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 is 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 ownerhsip of coins

Recall: a block includes many transactions

Website: blockchain.info

Create 25 coins and credit to Alice$_{\text{ASSERTED BY MINERS}}$
Transfer 17 coins from Alice to Bob$_{\text{SIGNED(Alice)}}$
Transfer 8 coins from Bob to Carol$_{\text{SIGNED(Bob)}}$
Transfer 5 coins from Carol to Alice$_{\text{SIGNED(Carol)}}$
Transfer 15 coins from Alice to David$_{\text{SIGNED(Alice)}}$

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

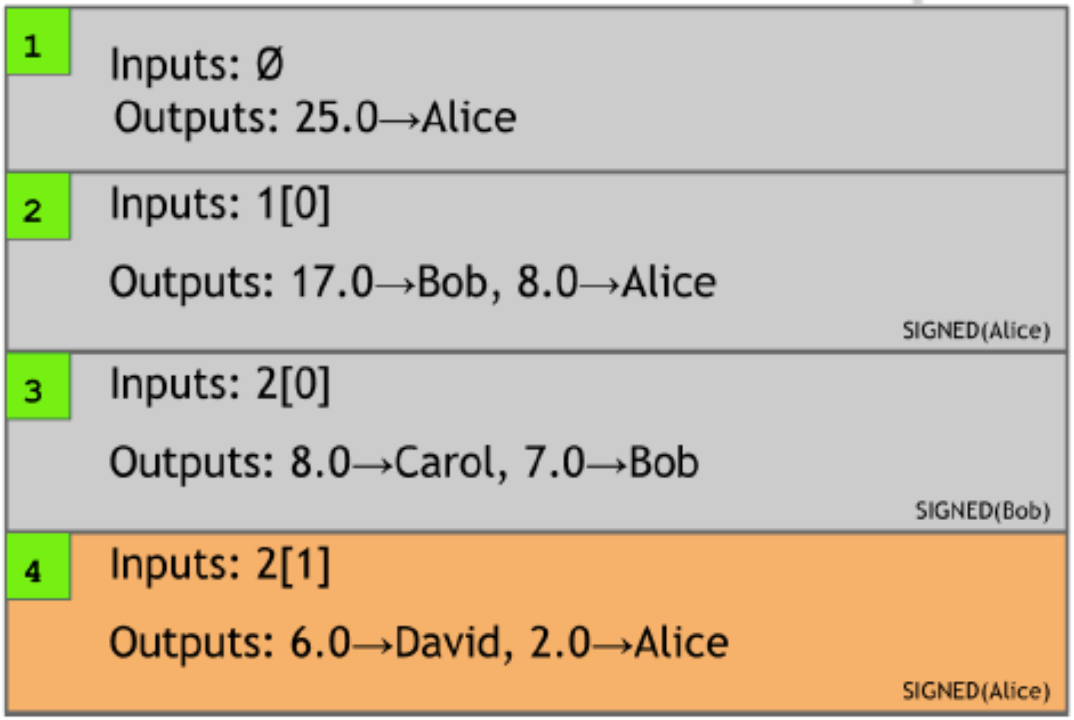


Figure 3.2 a transaction-based ledger, which is very close to Bitcoin

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	
Numero delle Transazioni	611
Totale Output	862.6764608 BTC
Volume stimato della Transazione	501.33305984 BTC
Commissioni di Transazione	0.06593639 BTC
Altezza	515279 (Catena Principale)

Hashes	
hash	0000000000000000028d76757be8eb798cc29545236b6d39a42824ef257a483
Blocco Precedente	0000000000000000000331647437fc2771f349336ad4f6997f97d11a25bb0d0a6
Blocco(chi) Successivo(i)	0000000000000000028bfaa550759f52d2da362aa535f5bf353a79d92b71400
Merkle Root	ff3f864534b264a2fc7742a3e3f3873a8dbfee101a60ada8246ef12e6167ae08

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

Bitcoin blocks

Transaction are grouped in blocks for optimization

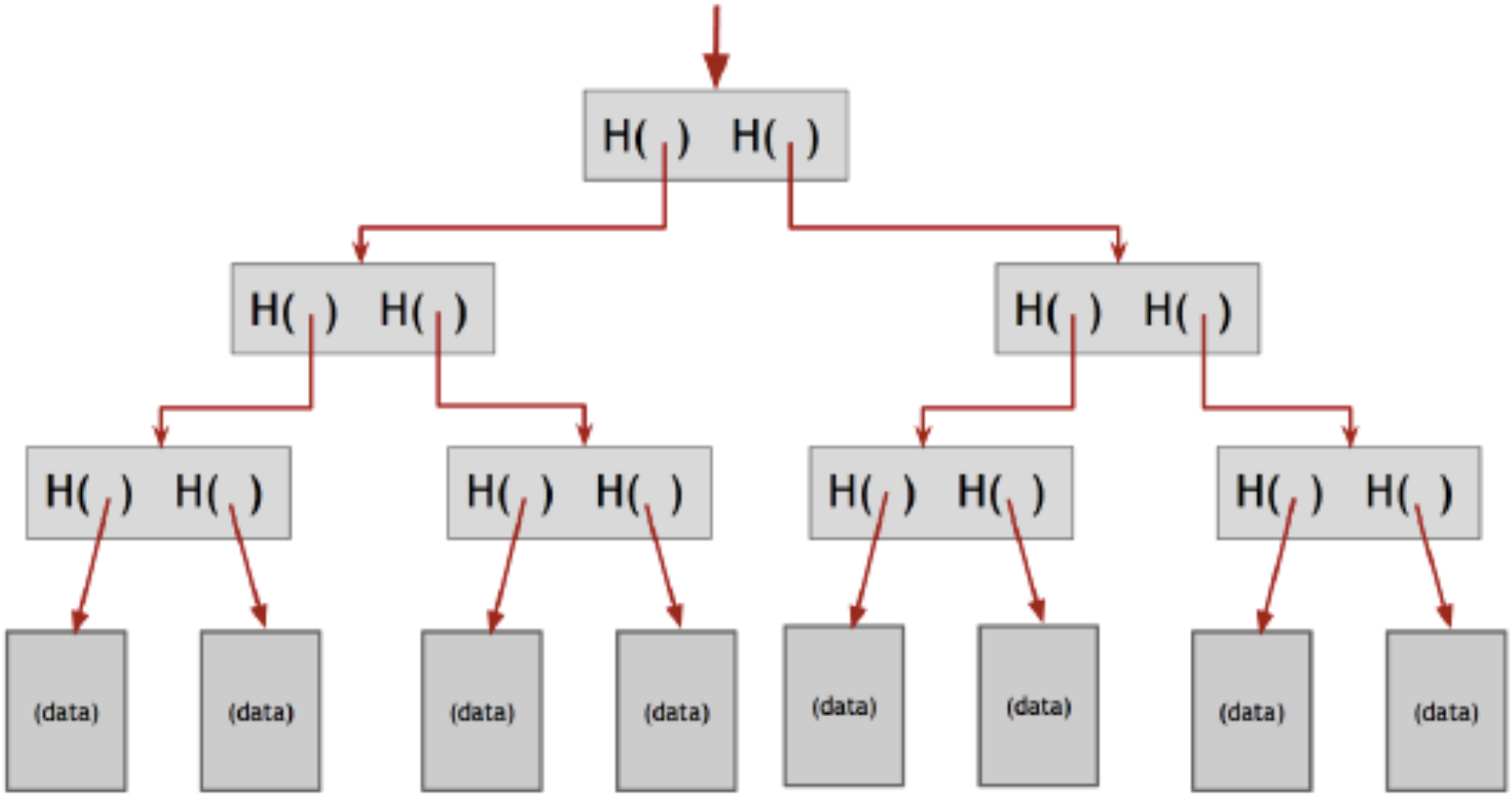
- If miners had to come to consensus on each transaction individually, the rate at which new transactions could be accepted by the system would be much lower.
- A hash chain of blocks is much shorter than a hash chain of transactions (many transactions can be put into a block). This allows to verify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

Hash blocks

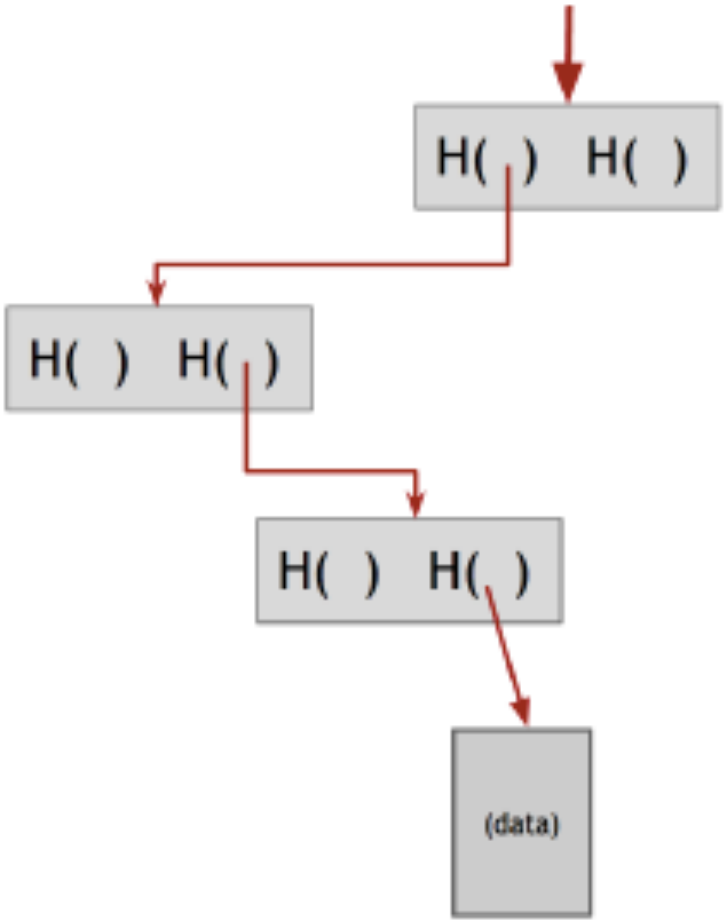
Bitcoin hashes many transactions in one block, why?

- 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

Merkle tree



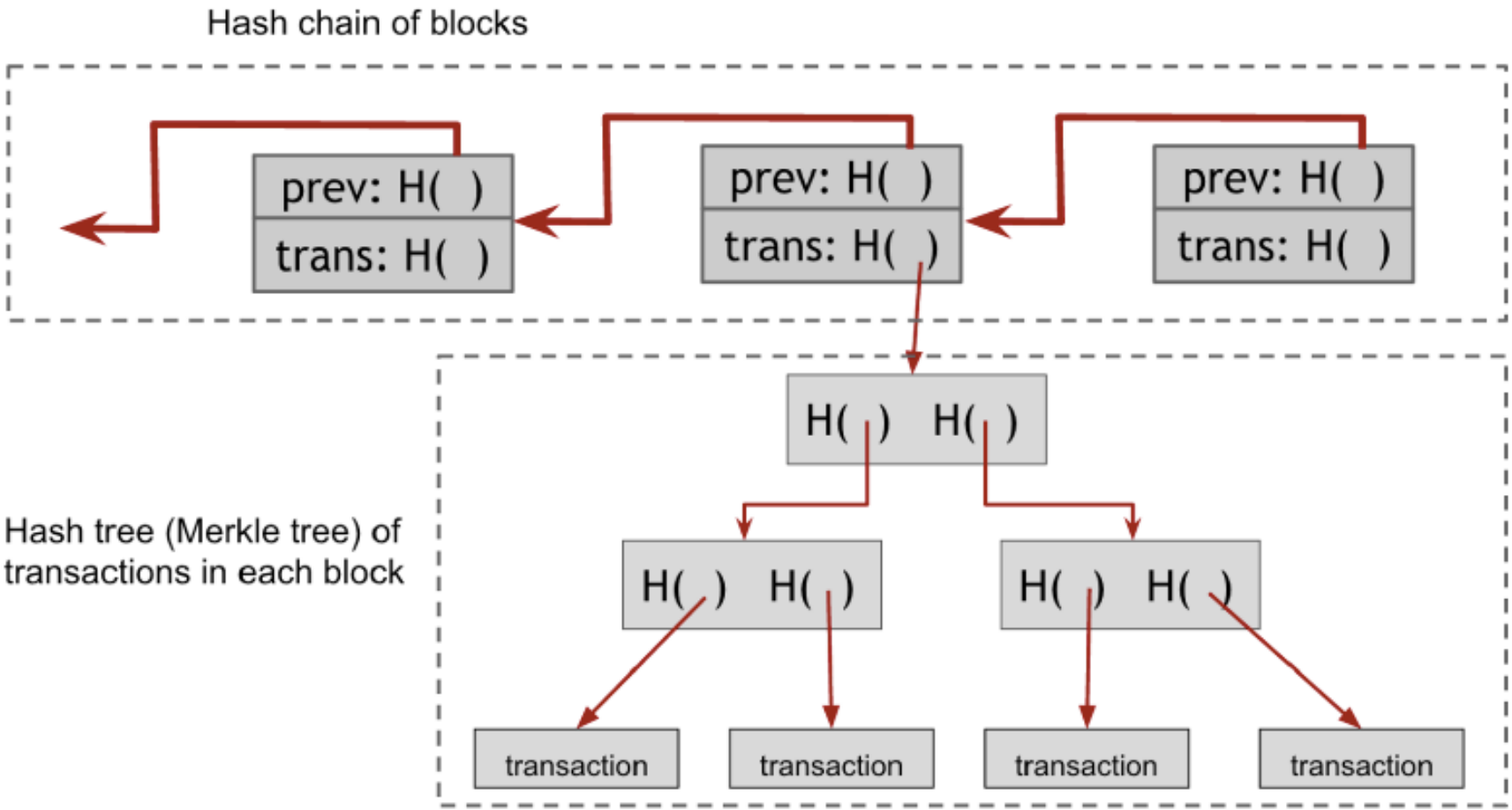
Merkle tree: proof of membership



To prove that a data block is included in the tree, one only needs to show the blocks in the path from that data block to the root.

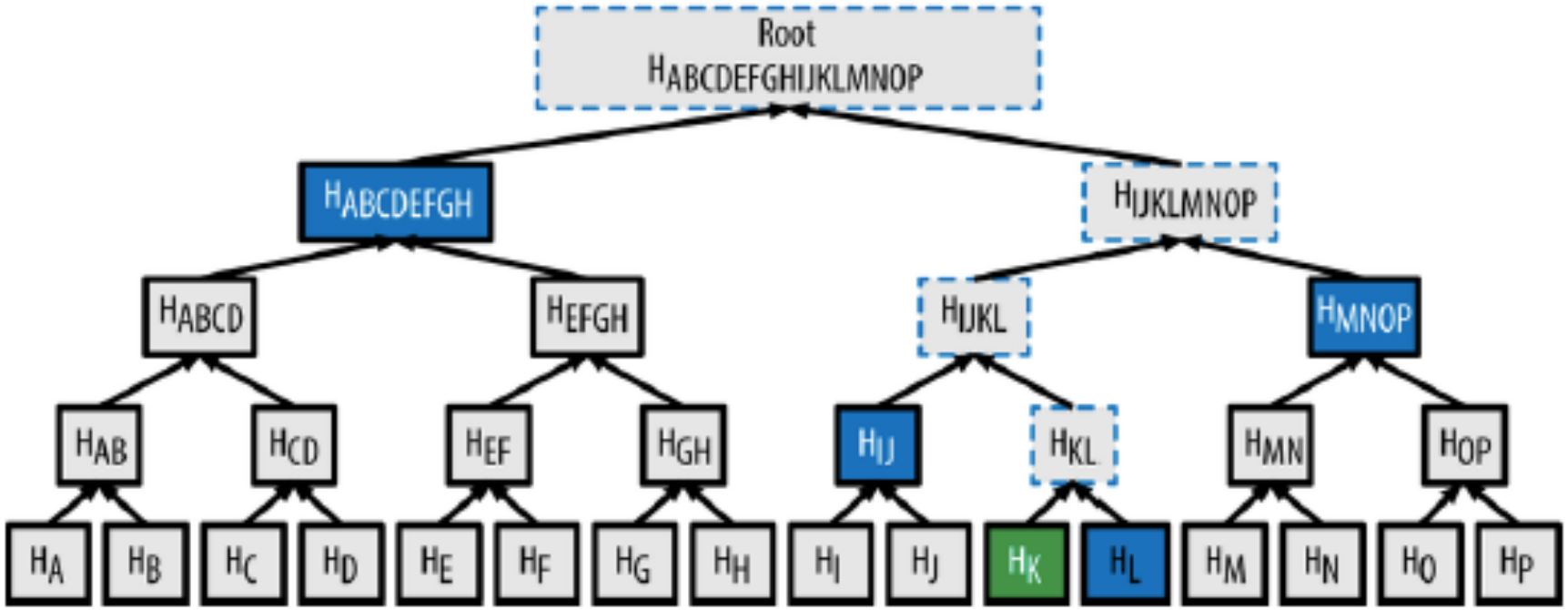
Note: in the case of a list you might search and check all blocks

Hash blocks



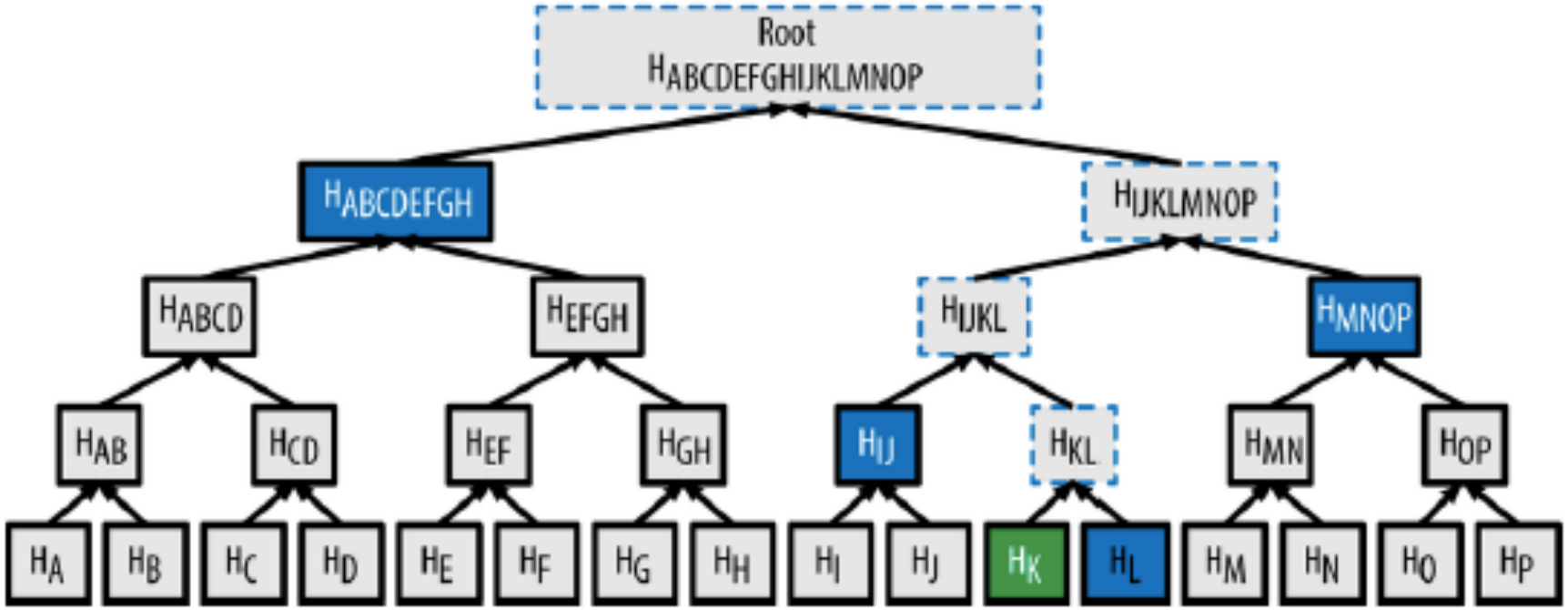
Top: a hash chain of blocks linking the different blocks
Bottom: internal to each block there is a Merkle Tree of transactions within the blocks

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, HIJKLMNOP, 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 transact. 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 alread 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

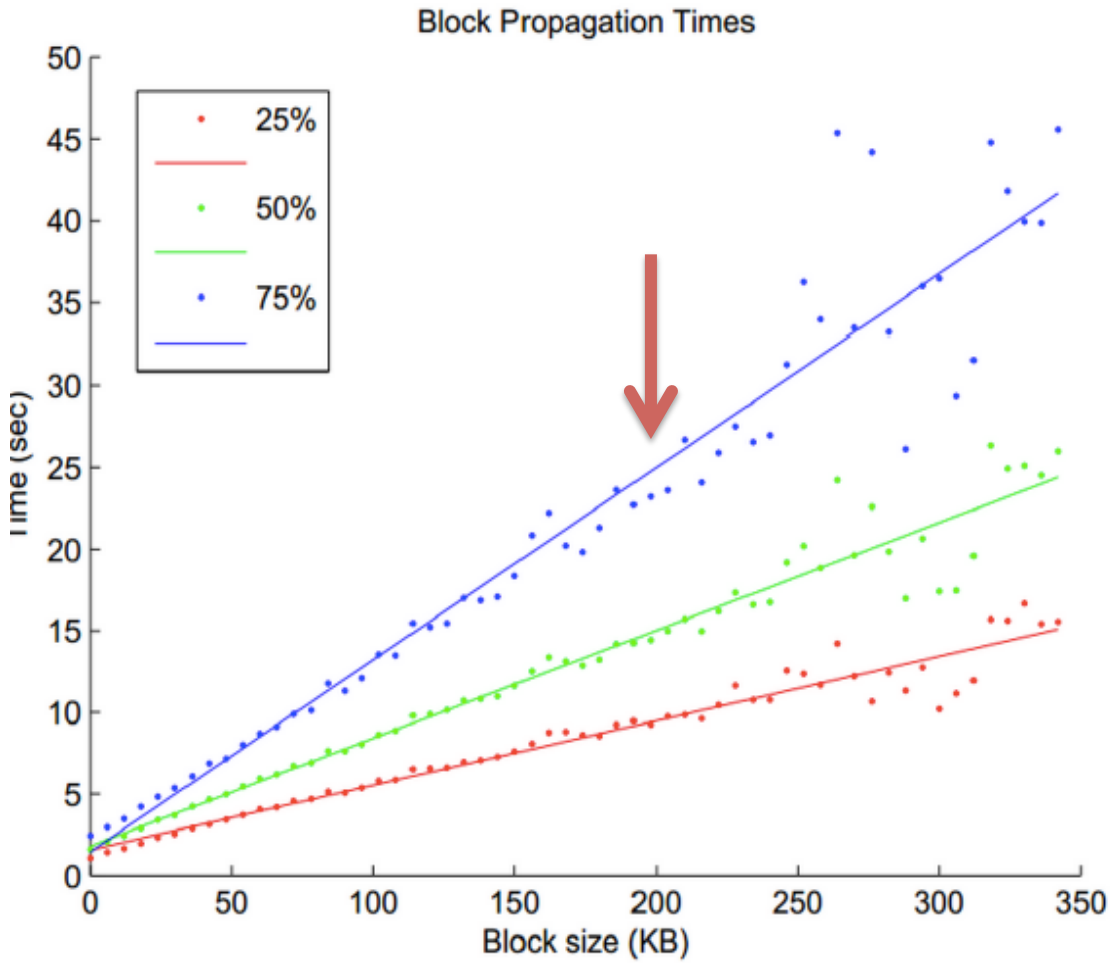
Bitcoin network: validating block

- Miner to validate ablock 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 (remmeber there can be bifurcations)
- When you receiv 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 August 2020 is ~ 285 GigaBytes (in April 2016 ~ 100 GB)
  - 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

Source: Yonatan Sompolinsky and Aviv Zohar: "Accelerating Bitcoin's Transaction Processing" 2014

Bitcoin network: size of block chain

block size April 2018: about
170 GB network
August 2020: 285 GB

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 toher 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 wll be halved to 6.25) .
- In additioncollect 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)

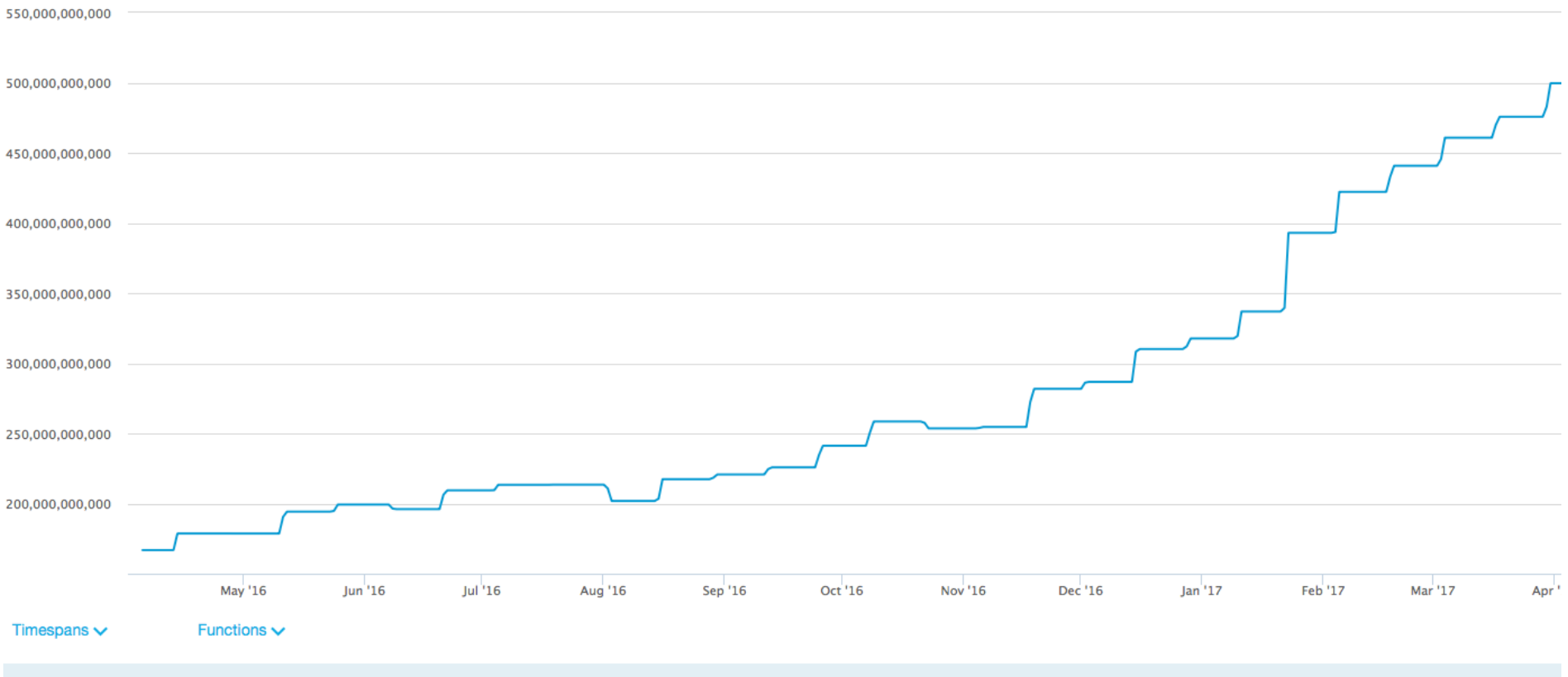
Transaction fees: conclusions

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,

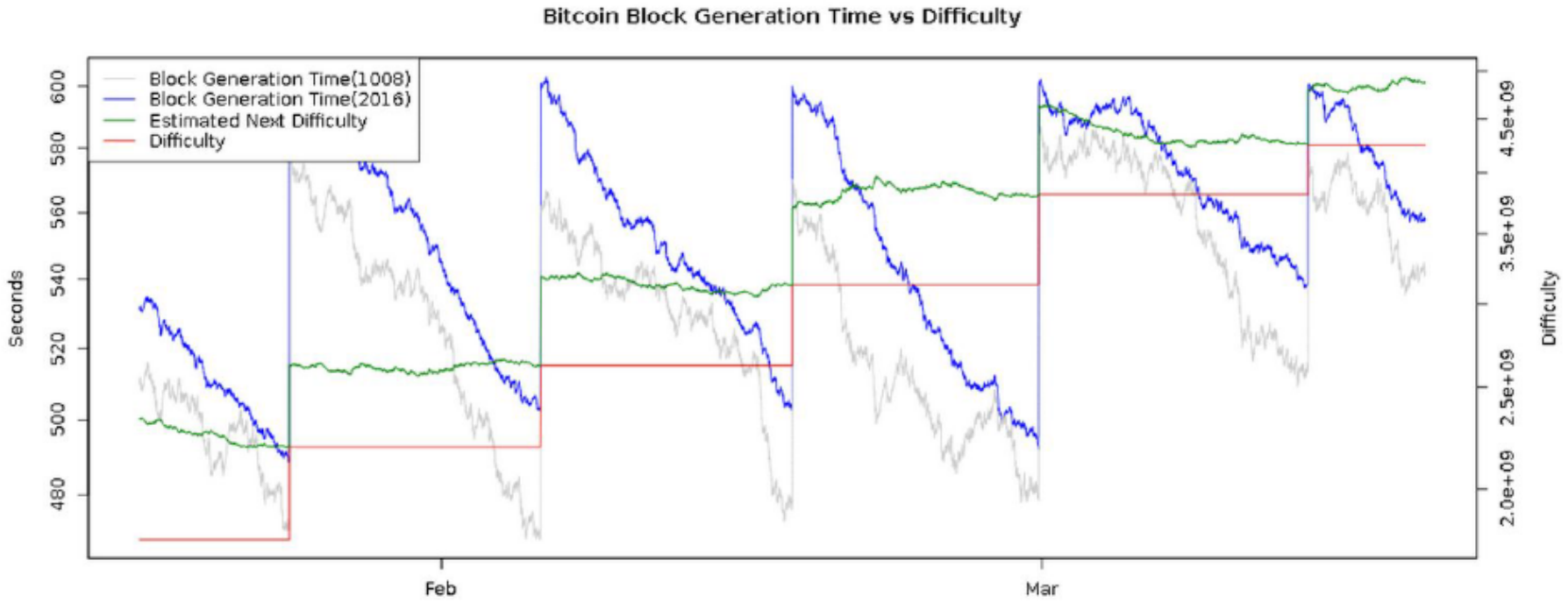
Bitcon mining: difficulty

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



Bitcon mining: difficulty

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



Bitcon mining: hardware

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

Bitcoin mining: hardware

- Today: there is no space for small miners
- Professional miners:

- BitFury (Georgia)

Bitcoin mining: hardware

Professional miners

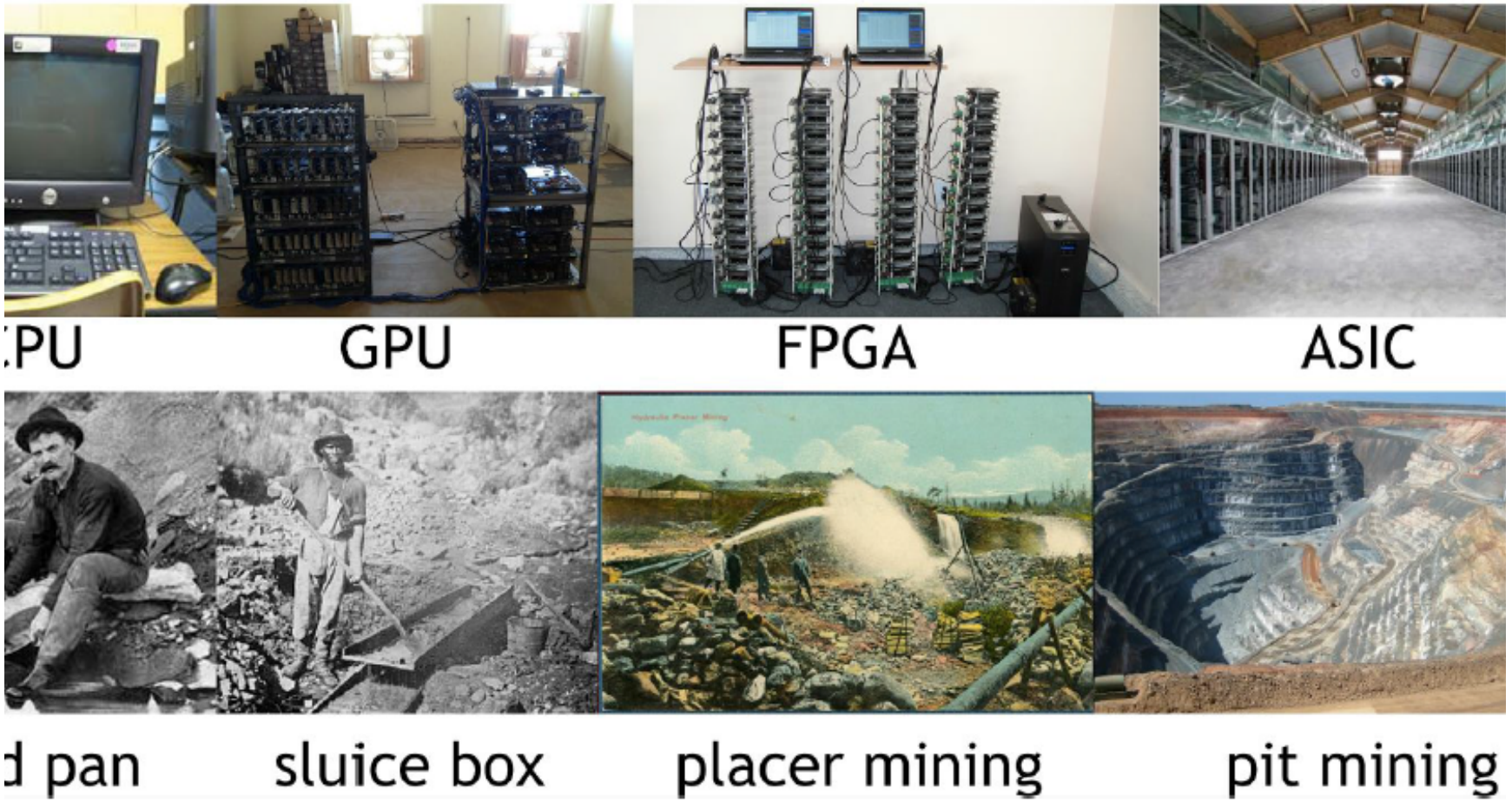
Use ASICs, Application-Specific Integrated Circuits .

- 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



Bitcoin mining: mining pool

If you start the mning business and you are smal 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.

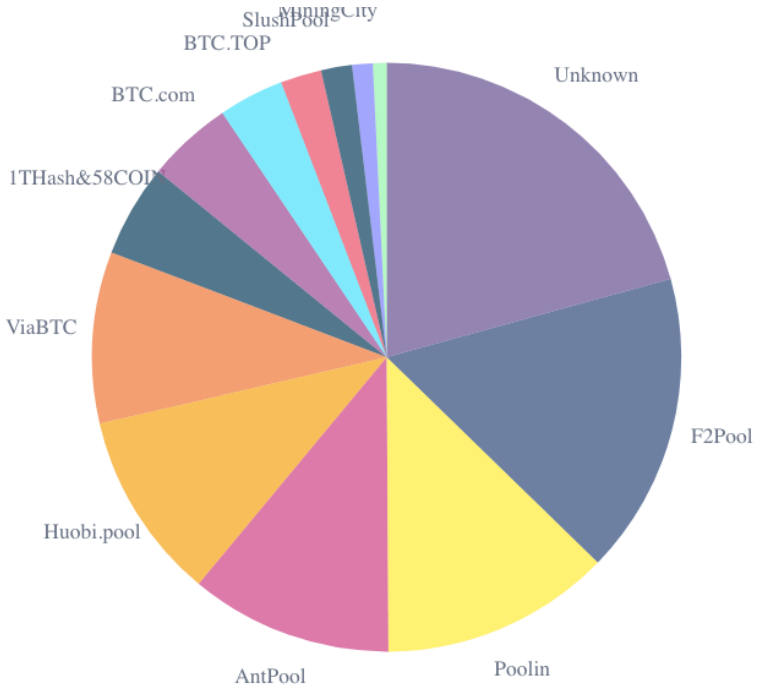
Bitcoin mining: mining pool

Mining pool: today

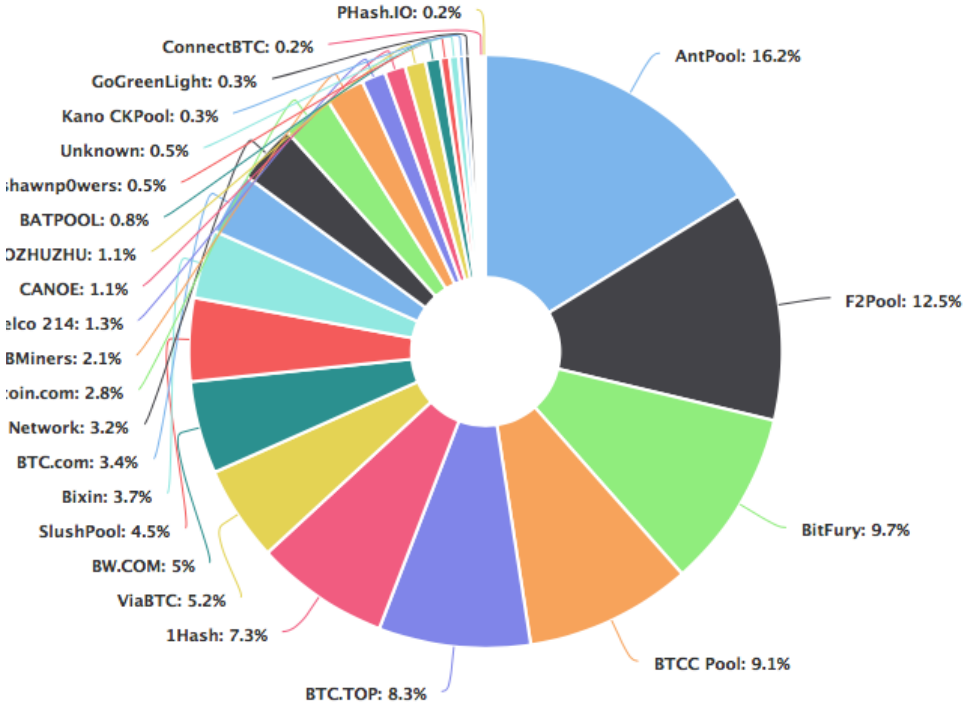
Note that a large organization might be part of several pools

Today 3 pools have ~50% of hash power; 6 pools ~ 80% of hash power

october 2020



october 2017



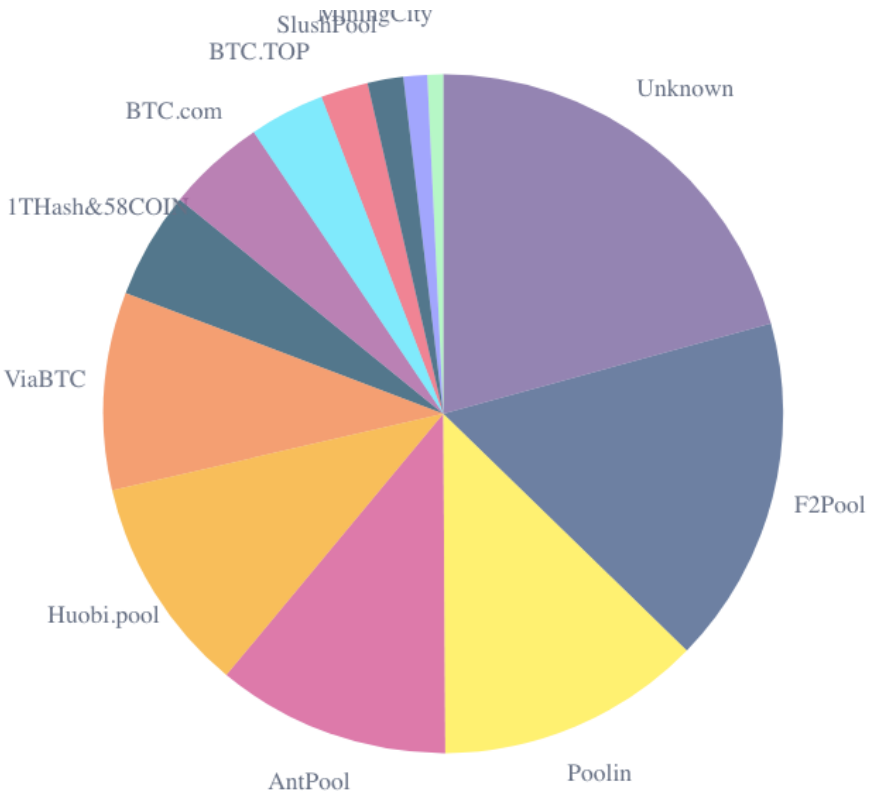
Bitcoin mining: mining pool

Mining pool: today

Note that a large organization might be part of several pools

Today 3 pools have ~50% of hash power; 6 pools ~ 80% of hash power

october 2020



top miner oct 2020

1. Unknown
2. F2Pool China
3. Poolin China
4. ANT.pool China

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 miningactivity 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.

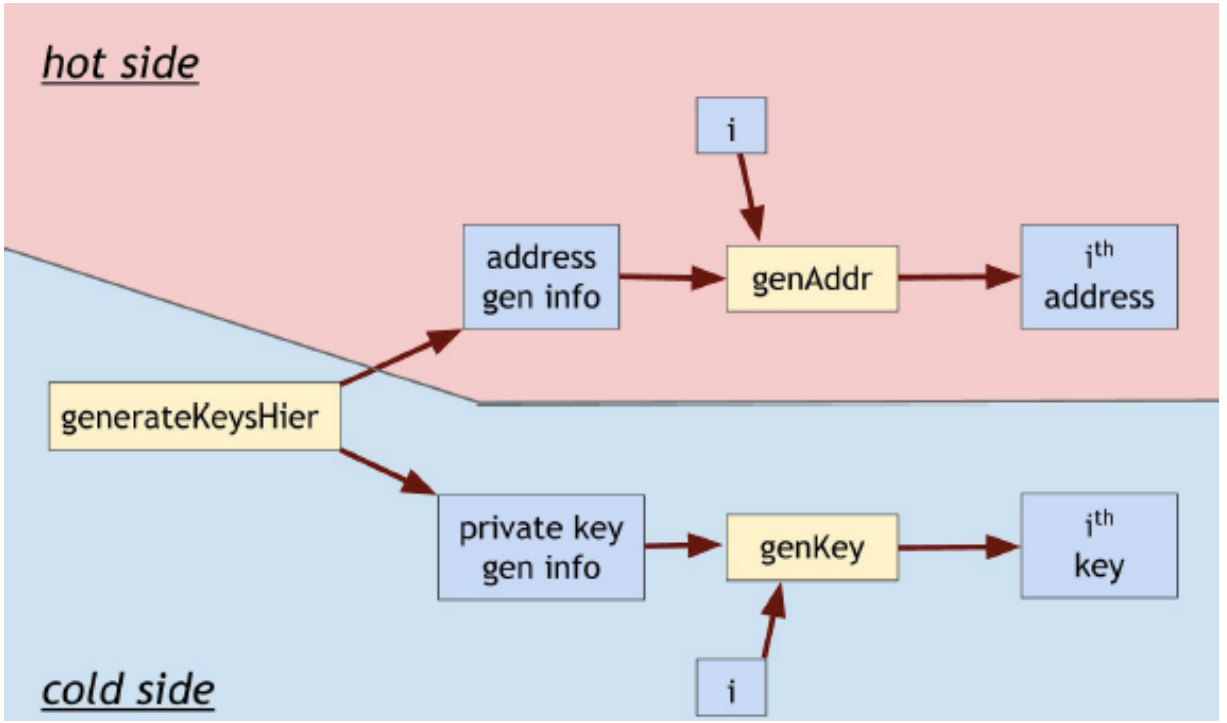
Hierarchical wallet

- 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 stroes 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 equivalnet of 65 M $ from clients' wallets. As a consequence Bitcoin valure dropped by 22% in a day.
  - Secret sharing mechanism: you divide the secret in pieces

Wallet: conclusions

- Users can lose bitcoin and other cryptocurrency tokens as a result of theft, computer failure, loss of access keys and more.
- Cold storage (or offline wallets) is one of the safest methods for holding bitcoin, as these wallets are not accessible via the Internet.
- Hardware wallets are potentially even safer, although users face the risk of losing access to their tokens if they misplace or forget their keys.

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.

Increase security with 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.

Increase security with 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

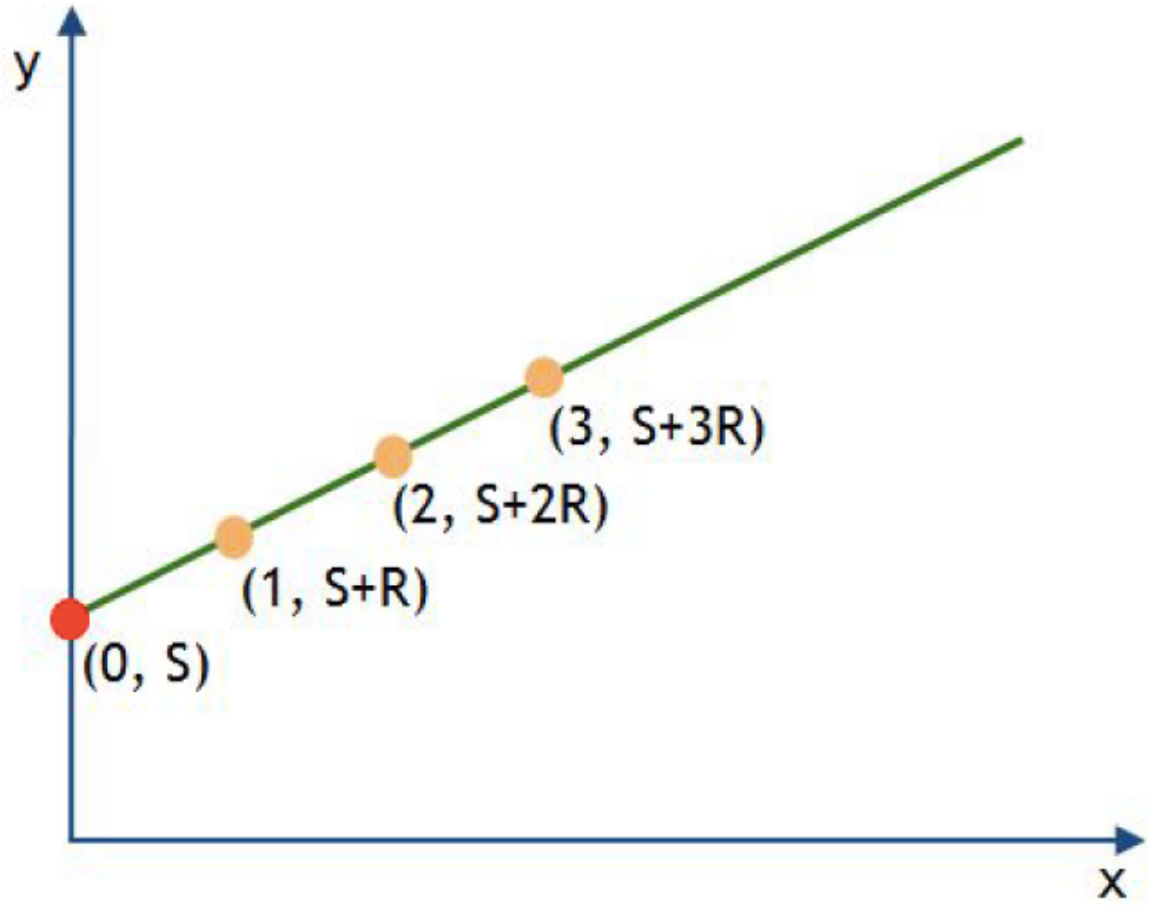


Figure 4.4: Geometric illustration of 2-out-of-N secret sharing. S represents the secret, encoded as a (large) integer. The green line has a slope chosen at random. The orange points (specifically, their

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: anonimity
  - 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 relaibility
  - 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

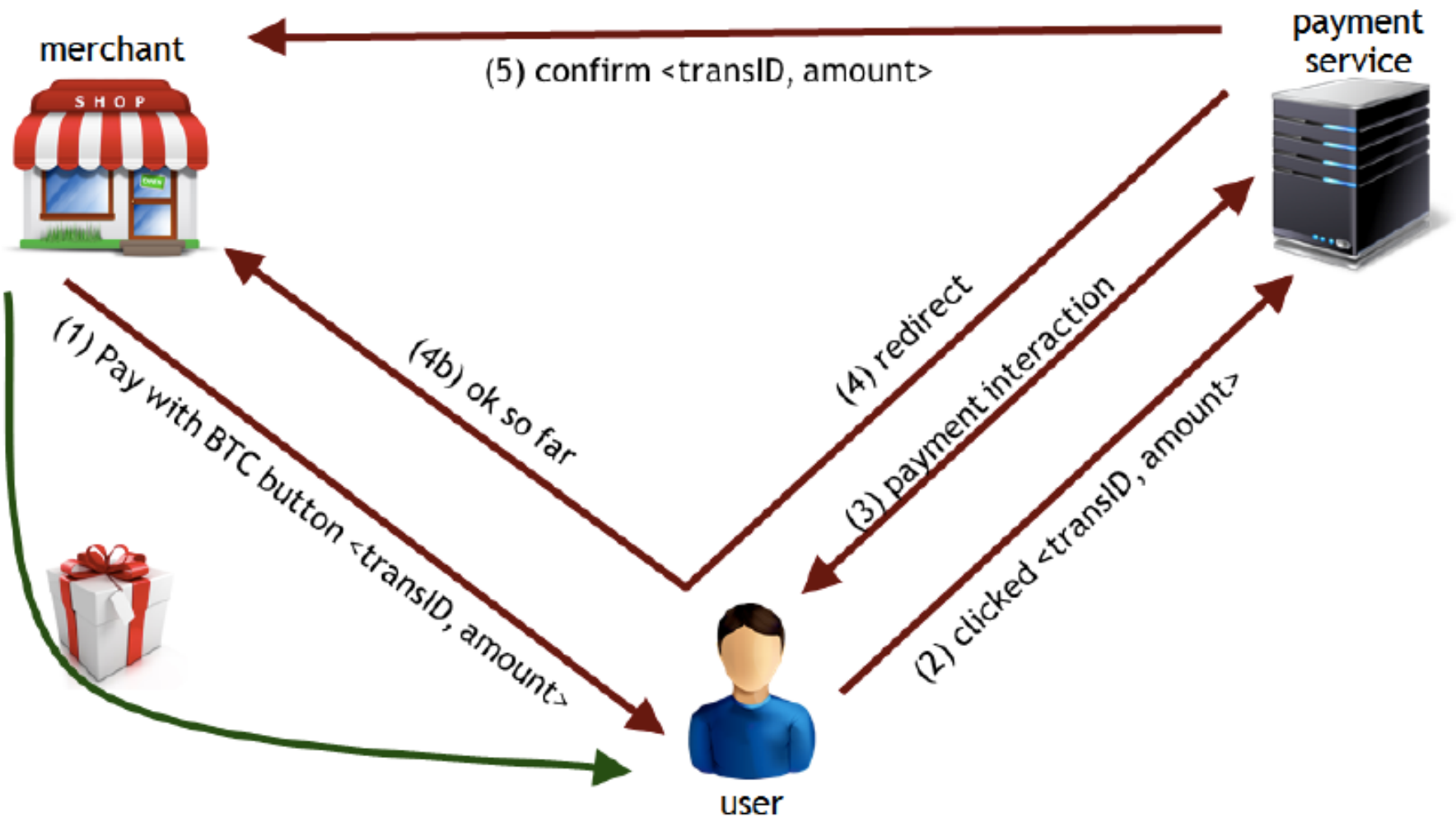


Figure 4.7: Payment process involving a user, merchant, and payment service.

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

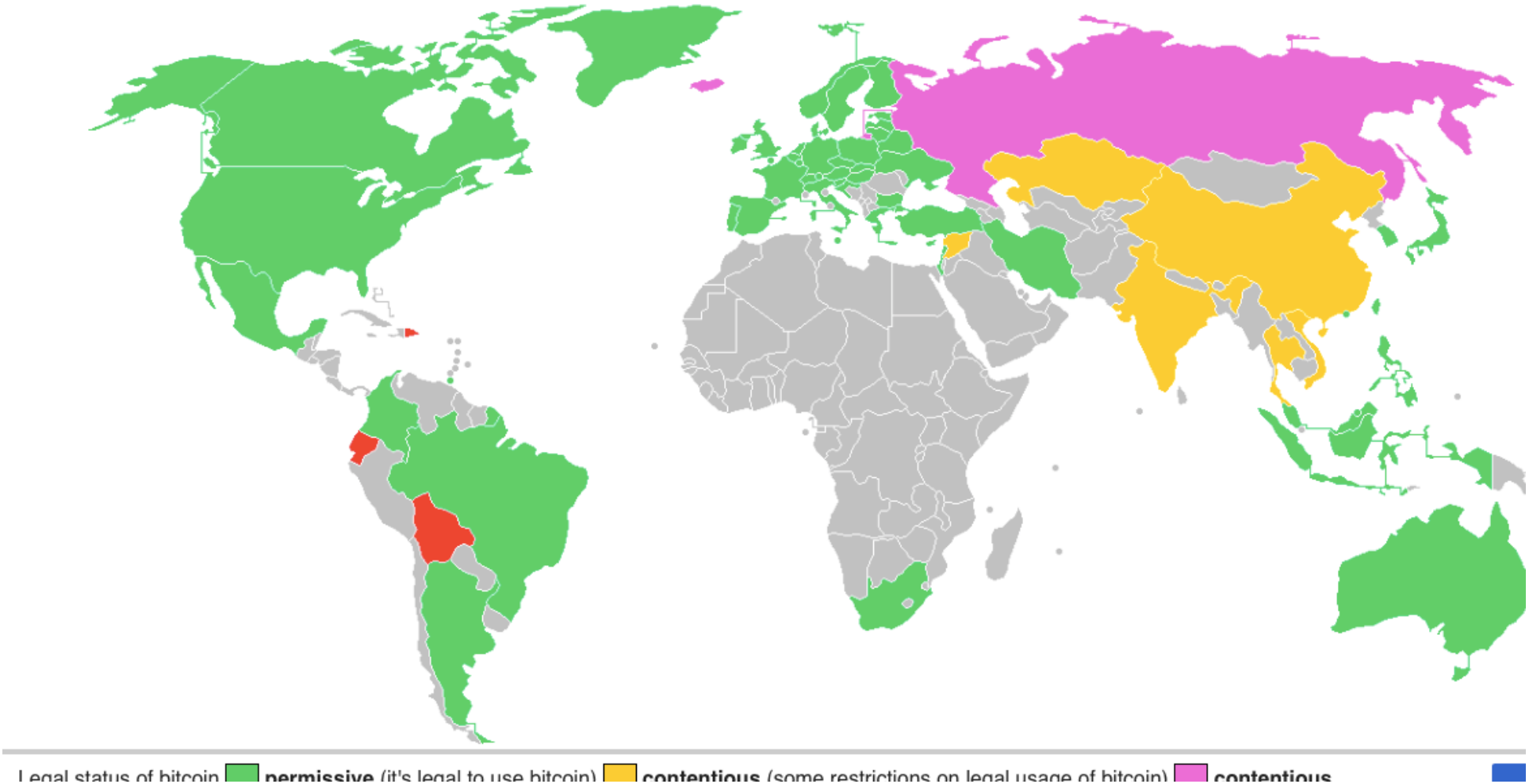
from bitcoincharts.com
(oct 2020) euro 9.900
Maximum about 17000 euro

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

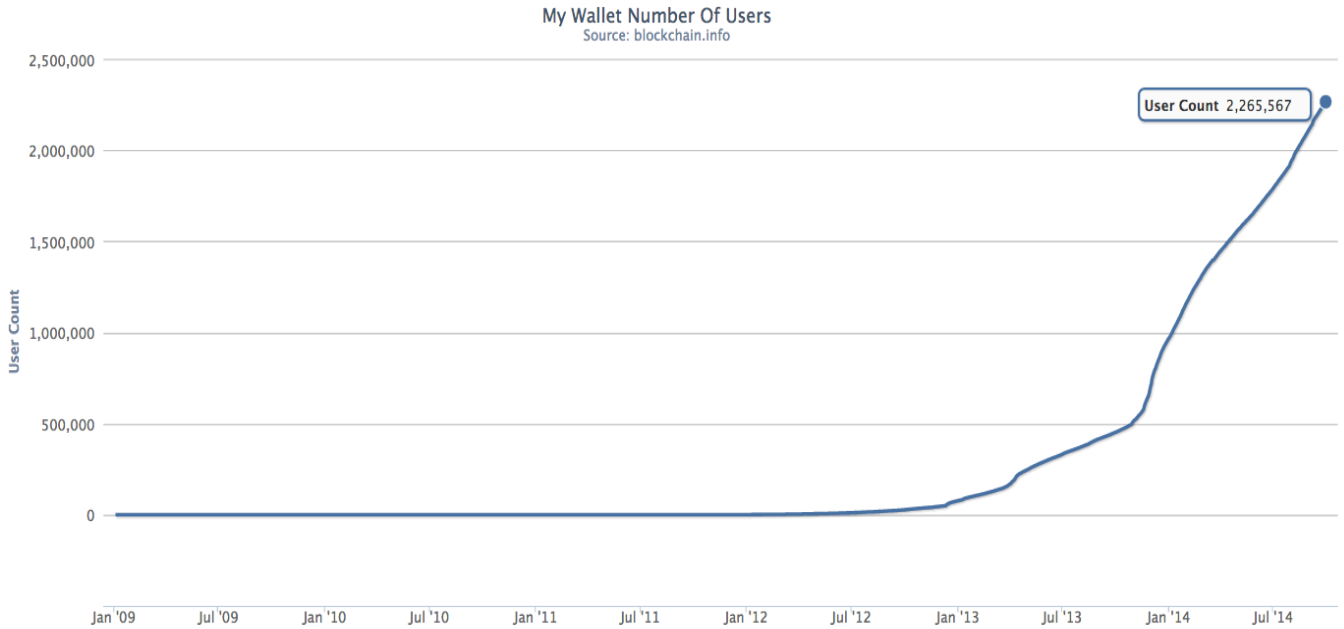
Regulation green legal

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 to5.8 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.

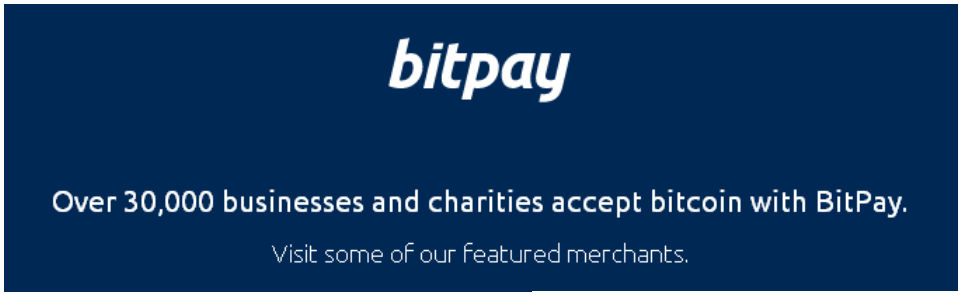
Your proposals/observations?

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
is a global bitcoin service provider
BitPay povedes services payment for merchants, founded in 2011 in 2014 processed 1 million USD.

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

bing, DELL, Square, United Way, Big Fish Games, Bloomberg
Cheapflir.com, intuit, Expedia, KHAN ACADEMY, Digital River, dish
overstock.com, REEDS Jewelers, Braintree, reddit, mint.com, WIKIMEDIA FOUNDATION
PayPal, CHICAGO SUN-TIMES, Budweiser, okcupid, Google, 1-800 flowers.com

Payment network

Rank	Network	Avg. Volume(millions $)
1	Visa, Inc.	16,518
2	MasterCard Inc.	9,863
3	China UnionPay	7,562
4	American Express Co.	2,434
5	Discover (PULSE Network)	438
6	Paypal	397
7	Discover (Discover Network)	299
8	**Bitcoin**	238
9	Western Union Company	216
10	Xoom Corp	15
11	Ria/AFEX	-

Rank	Network	Avg. Txs (1000s) ▲
1	Visa, Inc.	212,603
2	MasterCard Inc.	93,578
3	American Express Co.	14,521
4	Discover (PULSE Network)	11,838
5	Paypal	7,700
6	Discover (Discover Network)	5,052
7	Western Union Company	633
8	Ria/AFEX	84
9	**Bitcoin**	70
10	Xoom Corp	25
11	China UnionPay	-

Coinometrics

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	

coinmarketcap.com

Startups I

527 COMPANIES 1,939 INVESTORS 5,458 FOLLOWERS 125 JOBS

Coinbase
Making Bitcoin accessible to con...
San Francisco · Mobile Payments

Onename
The Decentralized Whitepages fo...
New York City · Application Platforms

BitPay
Accept bitcoin.
Atlanta · Mobile Payments

Buttercoin
White-label Bitcoin Exchange Ser...
Palo Alto · Bitcoin

SecondMarket
Simplifying transactions for privat...
New York City · Startups

Chain.com
Bitcoin developer platform
San Francisco · Developer APIs

Vaurum
We enable financial institutions t...
Palo Alto · Financial Exchanges

Filecoin
Filecoin is a data storage networ...
United States · Bitcoin Mining

HashFast
make bitcoins faster
San Francisco · Hardware + Software

ZipZap
Global payment network enablin...
San Francisco · Remittance

BTCJam
Peer to Peer Bitcoin Lending.
Silicon Valley · Finance Technology

ChangeCoin
Micropayment Infrastructure for th...
San Francisco · Bitcoin

Gem
Simple and secure Bitcoin platfor...
Venice · Developer APIs

Coinsetter
Wall Street-based high performa...
New York City · Trading

Localbitcoins
Run bitcoin exchange anywhere
Helsinki · Financial Exchanges

SFOX
Bitcoin Trading Platform
San Francisco · Bitcoin

Kraken
FOREX for Bitcoin, Ripple and ot...
San Francisco · Banking

GoCoin
Digital currency payments platfor...
Singapore · Online Shopping

LedgerX
Financial technology products for...
New York City · Finance Technology

MaiCoin
Taiwan · Financial Exchanges

Korbit
Korea's leading bitcoin exchange...
Seoul · Financial Exchanges

BitAccess
Bitcoin ATM
Mountain View · Billing

Bold
Instant access to digital currency
San Francisco · Banking

Coinalytics
Real-time Analytics for Bitcoin
Mountain View · Big Data Analytics

Bonafide
Use Bitcoin without getting coined
Mountain View · Personal Finance

Tealet
Online Farmer's Market for Tea o...
Las Vegas · Tea

CrowdCurity
Crowdsourced Web Security
Silicon Valley · Crowdsourcing

CoinJar
Advancing consumer finance wit...
Melbourne · Bitcoin

GogoCoin
The easiest way to buy bitcoin
Mountain View · Mobile Payments

Robocoin
The World's Largest Bitcoin ATM ...

BitPagos
The Future of Payments
Palo Alto · Emerging Markets

SNAPCARD
The easiest way to use your digit...
San Francisco · Bitcoin

PayStand
Next-gen online store & payment ...
San Francisco · SaaS

BitGo
Securing the World's Bitcoin
Palo Alto · Bitcoin

Neuroware.io
Bitcoin Framework & API #500str...
London · Open Source

Secure Asset Exchange
Smart Contracts for Realtime Re...
New York City · Blockchains

Gliph
The world's easiest way to send ...
San Francisco · Social Media Platforms

37coins
Bitcoin Wallet for Everyone
Sunnyvale · Remittance

expresscoin
Buy Bitcoin. Fast, Easy, and Safe.
Santa Monica · Bitcoin

Elliptic
Digital Currency Services
London · Finance Technology

angel.co/bitcoin

Startups II

Coinmail
Snapchat for Bitcoin
Rochester · Messaging

Bex
Bitcoin Exchange in a Box
Vancouver · Financial Exchanges

Monetsu
A next generation crypto-currency ...
San Francisco · Startups

Koinify
The Cryptofunding Platform
Palo Alto · Crowdfunding

BitWall
Content monetization platform
San Francisco · Bitcoin

Wow Such Business
Microtransactions that actually w...
Arcata · Dogecoin

Blade
Bitcoin Payments
New York City · Bitcoin

VerifyBTC
Identity verification platform for Bit...
San Francisco · Identity Management

QuickCoin
Social Bitcoin Wallet
San Francisco · Finance Technology

Volabit (Coincove)
Bitcoin-based financial services f...
Puerto Vallarta · Loans

Safello
Bitcoin evangelism
Stockholm · None

Stanford Bitcoin Group
Research into Bitcoin theory and ...
Stanford · Bitcoin

ZenBox
Turnkey Bitcoin ATM Distribution ...
Santa Monica · Distribution

Mastercoin Foundation
The Protocol Layer On Top of The...
Austin · Open Source

LibraTax
Accounting and tax software for B...
San Francisco · Finance Technology

Hedgy
Smart derivative contracts on the ...
Silicon Valley · Finance Technology

Bitso
Mexico's First Bitcoin Exchange
Puebla · Bitcoin

Monegraph
A Bitcoin for Digital Art
New York City · Bitcoin

HashPlex
HashPlex is the world's first hosti...
Seattle · Bitcoin

Bitbond
Global bitcoin peer-to-peer lending
Berlin · Loans

Honeybadgr
Building Teams at Bitcoin Startups
San Francisco · Startups

CoinHako
Leading Bitcoin wallet service in ...
Singapore · Finance Technology

Blockchain
The most used Bitcoin platform i...
Mobile Payments

coins.ph
Bringing banking services to the ...
Manila · Mobile Payments

HolyTransaction
Universal Multicurrency Wallet
Sunnyvale · Personal Finance

SolidX Partners Inc.
Institutional Access to Bitcoin an...
New York City · Digital Currency

CoinMKT
Trade Bitcoin & Other Cryptocurre...
Santa Monica · Trading

Coinmotion
The Coinbase for Europe, before ...
Helsinki · Bitcoin

BitBox
Changing the meaning of money ...
Ann Arbor · Finance Technology

Palarin
Coinbase of the Philippines
San Francisco · Personal Finance

AlphaPoint
Enterprise Bitcoin exchange soft...
New York City · Financial Exchanges

BlockCypher
Amazon Web Services for Bitcoin
San Mateo · Cloud Infrastructure

Leetcoin
Competitive gaming for bitcoins.
Las Vegas · Video Game Tournaments

API Network
Singly - Open Sourced
Austin · Developer APIs

HashTrust
Crypto Contracts Made Easy
Silicon Valley · Bitcoin

Waxis
Powerful digital currencies tradin...
Delaware · Bitcoin Exchange

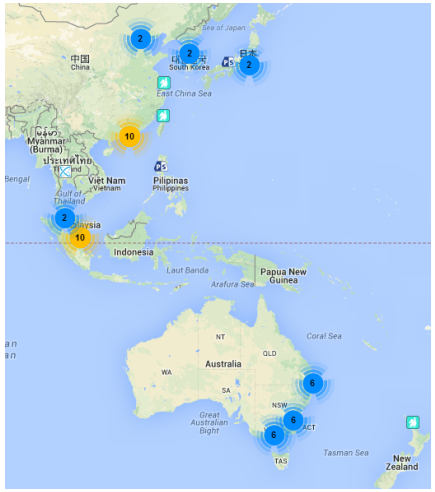
Hellobit
Cash remittance powered by the ...
San Francisco · Mobile Payments

Purse
Making Bitcoin Useful
San Francisco · Gift Card

InterWallet
Next Generation Bitcoin ATM Platf...
Santa Monica · Transaction Processing

BubbleCoin
Bitcoin news, culture and events ...
Silicon Valley · Bitcoin

ATMs



BTC Coin ATM Radar

Bank integration

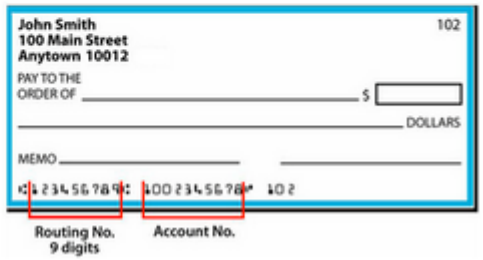
coinbase

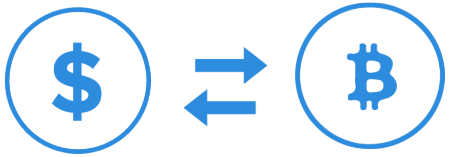
fidor BANK

Link A Bank Account

Routing number: bottom left of check, 9 digits

Account number: bottom center of check

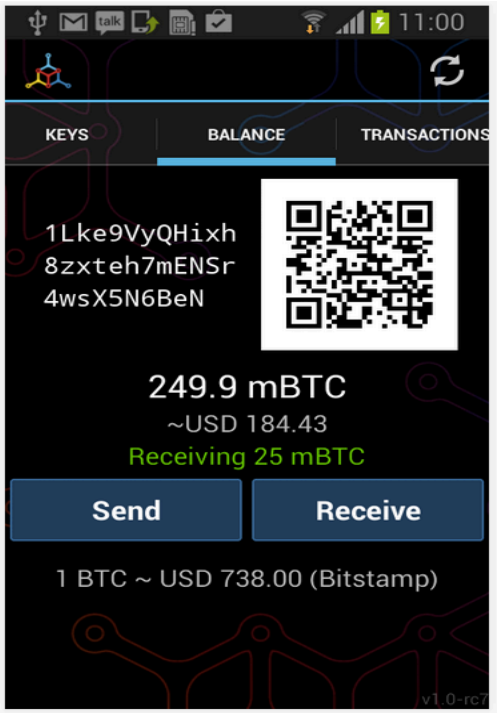




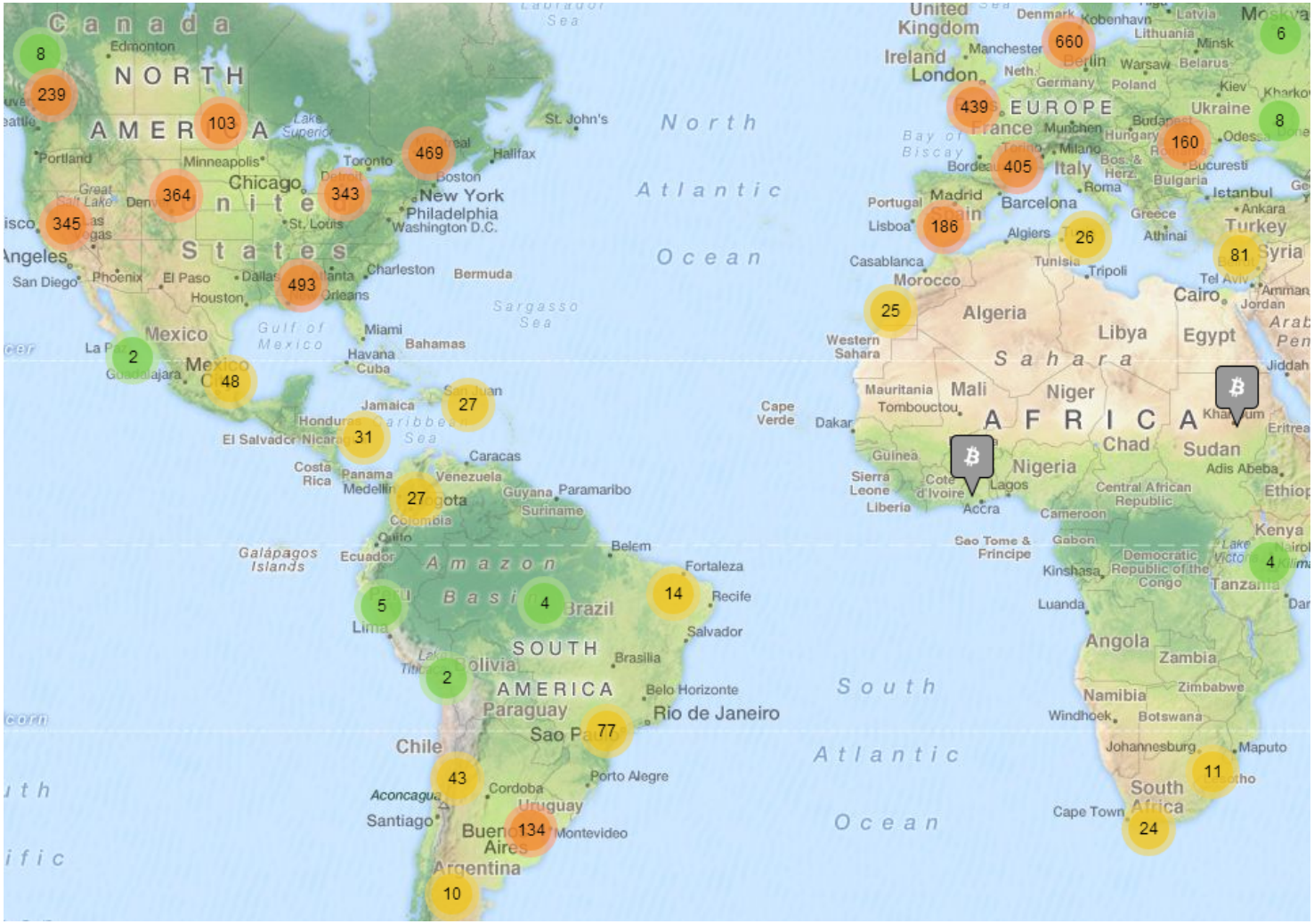
Mobile


00:57
Bitcoin Wallet
Your Bitcoin Address:
mx6WWrWgYHhH
2011/08/01 → darkly -0.0205
2011/08/01 → darkly -0.0105
This is entirely experimental. Use at your own risk!
Read the safety notes.


EE 5:53 PM 60%
BLOCKCHAIN wallet
0.1019 BTC
3 Transactions
RECEIVED Mon 8 September 2014 - 05:53 PM
12zBnfxqXE24LcAm4kH66bYtSQLSfqtsAh
Unconfirmed
0.1 BTC
SENT Wed 3 September 2014 - 02:13 PM
1D4QL5PQKPzKEcqVfeCvpcjCpftARor9wL
-0.0011 BTC
RECEIVED Sat 16 August 2014 - 08:22 AM
York

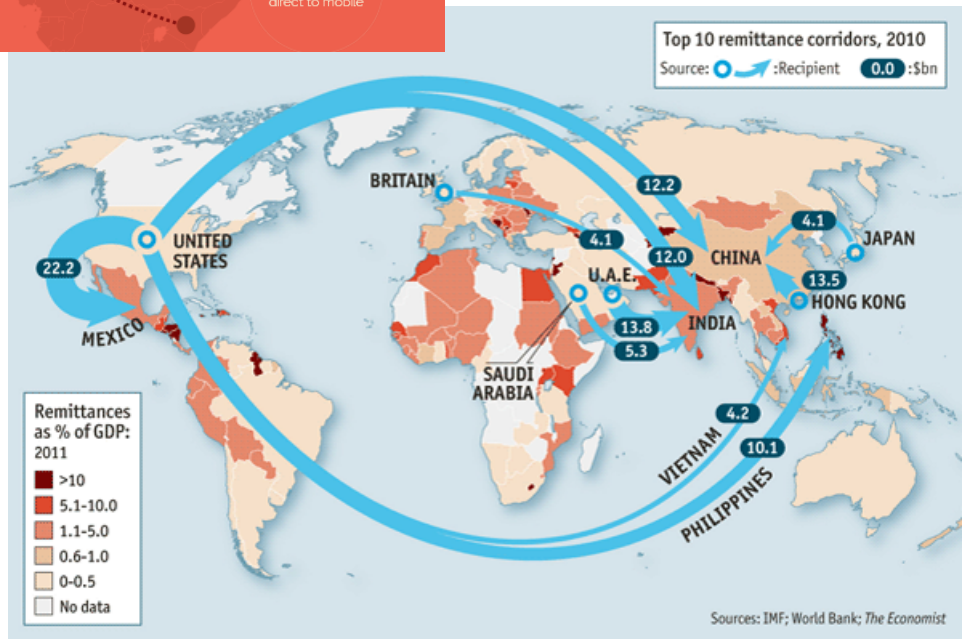

11:00
KEYS
BALANCE
TRANSACTIONS
1Lke9VyQHixh
8zxteh7mENSr
4wsX5N6BeN
249.9 mBTC
~USD 184.43
Receiving 25 mBTC
Send
Receive
1 BTC ~ USD 738.00 (Bitstamp)

Main Street



http://coinmap.org/

Remittances



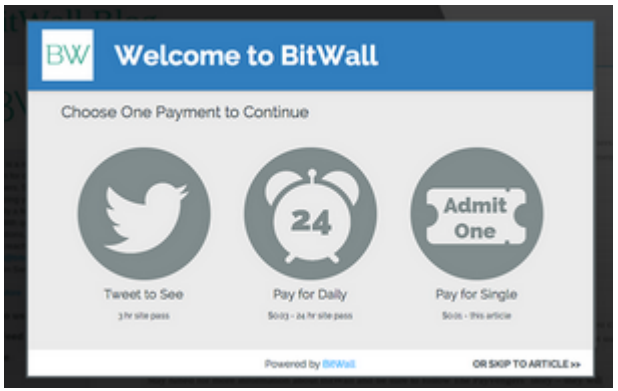
Philanthropy

Bitcoin Accepting Charities

- **Group B Strep International** (Funded in two parts – Part 1 / Pa
- **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**

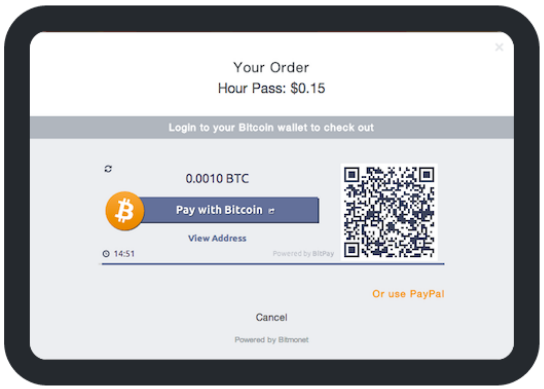
Roger Ver Gives FEE Highest-Valued Known Bitcoin Donation, Worth About $1 Million

Micropayments



BITMONET

Meet Bitmonet, the better way to monetize your content.



Satoshi box

1. Upload

2. Share

3. Profit!

Coin Lock

Sell Anything, Make Bitcoin.
The definitive content platform.

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

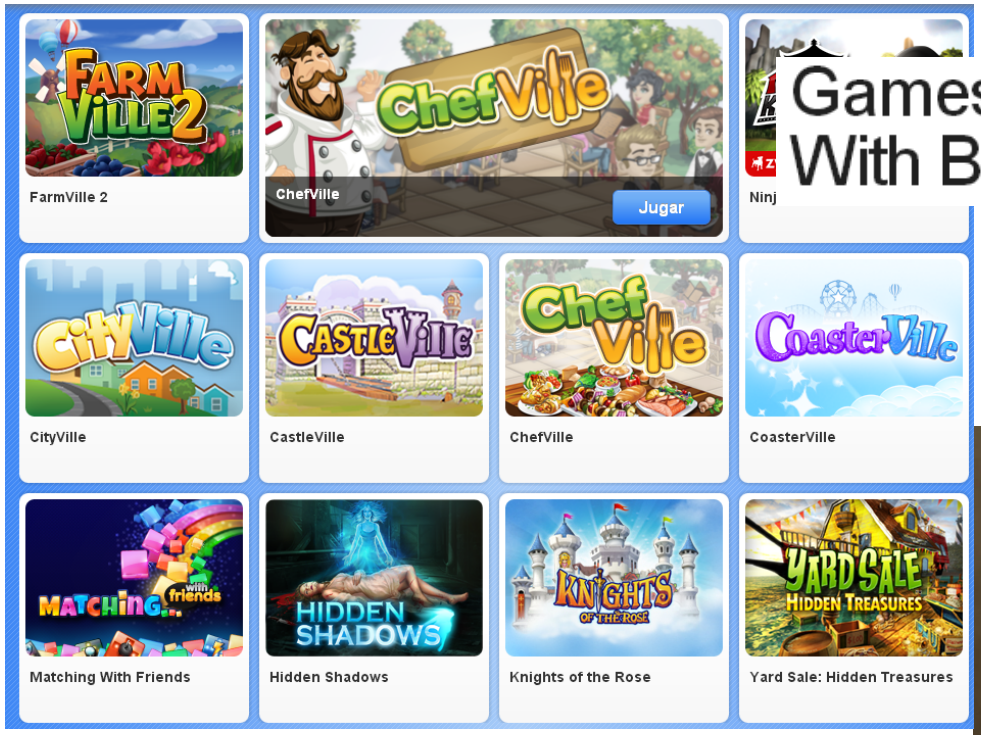
Bitcoin has been big news this year, and for good reason. Although crypto-currencies have been around for some time, only **Bitcoin** has achieved significant scale. This new entrant in the world of payments has people asking lots of questions – including how and if PayPal will decide to work with **Bitcoin**.

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.

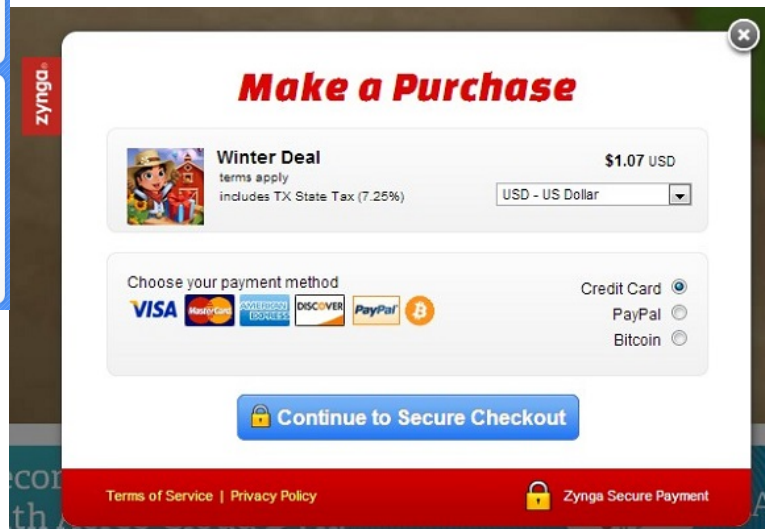
Today we are announcing PayPal's next step in helping merchants accept **Bitcoin** payments. PayPal has entered into agreements with leading **Bitcoin** payment processors BitPay, Coinbase and GoCoin. Starting today, these agreements let PayPal digital goods merchants accept **Bitcoin** with a simple 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

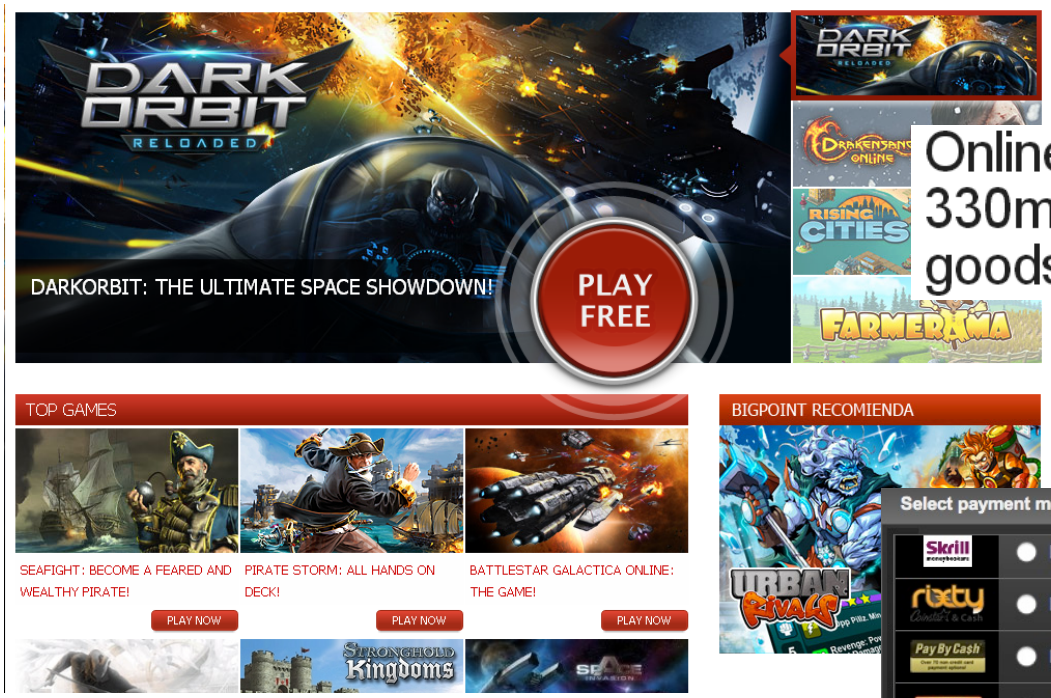


Games Giant Zynga Starts Playing With Bitcoin

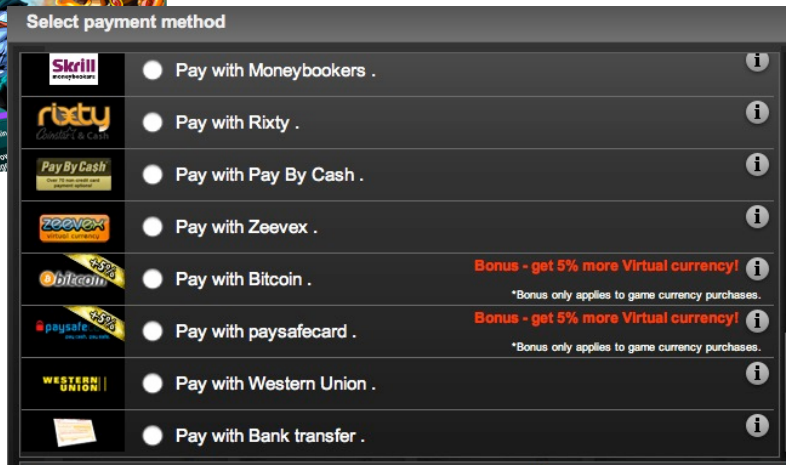


Bigpoint Games

BIGPOINT.COM
free to play



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



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

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.

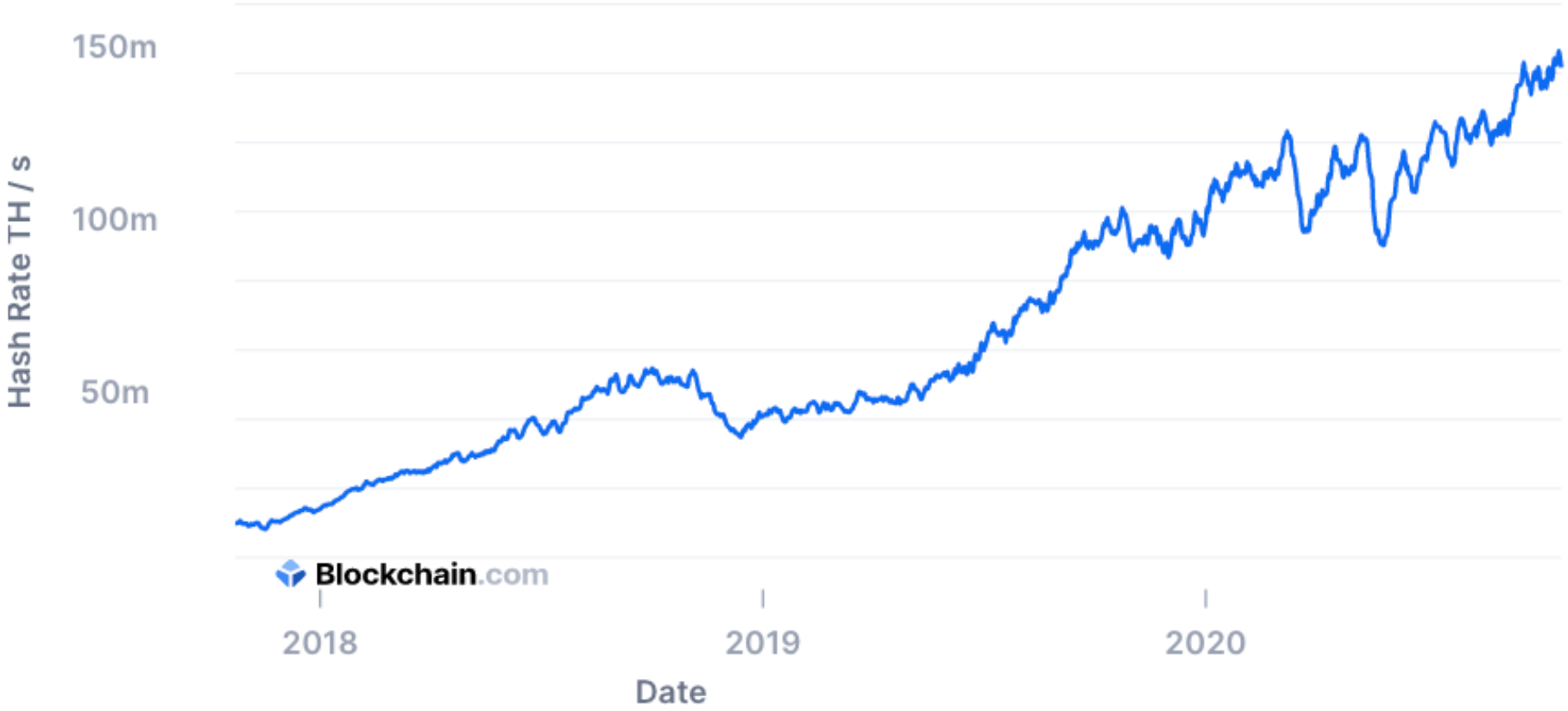
Impossibile visualizzare l'immagine. La memoria del computer potrebbe essere insufficiente per aprire l'immagine oppure l'immagine potrebbe essere danneggiata. Riavviare il computer e aprire di nuovo il file. Se viene visualizzata di nuovo la x rossa, potrebbe essere necessario eliminare l'immagine e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

BITCOIN: statistics

www.blockchain.com/en/stats

- Value of Bitcoin
  - October 2020 2017 2016
  - US $ 11000 1100 400

BITCOIN: total hash rate



BITCOIN: miner reward

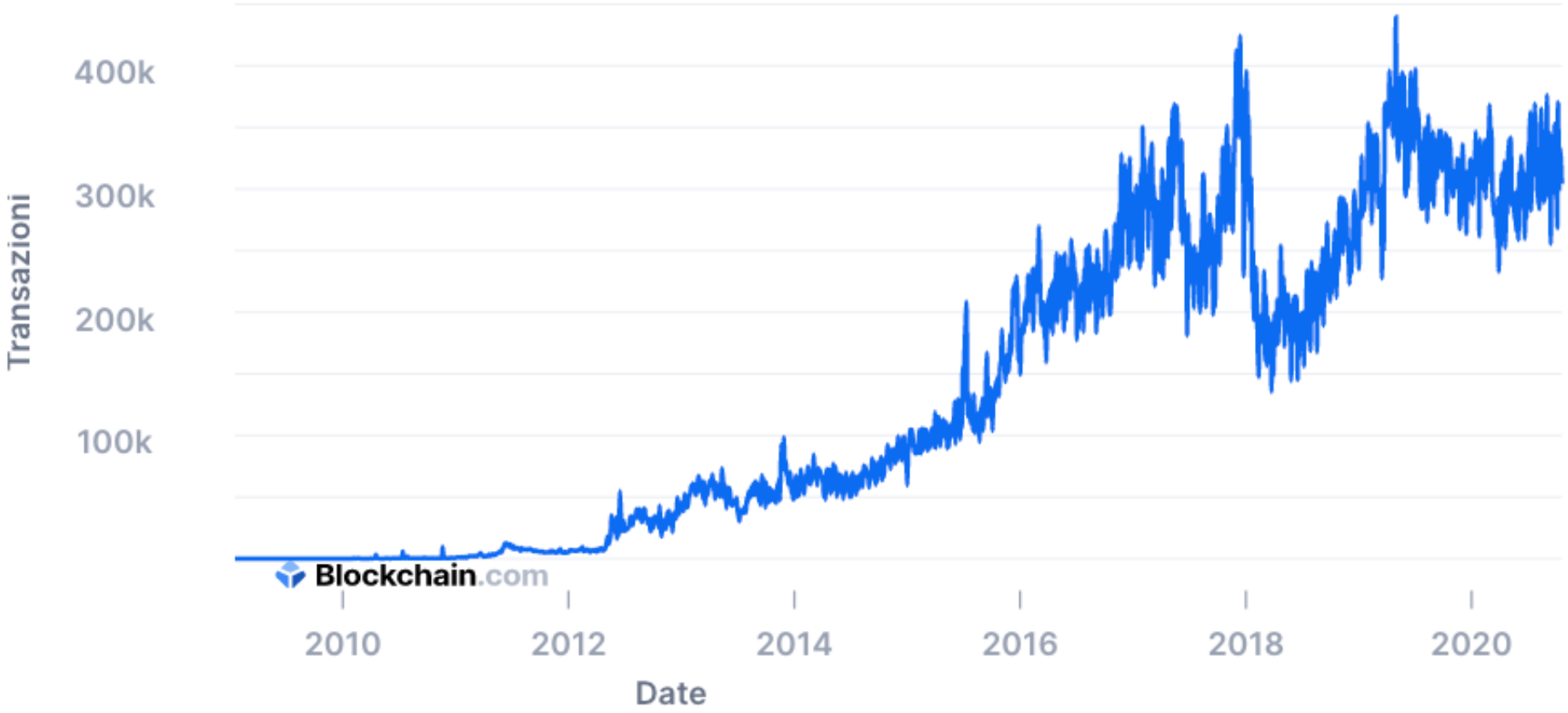
- Miner reward (in US $): why there was a big increase and then a drop in 2018

BITCOIN: puzzle difficulty

- Expected number of hash to propose a block

BITCOIN: number of transactions

- Last few years no significant increase



BITCOIN: number of transactions

- Last few years no significant increase