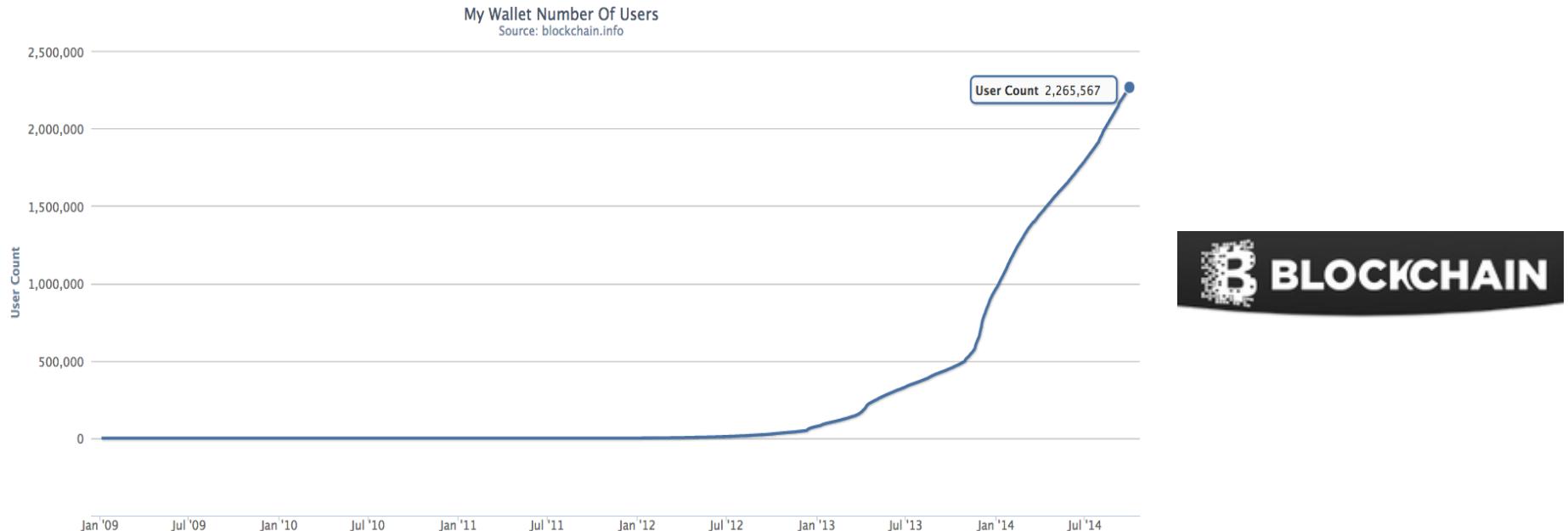
Regulation green legal

yellow: legal but some restrictions

red: forbidden purple: problematic



Growth: Users



Bitcoin users

Jan 2012	370	jan 2013	78 K	Jan 2014	930 K
Jan 2015	2,7 M	Jan 2016	5,5 M	Jan 2017	11M
Jan 2018	21 M				

Estimated unique users between 2.9 to 5.8 millions users

Value of Bitcoin in the future?

Amazon grosses \$38 billion per year. Assuming a 3% transaction fee, Amazon pays \$1 billion a year and nets \$1 billion per year. Amazon could double their profits by doing all transactions in Bitcoin. If the market cap for bitcoin was \$38 billion, each bitcoin would be worth \$5,400.

Gambling The online poker market is \$4.8 billion a year industry. Online gambling will follow poker and is a \$30 billion a year industry. If the market cap for bitcoin was \$30 billion, each bitcoin would be worth \$4,300.

Valuing Bitcoin:

Gas stations

Credit card companies charge gas stations a 2% transaction fee. By eliminating credit card transaction fees, gas station owners could double their profits. The US consumes 65 billion gallons of gasoline per year. At \$3.60 per gallon, this could be a \$234 billion dollars going through the bitcoin economy's per year. If the market cap for bitcoin was \$234 billion, each bitcoin would be worth \$34,400 dollars.

Valuing Bitcoin:

International Remittance

International remittance is the transfer of money by a foreign worker to their home country. In 2007, remittance worldwide transferred \$300 billion dollars.

Western Union fees for remittance can run from about 4 percent to 20 percent or more. If the market cap for Bitcoin was \$300 billion, each bitcoin would be worth \$42,000.

Your proposals/observations?

Potential value of Bitcoin:

- Amazon = \$5,400
- Gambling = \$4,300
- Gas stations = \$34,400
- International Remittance = \$42,000
- Bitcoin adoption world wide = ??????

Growth: Merchants

bitpay

Over 30,000 businesses and charities accept bitcoin with BitPay.

Visit some of our featured merchants.

BitPay

is a global bitcoin service provider

BitPay provides services payment for merchants, founded in 2011 in 2014 processed 1 million USD.

36,000 Businesses Trust Coinbase To Integrate Bitcoin Payments, Including...



intuit



REEDS
Jewelers



CHICAGO
SUN-TIMES



Payment network

Rank	Network	Avg. Volume(millions \$)	Rank	Network	Avg. Tx _s (1000s) ▲
1	Visa, Inc.	16,518	1	Visa, Inc.	212,603
2	MasterCard Inc.	9,863	2	MasterCard Inc.	93,578
3	China UnionPay	7,562	3	American Express Co.	14,521
4	American Express Co.	2,434	4	Discover (PULSE Network)	11,838
5	Discover (PULSE Network)	438	5	Paypal	7,700
6	Paypal	397	6	Discover (Discover Network)	5,052
7	Discover (Discover Network)	299	7	Western Union Company	633
8	Bitcoin	238	8	Ria/AFEX	84
9	Western Union Company	216	9	Bitcoin	70
10	Xoom Corp	15	10	Xoom Corp	25
11	Ria/AFEX	-	11	China UnionPay	-

Ecosystem

1. Protocol & client



2. Blockchain & miners



3. Exchanges



4. Payment processors



5. Applications



6. DACs & other promises



Other Cryptocurrencies

#	Name	Market Cap	Price	
1	 Bitcoin	\$ 4,543,836,817	\$ 340.10	
2	 Ripple	\$ 137,492,835	\$ 0.004743	2
3	 Litecoin	\$ 125,676,818	\$ 3.84	
4	 BitSharesX	\$ 55,927,142	\$ 0.027965	1
5	 Dogecoin	\$ 27,463,495	\$ 0.000292	93
6	 Nxt	\$ 24,876,528	\$ 0.024877	
7	 Peercoin	\$ 22,413,594	\$ 1.03	
8	 Darkcoin	\$ 10,677,591	\$ 2.26	
9	 Namecoin	\$ 9,807,149	\$ 0.980264	
10	 Counterparty	\$ 7,830,046	\$ 2.96	
11	 BitShares PTS	\$ 6,238,153	\$ 3.55	
12	 BitcoinDark	\$ 4,024,868	\$ 3.39	
13	 Monero	\$ 3,957,709	\$ 1.01	
14	 BlackCoin	\$ 3,456,021	\$ 0.046273	
15	 Stellar	\$ 3,193,117	\$ 0.002387	
16	 XCurrency	\$ 2,456,891	\$ 0.442906	
17	 NuBits	\$ 2,228,926	\$ 0.994854	
18	 Bytecoin	\$ 2,040,488	\$ 0.000012	1
19	 Feathercoin	\$ 1,712,977	\$ 0.030276	
20	 Mastercoin	\$ 1,642,355	\$ 2.92	

Startups I

527 COMPANIES

1,939 INVESTORS

5,458 FOLLOWERS

125 JOBS

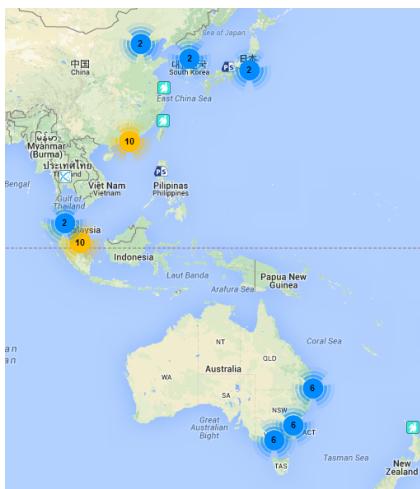
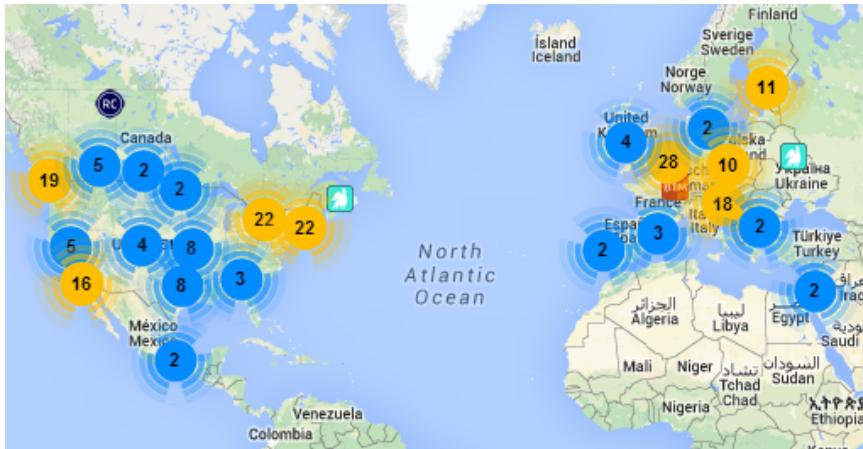
 Coinbase Making Bitcoin accessible to con... San Francisco · Mobile Payments	 BTCJam Peer to Peer Bitcoin Lending. Silicon Valley · Finance Technology	 Korbit Korea's leading bitcoin exchange... Seoul · Financial Exchanges	 BitPagos The Future of Payments Palo Alto · Emerging Markets
 Onename The Decentralized Whitepages fo... New York City · Application Platforms	 ChangeCoin Micropayment Infrastructure for th... San Francisco · Bitcoin	 BitAccess Bitcoin ATM Mountain View · Billing	 SNAPCARD The easiest way to use your digit... San Francisco · Bitcoin
 bitPay Accept bitcoin. Atlanta · Mobile Payments	 Gem Simple and secure Bitcoin platfor... Venice · Developer APIs	 Bold Instant access to digital currency San Francisco · Banking	 PayStand Next-gen online store & payment ... San Francisco · SaaS
 Buttercoin White-label Bitcoin Exchange Ser... Palo Alto · Bitcoin	 Coinsetter Wall Street-based high performa... New York City · Trading	 Coinalytics Real-time Analytics for Bitcoin Mountain View · Big Data Analytics	 BitGo Securing the World's Bitcoin Palo Alto · Bitcoin
 SecondMarket Simplifying transactions for privat... New York City · Startups	 Localbitcoins Run bitcoin exchange anywhere Helsinki · Financial Exchanges	 Bonafide Use Bitcoin without getting coined Mountain View · Personal Finance	 Neuroware.io Bitcoin Framework & API #500str... London · Open Source
 Chain.com Bitcoin developer platform San Francisco · Developer APIs	 SFOX Bitcoin Trading Platform San Francisco · Bitcoin	 Tealet Online Farmer's Market for Tea o... Las Vegas · Tea	 Secure Asset Exchange Smart Contracts for Realtime Re... New York City · Blockchains
 Vaurum We enable financial institutions t... Palo Alto · Financial Exchanges	 Kraken FOREX for Bitcoin, Ripple and ot... San Francisco · Banking	 CrowdCurity Crowdsourced Web Security Silicon Valley · Crowdsourcing	 Gliph The world's easiest way to send ... San Francisco · Social Media Platforms
 Filecoin Filecoin is a data storage networ... United States · Bitcoin Mining	 GoCoin Digital currency payments platfor... Singapore · Online Shopping	 CoinJar Advancing consumer finance wit... Melbourne · Bitcoin	 37coins Bitcoin Wallet for Everyone Sunnyvale · Remittance
 HashFast make bitcoins faster San Francisco · Hardware + Software	 LedgerX Financial technology products for... New York City · Finance Technology	 GogoCoin The easiest way to buy bitcoin Mountain View · Mobile Payments	 expresscoin Buy Bitcoin. Fast, Easy, and Safe. Santa Monica · Bitcoin
 ZipZap Global payment network enabling... San Francisco · Remittance	 MaiCoin Taiwan · Financial Exchanges	 Robocoin The World's Largest Bitcoin ATM ... London · Finance Technology	 Elliptic Digital Currency Services London · Finance Technology

angel.co/bitcoin

Startups II

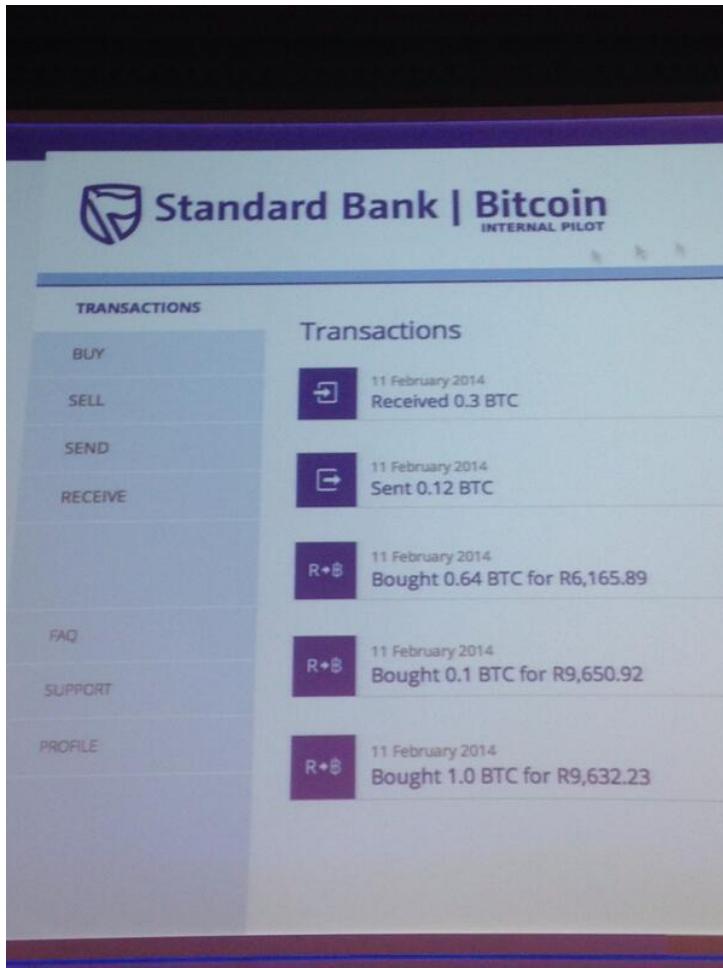
 Coinmail Snapshot for Bitcoin Rochester · Messaging	 Safello Bitcoin evangelism Stockholm · None	 Honeybadgr Building Teams at Bitcoin Startups San Francisco · Startups	 AlphaPoint Enterprise Bitcoin exchange soft... New York City · Financial Exchanges
 Bex Bitcoin Exchange in a Box Vancouver · Financial Exchanges	 Stanford Bitcoin Group Research into Bitcoin theory and ... Stanford · Bitcoin	 CoinHako Leading Bitcoin wallet service in ... Singapore · Finance Technology	 BlockCypher Amazon Web Services for Bitcoin San Mateo · Cloud Infrastructure
 Monetsu A next generation crypto-currency ... San Francisco · Startups	 ZenBox Turnkey Bitcoin ATM Distribution ... Santa Monica · Distribution	 Blockchain The most used Bitcoin platform i... Mobile Payments	 Leetcoin Competitive gaming for bitcoins. Las Vegas · Video Game Tournaments
 Koinify The Cryptofunding Platform Palo Alto · Crowdfunding	 Mastercoin Foundation The Protocol Layer On Top of The... Austin · Open Source	 coins.ph Bringing banking services to the ... Manila · Mobile Payments	 API Network Singly - Open Sourced Austin · Developer APIs
 BitWall Content monetization platform San Francisco · Bitcoin	 LibraTax Accounting and tax software for B... San Francisco · Finance Technology	 HolyTransaction Universal Multicurrency Wallet Sunnyvale · Personal Finance	 HashTrust Crypto Contracts Made Easy Silicon Valley · Bitcoin
 Wow Such Business Microtransactions that actually w... Arcata · Dogecoin	 Hedgy Smart derivative contracts on the ... Silicon Valley · Finance Technology	 SolidX Partners Inc. Institutional Access to Bitcoin an... New York City · Digital Currency	 Waxis Powerful digital currencies tradin... Delaware · Bitcoin Exchange
 Blade Bitcoin Payments New York City · Bitcoin	 Bitso Mexico's First Bitcoin Exchange Puebla · Bitcoin	 CoinMKT Trade Bitcoin & Other Cryptocurre... Santa Monica · Trading	 Hellobit Cash remittance powered by the ... San Francisco · Mobile Payments
 VerifyBTC Identity verification platform for Bit... San Francisco · Identity Management	 Monegraph A Bitcoin for Digital Art New York City · Bitcoin	 Coinmotion The Coinbase for Europe, before ... Helsinki · Bitcoin	 Purse Making Bitcoin Useful San Francisco · Gift Card
 QuickCoin Social Bitcoin Wallet San Francisco · Finance Technology	 HashPlex HashPlex is the world's first hosti... Seattle · Bitcoin	 BitBox Changing the meaning of money ... Ann Arbor · Finance Technology	 InterWallet Next Generation Bitcoin ATM Platf... Santa Monica · Transaction Processing
 Volabit (Coincove) Bitcoin-based financial services f... Puerto Vallarta · Loans	 Bitbond Global bitcoin peer-to-peer lending Berlin · Loans	 Palarin Coinbase of the Philippines San Francisco · Personal Finance	 BubbleCoin Bitcoin news, culture and events ... Silicon Valley · Bitcoin

ATMs



 Coin ATM Radar

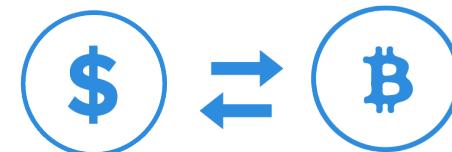
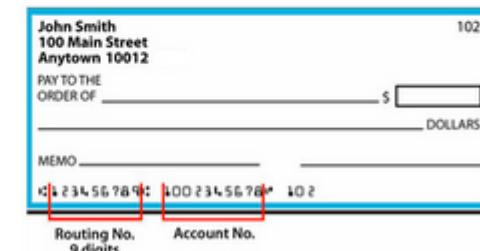
Bank integration



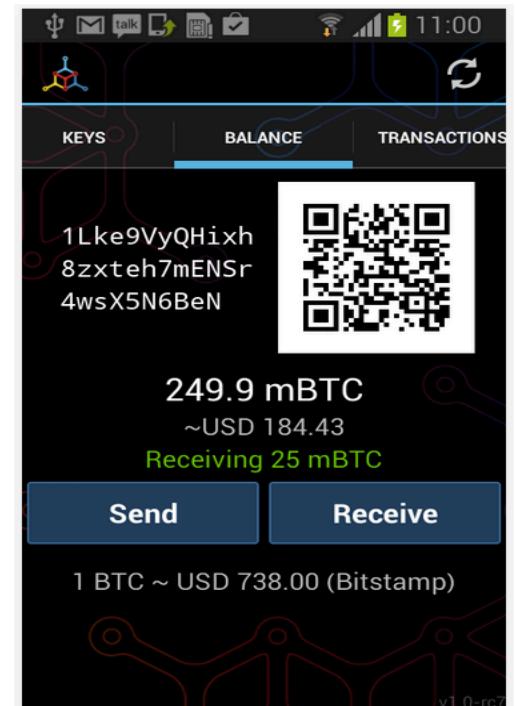
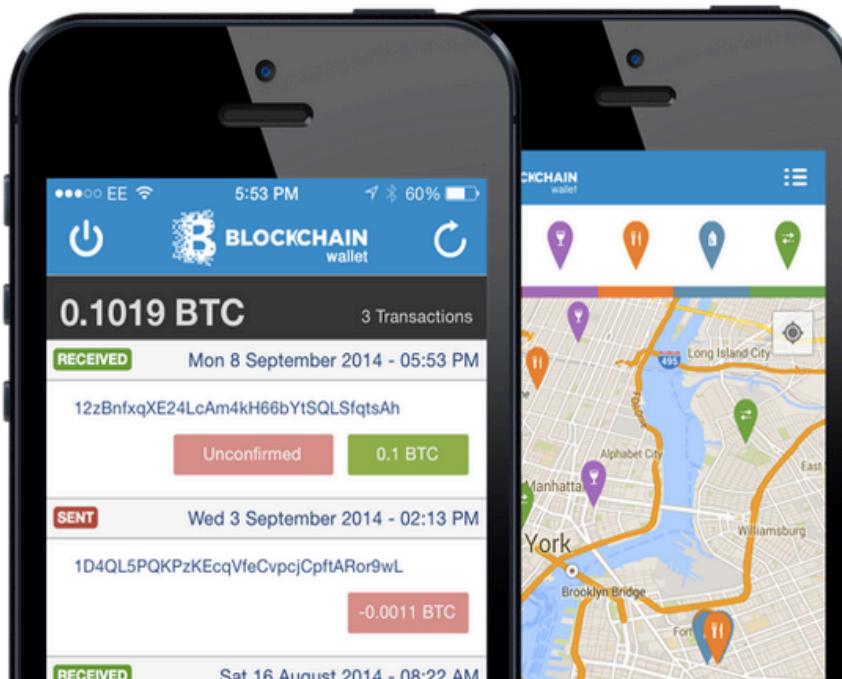
Link A Bank Account

Routing number bottom left of check, 9 digits

Account number bottom center of check



Mobile

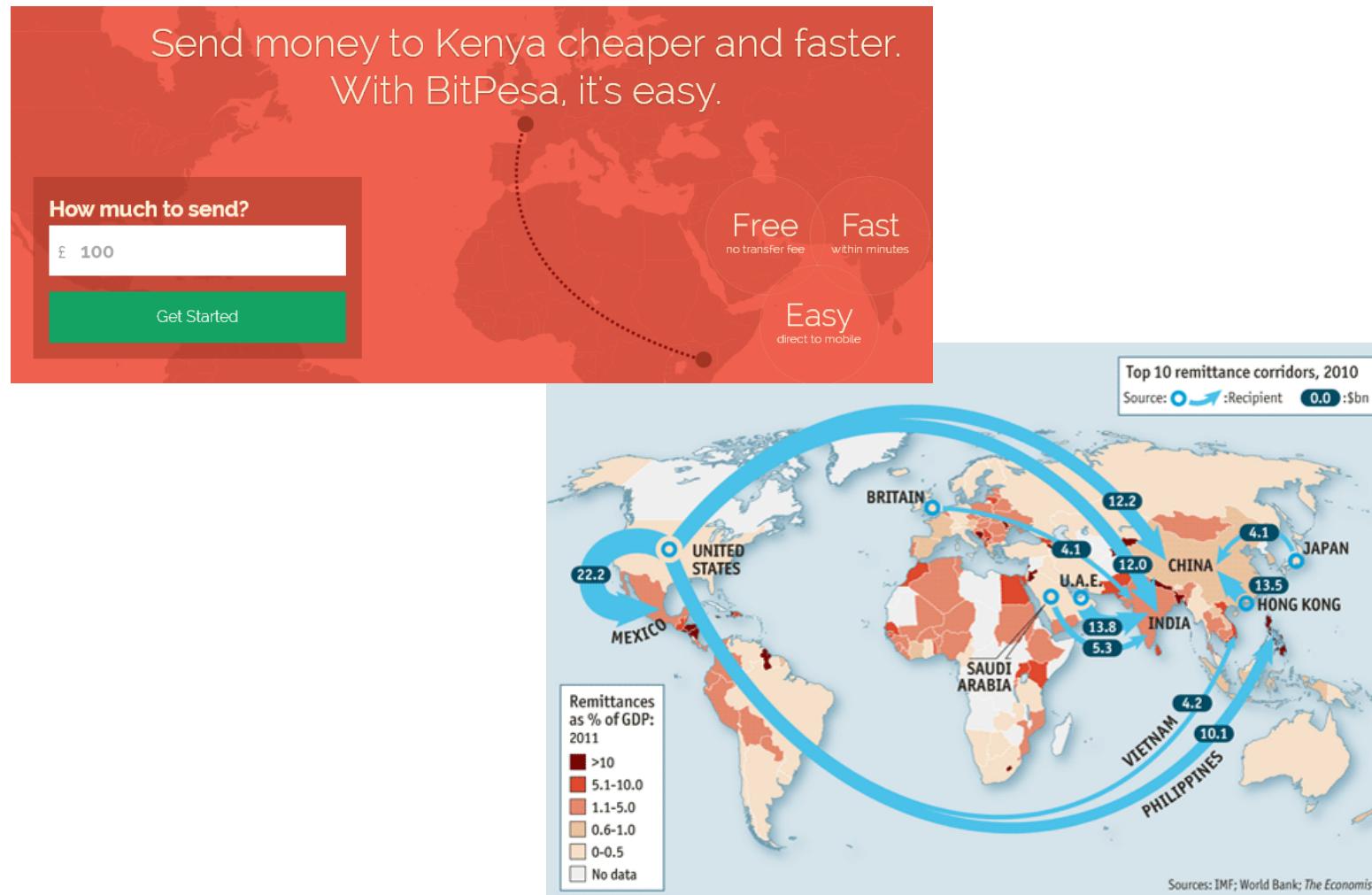


Main Street



<http://coinmap.org/>

Remittances



Philanthropy



Home About Bitcoin Accepting Charities Contact Press FAQ

Bitcoin Accepting Charities

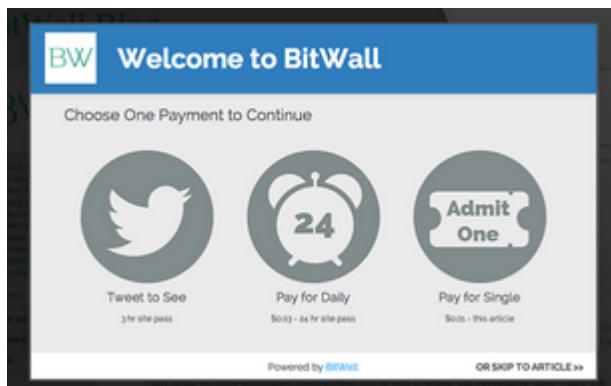
	Group B Strep International (Funded in two parts – Part 1 / Part 2)
	Kenya 2012 (Funded in three parts – Part 1 / Part 2 / Part 3)
	BUND-Berlin.de (Funded in two parts – Part 1 / Part 2)
	My Refuge House (Funded in three parts – Part 1 / Part 2 / Part 3)
	Generations of Hope
	Fr33 Aid
	AntiWar.com
	Songs of Love Foundation
	The Fessler Foundation



Roger Ver Gives FEE Highest-Valued Known Bitcoin Donation, Worth About \$1 Million

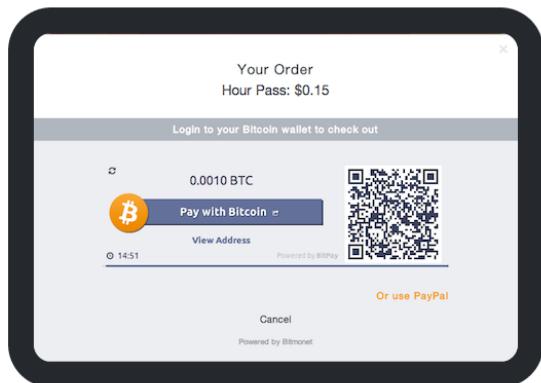


Micropayments



BITMONET

Meet Bitmonet, the better way to monetize your content.

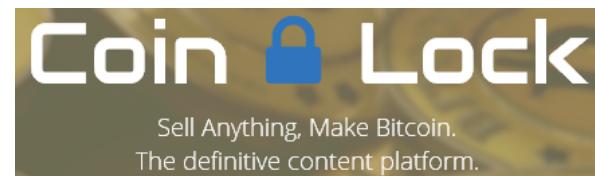


Satoshi box

1. Upload

2. Share

3. Profit!



coindl

Download digital goods with bitcoins

Paypal

PayPal officially allowing shops to accept Bitcoin

PayPal Announces First Partnerships in Bitcoin Space

PayPal and Virtual Currency

Scott Ellison, Senior Director Corporate Strategy, PayPal

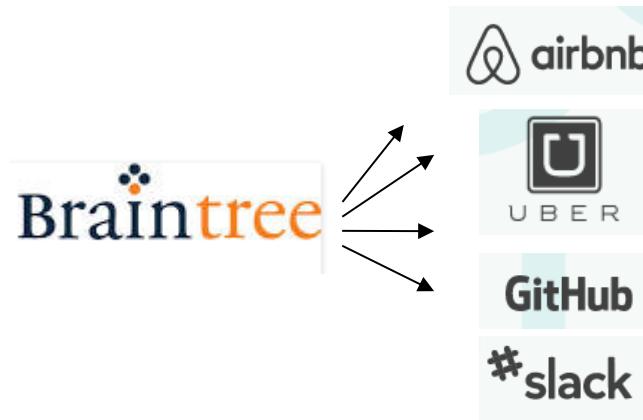
Sep
23

Bitcoin has been big news this year, and for good reason. Although cryptocurrencies have been around for some time, only **Bitcoin** has achieved significant scale. This new entrant in the world of payments has people asking lots of questions – including how and if PayPal will decide to work with **Bitcoin**.

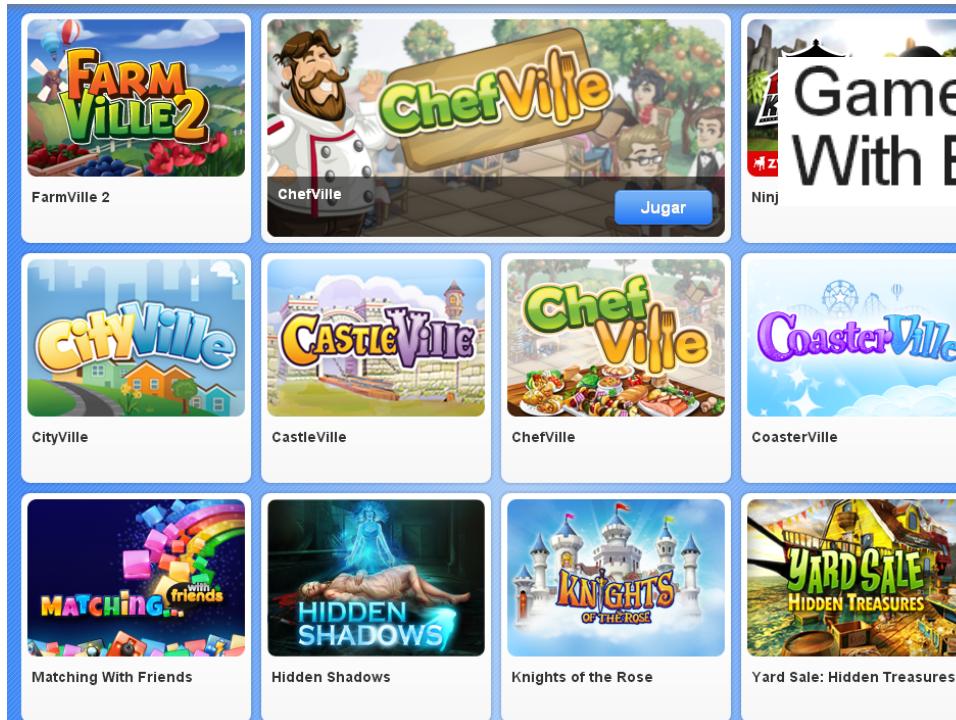
While we're focused on giving people everywhere safer and more seamless buying experiences, we're also fierce advocates of giving businesses -- and in turn their customers -- flexibility and the freedom of choice. Earlier this month we announced that businesses working with **braintree** will soon be able to accept **Bitcoin** as a payment option through their innovative v.zero SDK and [relationship with Coinbase](#).

Today we are announcing PayPal's next step in helping merchants accept **Bitcoin** payments. PayPal has entered into agreements with leading **Bitcoin** payment processors [BitPay](#), [Coinbase](#) and [GoCoin](#). Starting today, these agreements let PayPal digital goods merchants accept **Bitcoin** with a simple integration through the [PayPal Payments Hub](#). This will be available to merchants in North America first.

We chose to work with BitPay, Coinbase and GoCoin because of our commitment to offering innovative and safer ways for businesses to accept payments. All three companies have taken steps to ensure that they know their customers and that those customers are offered certain protections. We believe digital goods merchants will be excited to work with these industry-leading companies to sell ringtones, games and music and get paid with **Bitcoin**.



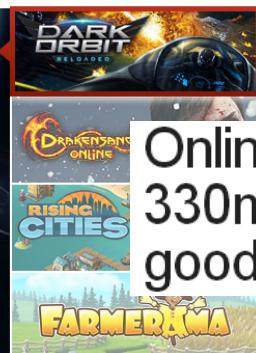
Zynga



Games Giant Zynga Starts Playing With Bitcoin

A screenshot of a Zynga game's payment interface. At the top, it says "Zynga" and "Make a Purchase". Below that, there is a "Winter Deal" for \$1.07 USD, which includes TX State Tax (7.25%). A dropdown menu shows "USD - US Dollar". The payment method section says "Choose your payment method" and lists VISA, MasterCard, AMERICAN EXPRESS, DISCOVER, PayPal, and Bitcoin. Radio buttons indicate that Credit Card is selected. Below this is a blue "Continue to Secure Checkout" button. At the bottom, there are links for "Terms of Service | Privacy Policy" and "Zynga Secure Payment" with a lock icon.

Bigpoint Games



Online game developer Bigpoint's 330m users can now buy virtual goods with bitcoins

TOP GAMES

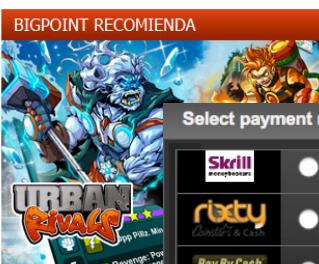
SEAFIGHT : BECOME A FEARED AND WEALTHY PIRATE! [PLAY NOW](#)

PIRATE STORM: ALL HANDS ON DECK! [PLAY NOW](#)

BATTLESTAR GALACTICA ONLINE: THE GAME! [PLAY NOW](#)

[Stronghold Kingdoms](#)

[Space Station 13](#)



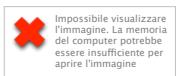
Select payment method

- Pay with Moneybookers . [i](#)
- Pay with Rixty . [i](#)
- Pay with Pay By Cash . [i](#)
- Pay with Zeevex . [i](#)
- Pay with Bitcoin . [i](#)
Bonus - get 5% more Virtual currency!
*Bonus only applies to game currency purchases.
- Pay with paysafecard . [i](#)
Bonus - get 5% more Virtual currency!
*Bonus only applies to game currency purchases.
- Pay with Western Union . [i](#)
- Pay with Bank transfer . [i](#)

E-sports



 Impossibile visualizzare l'immagine. La memoria del computer potrebbe essere insufficiente per aprire l'immagine oppure l'immagine potrebbe essere danneggiata. Riavviare il computer e aprire di nuovo il file. Se viene visualizzata di nuovo la x rossa, potrebbe essere necessario eliminare l'immagine e inserirla di nuovo.



 Impossibile visualizzare l'immagine. La memoria del computer potrebbe essere insufficiente per aprire l'immagine oppure l'immagine potrebbe essere danneggiata. Riavviare il computer e aprire di nuovo il file. Se viene visualizzata di nuovo la x rossa, potrebbe essere necessario eliminare l'immagine e inserirla di nuovo.

 Impossibile visualizzare l'immagine. La memoria del computer potrebbe essere insufficiente per aprire l'immagine oppure l'immagine potrebbe essere danneggiata. Riavviare il computer e aprire di nuovo il file. Se viene visualizzata di nuovo la x rossa, potrebbe essere necessario eliminare l'immagine e inserirla di nuovo.

 Impossibile visualizzare l'immagine. La memoria del computer potrebbe essere insufficiente per aprire l'immagine oppure l'immagine potrebbe essere danneggiata. Riavviare il computer e aprire di nuovo il file. Se viene visualizzata di nuovo la x rossa, potrebbe essere necessario eliminare l'immagine e inserirla di nuovo.

Questions

1. how the protocol does not allow i) Stealing Bitcoins, ii) Denial of service attack, and iii) Double spending Bitcoins.
2. Why do miners run “full nodes” that keep track of the entire block chain whereas Bob the merchant can get away with a “light node” that implements “simplified payment verification,” needing to examine only the last few blocks?
3. If a malicious ISP completely controls a user’s connections, can it launch a double-spend attack against the user? How much computational effort would this take?

Questions

4. Even when all nodes are honest, blocks will occasionally get orphaned: if two miners Minnie and Mynie discover blocks nearly simultaneously, neither will have time to hear about the other's block before broadcasting hers.
- 4a. What determines whose block will end up on the consensus branch?
 - 4b. What factors affect the rate of orphan blocks?
 - 4c. If Mynie hears about Minnie's block just before she's about to discover hers, does that mean she wasted her effort?
 - 4d. Do all miners have their blocks orphaned at the same rate, or are some miners affected disproportionately?

Questions

5. If a miner misbehaves, can other miners “boycott” her by refusing to build on her blocks on an ongoing basis?
6. Discuss potential problems that might arise in the future and that might dramatically limit the use of Bitcoin.

BITCOIN: statistics

- Value of Bitcoin
 - Today about US \$ 1100
 - One year ago US \$ 420

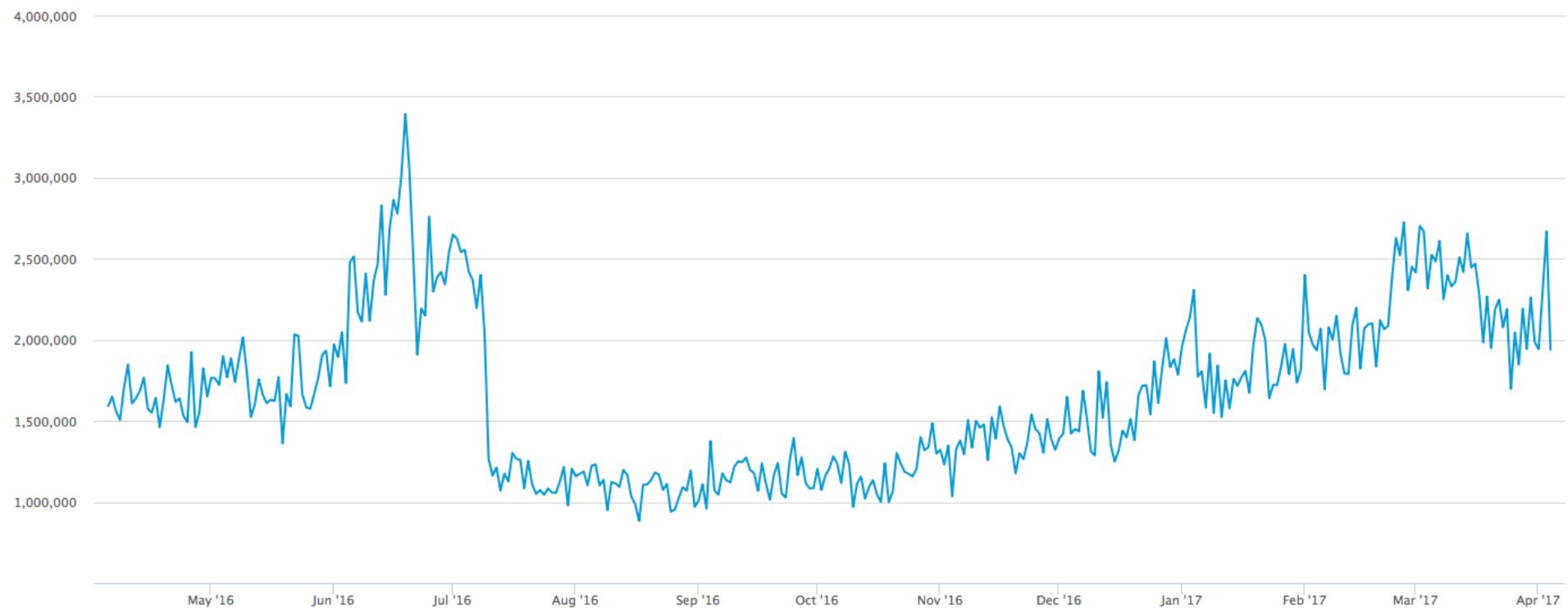


BITCOIN: statistics

- No. Transactions: about 300000 per day
- Orphan block: less than 1 per day (in the last year a maximum of 4 in a single day)
- Time to be included (transactions pay a fee): less than 10 minutes
- Total Hash rate:
 - Oct 2019: about 100×10^6 TeraHASH/ second
 - Oct 2018: about 50×10^6 TeraHASH/ second

BITCOIN: statistics

- Miner reward (in US \$): why there was a big drop in July 2016? why it is steadily increasing?



Hard fork: August 2013

Hard fork: a state of the network or a software update? Two definitions

1. Some nodes have accepted a block, but others have rejected it. The nodes accepting the questionable block keep and extend it. The nodes rejecting the block neither keep nor extend it, but rather build their own branch. The resulting "fork" is only visible to nodes that accepted the questionable block.
2. A hardfork is a change to the bitcoin protocol that makes previously invalid blocks/transactions valid, and therefore requires all users to upgrade. In other words, a hard fork is a kind of update to Bitcoin Core (given that Bitcoin Core is the protocol)

August 2013: A block that had a larger number of total transaction inputs than previously seen was mined and broadcasted. Bitcoin 0.8 nodes were able to handle this, but some pre-0.8 Bitcoin nodes rejected it, causing an unexpected **hard fork of the blockchain**. The pre-0.8 incompatible chain at that point had around 60% of the hash power ensuring the split did not automatically resolve.

It's not hard to see how a software update could lead to persistent block chain fork as seen by some nodes. So clearly the two ideas are connected.

Hard fork:

On a blockchain, a fork is a technical event that occurs because diverse participants need to agree on common rules (not orphan block)

At its most basic, a fork is what happens when a blockchain diverges into two potential paths forward — either with regard to a network's transaction history or a new rule in deciding what makes a transaction valid.

As a result, those who use the blockchain have to show support for one choice over the other.

So far, we know some forks resolve on their own, but others, fueled by deep rifts in a community, can cause a network to permanently split, creating two blockchain histories — and two separate currencies.

Along with that, there has also been confusion about the various types of forks, how they get activated and the risks they pose.

A hard fork is NOT an orphan block

Hard fork / soft fork

HARD FORK: A hard fork is a software upgrade that introduces a new rule to the network that isn't compatible with the older software. You can think of a hard fork as an expansion of the rules. (A new rule that allows block size to be 2MB instead of 1MB would require a hard fork).

What happens? Nodes that continue running the old version of the software will see the new transactions as invalid. So, to switch over to the new chain and to continue to mine valid blocks, all of the nodes in the network need to upgrade to the new rules.

What can go wrong? The problem comes when some sort of political impasse arises, and a portion of the community decides to stick by the old rules no matter what. The hash rate, or network computing power, behind the old chain is irrelevant. What matters is that its data (and ruleset) is still perceived to have value, meaning miners still want to mine a chain and developers still want to support it.

Hard fork / soft fork

SOFT FORK: A soft fork is any change that's backward compatible. Say, instead of 1MB blocks, a new rule might only allow 500K blocks.

What happens? Non-upgraded nodes will still see the new transactions as valid (500k is less than 1MB in this example). However, if non-upgraded nodes continue to mine blocks, the blocks they mine will be rejected by the upgraded nodes. This is why soft forks need a majority of hash power in the network.

What can go wrong? When a soft fork is supported by only a minority of hash power in the network, it could become the shortest chain and get orphaned by the network. Or, it can act like a hard fork, and one chain can splinter off.

Soft forks have been the most commonly used option to upgrade the bitcoin blockchain so far
Past examples:

- Bitcoin's reference implementation currently relies on OpenSSL for signature validation, which means it is implicitly defining Bitcoin's block validity rules.
- OpenSSL is not designed for consensus-critical behaviour, and thus changes to it can - and have - affected Bitcoin software.
- One specifically critical area is the encoding of signatures. Until recently, OpenSSL's releases would accept various deviations from the DER standard and accept signatures as valid.
- SoftForK: restrict to DER standard.

Hard fork: August 2013

What went wrong: a change of software

- A block that had a larger number of total transaction inputs than previously seen was mined and broadcasted. Bitcoin 0.8 nodes were able to handle this, but some pre-0.8 Bitcoin nodes rejected it.
- The pre-0.8-incompatible chain at that point had around 60% of the mining hash power ensuring the split did not automatically resolve (as would have occurred if the pre-0.8 chain outpaced the 0.8 chain in total work, forcing 0.8 nodes to reorganise to the pre-0.8 chain).
- In order to restore a canonical chain as soon as possible, miners BTCGuild and Slush downgraded their Bitcoin 0.8 nodes to 0.7 so their pools would also reject the larger block. This placed majority hashpower on the chain without the larger block, thus eventually causing the 0.8 nodes to reorganise to the pre-0.8 chain.
- During this time there was one large double spend; it was done by someone experimenting to see if it was possible (not a malicious double spending)

Hard fork: August 2013

What went right

- The split was detected very quickly.
- The right people were online and available in IRC or could be contacted directly.
- Marek Palatinus (Slush) and Michael Marsee (Eleuthria of BTCGuild) quickly downgraded their nodes to restore a pre-0.8 chain as canonical, despite the fact that this caused them to sacrifice significant amounts of money.
- Deposits to the major exchanges and payments via BitPay were also suspended (and then un-suspended) very quickly.
- Fortunately, the only attack on a merchant was done by someone who was not intending to actually steal money.

Hard fork: August 2013

Root cause

- Bitcoin versions prior to 0.8 configure an insufficient number of Berkeley DB locks to process large but otherwise valid blocks. Berkeley DB locks have to be manually configured by API users depending on anticipated load.
- Because max-sized blocks had been successfully processed on the testnet, it did not occur to anyone that there could be blocks that were smaller but require more locks than were available. Prior to 0.7 unmodified mining nodes self-imposed a maximum block size of 500,000 bytes, which further prevented this case from being triggered. 0.7 made the target size configurable and miners had been encouraged to increase this target in the week prior to the incident.
- Bitcoin 0.8 did not use Berkeley DB. It switched to LevelDB instead, which did not implement the same locking limits as BDB. Therefore it was able to process the forking block successfully.

Hard fork: August 2013

ACTIONS

Immediately

- Release a version 0.8.1, forked directly from 0.8.0, that, for the next two months has the new rules:
- Release a patch for older versions that implements the same rules, but also increases the maximum number of locks to 537,000
- Create a web page on bitcoin.org that will urge users to upgrade to 0.8.1, but will tell them how to set DB_CONFIG to 537,000 locks if they absolutely cannot.
- Over the next 2 months, send a series of alerts to users of older versions, pointing to the web page.

Alert system

A new hard fork soon?

Problem: efficiency of handling a block

A big discussion is going BU vs SegWit

BU (bitcoin Unlimited, miners) would allow miners and nodes to vote on increasing the block size as and when required.

- It would keep transactions in the main blockchain and effectively give them control to set transaction fees.
- Miners argue this is important, as the programming of bitcoin reduces the reward for finding a block

A new hard fork soon?

A big discussion is going on BU vs SegWit

- SegWit is the proposal favoured by many bitcoin developers and enthusiasts,
- SegWit would double the transactions per second capacity of bitcoin by simplifying transactions, stripping out some details such as signatures
- One criticism of SegWit is that it appears to be only a temporary solution. It just doubles the network's bandwidth, while BU allows miners to vote to increase the capacity when they need with no upper limit.

Who will win? There could be a hard fork?

The Transaction Throughput Problem

- The number of transactions on the Bitcoin blockchain has also increased, up to 400 K transactions per day; about 90 K trans. are backlogged
- Every time a user sends a Bitcoin transaction the transaction is added into the **memory pool** (mempool), which is essentially a pool of all unconfirmed transactions in the Bitcoin network
- From the mempool, miners select transactions that they want to verify. Once miners validate a transaction (i.e. confirm that the sender actually has enough bitcoins to send to the receiver), they add it to a new block, which is eventually published to the blockchain
- Other nodes then iterate through this newly published block's transactions to ensure the block is valid, before accepting the block as a part of its ledger.

The Transaction Throughput Problem

Let's calculate the throughput of transactions:

- A simple transaction (1 input 2 outputs) has size approx. 226bytes
- A block's size is limited to 1MB (1000000 bytes)
- A block is published in the blockchain once every 10 minutes on average (600 seconds).
- hence no. of transactions every 10 minutes is at most

$$1.000.000 / (600 * 226) = 7.37 \text{ per second}$$

In practice less between 4 and 7

The Transaction Throughput Problem

- If there are more unconfirmed transactions in the mempool, how does a miner select which transactions to verify? **Transaction fees!**
- The sender of a transaction has the option of adding a custom transaction fee for the miner, incentivizing a miner to select the transaction and have it verified faster
- Miners will select the transactions that have the highest fee attached to them to maximize profits.
- Theoretically, you can send a transaction with no fee. But if there are transactions that have fees higher than yours in the pool, why would yours ever get picked?

The Transaction Throughput Problem

The problem: if Bitcoin does change transactions fees will increase and people will leave Bitcoin

- As Bitcoin's user base grows, so does the average transaction fee. We observed that there are only 7 transact. that are processed every second and everyone wants to get their transaction verified first.
- At the moment, the average transaction fee is approximately 0.16 US\$ (transaction within 4 blocks, average) or 0.04 (transaction within 6 blocks, average)
 - (but in Dec. 2017 was more than 10US\$)
- This is too much for a transactions of 10 US\$

Solving the Trans. throughput Problem

Solution 1: raise the block size from 1 MB thus allowing more transactions per block

- This can be done if all miners agree therefore requiring consensus from the Bitcoin community.
- Millions of people use Bitcoin, gaining consensus is difficult and efforts should be made to avoid it.
- However Bitcoin's user base continues to grow, there will eventually be another backlog of unconfirmed transactions, so another block size increase will be needed, and subsequently another hard fork.

Solving the Trans. throughput Problem

Solution 2: blocks can have any size. Problems

1. To reach consensus is more difficult
2. Handling a big block is impractical and will restrict mining even more introducing an element of centralization.
3. Recall that once a block is mined, all other nodes must validate the block before accepting it. If the block size is incredibly large and somebody were to publish an invalid block, nodes would waste a large amount of time attempting to validate the block before discarding it as invalid and moving onto the next block.
4. This allows a denial of service attack by repeatedly publishing insanely large invalid blocks to the network, stopping valid blocks from being processed for a long period of time.

The Transaction Throughput Problem

- Satoshi was able to make numerous changes to the bitcoin network at the beginning; Changes are now more difficult (many users, huge economic value)
- Today no person or group can determine when and how bitcoin should be upgraded has similarly made the process of updating the system more complex.
- There has been many proposals with the main goal of allowing more transactions (i.e. large blocks)
- If there is no agreement among all miners and users there will be **a Fork in the blockchain**

Hard forks and soft forks

- During a **hard fork**, software implementing bitcoin and its mining procedures is upgraded; once a user upgrades his or her software, that version rejects all transactions from older software, **creating a new branch of the blockchain** (unless all miners agree)
- Those users who retain the old software continue to process transactions, meaning that there is a parallel set of transactions taking place across two different chains.
- A **soft fork** is a change to the software protocol where only previously valid blocks/transactions are made invalid (more restrictions). Since old nodes will recognize the new blocks as valid, a soft fork is backward-compatible. This kind of fork requires only a majority of the miners upgrading to enforce the new rules

Hard forks and soft forks

Example: some miners agree on 2MB block size

- Assume that a 2MB block is validated by an updated node and added on to the blockchain.
- What if the next block is validated by a node running an older version of the protocol? It will try to add its block to the blockchain. Since the latest block is not valid it will ignore that block and **attach its new validation to the previous one**.
- Therefore **you have two blockchains, one with both older and newer version blocks, and another with only older version blocks**. Which chain grows faster will depend on which nodes get the next blocks validated, and there could end up being additional splits. It is feasible that the two (or more) chains could grow in parallel indefinitely.

Hard forks and soft forks

Problem: efficiency of handling a block

A big discussion is going. Some forks

- Bitcoin XT (2014), blocks of 8MB (joined with Bitcoin Classic)
- Bitcoin Classic (2016), blocks of 2MB (now dead)
- Bitcoin Unlimited (2014), blocks of variable size (up to 16MB)
decided by users (now 1 BTC Unlimited ~ \$ 53)

Note: when there was a fork people received 1 BTC and 1 unit in the new currency ofr each BTC they owned

Conclusion: The majority of hash power did not begin to use these clients.

Hard forks and soft forks

Intended hard forks splitting the cryptocurrency

Hard forks splitting Bitcoin are created via changes of the blockchain rules, sharing a transaction history with bitcoin up to a certain time and date. New coins:

- Bitcoin Cash (2017): reduce size of transaction, hard fork, (now 1 BitCoin Cash is about 400 euro)
- Bitcoin Gold (2017): hard fork, new mining algorithm that tries to limit the use of big data center (1 BTC Gold about 22 euro)
- Bitcoin Private (2018): hard fork merge of Zcash (other crypto currency) allows zero knowledge evidence of ownership without revealing which coins are owned (1BTC Private about 2 euro)

Hard forks and soft forks

SegWit 2x (2017): increase size blocks in a compatible way

- It hides its increased block size by changing the definition of a block to be measured as one million "units" instead of bytes. The signature data is separated from and moved to the end (details omitted)
- The overall effect is to change the block size from 1MB to 1.8MB (on average) ***without changing the Bitcoin protocol!***

July 2017 it became apparent that miners supported implementation of the Segwit (about 90% of hash power) thereby attempting to avoid the risk of a hard fork for the bitcoin network

November 2017: proposers renounced