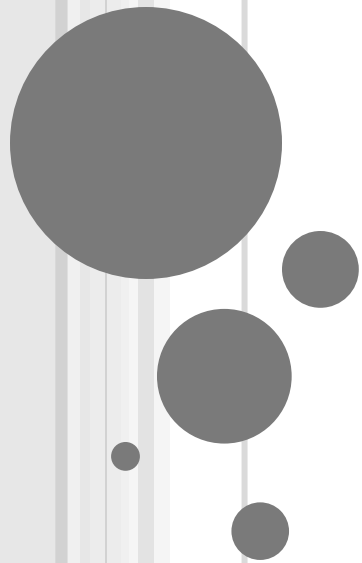


DIGITAL CURRENCIES

Ghada Almashaqbeh
Columbia

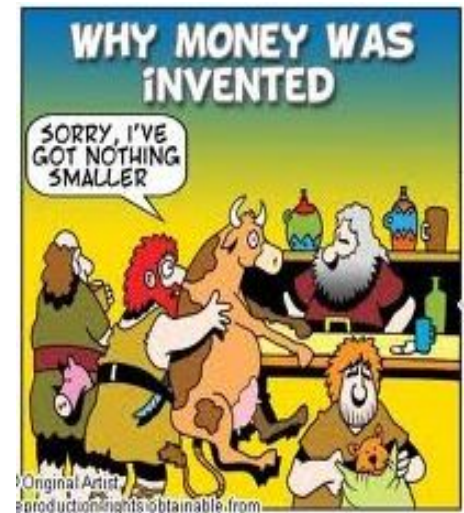


OUTLINE

- Electronic money.
 - Evolution,
 - Types,
 - Digital wallets.
- Cryptocurrencies.
 - Bitcoin.
- Security issues.

REAL MONEY \$\$\$

- Market emerged phenomenon.
- Main purpose is providing a medium of exchange to avoid pure barter systems.
- International rules to regulate money flow.
- Acceptable, trusted, and strong belief in its value.
- Are we satisfied with that in the digital world we are living in?



ARE WE SATISFIED?

In the digital world we want:

- Digital / virtual market.
- Digital / virtual money.
- Digital / virtual contracts, checks, accounts, etc.

ELECTRONIC MONEY

- Also called e-currency, e-money...
- Many forms:
 - Credit/Debit/Gift cards.
 - Network money: applications that allow money flow over the Internet.
 - Electronic banks-based transactions: deposit, withdraw, transfer, etc.
 - Digital currency (or cryptocurrency).

TYPES OF ELECTRONIC MONEY I

- Based on the underlying infrastructure:
 - **Centralized:** a trusted entity is involved in all transactions.
 - E.g.: Paypal.
 - **Decentralized:** No centralized entity exists, money creation and flow control are done in a fully distributed way.
 - E.g.: Bitcoin

TYPES OF ELECTRONIC MONEY II

- Based on transaction flexibility:
 - **Soft:**
 - Transactions can be reversed, refunded, etc.
 - E.g.: Credit card payments.
 - **Hard:**
 - Transactions cannot be reversed, a new transaction need to be issued to overwrite an undesired state change.
 - E.g.: Wire transfer, Bitcoin.

HISTORY I

- **DigiCash:**
 - Founded by David Chaum in 1990.
 - Based on his work on blind digital signatures to enable untraceable (anonymous) payments.
 - Declared bankruptcy in 1998 and was sold to eCash.
- **Fast Virtual:**
 - Successor of DigiCash.
 - Restricted money flow between individuals and merchants.
 - Credit card numbers are registered with First Virtual by phone.

HISTORY II

- **Paypal:**
 - Replaced Fast Virtual in 1998.
 - An online bank with higher flexibility than traditional ones.
- **WebMoney:**
 - Another online bank established in 1998.
- **E-gold:**
 - Launched online in 1996 but fully effective in 2000, stayed until 2009.
 - Opened accounts are backed by gold or any other precious metal.
 - The first successful digital currency system.
- **Bitcoin:** The focus of this talk.

DIGITAL WALLETS

- All your money is electronic now; cards, online bank accounts, etc.
- But, are not you bothered by holding cards in a Wallet?
- Digital wallets provide an effective solution. Examples:
 - Google Wallet.
 - Apple Passbook.
 - Apple Pay.
 - Paypal.
 - Square wallet.

DIGITAL WALLET TYPES

- Several forms, the most widely used are:
 - **Server side wallet:** payment information are stored on the server side. Auto fill for the check out forms, usernames/passwords to authenticate users.
 - **Client side wallet:** install specific applications that enable storing cards information on the client side.
- To enable compatibility, the retailers websites and wallet application should use the Electronic Commerce Modeling Language to set up the checkout forms.

THE ROAD AHEAD

- Most of the previous discussion is related to REAL money stored in an electronic form.
 - Credit cards, debit cards, digital wallets, etc.
- However, these are centralized.
 - You are being watched by a centralized bank or payment company.
- Still seeking for a new form of money, a currency for the digital world, a decentralized one.

CRYPTOCURRENCIES

- The use of cryptographic primitives to secure money creation and flow.
- Bitcoin is considered the first successful implementation of decentralized cryptocurrency.
 - Digital currency history is defined now as before and after Bitcoin.
- Other examples include Litecoin, Ripple, Dogecoin, Monero, Nxt, and many others.
- We will mainly focus on Bitcoin for the rest of the talk.

BITCOIN



BITCOIN

“A type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” - **European Central Bank.**

HISTORY

- Satoshi Nakamoto posted a paper online in 2008: “Bitcoin: A Peer-to-Peer Electronic Cash System”.
 - The paper described a distributed e-currency not backed by any government or any form of fiat currency.
- The name is pseudonym for a single person or a group of people who invented Bitcoin.
 - Satoshi is associated with certain public keys, was active till 2010.
- The system went alive in January 2009.

BITCOIN AT A GLANCE

- Powered by a peer-to-peer network.
- No real identities, Bitcoin addresses are used instead.
- Utilize cryptographic primitives and data structures:
 - Hash functions.
 - Digital signatures.
 - Hash pointers, hash linked lists, hash puzzles.
- Simulate a distributed banking system with:
 - a public ledger logging every transaction,
 - miners verifying these transactions and recording them on the ledger.

DECENTRALIZATION IN BITCOIN

- **Open access Peer to peer network:** anybody can join and leave at anytime.
- **Mining:** open to anyone but requires high computation power.
- **Updates on the used software:** open to the community through an organized proposal process.
- **Maintaining the public ledger:** done by all miners within the network.
- **Transactions:** announced publicly to everyone.
- **Creating new coins:** miners can do that based on their work, no central authority.

BITCOIN ADDRESSES

- To participate, any party needs only a public address.
 - 26 - 35 characters long.
 - starts with 1 or 3 based on whether it is a normal address or a script hash.

• E.g:

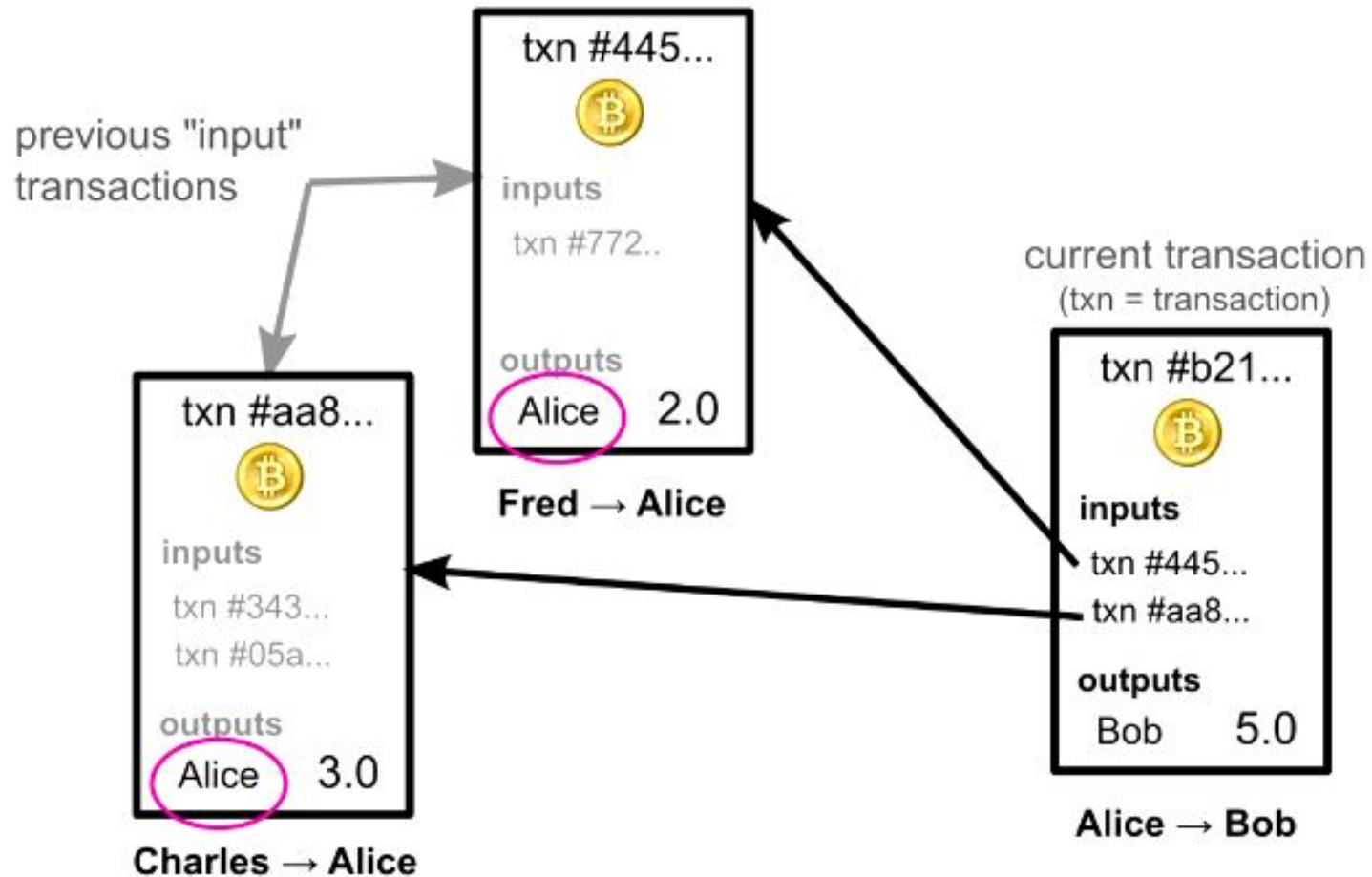
3B74t1WpEZ73CNmQviecbaciWRnqRhW NLy

- No "O","0","I" and "l"
- It is a 160-bit hash of the public key associated with the private key a party uses to sign its transactions.
- The private key is needed to spend the coins.
 - Losing a private key means losing the coins locked under the public key (aka address) associated with this private key.

BITCOIN TRANSACTIONS

- A basic currency transfer transaction is a byte structure containing:
 - A set of inputs: unspent transactions owned by the transaction sender.
 - A set of outputs: list of bitcoin addresses, which are the destinations of the input coins.
 - A signature(s) to authorize the transaction and prove its integrity.
- Other useful transaction type is pay to script hash (P2SH).
- The sender broadcasts the transaction over the network.
 - It is confirmed once it is included in a block on the blockchain buried under at least 6 blocks.

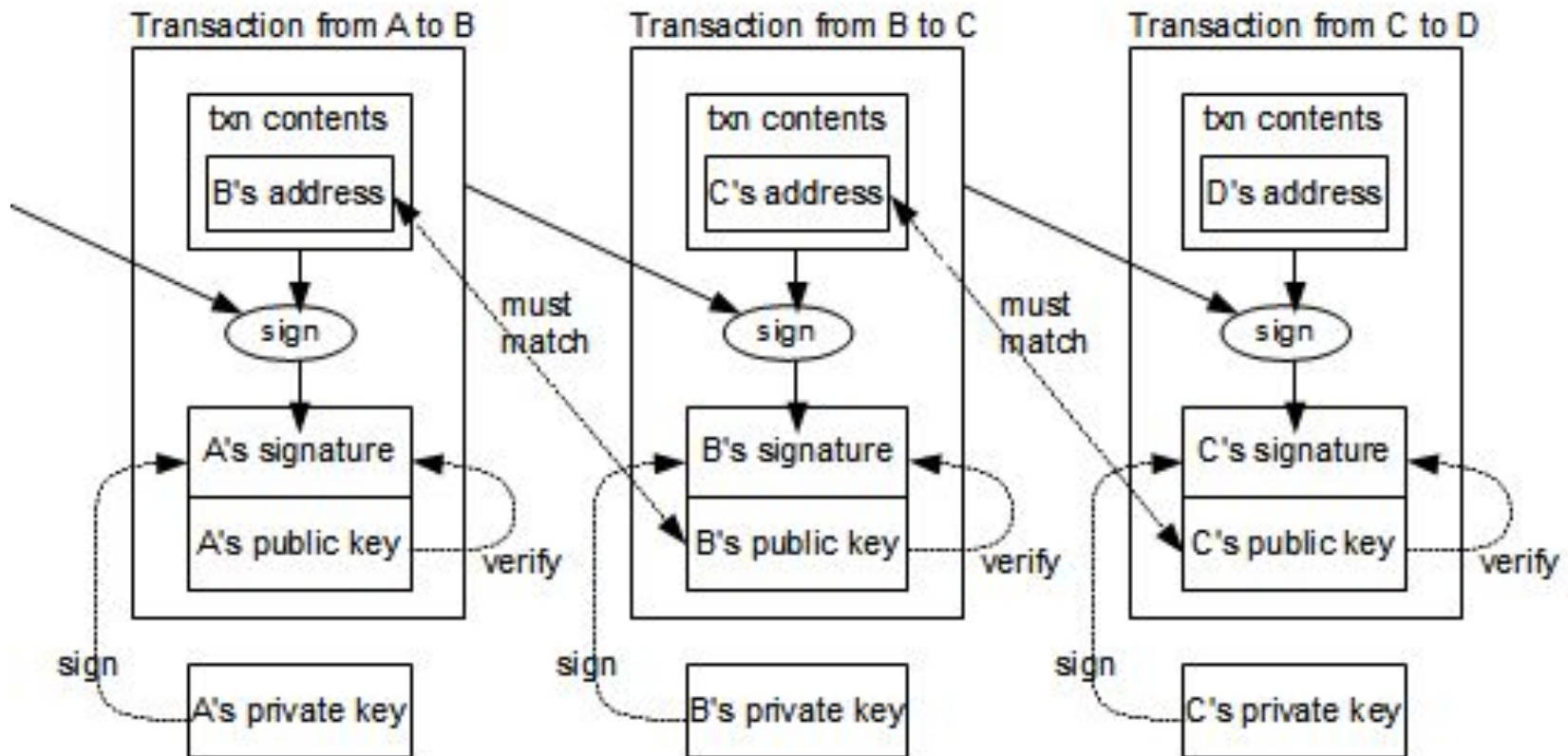
THE BIG PICTURE



Source:

<http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html>

DEEPER LOOK



Source:

<http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html>

AN INTERESTING ASPECT

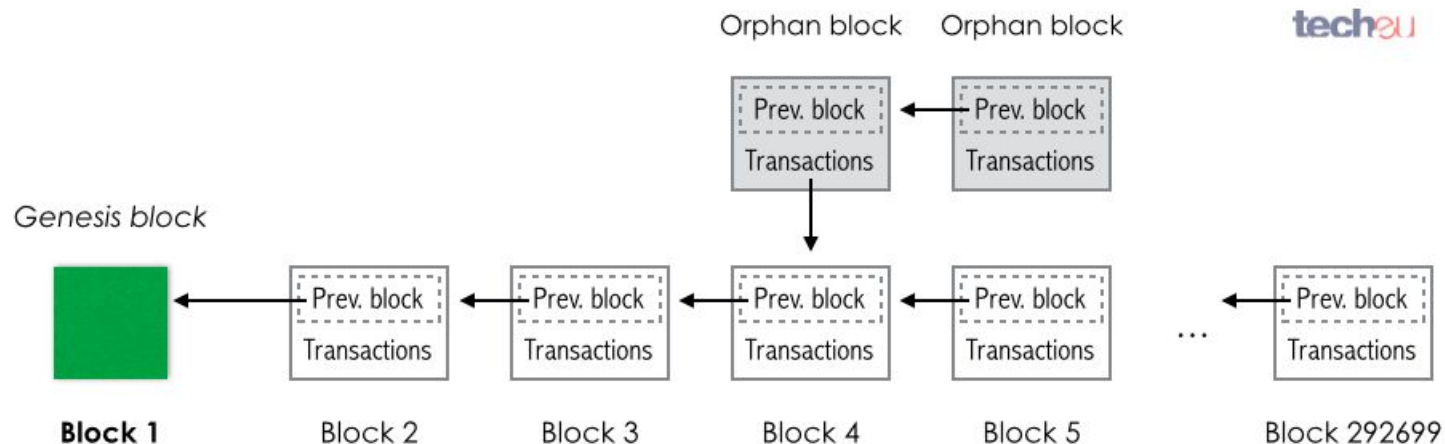
- No change!
- The total input value goes to the output.
 - Like paying \$2 cookie with a \$100 bill.
- If the output amount is less than the input, the difference is considered a transaction fee that the miner collects.

Solution??

- Direct the change to an address that you own, i.e., provide an additional output that you control.

THE PUBLIC LEDGER - BLOCKCHAIN

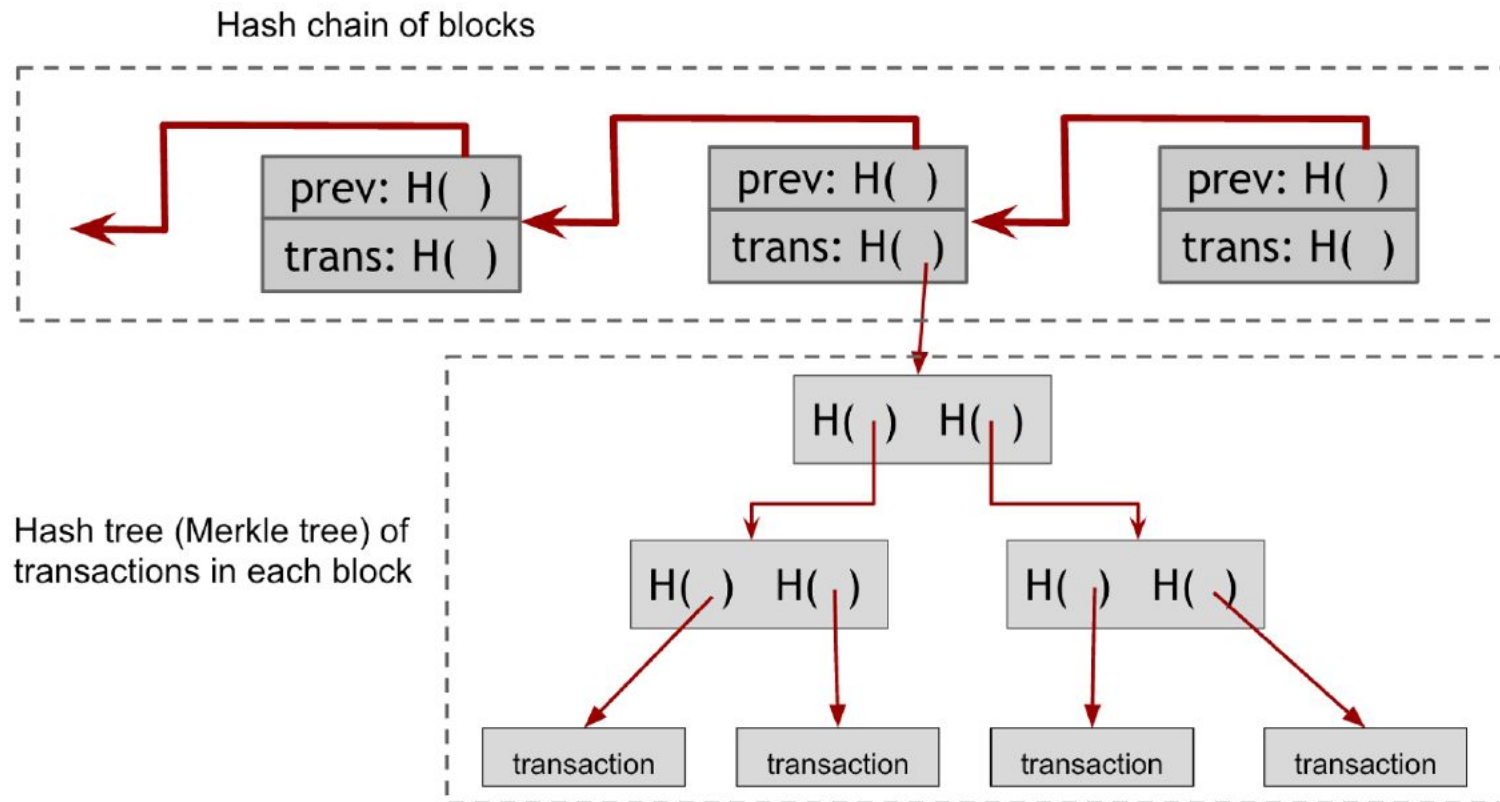
- Public log of all transactions issued so far.
 - Each block in this chain is a page in the ledger.
- Miners work on maintaining and extending this chain.
- The first block is called the *Genesis block*.



EXTENDING THE BLOCKCHAIN

- Upon receiving a new transaction, a miner does the following:
 - Verify the signature(s) on the transaction and check its format,
 - Check that the input transactions are unspent ones,
 - Add the transaction to the pool of pending transactions,
- This pool is used to form a new candidate block.
- The header of this block contains a hash pointer to the previous block in the chain.
- A miner then tries to solve a proof of work puzzle over the new block.
 - Once the solution is found, the miner announces the new block to the network.

CLOSER LOOK



Two hash structures are included in a block header:

- A hash chain or linked list to connect all blocks with each other.
- A hash tree inside each block that includes all transactions in that block.

IMPLICIT CONSENSUS IS THE KEY IDEA

- Other miners in the network can either accept or reject the new block:
 - Accept by including it in the chain and start working on top of this new block.
 - Reject by ignoring the new block and continue working on the older chain.
- **Remember:** Bitcoin network is not perfect, propagation delays and connectivity issues, nodes may crash at any point of time.
- **Result:** the blockchain may have multiple branches, called forks, the longer is the better
 - Since it means more work is needed by an attacker to rewrite the blockchain.

ROUND LEADERS

- Each miner works on producing a new block that has specific pattern in its hash.
- At each round the winner miner is the one who solves the PoW puzzle and has its block adopted by the majority of the network.
 - This miner is called a round leader.
 - This process results in a random selection of the round leader.
- On average a new block is mined every 10 minutes.

PROOF OF WORK I

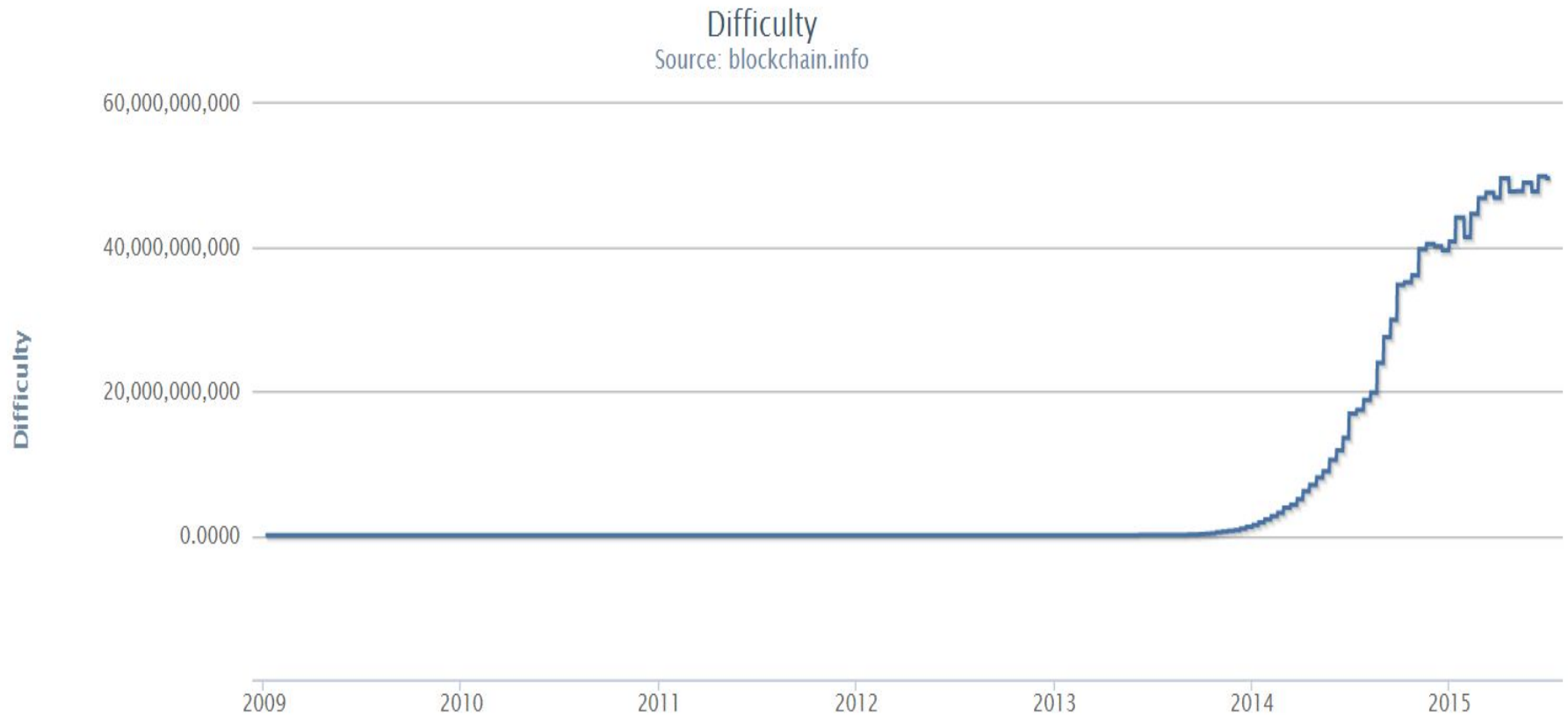
$$H(\text{new block header}) < \text{network difficulty}$$

- For secure hash functions, the only way to solve the puzzle is through a brute force of the input space (i.e., nonces) until the desired digest is found.
- Verification is very easy, the winner should announce the nonce as part of the new block.
 - Other miners can verify the correctness of the solution by a single hash operation.

PROOF OF WORK II

- The target value or network difficulty is not a fixed one.
 - The network nodes readjust the target every 2016 block (roughly every two weeks).
 - This is done to maintain the block generation rate somehow fixed.
- Purpose of target adjustment:
 - More powerful miners may join the network.
 - They will be able to solve the puzzle faster.
 - This will result in mining blocks at a much faster rate.
 - May lead to security issues like the ability of rewriting the blockchain and other system instability issues.

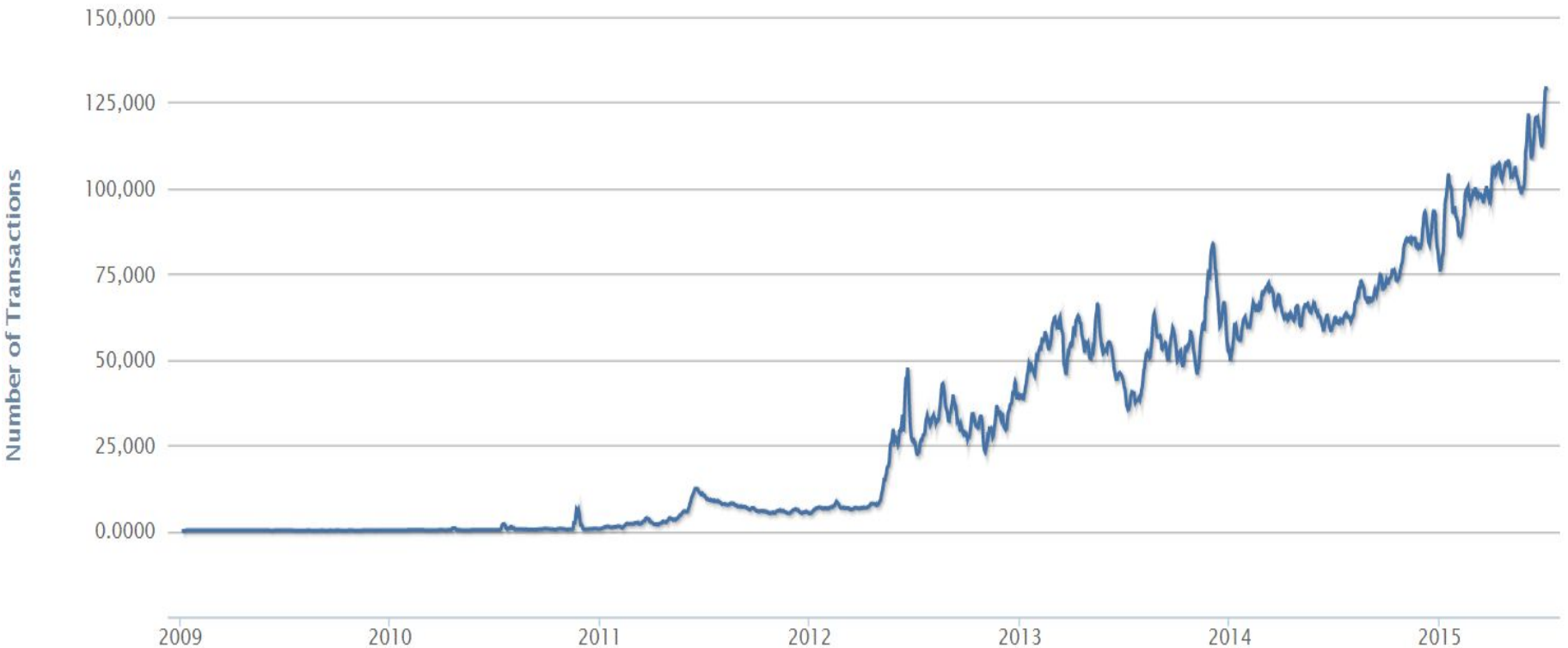
NETWORK DIFFICULTY



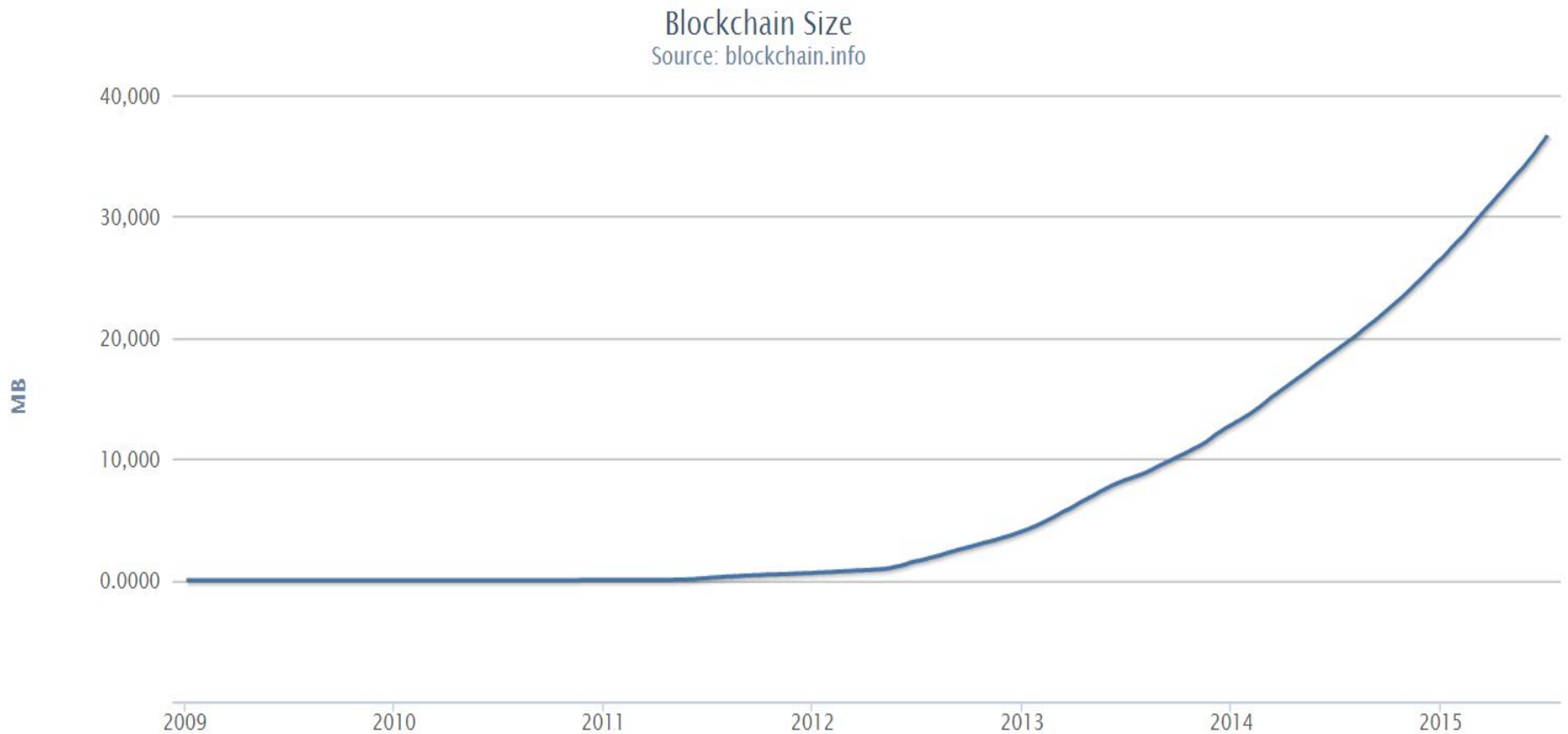
AVERAGE NUMBER OF TXS PER DAY

Number Of transactions Per Day

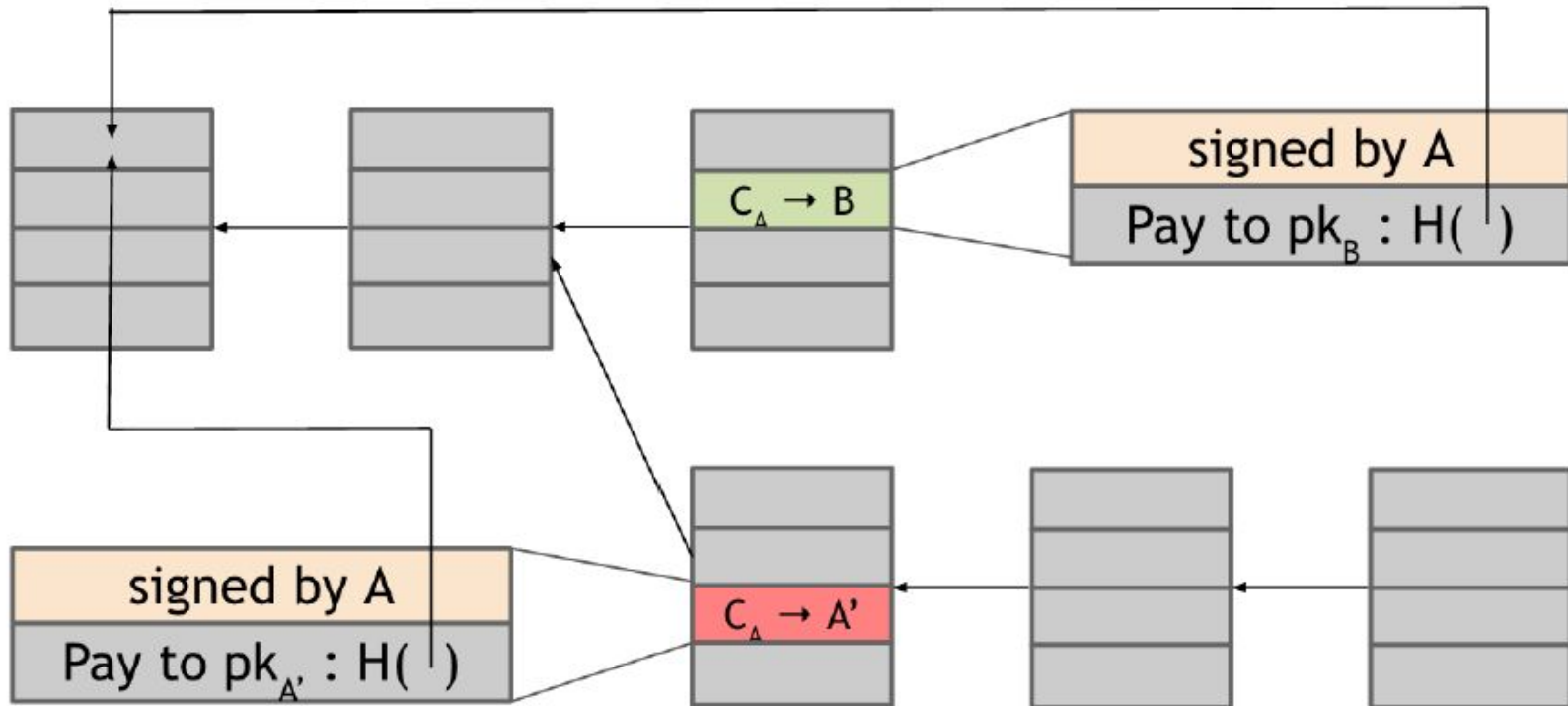
Source: blockchain.info



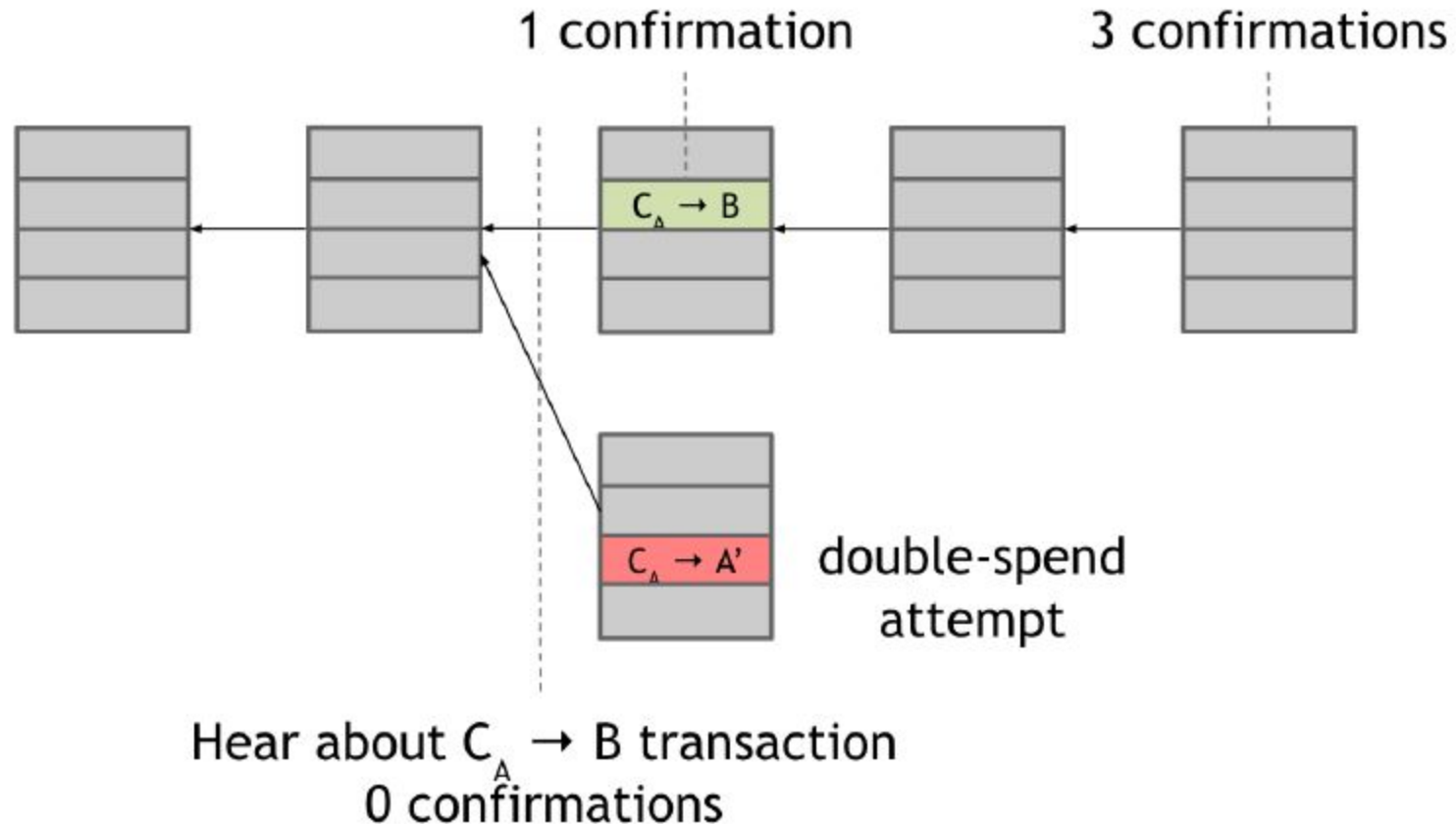
BLOCKCHAIN SIZE



DOUBLE SPENDING ATTACK



RECEIVER VIEW



The merchant should wait the transaction till it get confirmed and then accept the payment to deliver the service/goods.

VALIDATING TRANSACTIONS

- Two types of nodes
 - **Fully validating nodes or miners:**
 - Maintain a full copy of the blockchain.
 - Validate all transactions they receive
 - Work on extending the chain, and hence, mint new currency.
 - **Lightweight nodes or clients:**
 - Also called thin clients or simple payment verification clients.
 - The vast majority of Bitcoin nodes are lightweight ones.
 - Do not store the whole blockchain, only specific parts to verify the transactions they care about.

THE MINERS

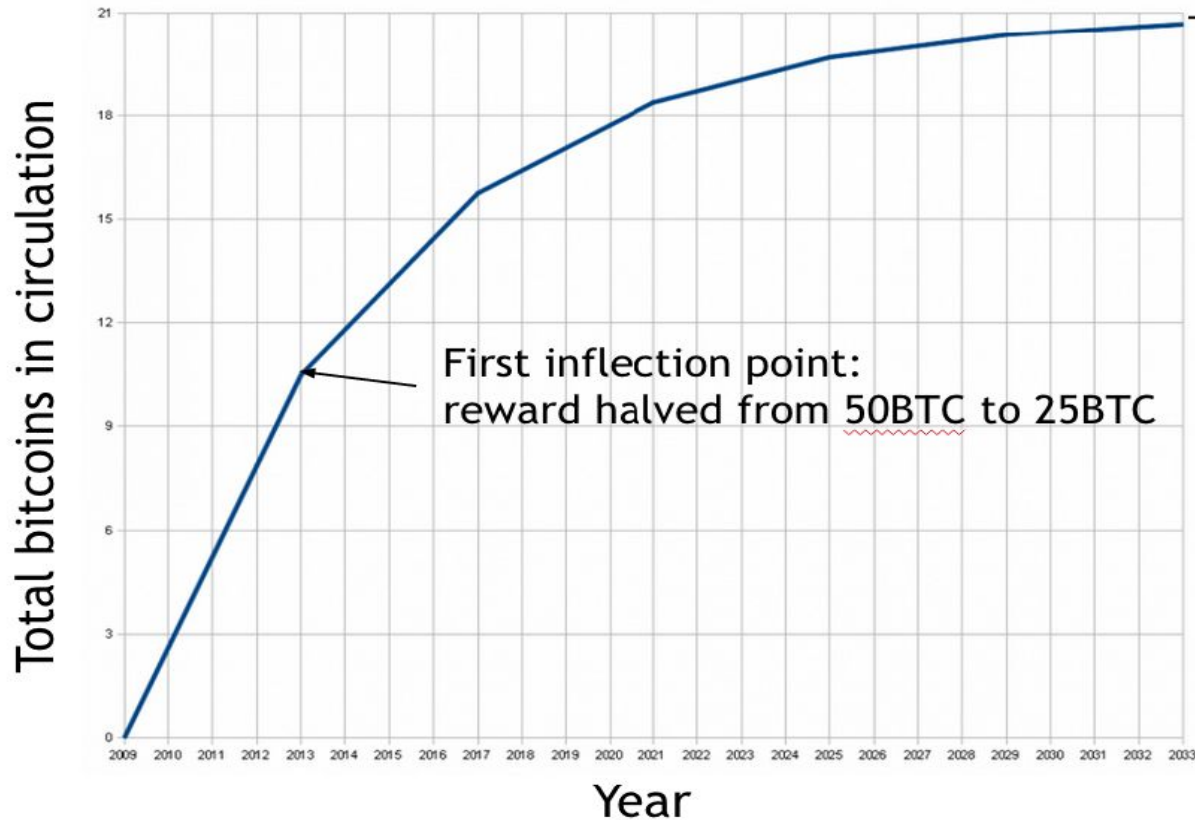
- Usually, huge powerful machine farms.



MINING FEES

- Miners mint new coins as a reward for their work on mining new blocks.
- Each miner includes a special transaction directing the new minted coins to itself.
 - Called a coinbase transaction.
- Currently the incentive is 25 BTC and it halves every four years.

BITCOIN CIRCULATION



- The cap is 21 million BTC.
- This will be reached around 2040.

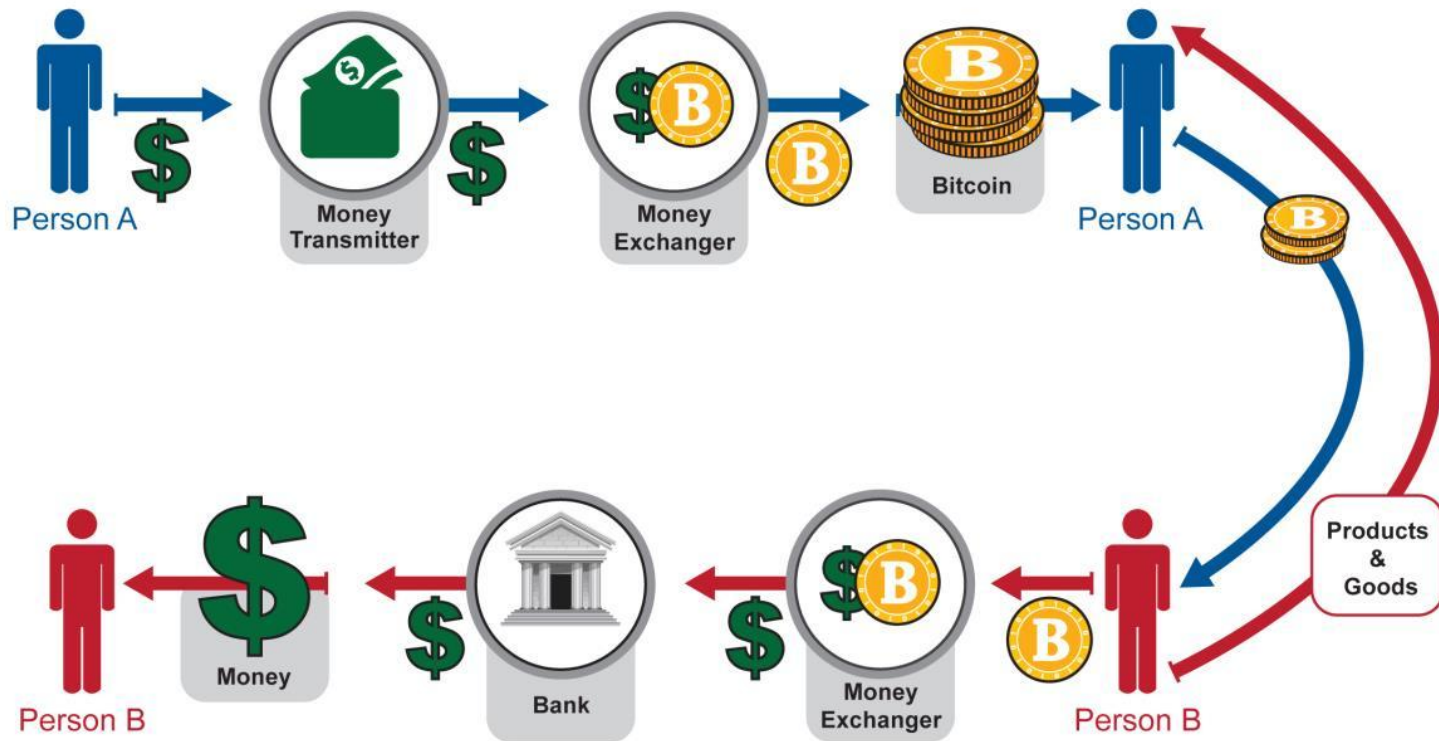
TRANSACTIONS FEES

- Tips for block creators.
 - Considered the second income source for miners.
- The issuer of a transaction selects to include a transaction fee that goes to the miner who adds this transaction to the blockchain.
 - Done by having the input Bitcoin value larger than the output by the tip amount.
- Voluntary but a higher fee motivates the miner to record a transaction faster on the blockchain.

SOME USER RESPONSIBILITIES

















- Keep the set of private keys safe.
 - Remember without the private keys one cannot spend her/his coins.
- This involves choosing a secure bitcoin wallet.
- Change the public key periodically.
 - Contributes in breaking the linkability between the transactions, and thus, promote anonymity (as possible).
 - Can be done automatically by the wallet.

BITCOIN AND FIAT CURRENCY



Source: <http://www.fincen.gov/>

EXCHANGE RATE

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$ 3,850,131,053	\$ 268.29	14,350,525 BTC	\$ 44,495,400	2.25 %	
2	 Ripple	\$ 319,458,846	\$ 0.010012	31,908,551,587 XRP *	\$ 871,949	-7.01 %	
3	 Litecoin	\$ 195,976,812	\$ 4.83	40,533,704 LTC	\$ 14,893,000	16.81 %	
4	 Dogecoin	\$ 19,124,985	\$ 0.000191	100,067,420,606 DOGE	\$ 266,062	-1.15 %	
5	 Dash	\$ 17,054,029	\$ 3.08	5,538,623 DASH	\$ 104,201	-1.00 %	
6	 BitShares	\$ 15,991,269	\$ 0.006366	2,511,953,117 BTS *	\$ 64,699	-4.87 %	
7	 Stellar	\$ 15,583,351	\$ 0.003221	4,837,356,606 STR *	\$ 34,289	-1.07 %	
8	 Nxt	\$ 12,923,062	\$ 0.012923	999,997,096 NXT *	\$ 36,536	-1.00 %	

Source: www.coinmarketcap.com/

WANT TO USE BITCOIN?



- Install a wallet.
- Buy Bitcoin.



BITSTAMP



- Start transacting 😊

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



BITCOIN APPLICATIONS

- Beyond money transfer, the Blockchain and Cryptocurrencies can be utilized for:
 - Data timestamping, copyrights, ownership proofs, etc.
 - Escrow construction.
 - Ensure fairness in secure multi-party computation.
 - Lottery protocols.
 - And many more ...

SECURITY THREATS

- 51% attack.
 - Centralized mining pools.
- Deanononymization.
- Denial of Service.
- Eclipse attack.
- Selfish mining.
- Goldfinger attacks.

QUESTIONS?

