



# Introduction to Bitcoin

Oleg Andreev  
[oleganza.com](http://oleganza.com)

Epitech, Paris  
April 25, 2013

Oleg Andreev  
@oleganza

19:00 Boring speech

19:40 Questions

22:00 End

**What is money?**

# Why use money?

**Why store money?**

# Kinds of money?

**How to move money?**





**The first digital commodity**

**Protocol + Software + Network**

**Like e-mail over Bittorrent**

**To receive: publish an address**

**To send: sign a transaction**

Decentralized

Inexpensive

Secure

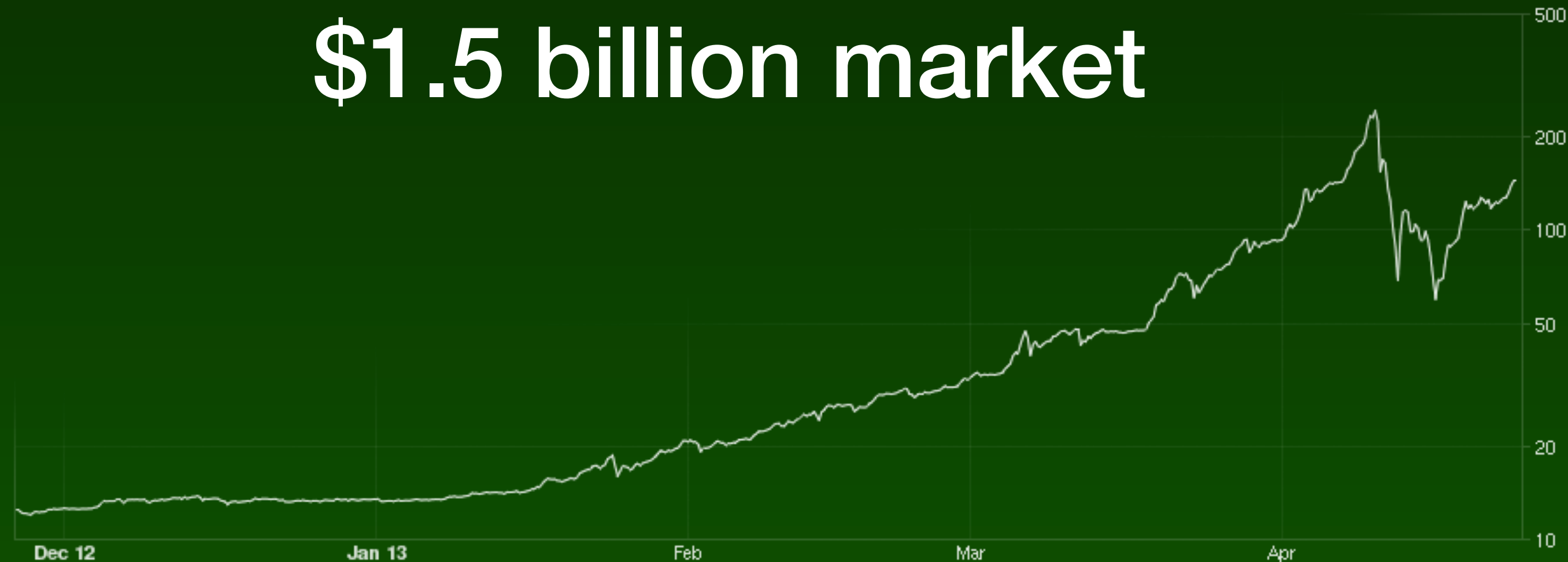
Private

Finite

4 years old

120€ per BTC

\$1.5 billion market



# How it works



# Dr Vincent

1817

Jan'y	28	To Sundries	10	1	6
	30	" Making 1 <sup>st</sup> Shoes	"	5	"
		" 2 Days Drying Flax	10	"	"
March	19	" Taping & mending 1 <sup>st</sup> Shoes	2	"	"
	23	" Taping & d <sup>o</sup> 3 shoes	"	2	9
	26	" Mending 1 <sup>st</sup> Boots	"	1	"
April	5	" Taping & m <sup>o</sup> lt Boot	2	"	"
	26	" Mending 2 <sup>nd</sup> Shoes	3	"	"
May	8	" Mending 1 <sup>st</sup> Boots 1 Shoe	2	6	"
			£ 11 1 9		

1817

May	27	To Balance Due	1	"	8
	29	" Making 1 <sup>st</sup> Shoes binding	6	"	"
June	12	" Making 1 <sup>st</sup> Shoes d <sup>o</sup>	"	5	6
		" Making 1 <sup>st</sup> Shoes	"	1	6
	21	" Making 1 <sup>st</sup> Shoes	"	6	"
August	9	" Taping 1 <sup>st</sup> Shoes heels	"	2	6
		" Rake	"	2	"
Oct <sup>r</sup>	4	" 1/2 Bushel Uncom	"	4	"
		" 1 Day haying	"	9	"
		with Boy			
		" 1 Day Curing Corn	"	8	"
		with Boy			
	7	" Making 1 <sup>st</sup> Shoes binding	5	6	"
	20	" Making 1 <sup>st</sup> Shoes	"	5	6
		" 1 Day Whem-har Draining	"	2	"
	24	" Making Buck Wheat	"	6	"

# Stillwell Dr

1817

Jan'y	28	By Sundries	9	16	1
May	17	" Horses & Plow	"	5	" 8
		" Balance Due on Settlement	£ 11 1 9		

This day recon'd & settled all acc<sup>ts</sup>  
& find due two Dollars fifty Eight

Cents Durham May 27<sup>th</sup> 1817

Christ<sup>o</sup> Watrous

Vincent Stillwell

July	1	By 3/4 bushel Plaster	"	4	6
		" horse to Plow Corn	"	2	"
		" Hammer	"	2	"
Oct <sup>r</sup>	4	" Horses & Plow	"	6	"
		" Flax ground	"	1	" 0
		" Herring glassed	"	3	9
Dec <sup>r</sup>	4	" 8 Bus. Buck Wheat	"	4	"
			3 2 3		

Feb <sup>y</sup>		To Sundries	4	9	5
		" Mending 1 <sup>st</sup> Shoes & Boot	"	1	6
March	3	" Mending 3 Shoes	"	2	3



# Traditional ledger

From	To	Amount
Pascal	Oleg	10
Oleg	Gwendal	5
Gwendal	Thomas	4
Thomas	Oleg	3
...	...	...

# Computing balance

From	To	Amount
Pascal	Oleg	10
Oleg	Gwendal	8
Gwendal	Thomas	4
Thomas	Oleg	3
...	...	

**Total: +5**

# Problem

Easy to manipulate

Single point of failure

15th century tech

# Git-like ledger

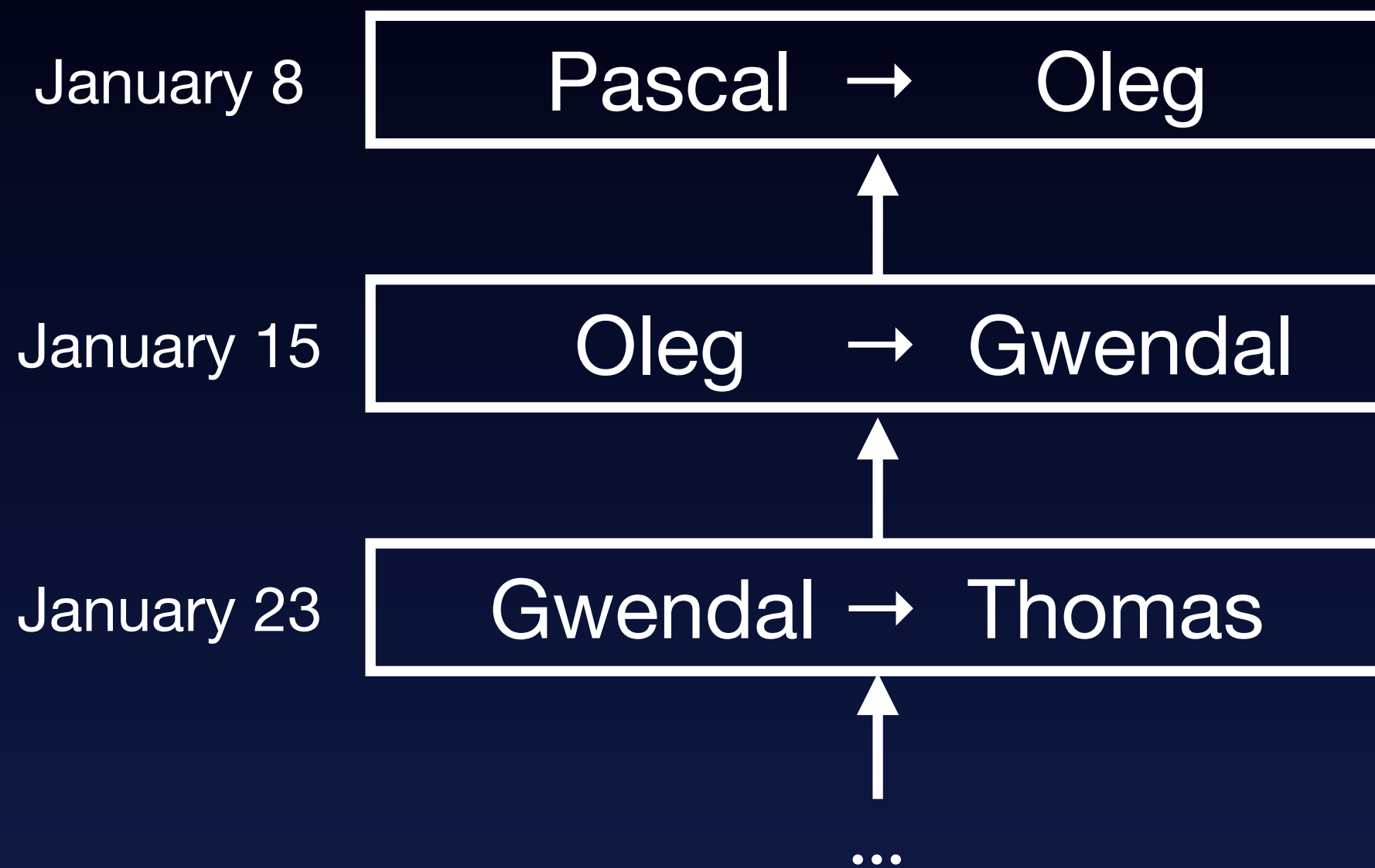
Directed acyclic graph

Input: signed parent hash

Output: signature requirement

Ownership via private keys

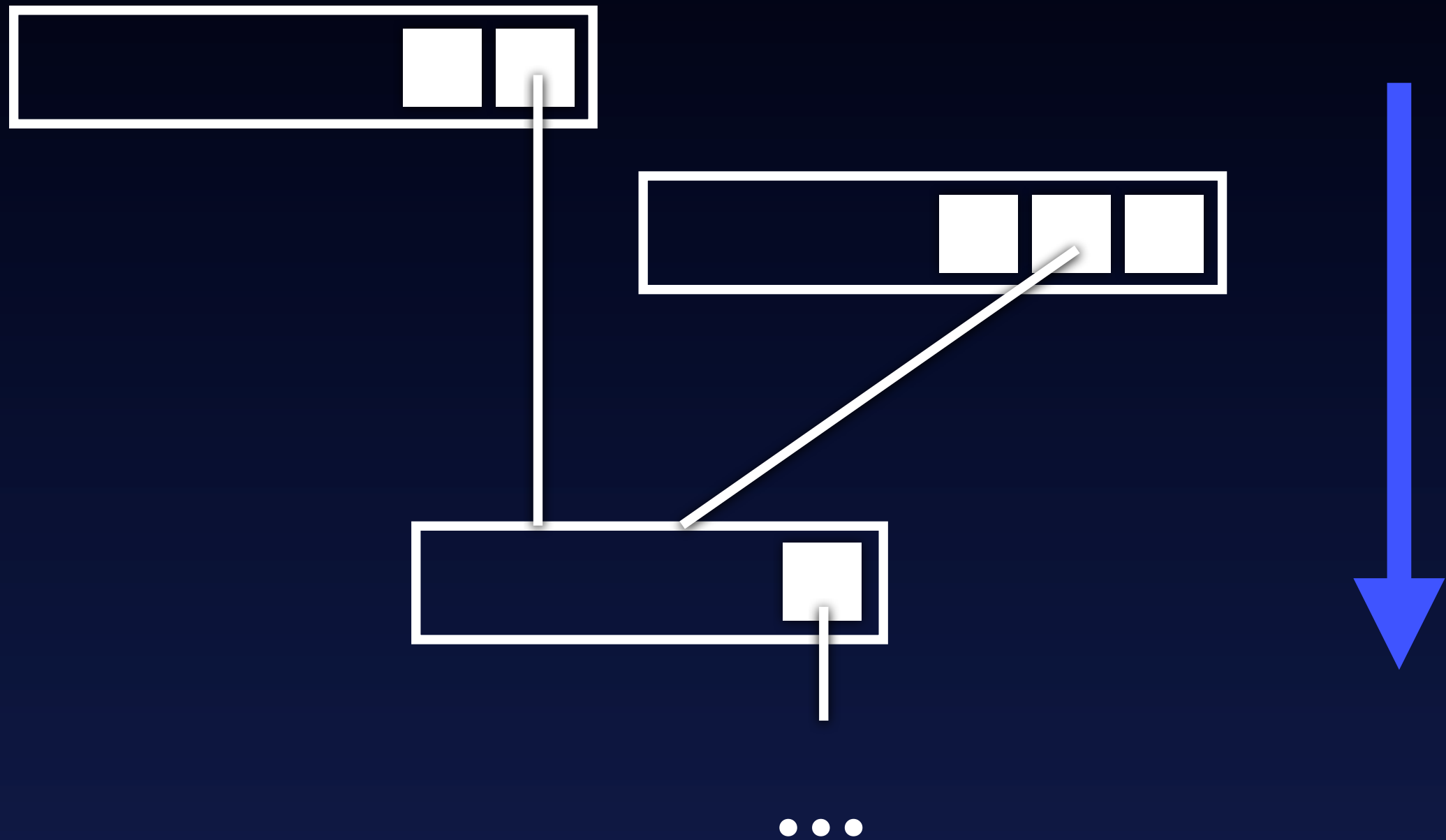
# Transaction chain



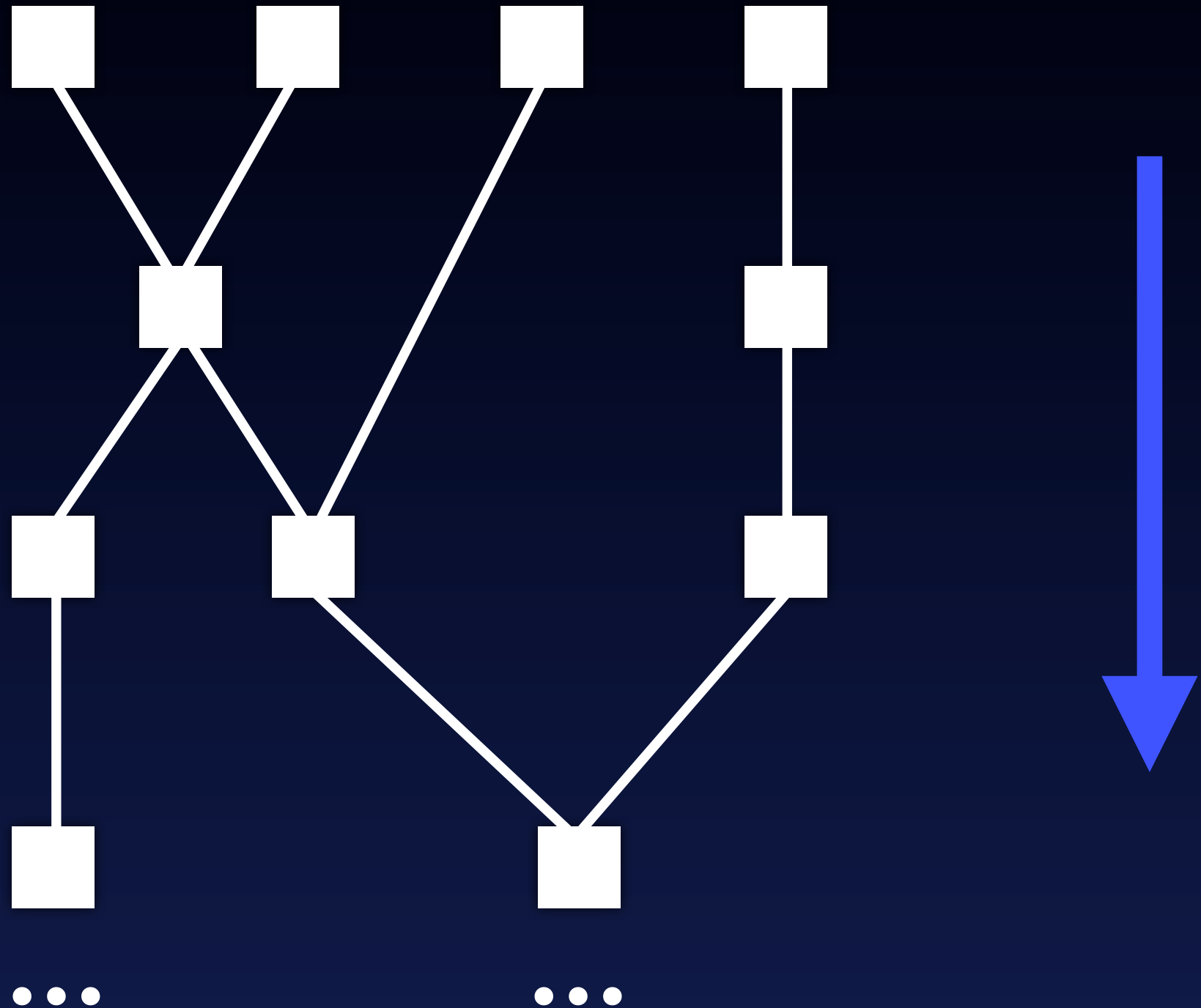
# Transaction

Input		Output	
parent hash ←	signature	3.14฿	pubkey ←

# Multiple outputs



# Transaction graph





# Multiple outputs

Inputs			Outputs		
tx1 hash	1	signature1	0	3.00฿	pubkey1
tx2 hash	5	signature2	1	0.14฿	pubkey2
tx3 hash	0	signature3			

# Valid transaction

- 1) All hashes are valid
- 2) All signatures are valid
- 3) Sum of outputs  $\leq$  sum of inputs
- 4) No double spends
- 5) Valid origin (first transaction)

# Remaining issues

- 1) All hashes are valid
- 2) All signatures are valid
- 3) Sum of outputs  $\leq$  sum of inputs
- 4) No double spends
- 5) Valid origin (first transaction)

# Double spends

First transaction wins

Decentralized agreement on order

# Proof-of-work

Voting with CPU power

Easy to verify

Hard to redo

# Blockchain

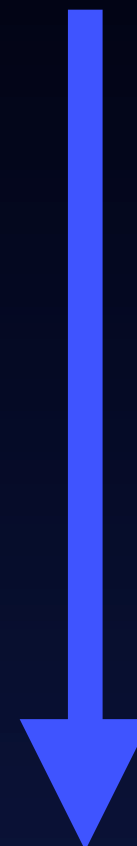
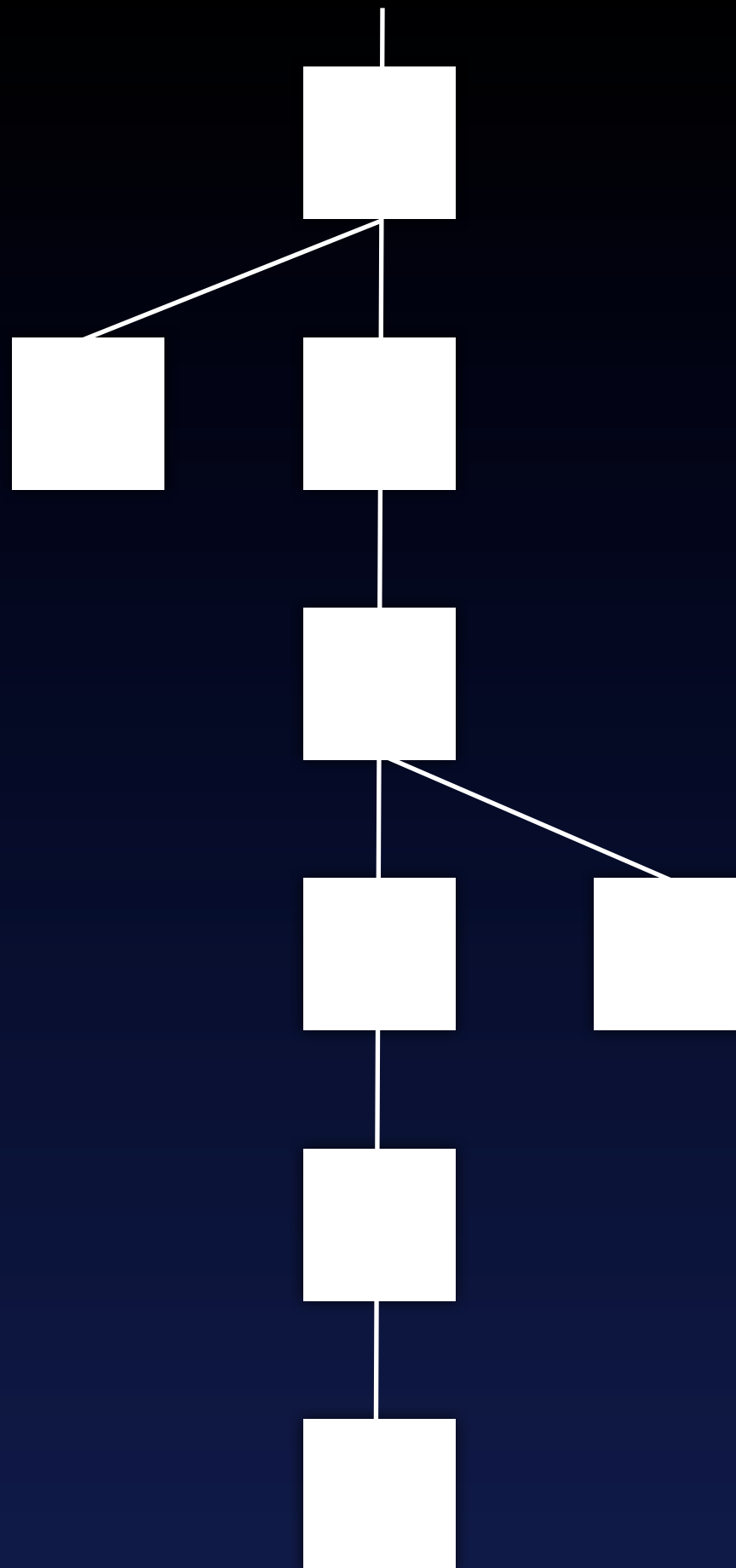
Block is a group of transactions

Blocks form a hash tree

Block hash is hard to compute

Main chain = most difficult chain

Forks possible, but unsustainable



# Block

hash	000000000360d3f28a3fb7ef891385...
parent	0000000005c1d865d28ee6c3f495a...
tx hash	b5f82255db7f8ad9ffd67d6b7f8ad2d...
timestamp	1360137751
nonce	123456
transactions	<i>list of transactions</i>



# Difficulty = number of zeros

hash	000000000360d3f28a3fb7ef891385...
parent	0000000005c1d8b5d28ee6c3f495a...
tx hash	b5f82255db7f8ad9ffd67d6b7f8ad2d...
timestamp	1360137751
nonce	123456
transactions	<i>list of transactions</i>

# Valid block

All hashes are valid

All txs are valid in the block

All txs are valid in the block chain

Proof-of-work is valid

# How to make a block

Collect transactions

Collect previous blocks

Iterate nonce

Compute hash for the block

Publish if hash  $<$  target number

# Incentives

Blocks require real energy and time

Transaction fees

New coins

Call it “mining”

# Money supply

Block is created every 10 minutes

Difficulty adjusts every 2 weeks

Reward is halved every 4 years

99% of supply by 2030

Max 2000 trillion atomic units

# Money supply

millions

20

15

10

5

0

2009

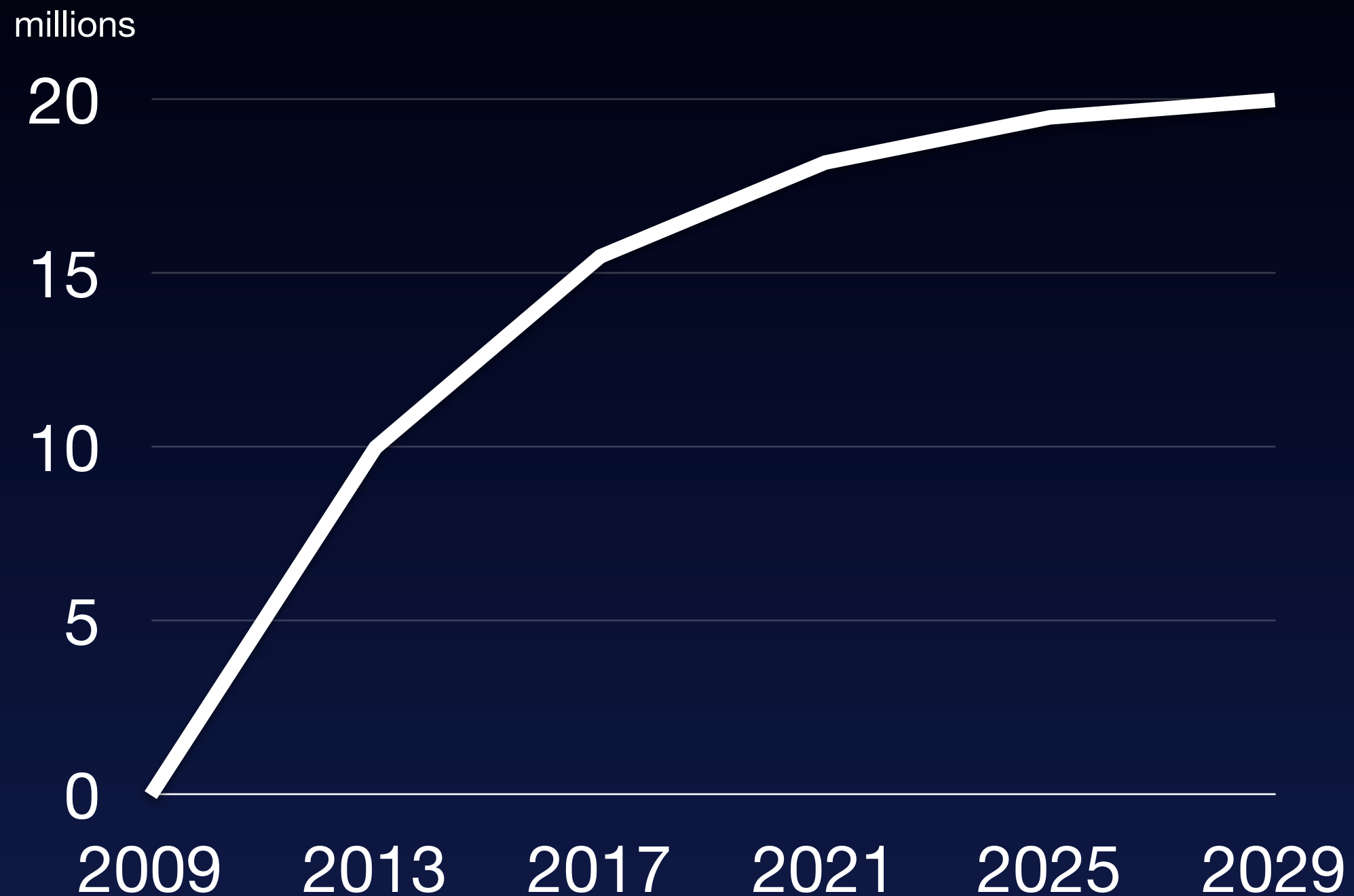
2013

2017

2021

2025

2029



# Security

256-bit ECDSA for keys

Double SHA-256 for block/tx hashes

51% of power allows double spends

Economically impractical

850 PetaFLOPs (4x Top500 supercomputers)











# Insecurity

Lost passwords

Lost backups

Trojans

# Insecurity

Exchanges and web wallet hacks

Overflow bug in 2010

Hard fork in 2013

# Summary

Inexpensive and private currency

Fault-tolerant

Many security options

Allows micropayments

Protects fortunes

# References

Slides: <http://oleganza.com/bitcoin-epitech.pdf>

Paper: <http://bitcoin.org/bitcoin.pdf>

Wiki: <http://bitcoin.it>

Browser: <http://blockchain.info>

Charts: <http://bitcoincharts.com/charts>

Buy: <http://bitcoin-central.net>



<http://oleganza.com/bitcoin-epitech.pdf>