Bitcoin

Understanding and Assessing potential Opportunities

January 2014

QUASAR
VENTURES

QUASAR
VENTURES

We are an experienced entrepreneurial team focused on building successful tech companies in Latin America and Beyond

Investigation and analysis led by

Julieta Duek
Stanford MBA, 2013

Demian Brener
Senior Analyst at Quasar Ventures

Index

Bitcoin is an electronic payment system based on a decentralized global ledger

Bitcoin

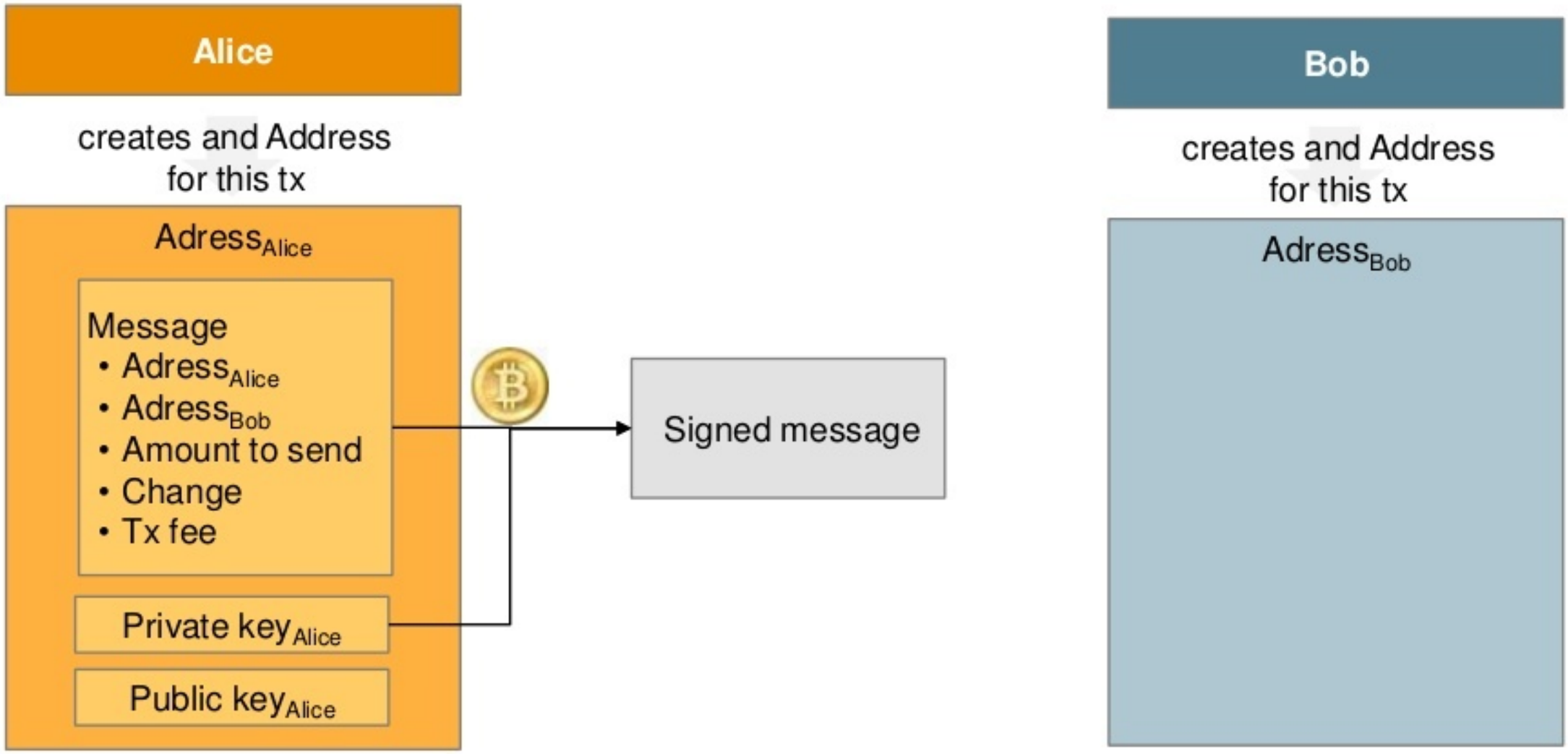
- An **electronic payment network**
  - Based on a **global ledger** that records all txs ever made in the system
  - Ledger cannot be overwritten or changed
- Bitcoin is also the name of the **currency unit** of the payment system

Main features of the Bitcoin network

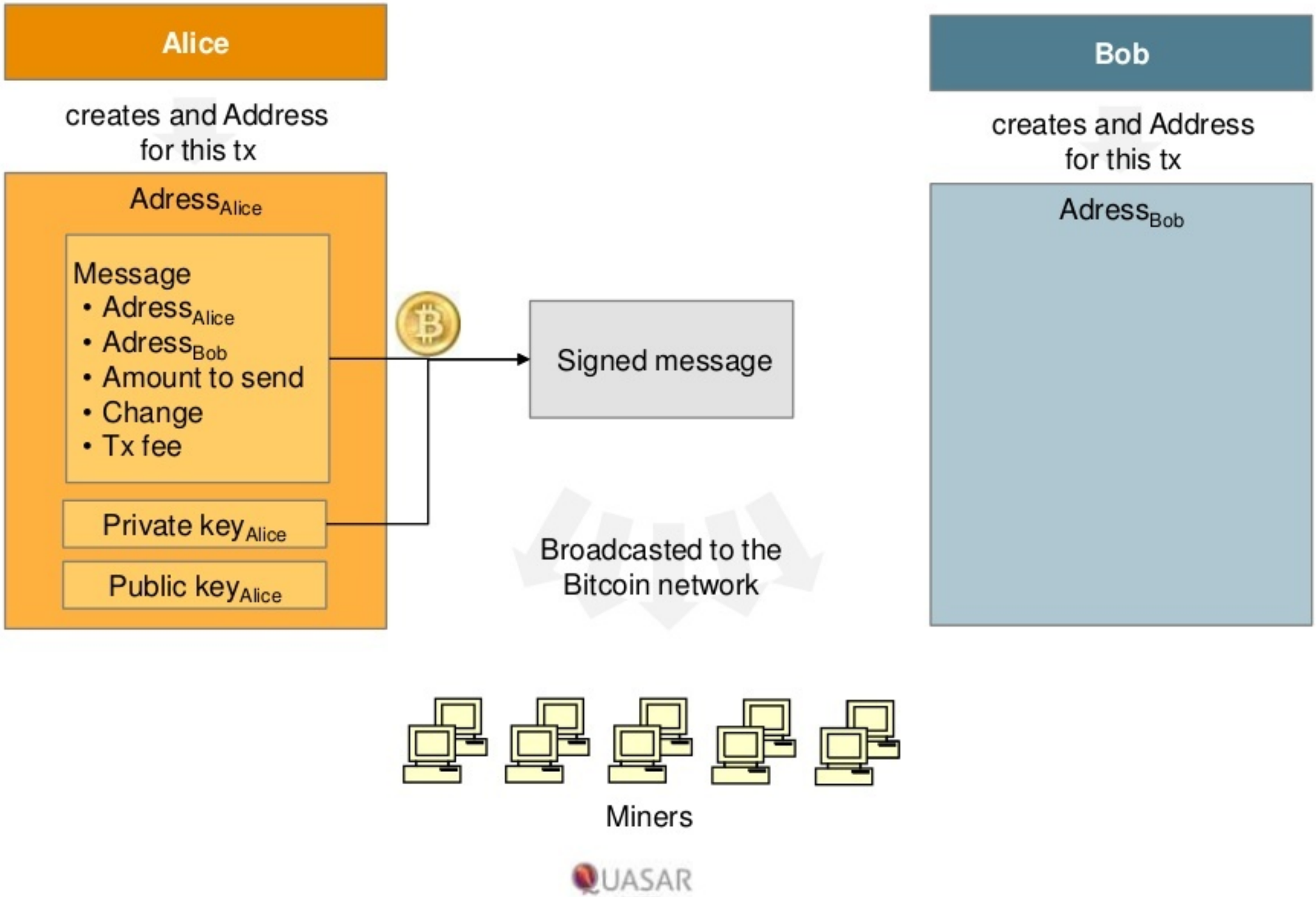
Decentralized	Network maintenance and tx processing done by a network of individuals' computers ("miners")
P2P network	Theoretically, transactions can be done P2P; there are also exchanges to facilitate txs
Global	The system doe not care about the tx origin, destination, or where it is processed
Secure	Ownership and tx of bitcoins are secured by protocol rules and mathematical algorithms
Open source	Software changes can be proposed by any node, and are widely implemented when 80% of the nodes adopt the change
Zero or low processing fees	Initially free processing, with miners rewarded with newly generated bitcoins As # bitcoins reaches 21M, tx fees will prevail

QUASAR

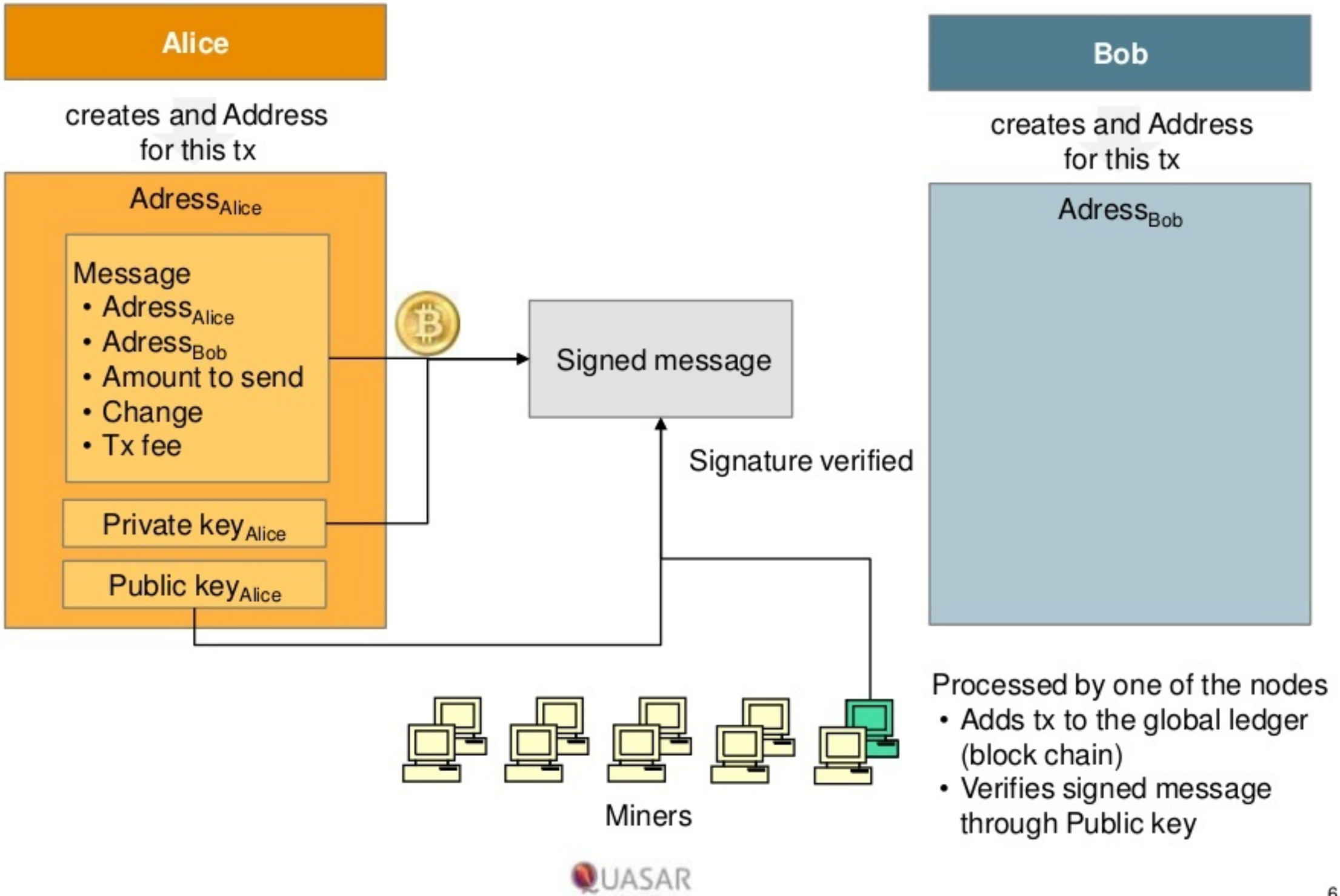
How a transaction works: Alice sends bitcoins to Bob (I)



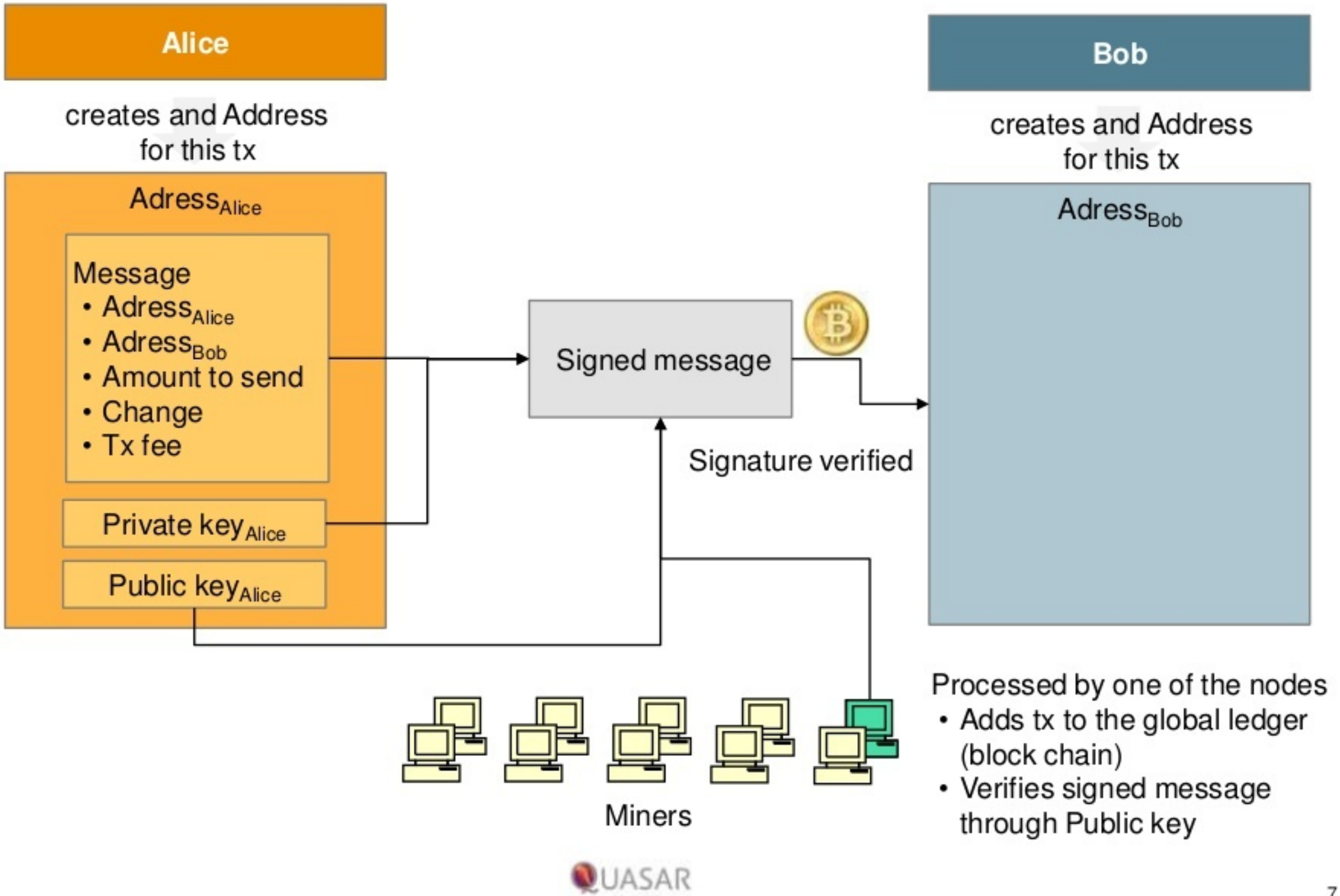
How a transaction works: Alice sends bitcoins to Bob (I)



How a transaction works: Alice sends bitcoins to Bob (I)

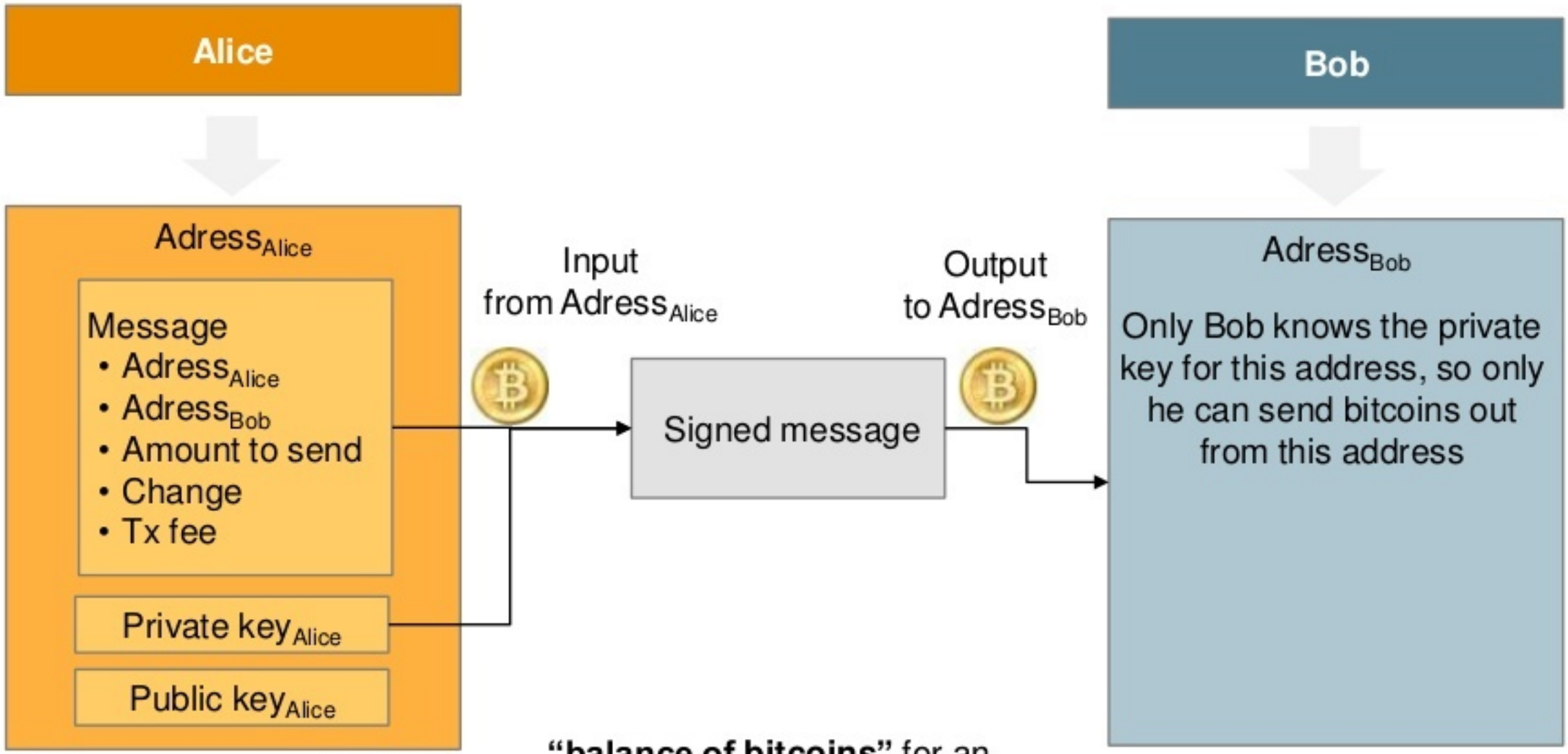


How a transaction works: Alice sends bitcoins to Bob (I)



How a transaction works: Alice sends bitcoins to Bob (II)

The ledger registers input and outputs that record the "balance of bitcoins" for each address

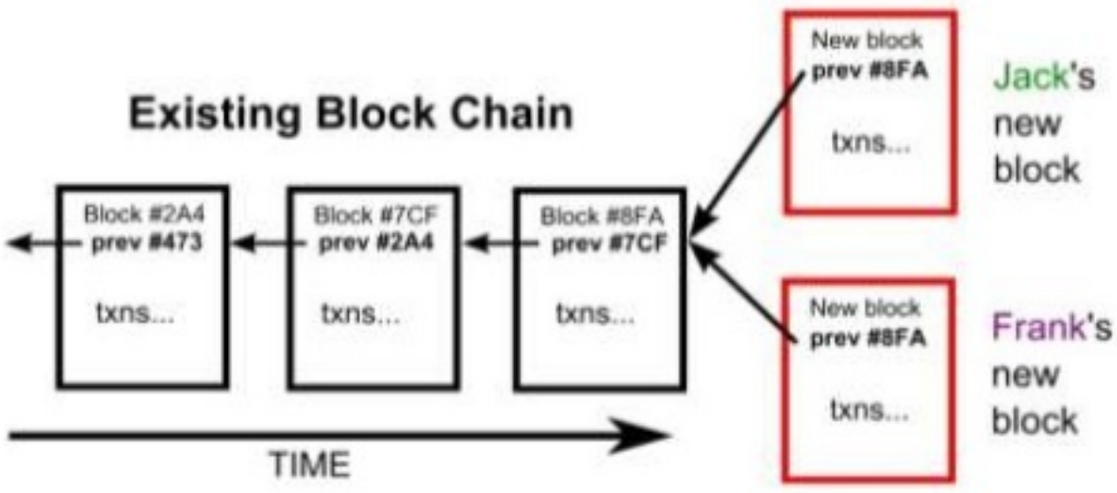


"balance of bitcoins" for an address: all the outputs referenced to the adress' public key, that haven't been used as inputs in later txs

The Block chain orders who processes each tx block

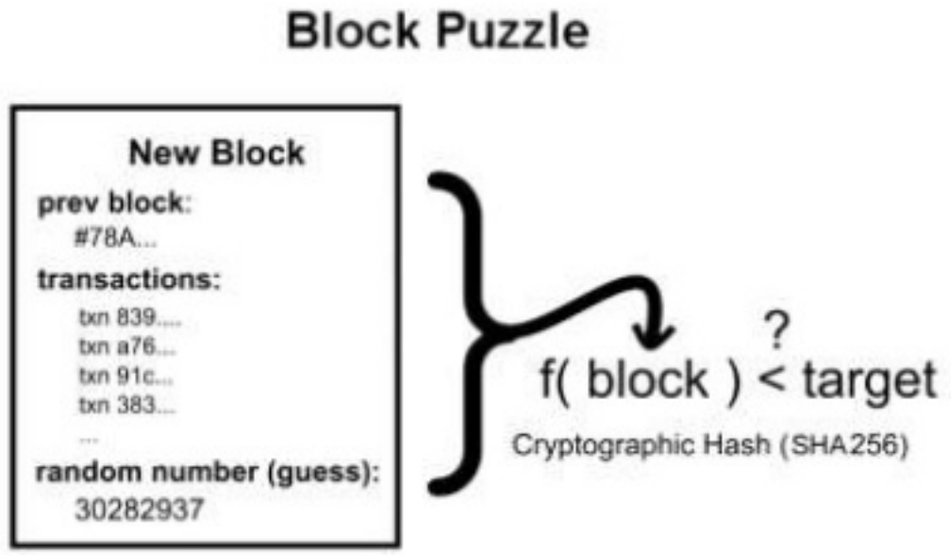
Miners create blocks of processed txs to be added to the block chain

- Txs are bundled in blocks by miners
- Blocks linked together form the block chain (the giant ledger)
- Each block is referenced to the previous block, which gives a time order to the txs
- The system has to determine whose block will be the next to enter the block chain



The first miner to solve a certain math problem adds his block to the chain

- The next valid block is the one that contains the answer to a certain mathematical problem



- The 1st miner to solve it gets to add his block to the block chain
  - It takes an average of 10 min for someone to find a solution
  - That miner is rewarded with newly generated bitcoins

What is a hash function?

A **hash function** creates a fixed short digest (H) from any arbitrary length of text (M)

$$H = hash(M)$$

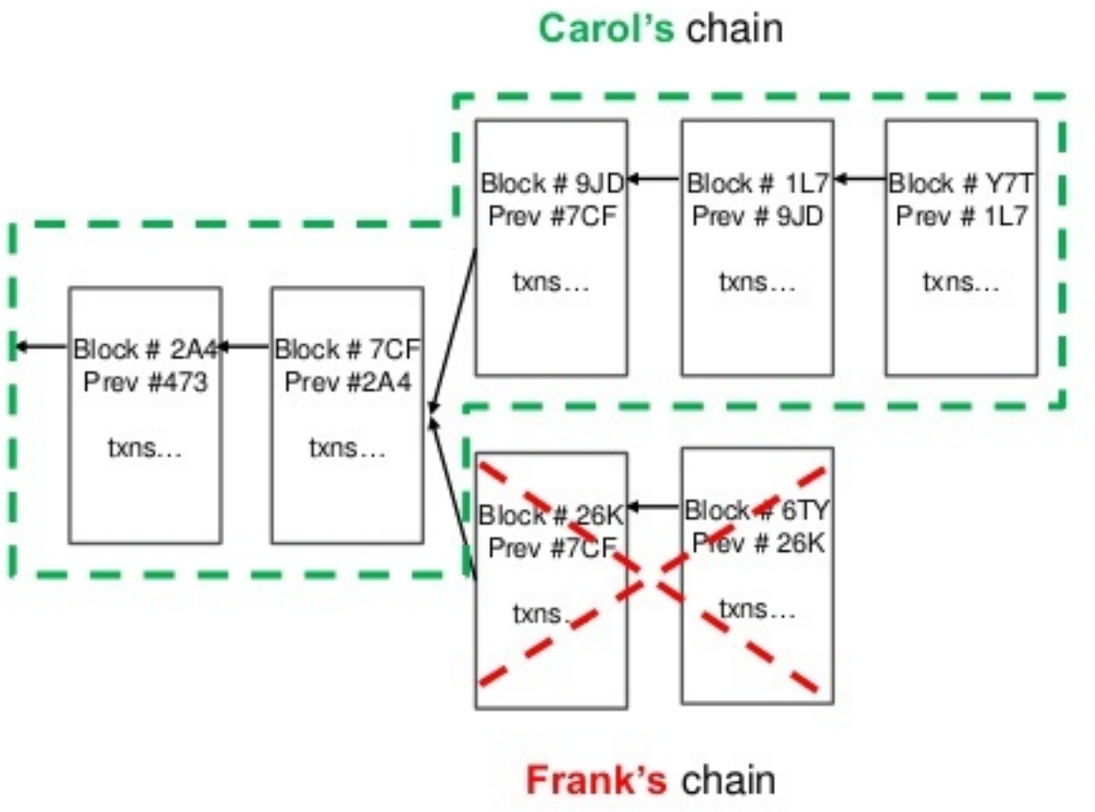
Bitcoin uses a SHA256 function, resulting in a 32 byte number.

Properties of a hash function

- It is easy to compute the hash value for any given message
- It is infeasible to generate a message that has a given hash
- It is infeasible to modify a message without changing the hash
- It is infeasible to find two different messages with the same hash
- Pre-image resistance. It is a one-way function: given a hash H it is difficult to find any message m such that H = hash(M)
- Collision resistance. It should be difficult to find two different messages M1 and M2 such that hash(M1) = hash(M2).

If two miners solve the math problem at the same time, two branches are created, but only the longest one will prevail

Two miners solve the math problem at the same time, creating two branches

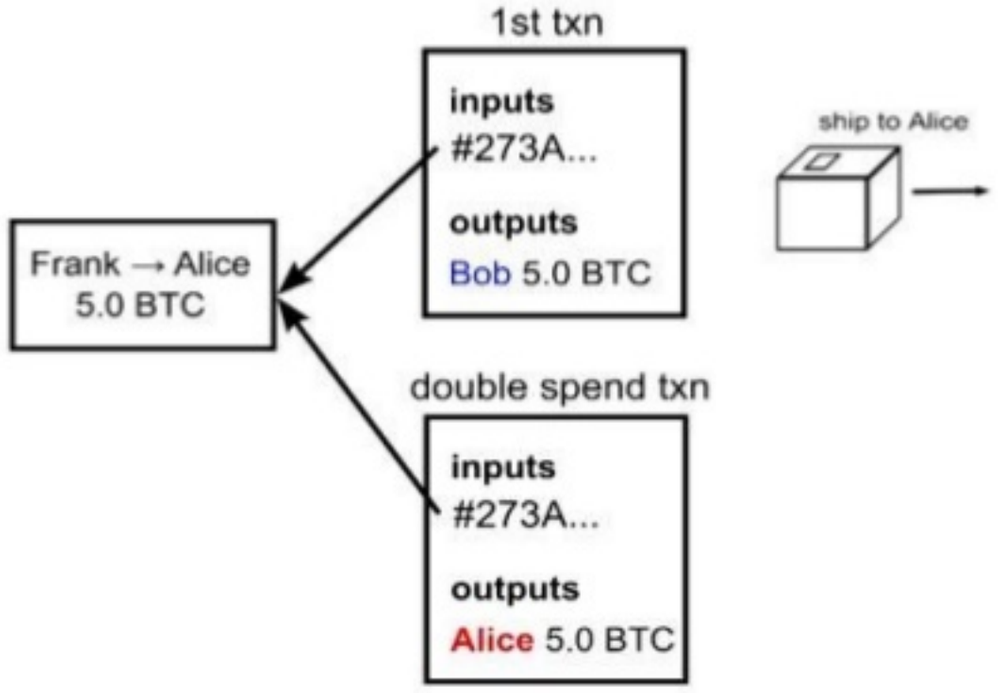


Only the longest chain will be part of the block chain

- Nodes keep building the blocks on top of the two blocks created by Carol and Frank
- Nodes immediately switch to the longest branch available
- Blocks that belong to the shortest chains, and the blocks built on top of them, are destroyed

The Block chain prevents double spending fraud

The decentralized processing could be risky of double spending fraud…



- Alice could create a longer branch with the double-spend tx, that replaces the chain with the tx to Bob
- The chain with the tx to Bob would get erased for being shorter
- Bob´s money would get erased

…but the block chain structure makes it impossible

- To execute the double-spending Alice would have to pre-create a “longer chain”
- But the previous-block-reference is part of the text that goes through the hash function of the next block
- So she cannot pre-create the chain, because she needs info from previous blocks to generate it
- The only way to do it is being the 1st to create that chain
-
- She could only win if she has >50% of the computing power of the network, one of bitcoins risks

Mining and bitcoin generation

Miner´s incentive = ① Reward for verifying a block of txs + ② Tx fees

① Reward for verifying a block of txs

- Miners receive 50 newly generated bitcoins for the first 210,000 blocks and half the previous amount of bitcoins for each subsequent 210,000 blocks
- Each block takes an average of 10 min to be verified (210,000 blocks take ~4 years)
  - The difficulty of the math problem to verify a block is adjusted every 2 weeks so that the average time to solve a block remains around 10 mins
- Newly minted BTCs cannot be spent for 100 blocks

② Tx fees

- Incentive for miners verify those txs faster, by including them earlier in the block chain
- They arise from the difference between the values of input and output on a tx
- When all bitcoins are issued, tx fees will be the only compensation for miners to verify txs, so eventually sending money through bitcoins will not be free
- Rewards and tx fees are a transaction with no input called “coinbase“, included in the block the miner just created

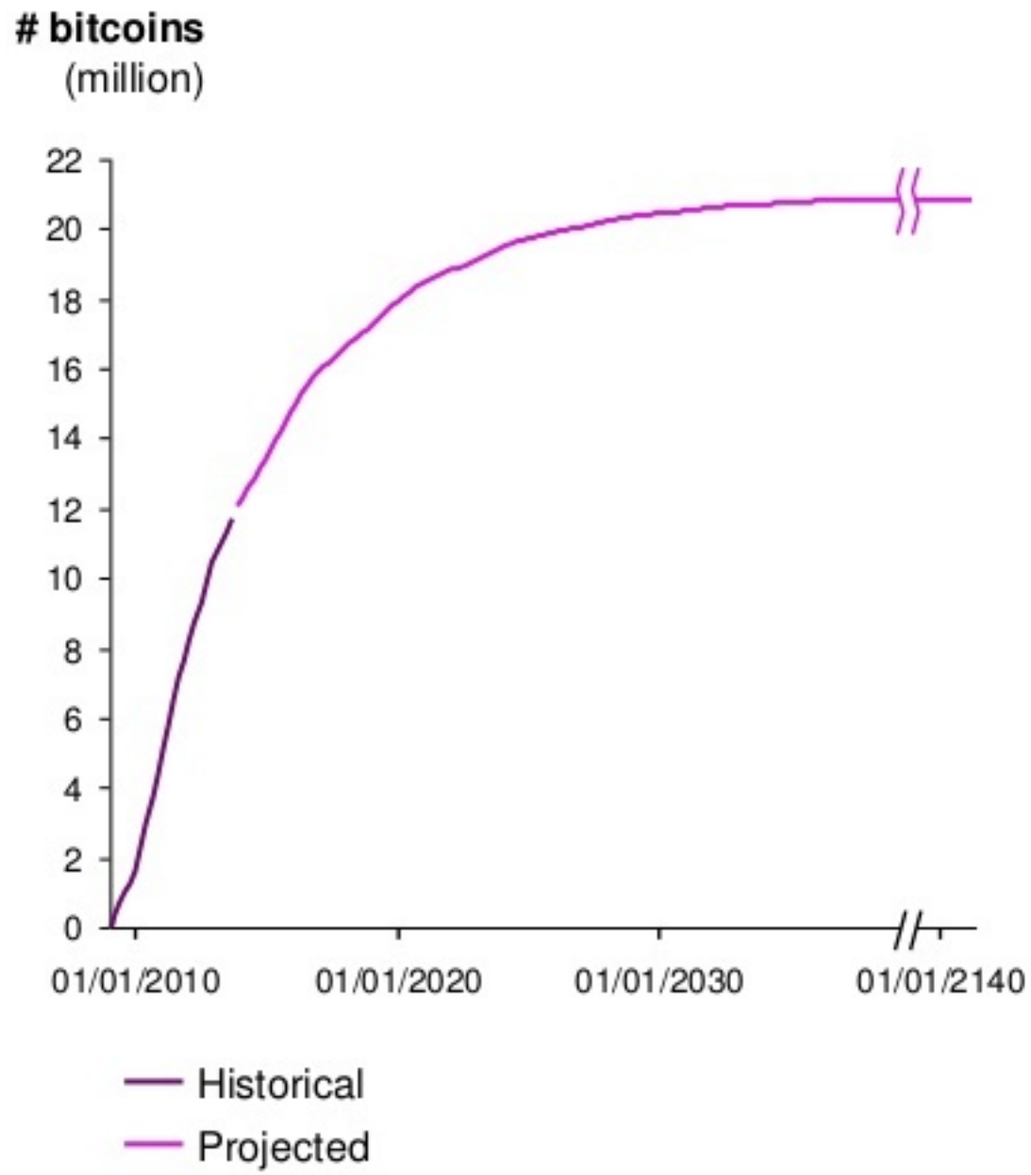
Bitcoin current status (I)

Price grew explosively to $1200 (Mt. Gox) in December, but stabilized around $950 in January

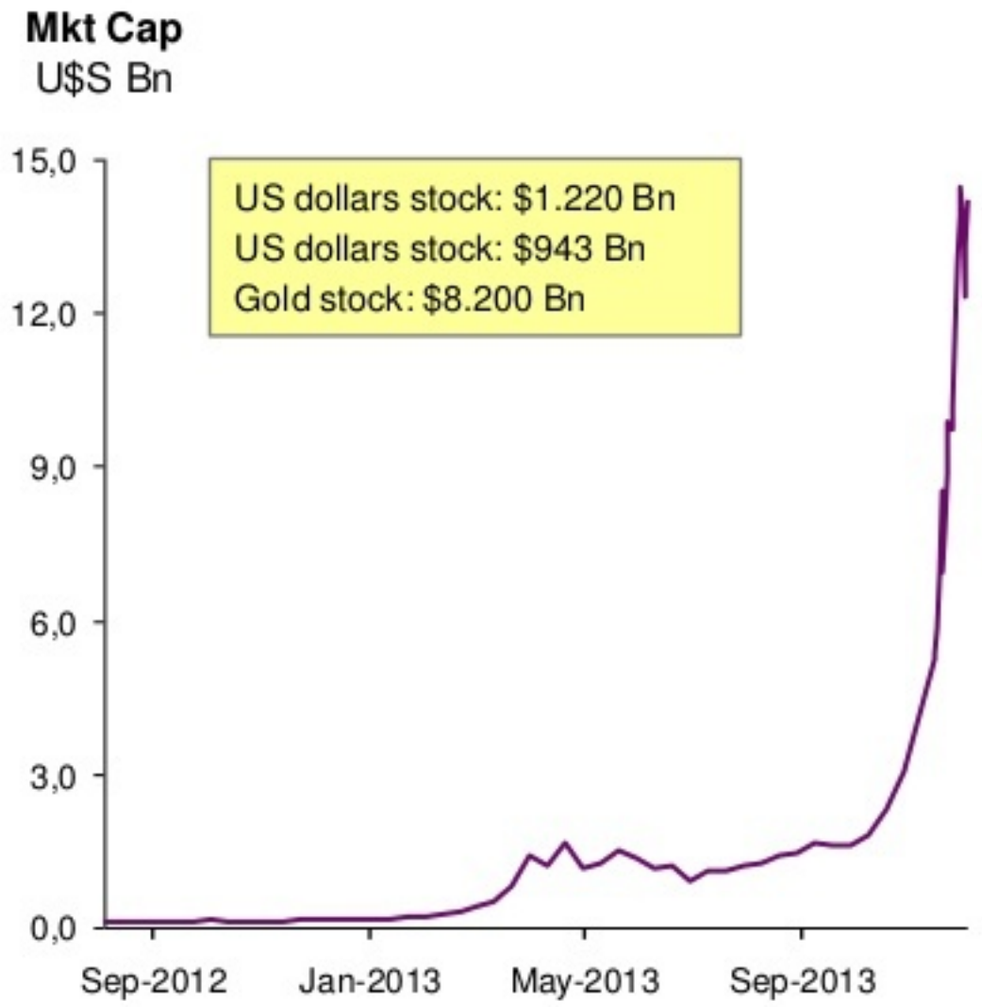
Bitcoin current status (II)

Total volume of bitcoins, and Market Cap

Total # bitcoins is predictable and will reach 21M in 2140



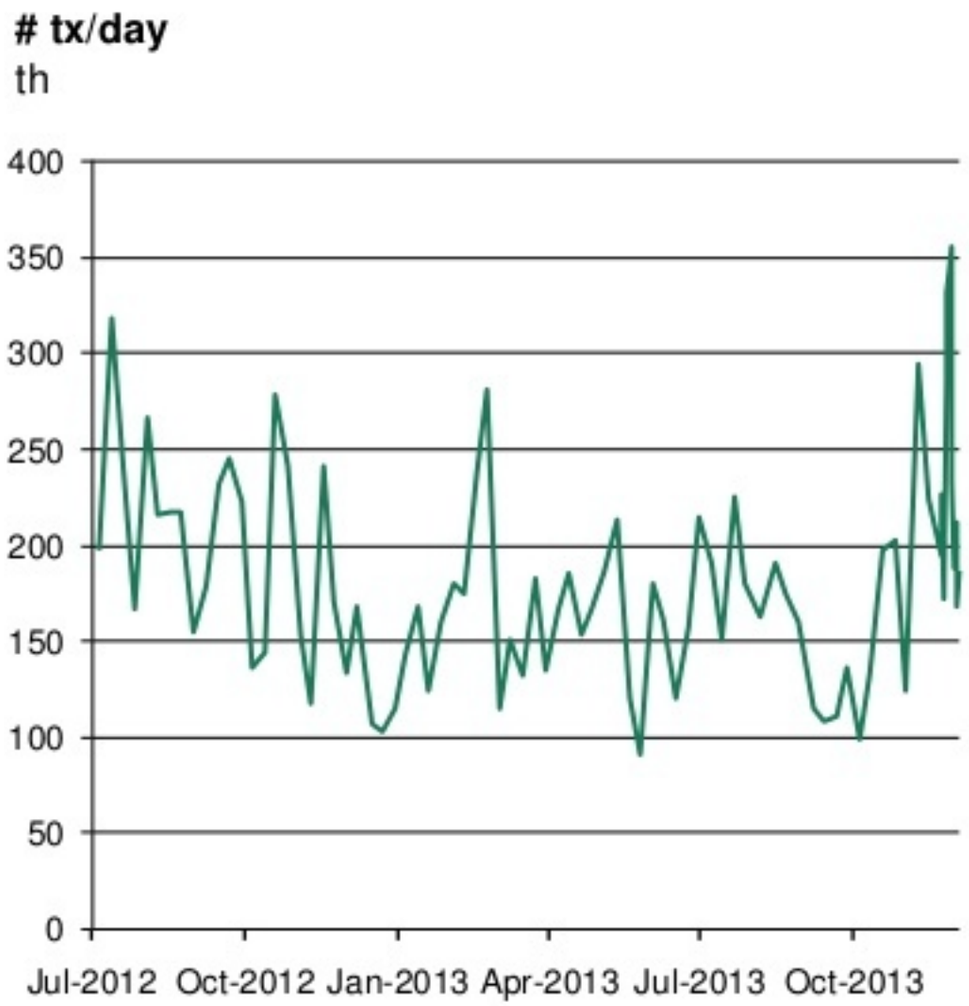
Market Cap fueled by price increase was around $11.5 Bn in Dec-2013



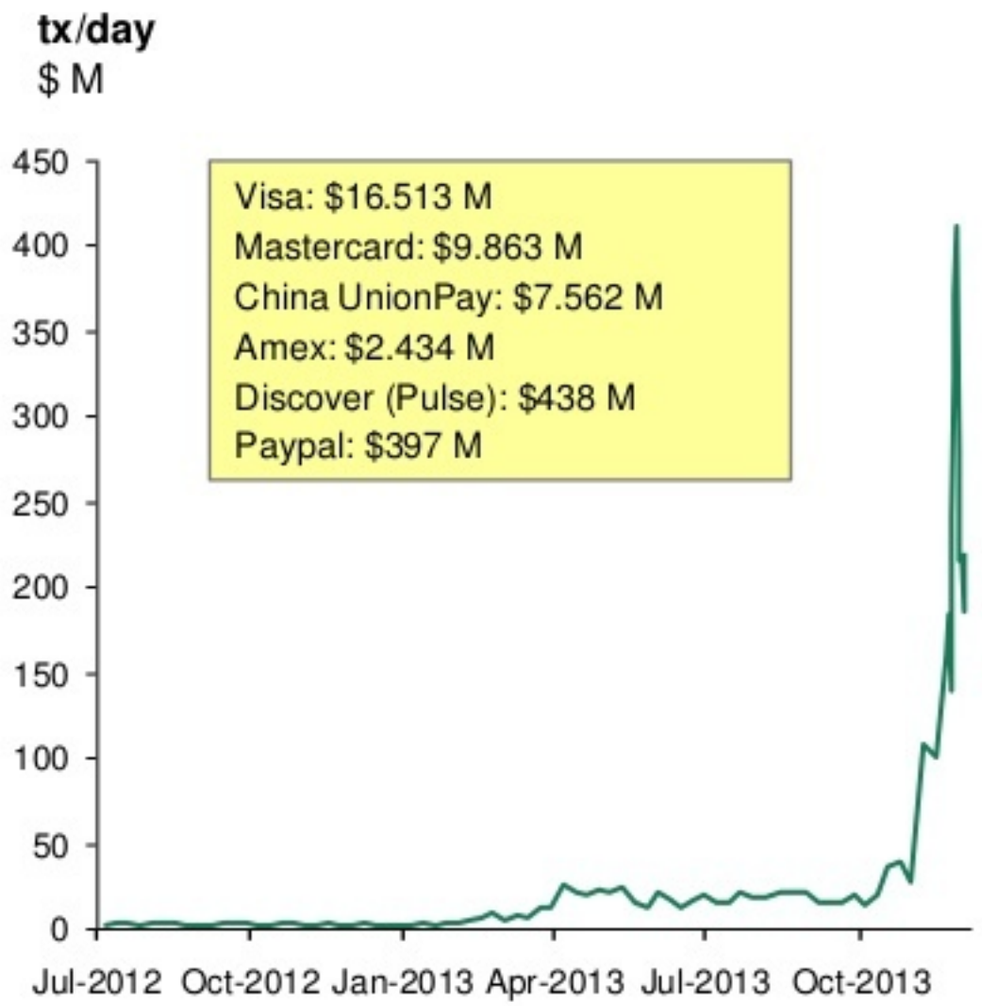
Bitcoin current status (III)

Bitcoin volume of transacions per day

tx/day highly volatile



Daily tx volume between $200 – 400M reaching the level of Paypal



Emerging crypto currencies can be classified as Bitcoin alternatives and currencies for Other Uses

Alternatives to Bitcoin

- Used as currency, for purchases, money transfer, store of value, etc
- With slight different functionalities:

Litecoin	Faster txs Useful for small amounts
Peercoin	Less energy consumption to process txs
Ripple	Centrally administered Bitcoin Only one exchange
Quarkcoin	Could be more secure Not really much different than Btc
Worldcoin	30 second tx time Direct competitor of Litecoin

- All their functions could be easily incorporated to Btc as needed
  - Except Ripple's centralized governance

Crypto currencies for other uses, based on protocols similar to Bitcoin

- Based on the Bitcoin protocol
- Created ledgers to transact, register, or represent other things that are not necesarily monetary value

Namecoin	Same protocol as BTC for representing asset ownership
Photoshares	Similar protocol to Bitcoin but to acquire shares in Invictus Innovation DAC

- Could be replaced by Btc.
  - I.e.: buying the domain with Btc instead of Namecoins

Alternatives to Bitcoin

Litecoin (Mkt Cap $727.9M)

- 84 M total coins, four times more than Btcs
- Tx time 4x less than Btc (2.5 min/block)
- Trying to be the Btc for small txs

Peercoin (Mkt Cap $93.4M)

- "Proof of Work/Proof of Stake" makes processing less energy consuming
- Inflationary: volume grows 1% per yr, proportional to PCP held
- Fixed 0.01 PCP tx fee
- Not decentralized, founder Sunny King has checkpoint control of txs

Ripple ((Mkt Cap $3.7Bn)

- Central control by Ripple Labs
- Shared public ledger that holds balances in any currency
- It is an exchange: ledger registers offers to buy or sell assets
- Fee in XRP required to transact
- Founders held XRP 100M initially, gifted XRP 80M to Ripple Labs, who will distribute 55M XRPs to users

Quarkcoin (Mkt Cap $52.3M)

- 245M Quarkcoins, with 98% already mined
- Some claim that the more stable stock of Quarkcoins will make it less volatile
- With a 6-way hashing method, claims to be more secure than Btc but a 51% attack is equally possible

Worldcoin (Mkt Cap $22.9M)

- 30 second tx time
- Mining has 1% reward reduction per week, encouraging fast mining

Crypto currencies for other uses, based on protocols similar to Bitcoin

Namecoin (Mkt Cap $46.9 M)

- Same protocol as Btc but to represent asset ownership
- Platform can also be used to register messages, votes, and as login system
- Colored Coins is another service for representing asset ownership, but can run on top of BTC or any protocol
- Transaction cost is 0.01NMC
  - E.g.: registering a domain or transferring it costs 0.01 NMC

Photoshares (Mkt Cap $21.8 M)

- Photoshares represent shares in Invictus Innovation Decentralized Autonomous Corporations (DACs)
- Invictus is a platform that brings together and coordinates developers who want to build DACs
- Only 2 M Photoshares are available

New application platforms and programming languages are being built using the blockchain technology and protocol

Ethereum[1]

- Ethereum is a decentralized mining network and software development platform designed to allow users to encode advanced transaction types, smart contracts and decentralized applications into the blockchain
- It includes a Turing-complete programming language that can be used to build applications and features on top of the ledger using contracts as building blocks
- A contract is like a computer program that lives inside the Ethereum network, which is triggered every time a transaction is sent to it

Bitcloud[2]

- Bitcloud works on a variation of proof of stake known as proof of bandwidth. The nodes in this system are similar to the miners in the Bitcoin protocol in that they mine cloudcoins by providing bandwidth to the network
- Instead of using a proof of work system where miners are looking for the solution to a complex mathematical equation, the nodes in Bitcloud are rewarded based on their share of the total amount of bandwidth used in the Bitcloud network
- Each block reward is distributed among the nodes based on their share of the overall amount of bandwidth needed by the Bitcloud users

1.Ethereum.org
2.GitHub Bitcloud white paper at https://github.com/wetube/bitcloud/blob/master/Bitcloud%20Nontechnical%20White%20Paper.md

Index

What are the benefits compared to Fiat and Gold?

What is Money? Medium of exchange, unit of account and store of value

	Fiat	Gold	Bitcoin
Scarce	Neutral	Yes	Yes
Durable	Neutral	Yes	Yes
Portable	Neutral	No	Yes
Divisible	Yes	Neutral	Yes
Easily Verifiable	Yes	Neutral	No
Easily Stored	Neutral	No	Yes
Fungible	Yes	Neutral	Yes
Authenticity	Neutral	Neutral	Yes
Mass adoption	Yes	Neutral	No

The rules of the Bitcoin system have implications and consequences

Deflation

Due to limited number of coins

Does not invalidate most of its uses
- It does invalidate debt txs

Implications of decentralization

(+) Harder to stop by states or companies

(-) Very vulnerable to market reactions
(-) No central leader to deal with governments

Concentration of Bitcoin holders

(-) Are market makers, thus controlling price

(+) Could lead development of the ecosystem if they can coordinate themselves

Mining power structure

Grouping of miners to stabilize profits

Pools are not a risk
- But governments could take over mining for an attack

Volatility

Compare with other currencies/gold

Understand if higher volume would solve it

Open source governance

Anyone can
- Find bugs or errors
- Propose changes

Prioritization and implementing is led by the core developers

Mining incentives and tx fees

Still evolving in the protocol

Will probably end in market-set tx fees

Anonimity

Currently achievable

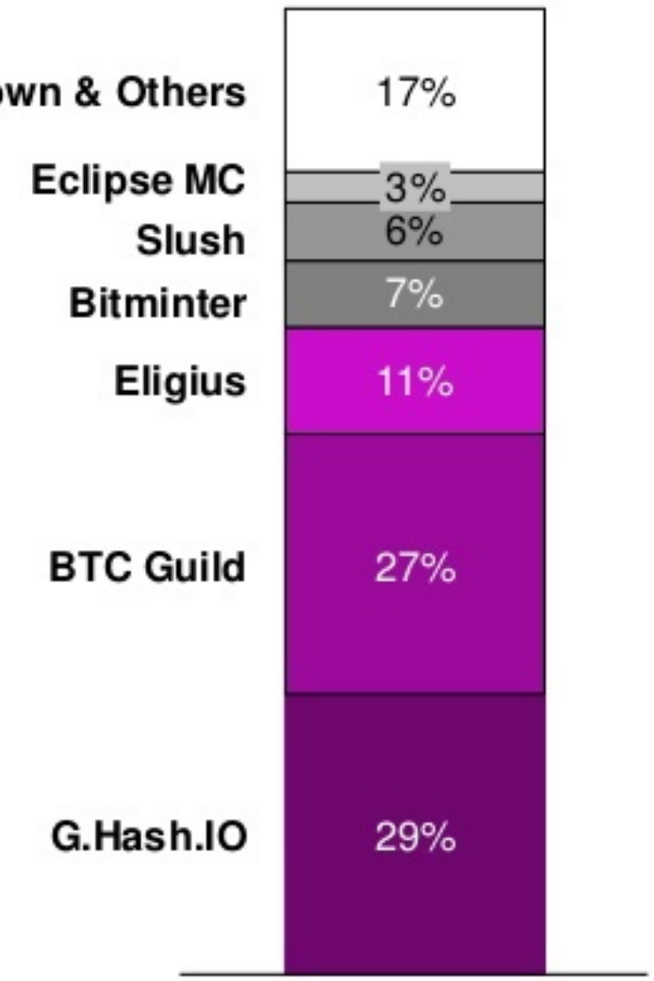
In the future, regulation will eliminate it

Five mining pools concentrate 80% of the revenues

Mining generates $4M revenues per day but is currently not profitable

- **Total nodes: ~5000**
- **Around $4M revenues per day**
- **Mining is no longer profitable**
  - Excess investment caused excess supply
  - Raising the Difficulty levels set by the system
  - Causing an arms race of mining technology that is now slowing down

Top five mining pools concentrate 80% of revenues



The formation of mining pools could pose a risk for the Bitcoin system: the 51% attack

The *51% cartel* attack is unlikely

An attack would be costly and difficult to implement

- Requires controlling >33% mining power
- Bitcoin processing power is now >500 most powerful computers in the world
- Will become even more costly over time
- Building this power takes time[1]
- The attack itself would have last 20-30 min
- Nodes have tools to report bad behavior

Rewards are limited[2]

- The attacker could:
  - Double-spend his/her own Bitcoins
  - Delay others' txs confirmations
- The attacker could NOT
  - Create or destroy coins
  - Fake transactions
  - Take someone else's Bitcoins

A *Goldfinger attack*[3] could be possible

The attack won't come from

- Those who own Bitcoins, profit from Bitcoin industry, or would gain Bitcoins in the attack

The attack could come from:

- Someone who would achieve utility outside the Bitcoin economy through the attack

1. http://hackingdistributed.com/2013/11/04/bitcoin-is-broken 2. https://en.bitcoin.it/wiki/Myths and https://en.bitcoin.it/wiki/Myths
3. The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, by Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, Princeton University

Governance of Bitcoin by emerging leaders whose power is constrained by the possibility of a fork

Core developers have to push improvements and avoid forks

Core developers rise and get respect through their skills and contributions to the system

- Satoshi still has some lingering influence

New core developers can arise anytime

- Power changes have happened in the past[1]

Main incentives of the core developers are

- Improve the system
  - Eliminate bugs and vulnerabilities
  - Implement changes to increase adoption and make the system sustainable
- Generate consensus
  - Sometimes the optimal solution is unclear
  - If a hard fork happens, and Bitcoin gets split in two sub-Bitcoins, everyone loses

Upcoming features

Solve the long confirmation time

Develop capabilities for refunds

Multisignature transactions

Smarter tx fee system

- Based on free market rule instead of fixed as it is today

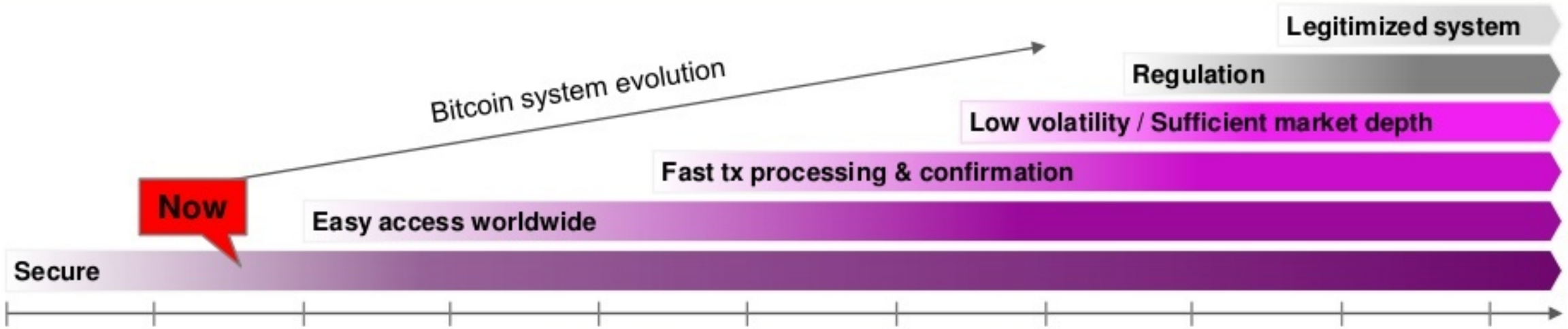
Put a node in the space as backup to the nodes on Earth

Researchers[2] consider that some governance will have to emerge to deal with the government intervention risk

1.GitHub history of Bitcoin protocol, where the change of core developers can be seen http://www.youtube.com/watch?v=OztVYTS_Ei8
2. The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, by Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, Princeton University

Index

Different Bitcoin businesses are dependent on different stages of evolution and adoption of the system



Mining (Btc generation and tx processing)

- Mining hardware manufacturing and selling
- Mining pools
- Cloud mining
- Equipment reselling
- Equipment and/or platforms to optimize mining

Enablers to hold and transact Btcs

- Wallets
- Exchanges
- Storage safety
- Identity proofing

Enablers to buy/sell Btcs with fiat

- Wallets
- Exchanges
- Links between local banks and exchanges/wallets
- In person exchange organizers
- ATMs
- Instant tx provider
- Issuers of physical unit of Btc
- Btc investment funds

Niche based adoption

- Online payment services
  - Cross-border (hotels, flights, etc)
- Individuals' money transfer
  - Cross-border (remittances)
- Escrow and settlement of high cost tx (e.g.: real estate)
- Micropayments for current businesses

Widespread adoption

- Merchant services (online and offline)
- Corporate money transfers & payments
- Imports/Exports payments
- New business models based on micropayments
- Financial instruments for Btc
- Investment firm in Btcs

Non-currency use of the protocol

- Time stamping
- Asset ownership and contracts
- Notary services

Btc as store of value

- Btc investment fund
- Investment advisors
- High security storage systems
- Store of value financial instruments

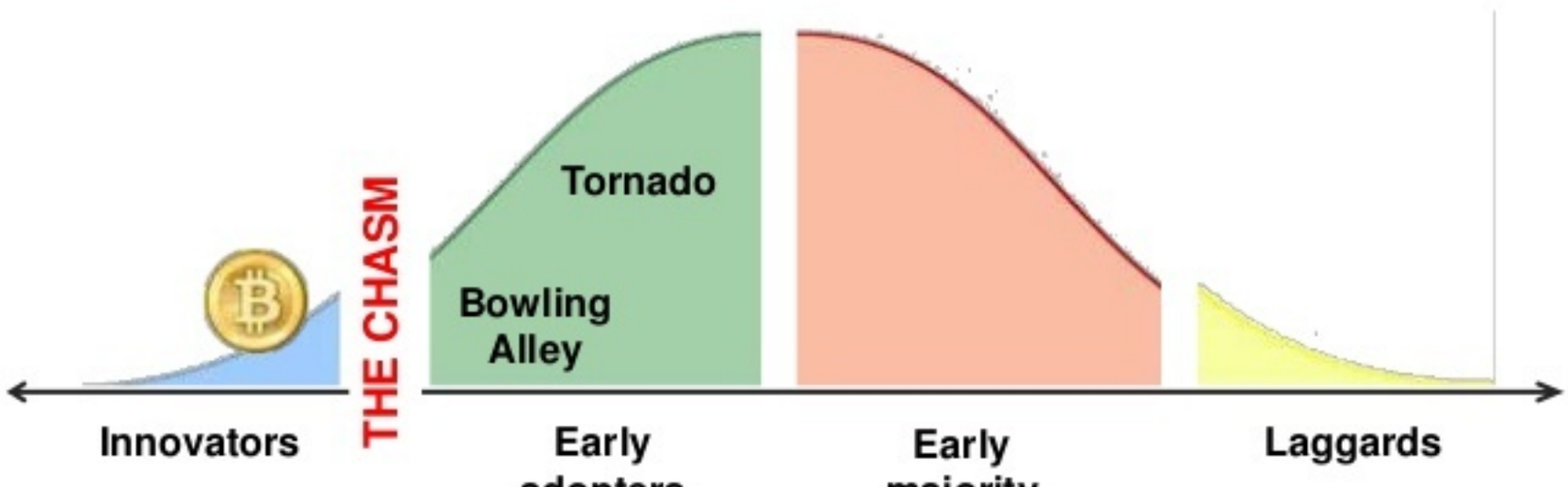
Support services

- Providers of market and blockchain info
- Tx fee calculator
- Btc tax advisory

QUASAR

Bitcoin is at the chasm in the technology adoption cycle

Moore's adoption cycle for disruptive technologies

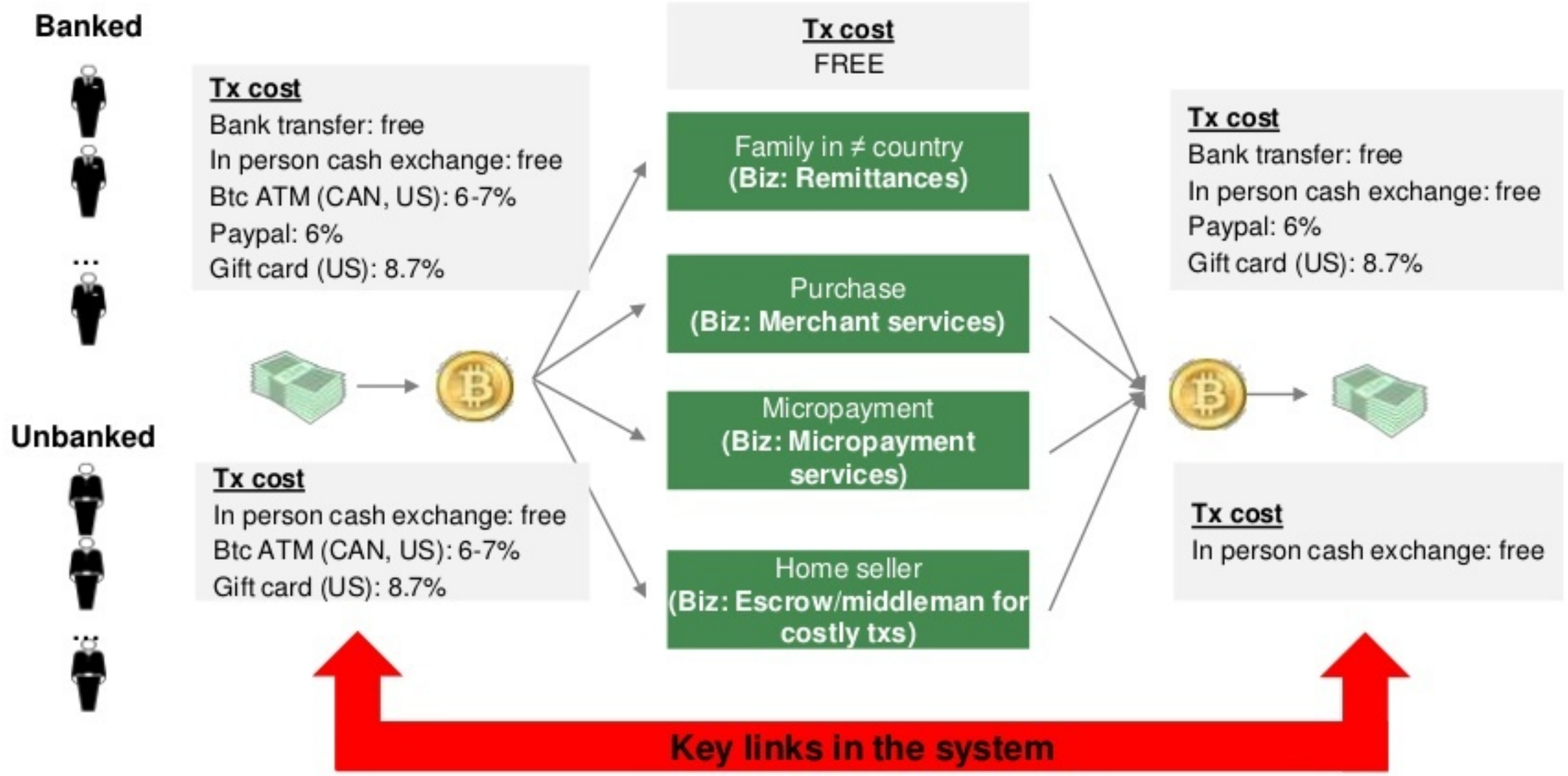


Innovators or Visionaries		Early adopters
Don't need the technology to work perfectly • Will make an effort to make it work	≠	**Will only buy a complete solution**
Motivated by their vision of the technology		**Motivated by economic rationale**

Bowling Alley: **niche-based adoption, driven by compelling customer needs and vendors crafting niche-specific complete products**

QUASAR

Currently, the bottle neck in the chain is the exchange from $ to Btc and viceversa



- **In US these links are solved → a business focused in the US doesn't have to worry about that**
- **For businesses outside the US, there are two options**:
  - Build those links
  - Find a way to go around them (e.g. focus on payments from US to Argentina, work with large Btc holders)

Map of opportunities that are feasible in the short term (I)

Business opportunity		High-level business hypothesis	Target market
Mining	**Platform to optimize Btc mining overall cost**	• Develop a platform to optimize mining • E.g.: mine where electricity is cheaper, etc	Global or LatAm
System enablers	**Give access to buy/sell Btcs in new markets**	• Btc can offer payments with lower tx costs • Help building the key gates to the system, and keep part of the value created	LatAm (there are already big players in developed markets)
	Merchant services		
System improver	**Instant Btc txs for a fee**	• Price volatility and tx confirmation times have a cost for users • A centralizer could neutralize part of the volatility, reduce the overall cost, and charge a fee lower than the cost borne by individual transactors	Global
	Instant fiat/Btc txs for a fee		
	Hedging of Btc txs for a fee		
	Id proofing services	• Needed to make the system more secure • Should grow as Btc becomes more regulated	Global
	Safety storage tools	• The need is clear • Not a clear winner yet	Global
	Compliance services	• Need will grow together with regulation • At Western Union, compliance is ~20% of cost	Global
	Tx fee optimizer	• Tx fees ~0.6 M /month, high growth expected • Available best practices are not widely used	Global

Map of opportunities that are feasible in the short term (II)

Business opportunity		High-level business hypothesis	Target market
Complete solutions	**International money transfer**	• High prices of current remittances services • Leverage lower tx costs of Btc	US/LatAm
	International payments	• Leverage low tx costs of Btc • Niche need in payments of foreigners to Arg.	US/LatAm
	Btc accounts for foreign investment	• Btc global nature and low tx costs used to enable individuals to invest abroad	Global
	Micropayments solutions	• Can help increase monetization of sites • Tx fee costs kept low taking the txs off-block	Global
Support services	**App to locate Btc holders and merchants**	• As Btc grows people will need to know where Btc is accepted	Global
	Price and blockchain data provider	• There are sites currently available • Could be improved and made local	LatAm
	Btc news provider	• There are sites currently available • Could be improved and made local	LatAm
Use of Btc protocol	**Registering info ultra-securely**	• Unclear how big is the market • Cost/registration would be 5 to 50 cents	Global

Map of Bitcoin existing businesses (non-comprehensive)

Mining ecosystem (Btc generation and tx processing)

ASICMINER · alydian · AVALON · BUTTERFLYLABS · LAMASSU BITCOIN VENTURES · Cognitive Mining · CLOUD HASHING

Enablers to hold and transact, and buy/sell Btcs with fiat

Wallets

bitcoin Wallet · Block chain · coinbase · PIKAPAY · BIPS · WalletBit

Exchanges

MT.GOX · Buttercoin · Bitfinex · BITSTAMP · BTC · BTCChina

Enablers to buy Btc

LocalBitcoins.com · BITCOIN ATM · AstroPay · VirWoX

Identity proofing

GLIPH · BLOCKSCORE · VerifyBTC · miiCard

Niche based adoption

Gaming

satoshiDICE! · arbitter

Remittances

bitcoin Wireless · BitPesa · moola

Merchant services

bitpay · BitMonet · BitMerch · BITPagos · BITS · Merch · BW · BIPS

Btc as store of value - trading

BITCOIN INVESTMENT TRUST™ · EXANTE · secondmarket · MPEx · kraken

Support services

CoinDesk · BITCOIN MAGAZINE · Blockchain · bitcoin charts

QUASAR VENTURES

QUASAR

VENTURES

quasar-ventures.com

@QuasarVentures