How I could be a millionaire

or

a bit* about Bitcoin

*simplified

Vitalii Iarko

Outline

0) Modern money and Internet payments.

1) What is Bitcoin?

2) How it works?

3) Disadvantages.

Modern money.

- Fiat money
- Value guaranteed by government or law
- Not valuable itself

One needs to trust 3rd party…

(money emission and so on)

Internet payments

- Financial institutions serving as trusted third parties
- No 100% nonreversible transactions
- Transactions fee
- No anonymity

Again trusting 3rd parties…

- But I do not like to trust someone…
- What about cryptographic proof?

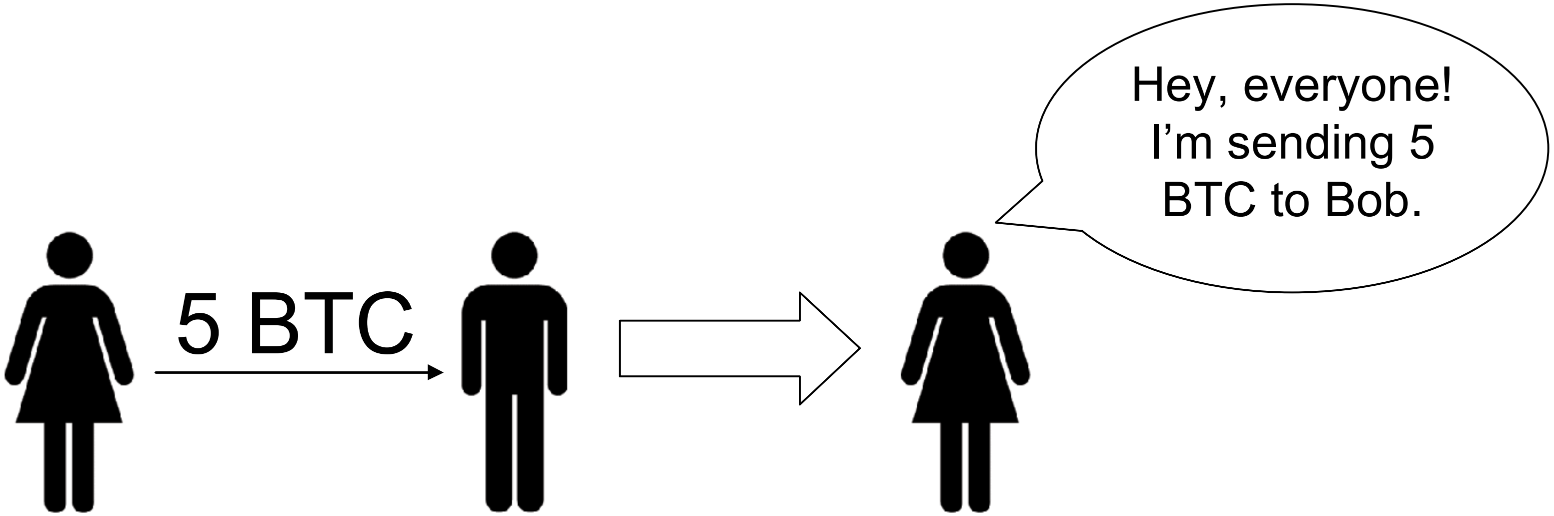
What is Bitcoin?

- Online payment system
- Decentralized (peer to peer)
- So called cryptocurrency (does not require trusting at all)
- …complex system of strongly interacting agents with equal opportunities!

How it works?

List of all accounts (Ledger)

Alice	123 BTC	-5 BTC
Bob	0.0001 BTC	+5 BTC
Victor	0 BTC	
…	…	



5 BTC

Hey, everyone!
I’m sending 5
BTC to Bob.

Alice Bob Alice

List of all transactions (and no balances)

Transaction ID	From, to	Amount
ah32...	Victor to Alice	3 BTC
28ba...	Peggy to Alice	4 BTC
fe39…	Romeo to Juliet	0.1337 BTC
…	…	…

Hey, everyone!
I got 7 bitcoins in transactions
ah32... and 28ba...
Now I’m sending 5 BTC to Bob
(and 2 BTC back to me).

Alice

Why can’t Mallory send Alice’s bitcoins?

Digital signature ECDSA
(**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm).

Only Alice knows

Private key

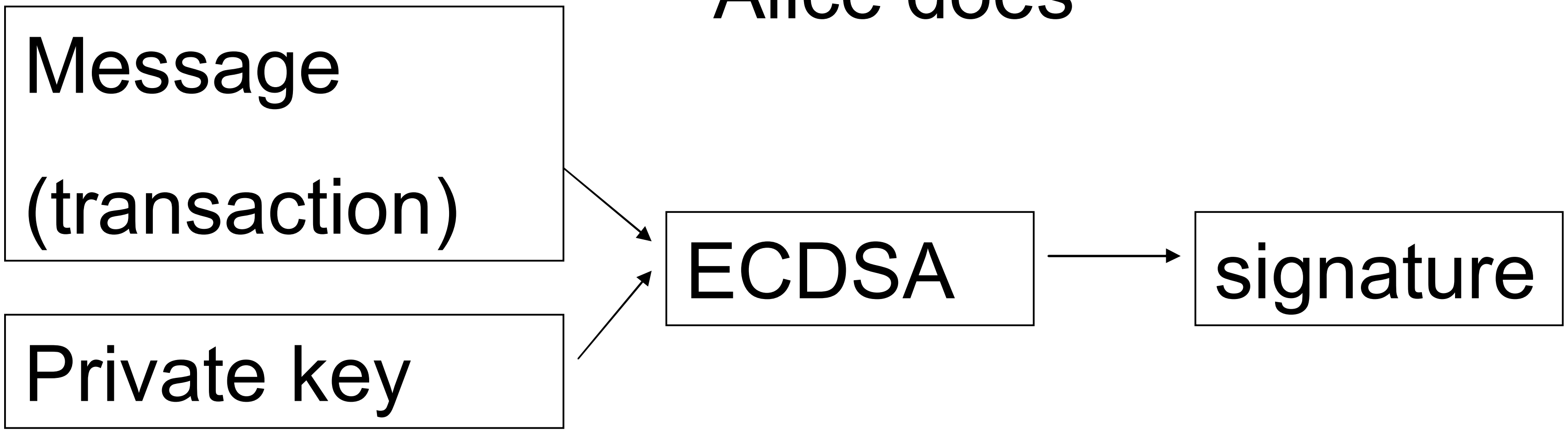
anyone knows

Public key

Public key = some function(private key)

Inverse of some function is hard to compute

Alice does



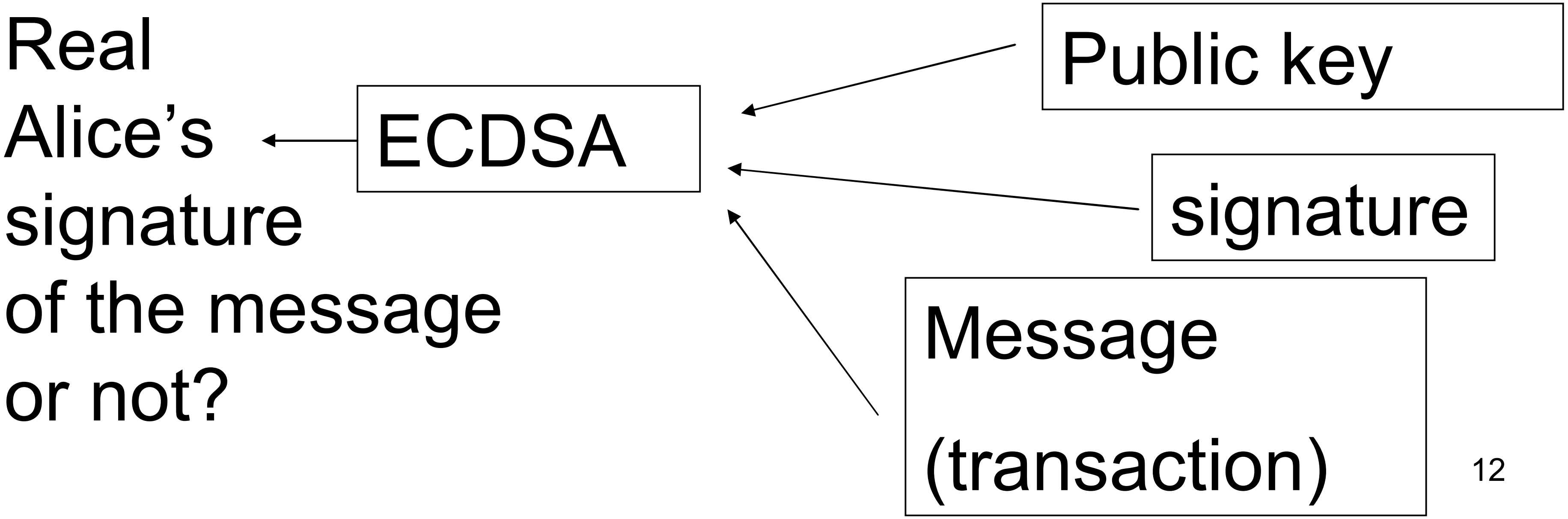
Message (transaction)

Private key

ECDSA

signature

Others do



Public key

signature

Message (transaction)

ECDSA

Real Alice's signature of the message or not?

Double spending

1) Alice broadcasts that she sents 5 BTC to Bob.
2) Bob gets message and sends her goods.
3) Alice broadcasts that she sends this 5 BTC to herself.
4) Nodes that receive 3) before 1) discard 1).

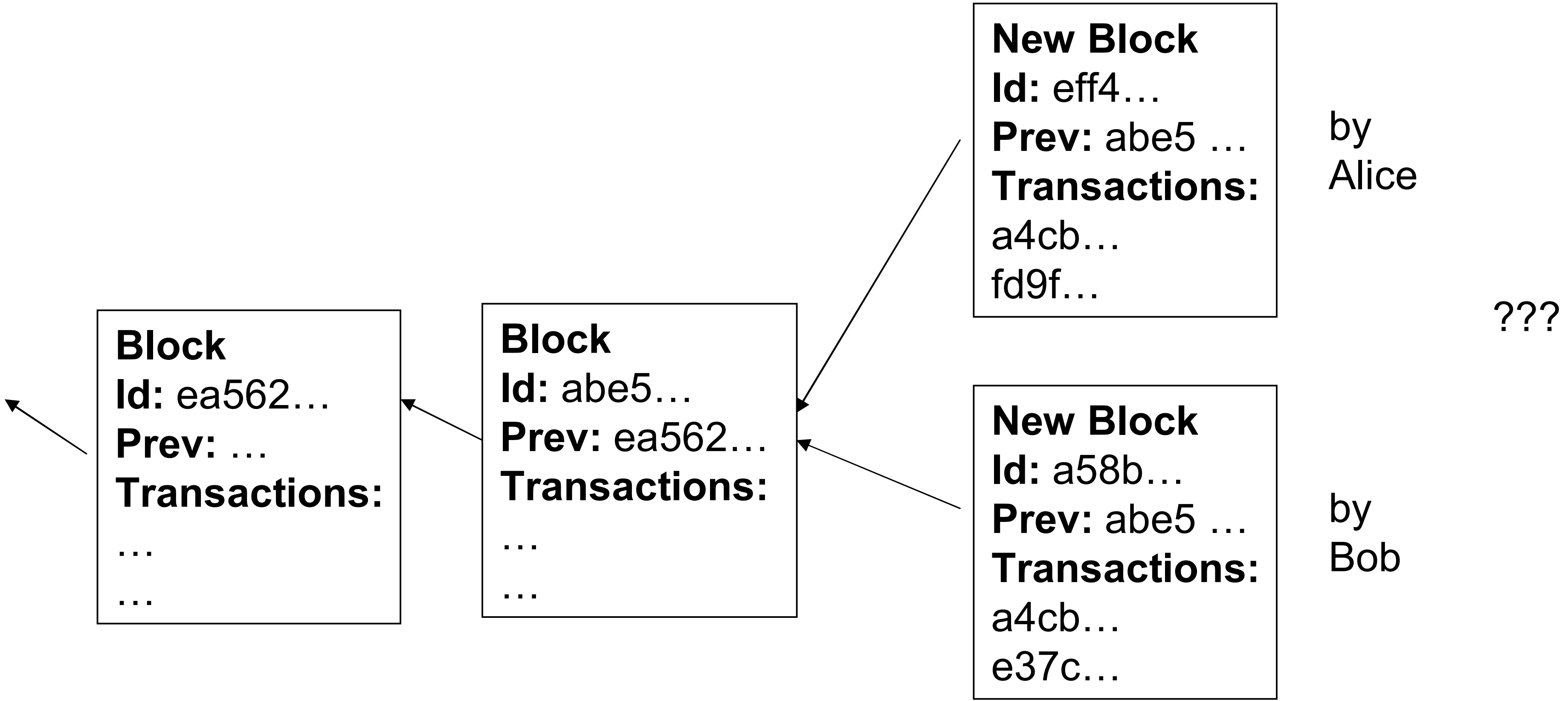
>>Contradiction in the network.

unconfirmed (unordered) transactions

a4cb…

fd9f…

e37c…



Block
Id: ea562…
Prev: …
Transactions:
…
…

Block
Id: abe5…
Prev: ea562…
Transactions:
…
…

New Block
Id: eff4…
Prev: abe5 …
Transactions:
a4cb…
fd9f…

by Alice

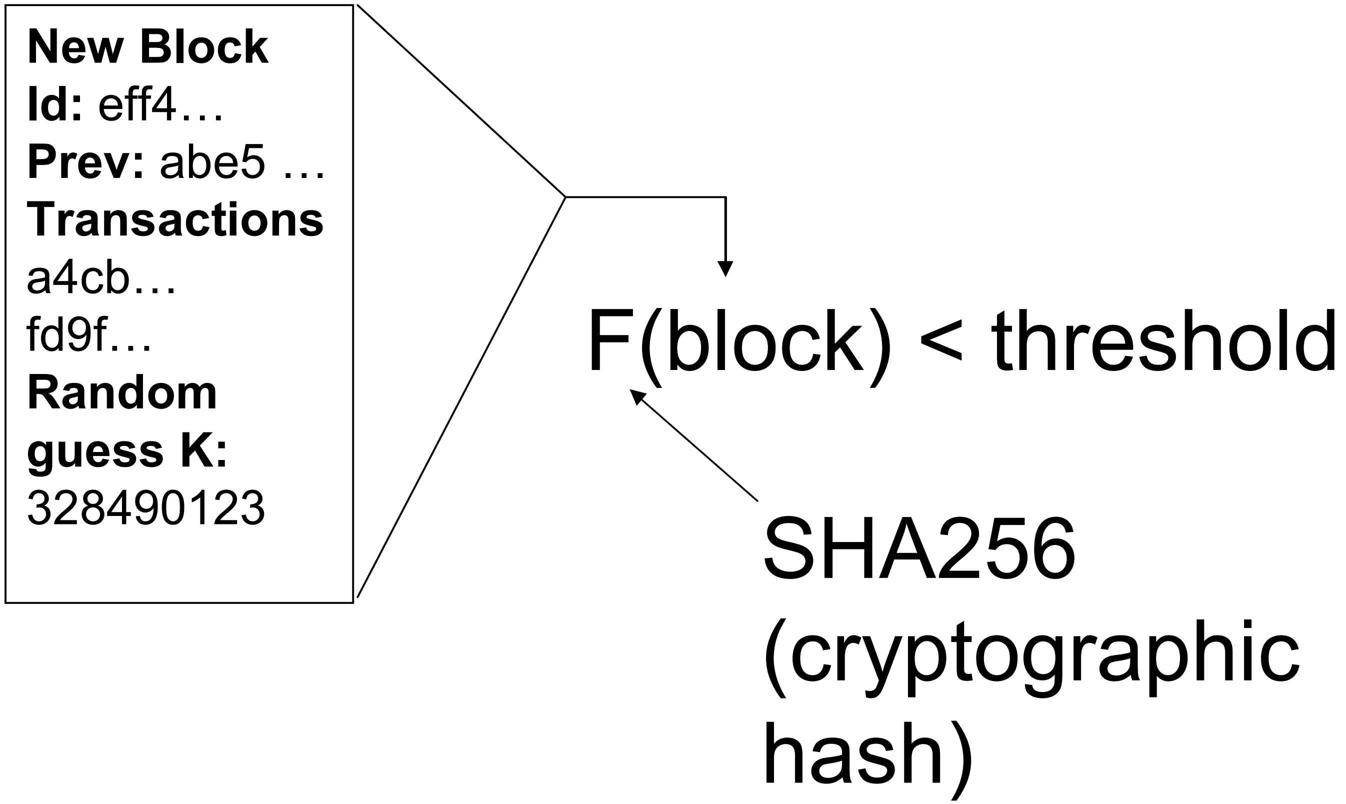
New Block
Id: a58b…
Prev: abe5 …
Transactions:
a4cb…
e37c…

by Bob

???

Math “puzzle”

To “solve” a block = find K such that



New Block
Id: eff4…
Prev: abe5 …
Transactions
a4cb…
fd9f…
Random guess K:
328490123

F(block) < threshold

SHA256 (cryptographic hash)

SHA256(“Complex Systems Seminars 2015”)

b5c941cdc49d79fa9fd3f777709c506f4d2256f4dfd615a54f79027b31e7b0f7

SHA256(“Complex Systems Seminars 2014”)

27c7b1fe7862b1d22ec190c26e0dfd657a0b85883f44fdae649fb1709ba874b3

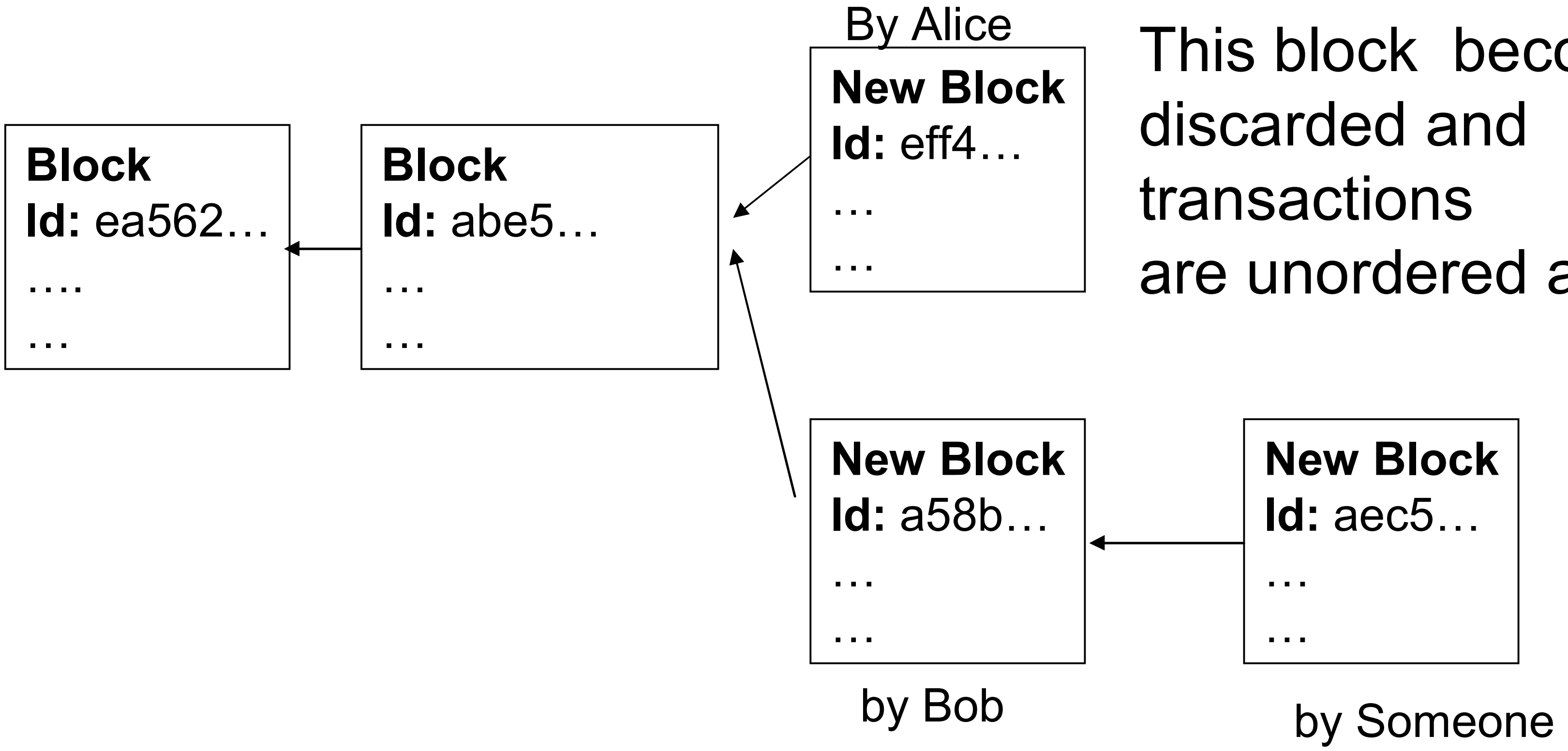
Very unpredictable

unconfirmed (unordered) transactions

a4cb…

fd9f…

e37c…



By Alice

New Block
Id: eff4…
…
…

Block
Id: ea562…
….
…

Block
Id: abe5…
…
…

New Block
Id: a58b…
…
…

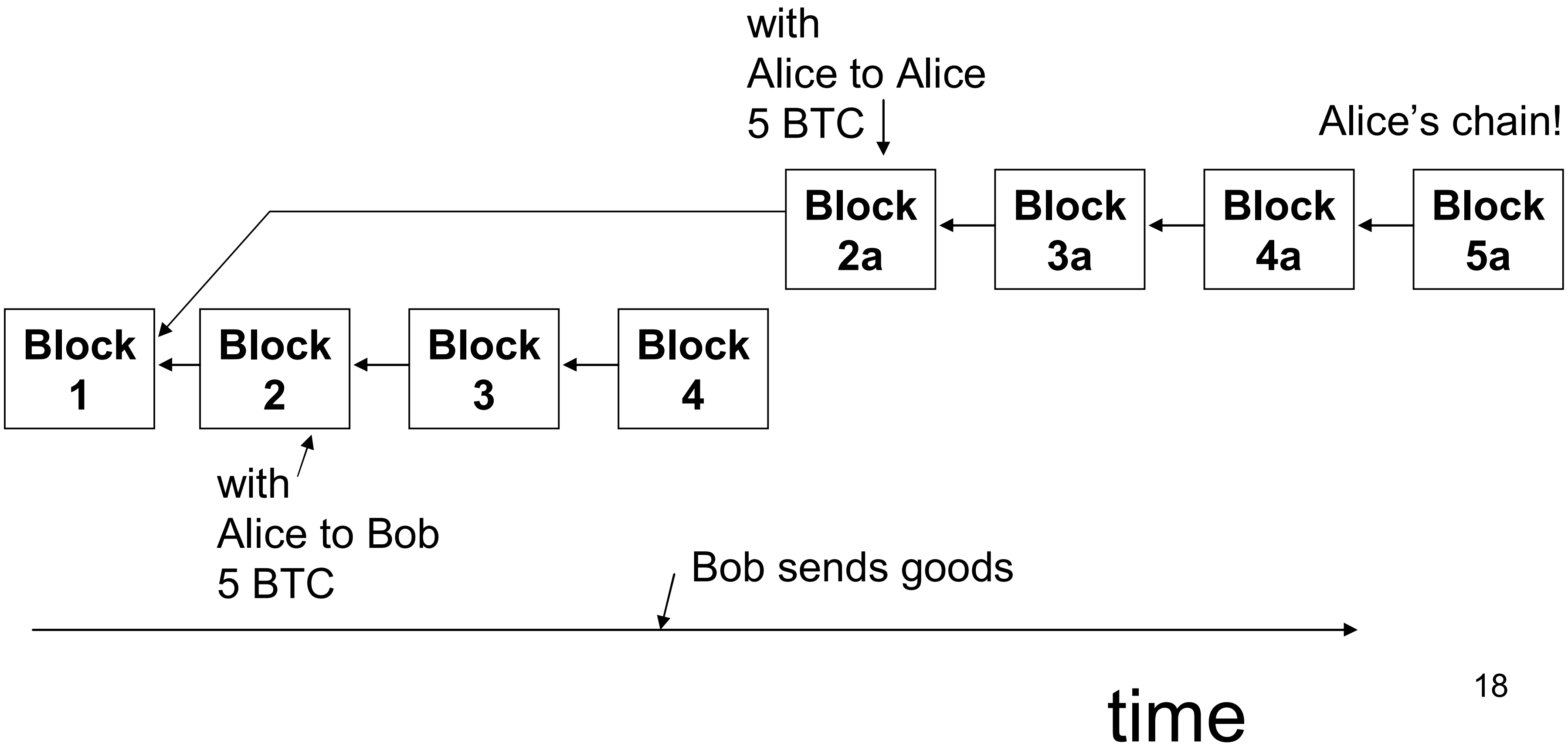
New Block
Id: aec5…
…
…

by Bob

by Someone

This block becomes d discarded and transactions
are unordered again.

Again double spending



with
Alice to Alice
5 BTC

Alice's chain!

with
Alice to Bob
5 BTC

Bob sends goods

time

New Block
Id: eff4…
Prev: abe5 …
Transactions
a4cb…
fd9f…
Random guess:
328490123

Block id = SHA256(block without id)

But with random guess

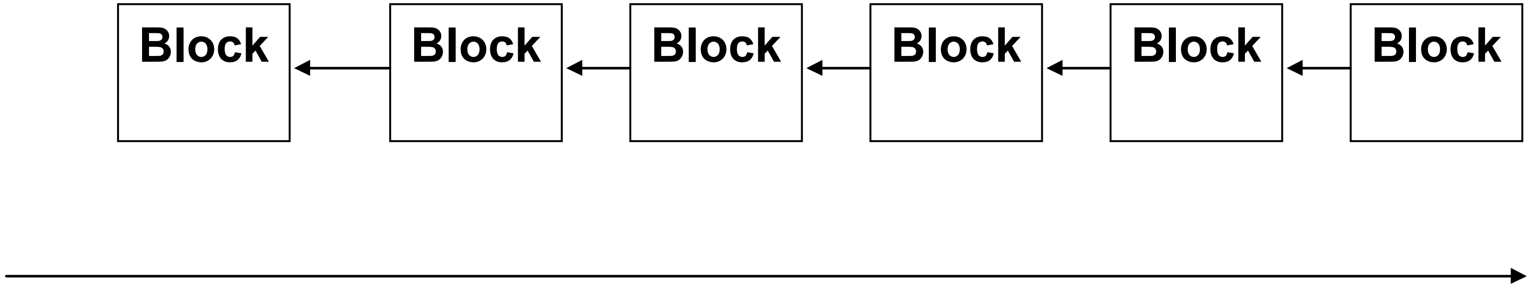
Alice

versus

~3*10^17 hashes \ second

More secure

less secure



Block

Block

Block

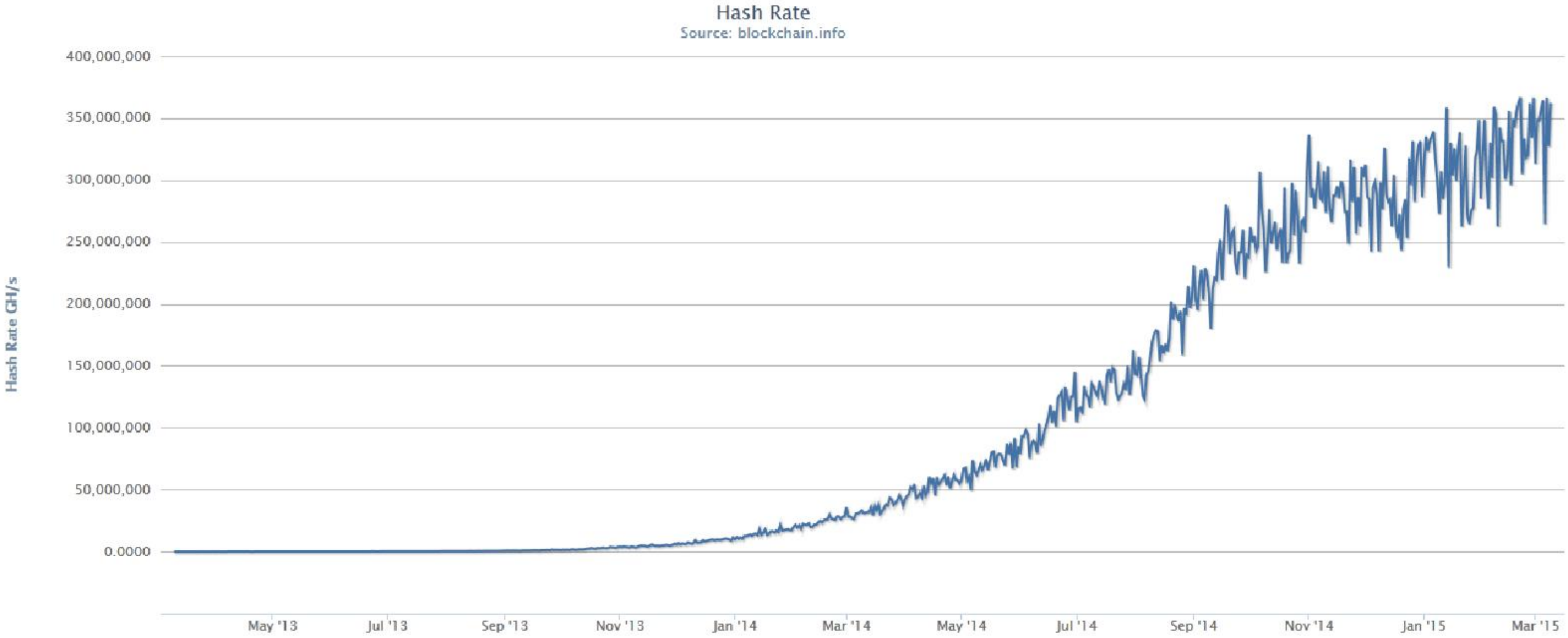
Block

Block

Block

time

Hash rate (1 GH\s = 10^9 H\s)



F(block) < threshold

How bitcoins are generated?

Mine them! Solved block = X bitcoins!

X <- X / 2 every 210000 blocks (four years)

Now X = 25 BTC

Already mined = 14 * 10^6 BTC

Overall = 21 * 10^6 BTC

Last will be mined in 2140

What if all bitcoins are mined?

Fees!

Transaction may have optional fee

Miners can prefer transaction with fees

Solved block gives fees from transactions in it.

Anonymity?

- All accounts and transactions are known.
- But which account is yours?
- New account for each transaction.

Disadvantages.

- Wrong address? Very likely BTC will be lost forever (2^160 addresses overall).
- Nobody guarantees anything (worse than fiat?).
- Waiting for transaction “confirmation”.
- Fees.
- Energy wasting.

Quick recap

Alice

Public key:
aaaaa…

Bob

Public key:
bbbbb…

transaction with
Alice as receiver:
3 BTC, id #fe12…
4 BTC, id #cd62…

Alice broadcasts (caricature):

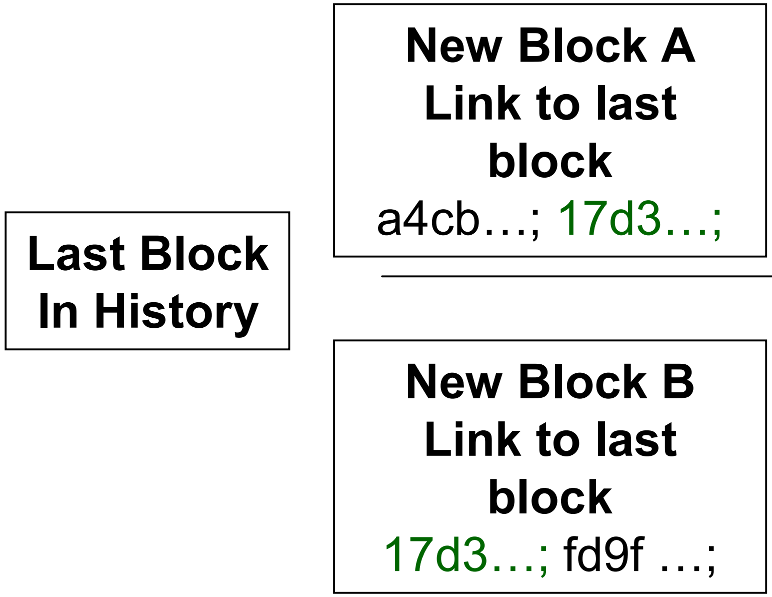
Current id #17d3…,
previous transactions #fe12…, #cd62…
to bbbbb… 5 BTC, fee 0.01 BTC,
remaining 1.99 BTC to aaaaa…

Miners side

unconfirmed (unordered) transactions

a4cb… fd9f… e37c… 17d3…

Miner A



Last Block In History

New Block A Link to last block a4cb…; 17d3…;

New Block B Link to last block 17d3…; fd9f …;

F(New Block A, K = 123)=135151>1000

F(New Block A, K = 124)=686976>1000

….

F(New Block A, K = 531)=789959>1000

F(New Block B, K = 6732)=351412>1000

F(New Block B, K = 6733)=576489>1000

….

F(New Block B, K = 9859)=997<1000

Miner B

Miner B solves puzzle (~10 minutes)

Then Miner B broadcasts (caricature):

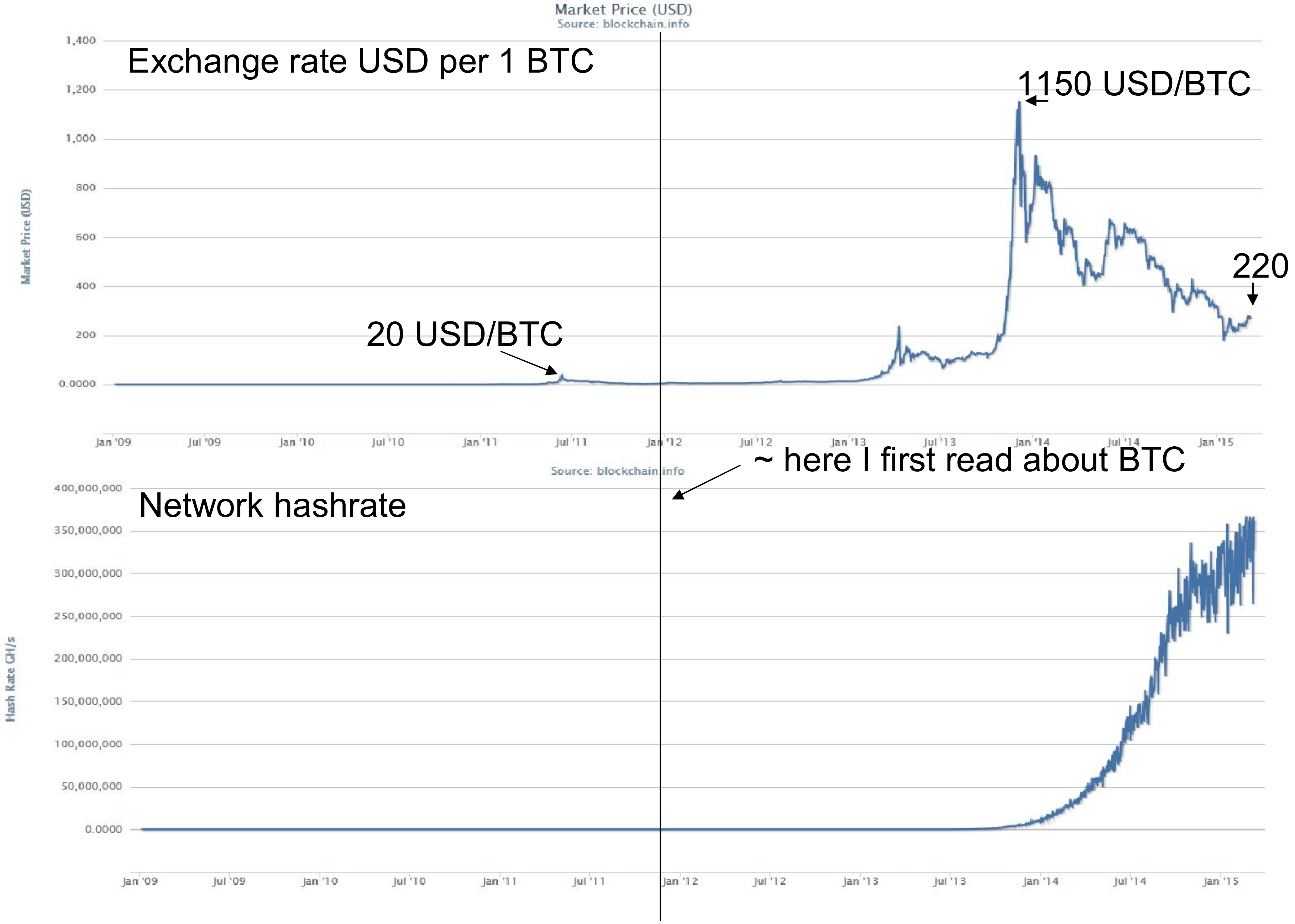
I (public key …) propose next block with transactions 17d3…; a4cb… and puzzle solution is K = 9859.

All participants (including Alice and Bob):
Get Miner B’s message, check the solution, update the history.
According to the rules Miner B’s gets 25 BTC and all fees from 17d3…; fd9f…; (including 0.01 BTC from Alice). This block in history is a proof.

Bob

- Knows that one block is quite risky confirmation – may be discarded by longer brunch.
- Therefore, he waits K more blocks (~K * 10 minutes) and sends goods.
- Success!

You said “a millionaire”



Exchange rate USD per 1 BTC

1150 USD/BTC

220

20 USD/BTC

~ here I first read about BTC

Network hashrate

On 22nd May 2010
Laszlo Hanyecz
bought
a pizza
for 10000 BTC
(25 USD at that time).

Sources:

0) Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-to-Peer Electronic Cash System"

1) bitcoin.org

2) How Bitcoin Works Under the Hood (youtube)

Simpler view:

The Essence of How Bitcoin Works (Non-Technical) (youtube)

How Bitcoin Works in 5 Minutes (Technical) (youtube)

Interesting:

Life Inside a Secret Chinese Bitcoin Mine (youtube)

(1.5 kkUSD per month)