

Virtual Currencies: Obstacles and Applications Beyond Currency

Sarah Meiklejohn (University College London)

ECB categories of virtual currencies

ECB categories of virtual currencies



ECB categories of virtual currencies



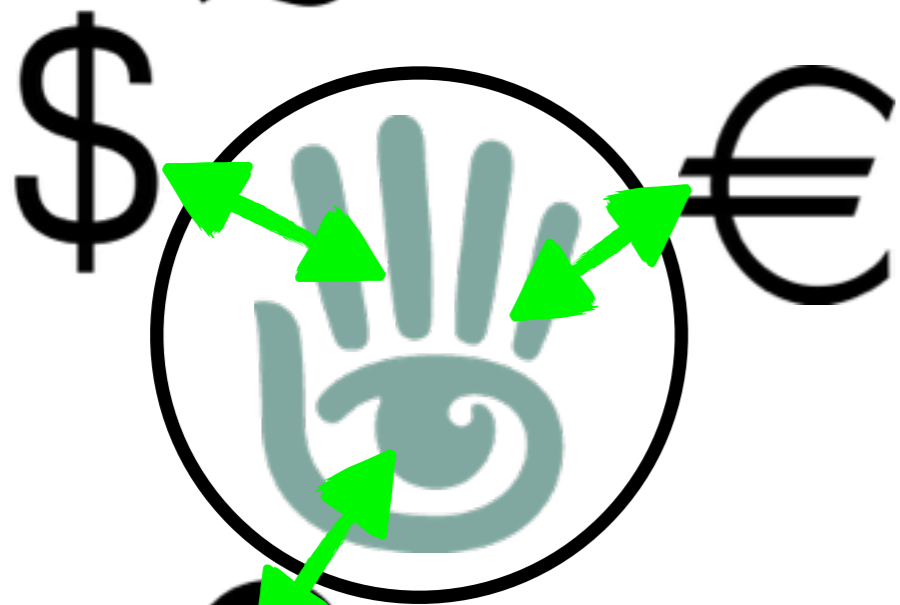
ECB categories of virtual currencies



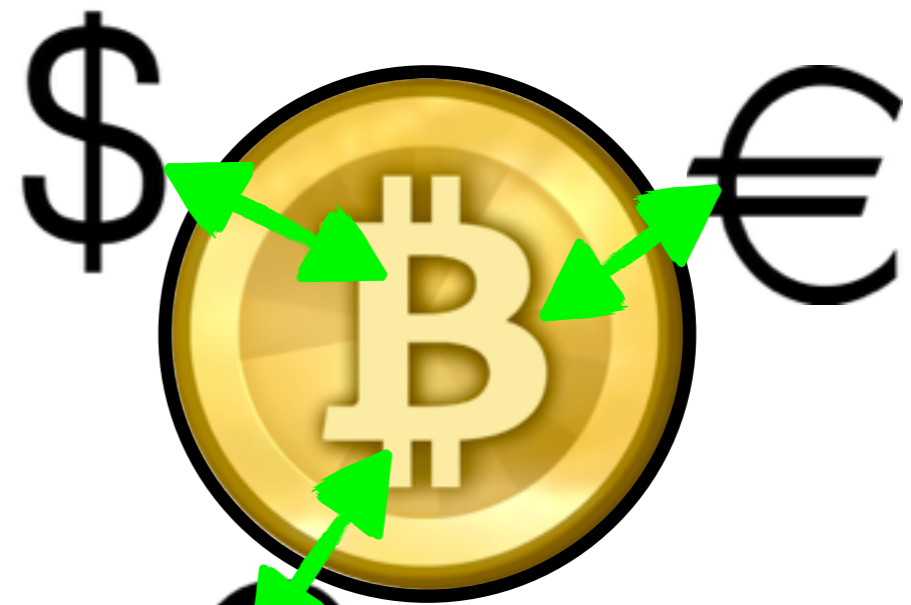
“closed”



“one direction”



“convertible”



“convertible”

ECB categories of virtual currencies



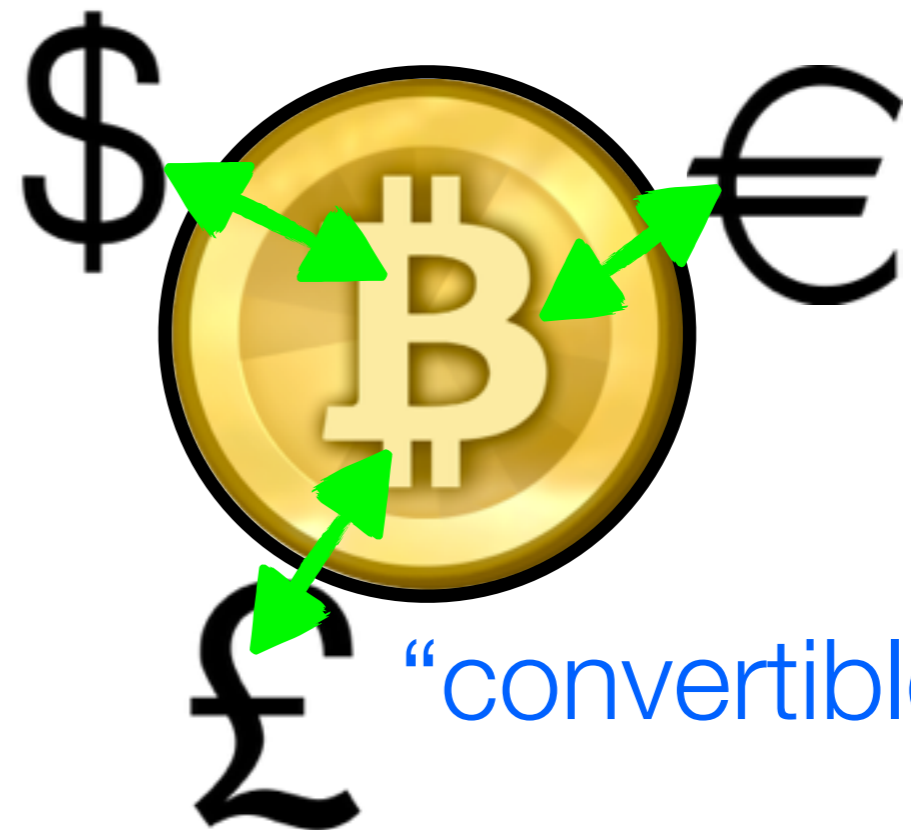
“closed”



“one direction”

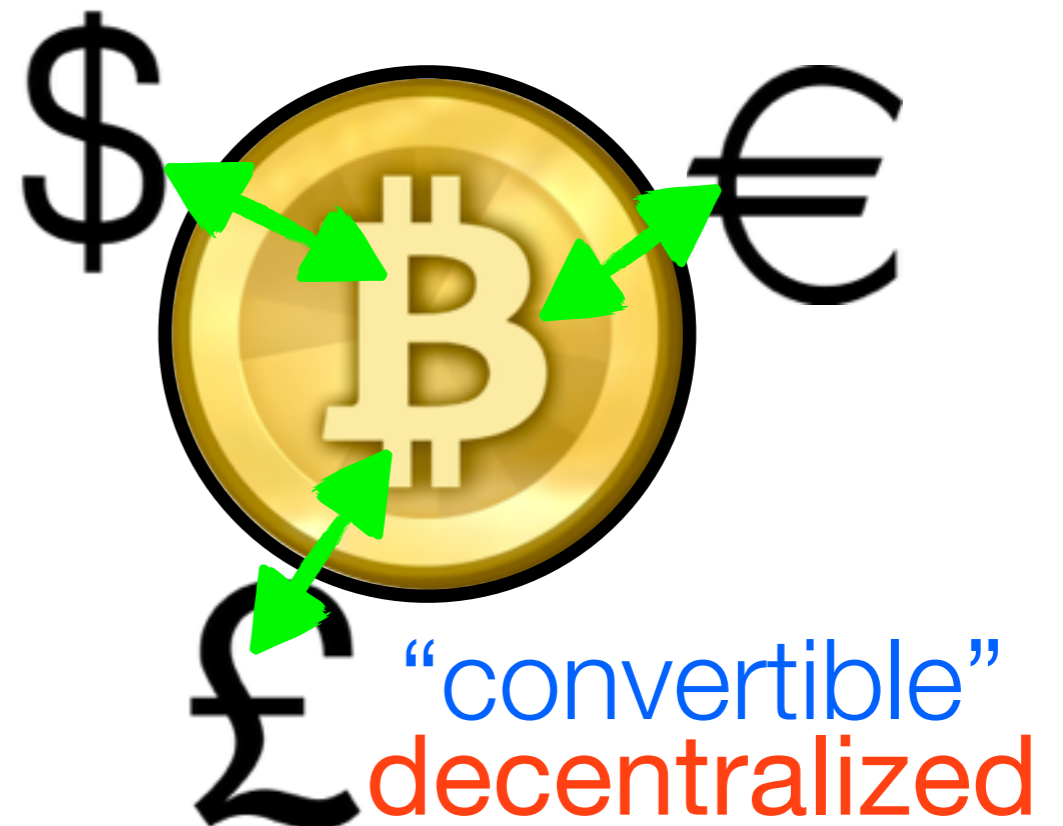


“convertible”
centralized

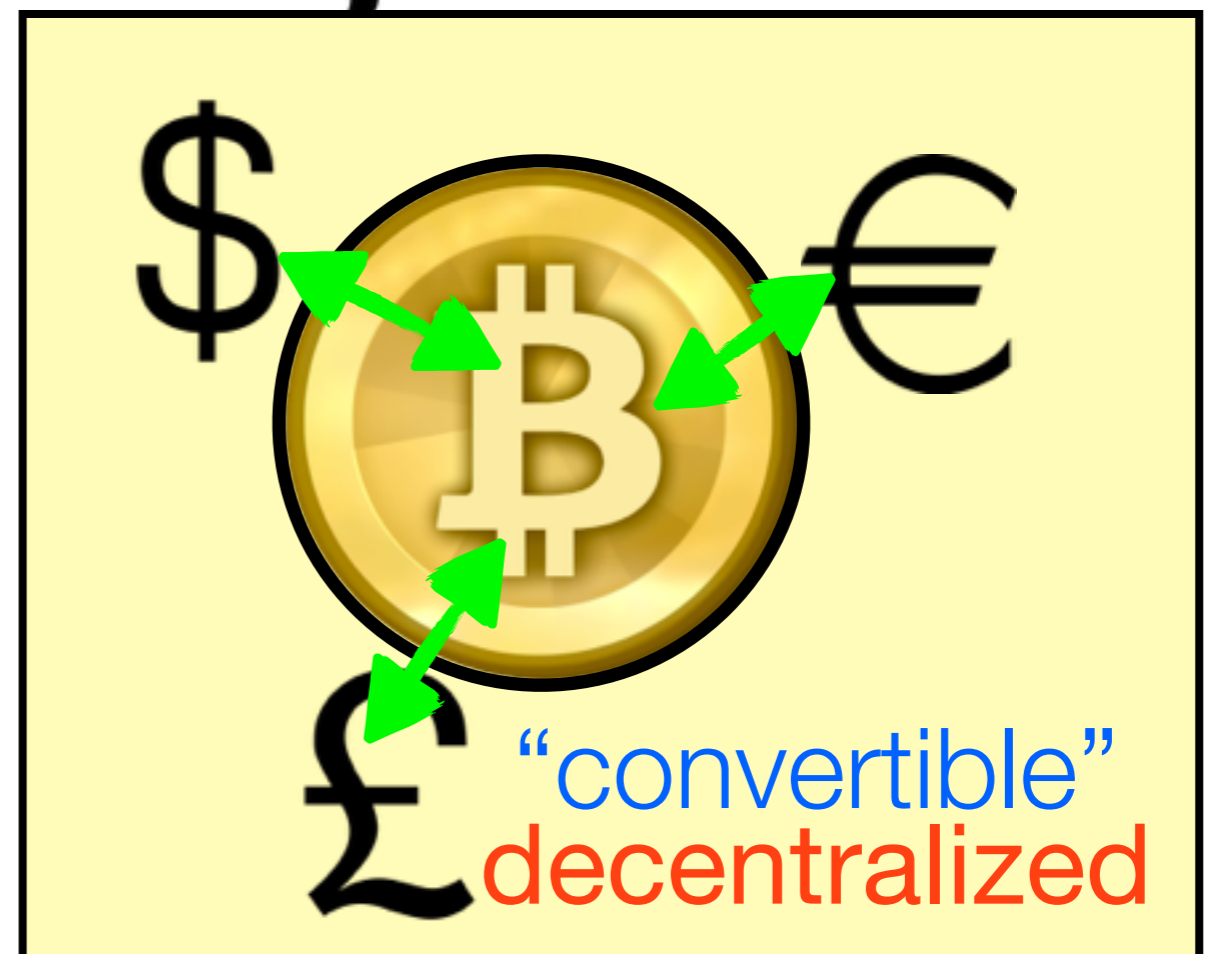
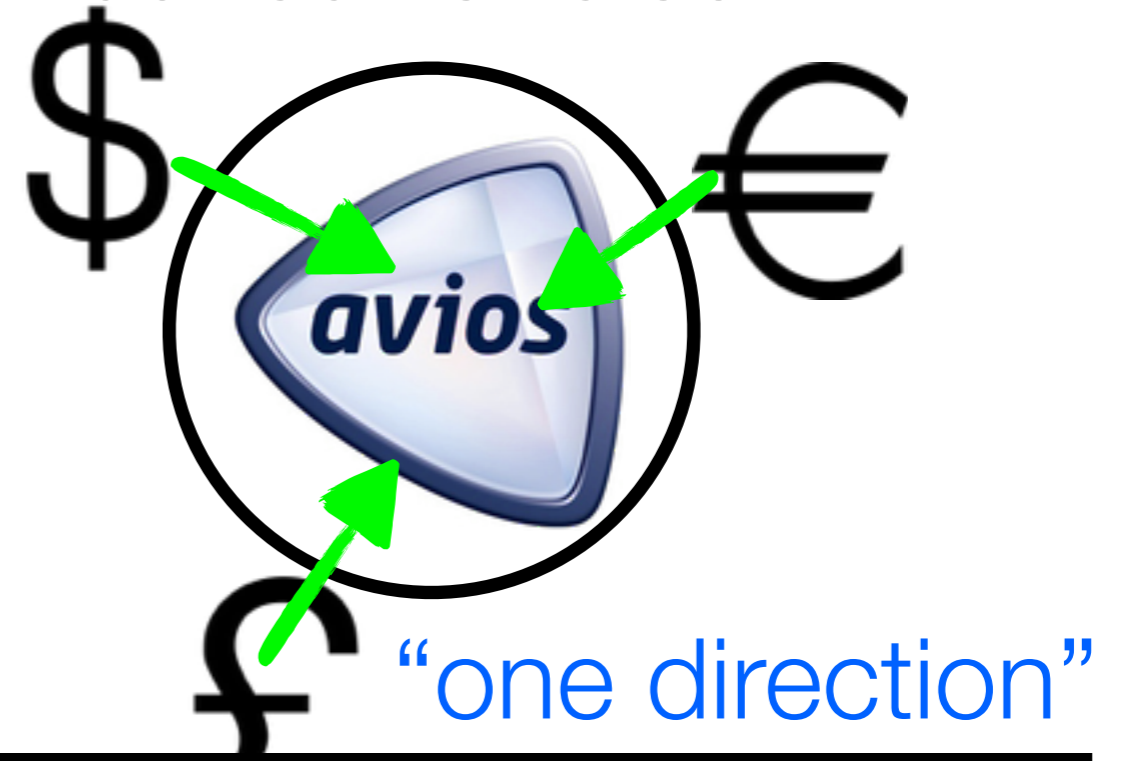


“convertible”

ECB categories of virtual currencies



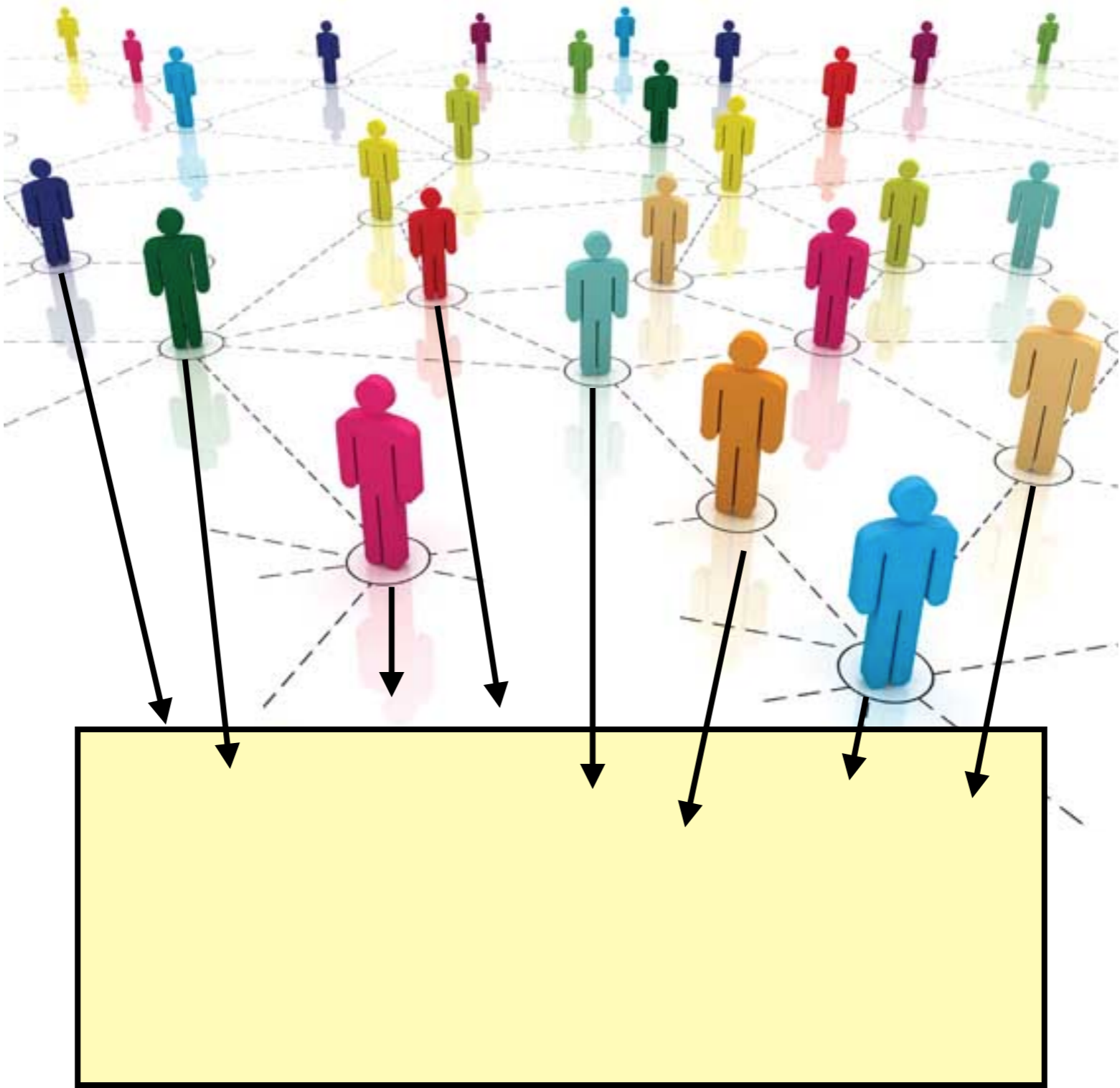
ECB categories of virtual currencies



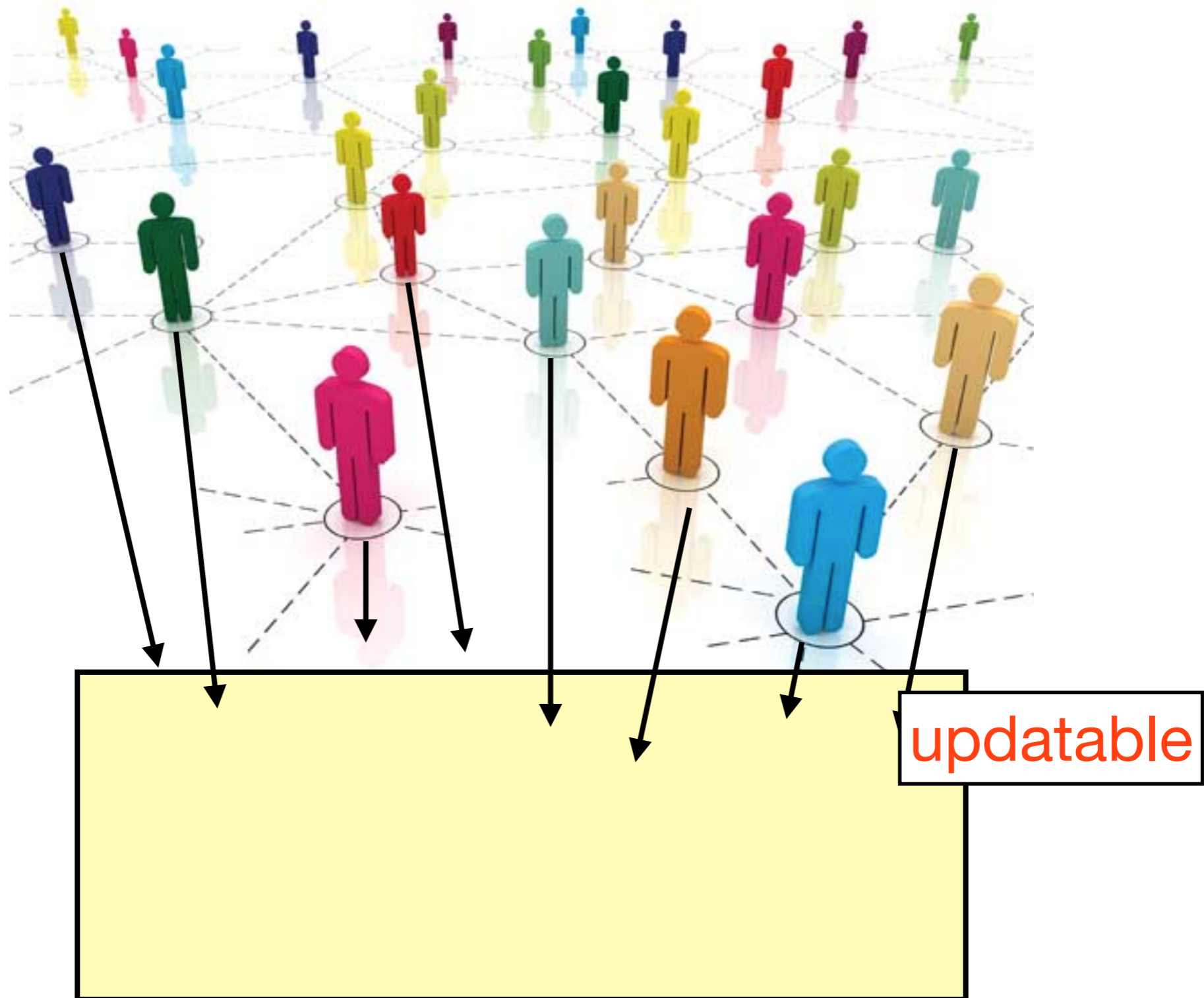
decentralized consensus



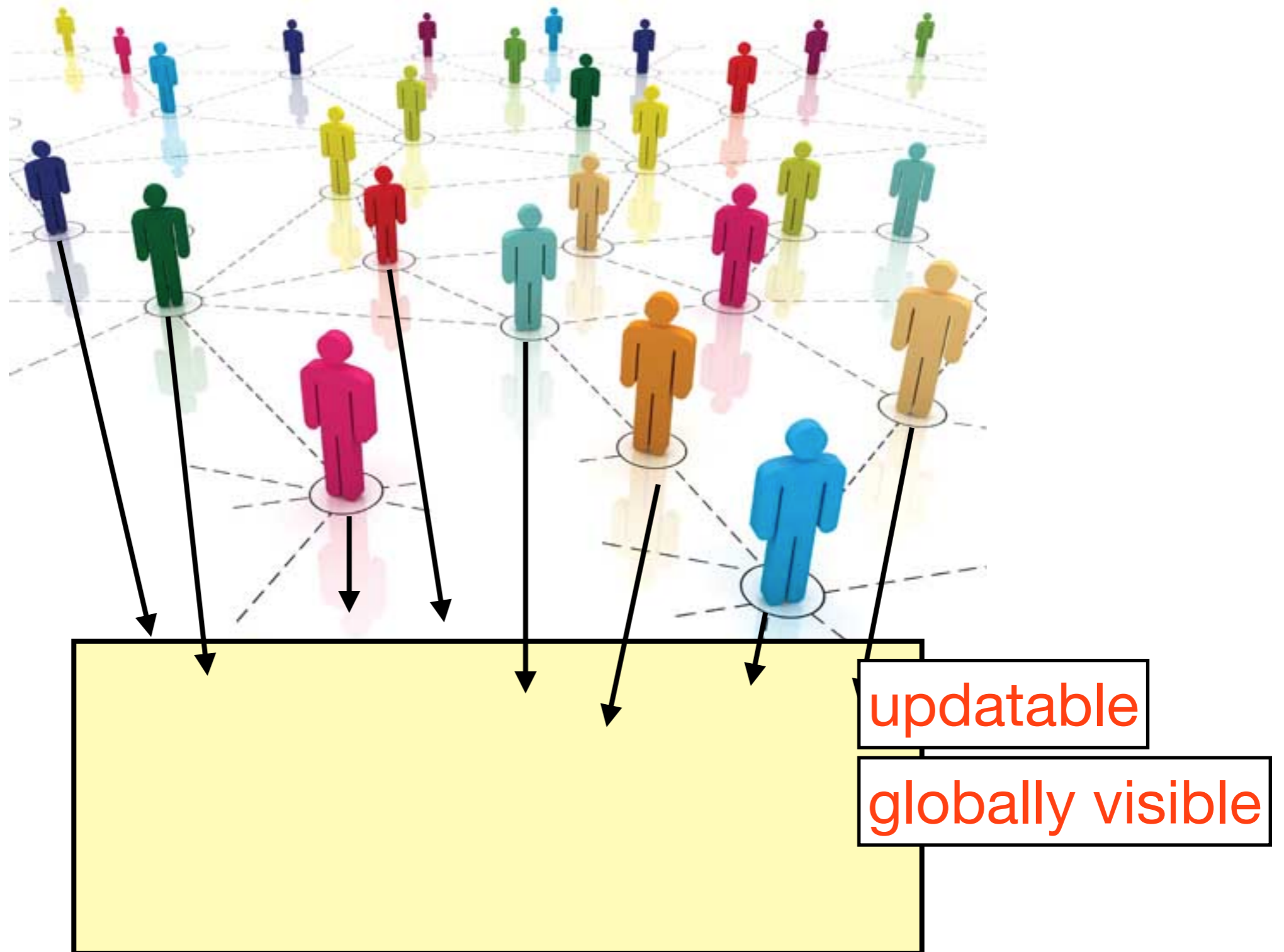
decentralized consensus



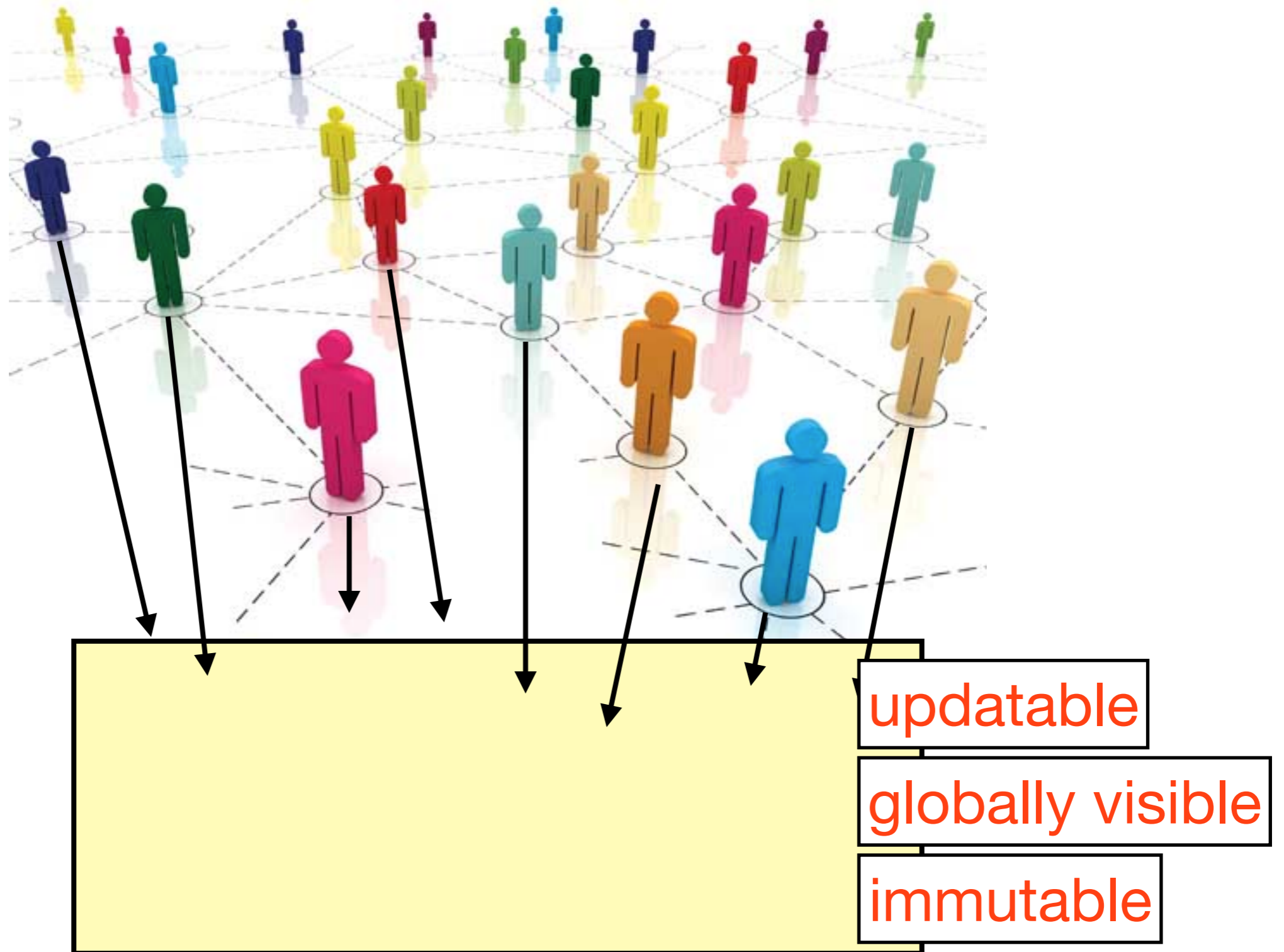
decentralized consensus



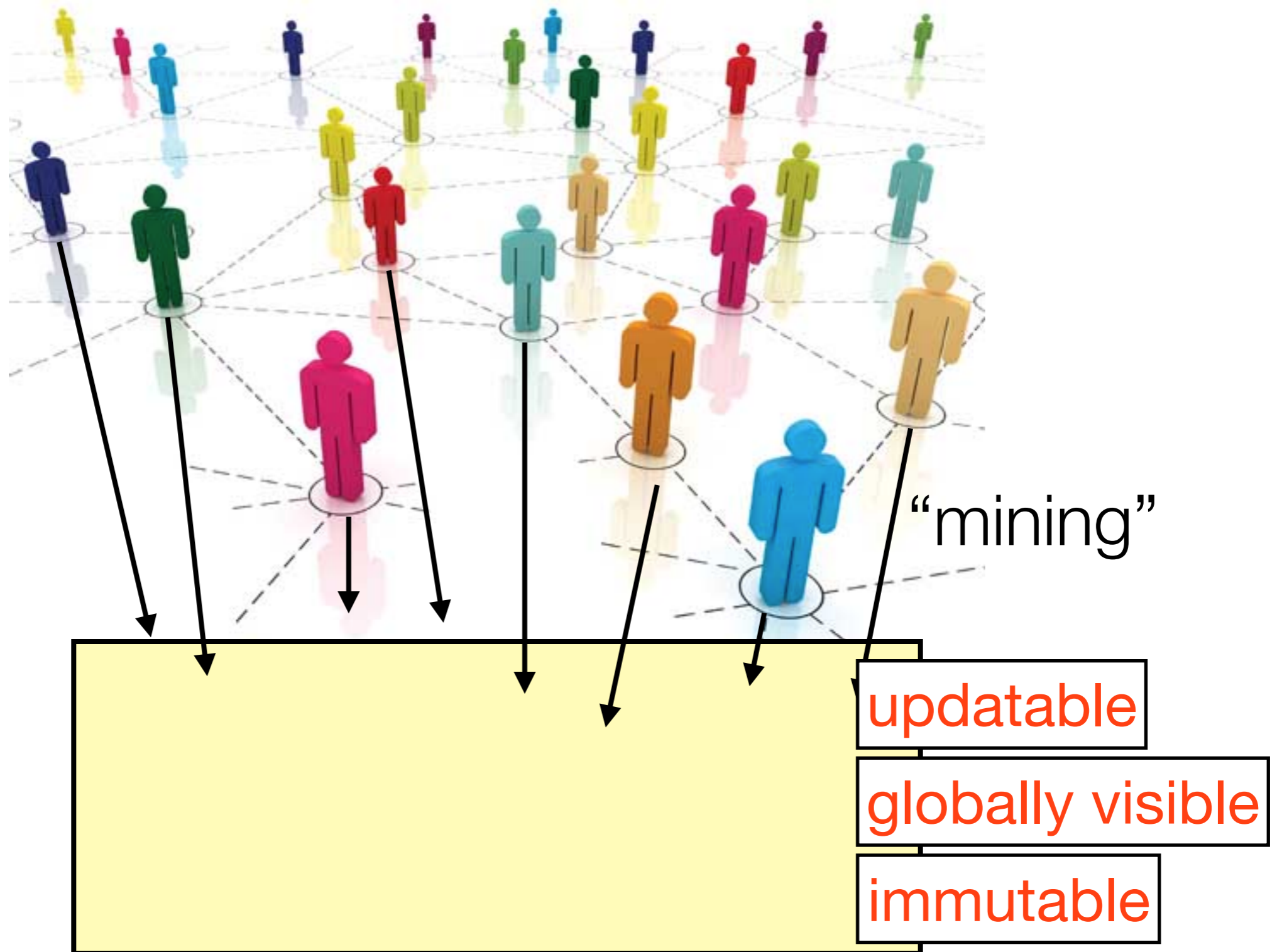
decentralized consensus



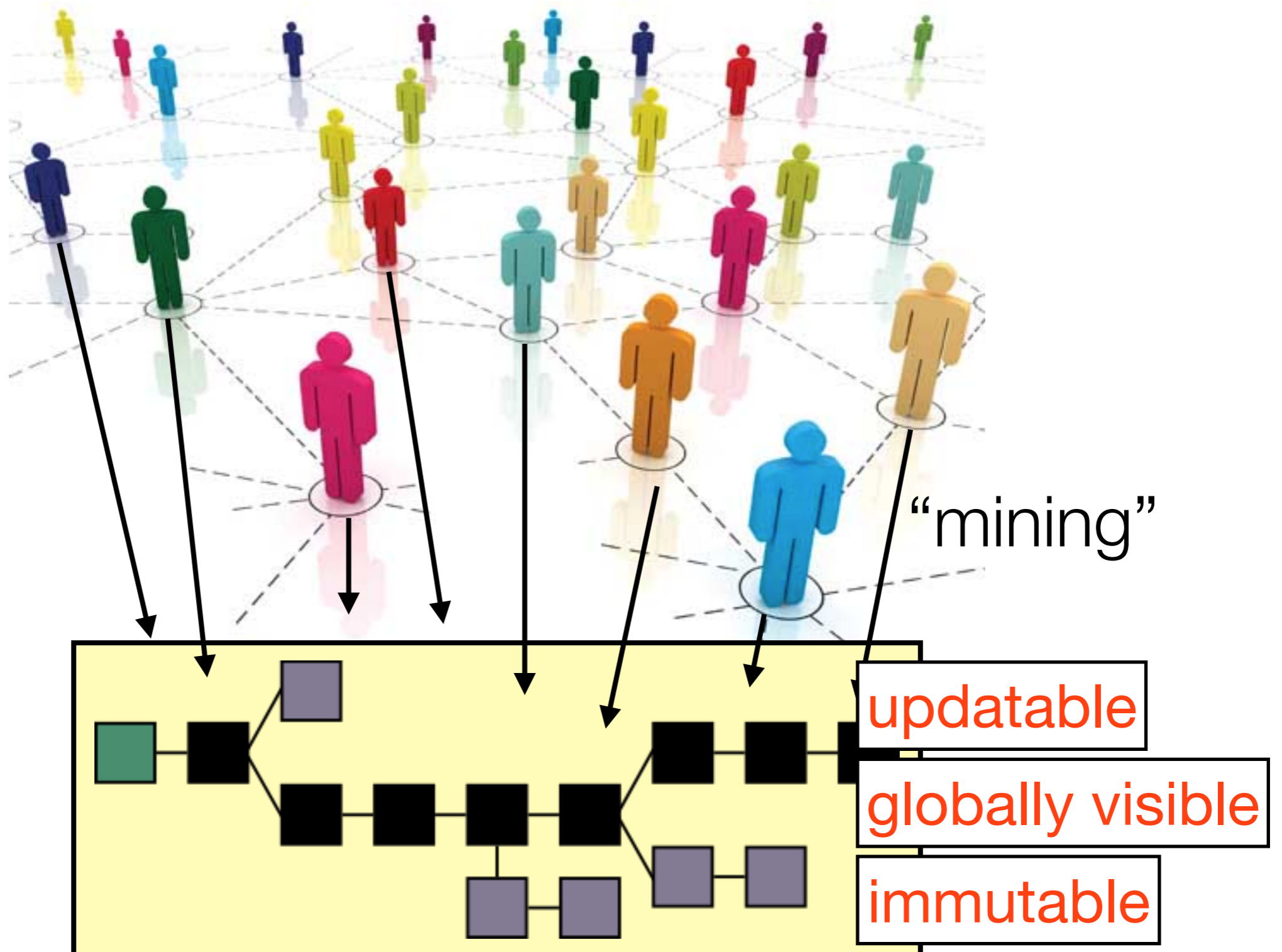
decentralized consensus



decentralized consensus

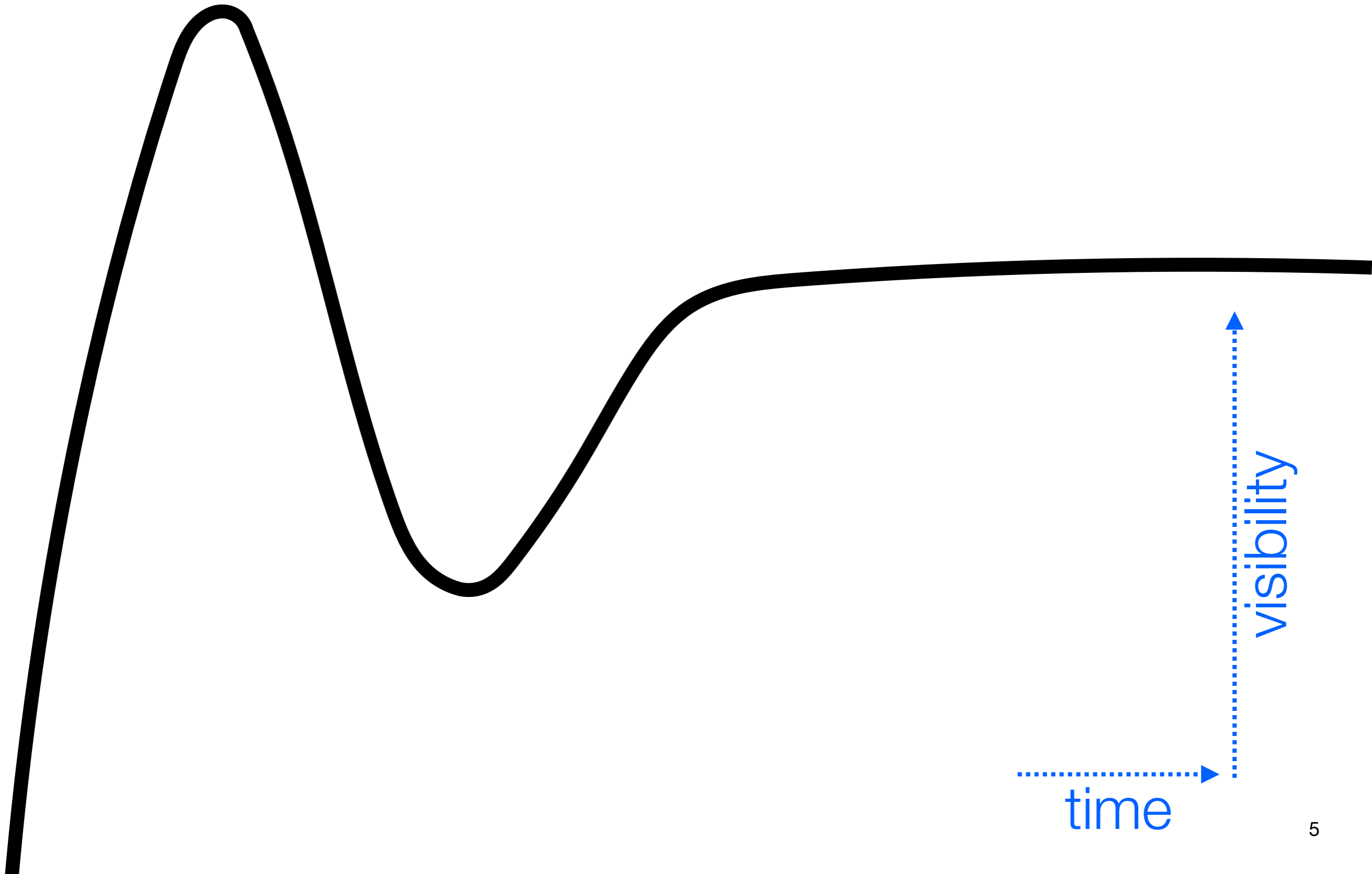


decentralized consensus

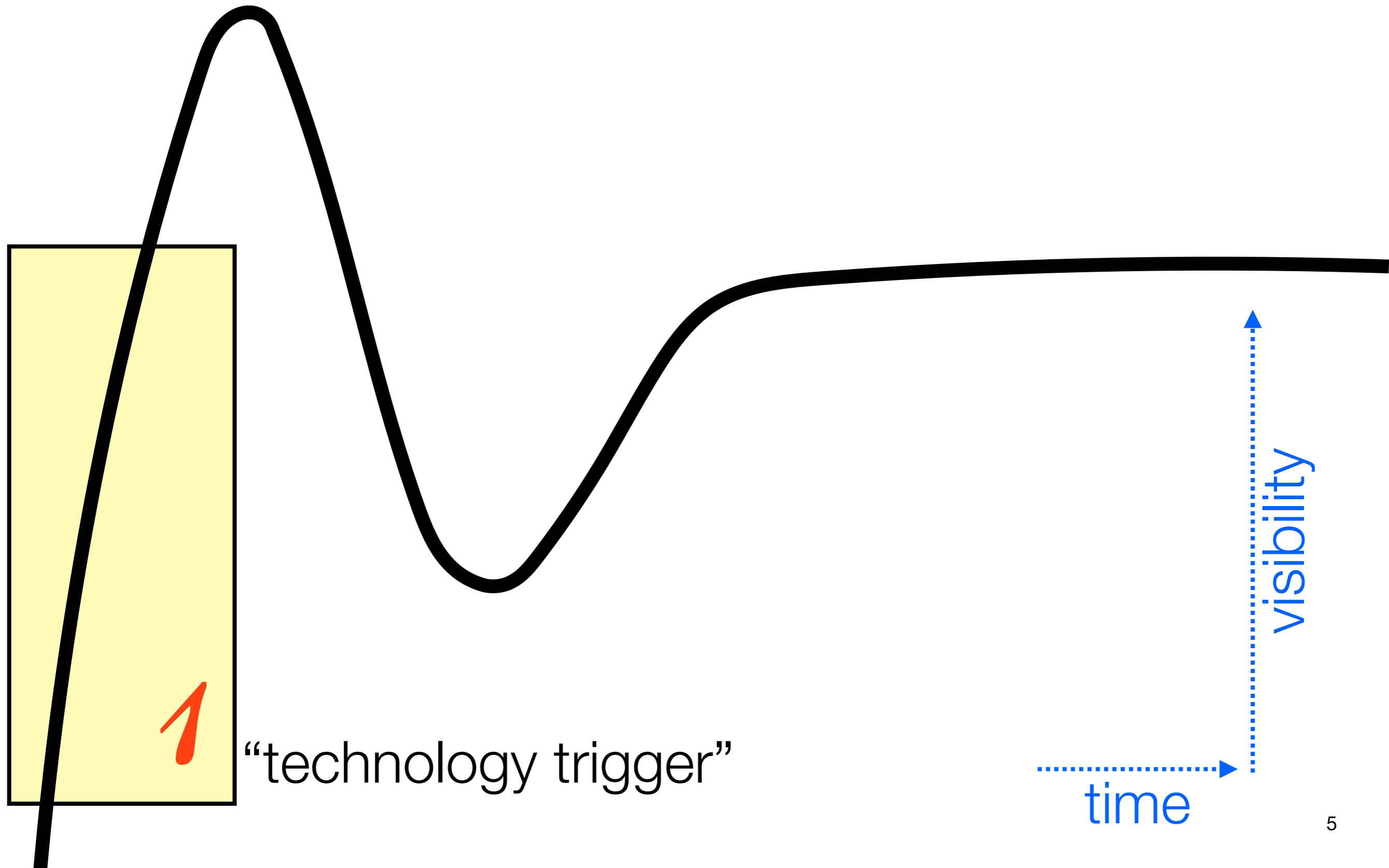


the **hype cycle** of cryptocurrencies

the **hype cycle** of cryptocurrencies



the **hype cycle** of cryptocurrencies



Bitcoin
paper



time

Bitcoin
paper



2009

2010

2011

2012

2013

2014

Bitcoin
deployed



time

Bitcoin
paper

฿1 =
\$0.0007

2009

2010

2011

2012

2013

2014

Bitcoin
deployed

time

Bitcoin
paper

฿1 =
\$0.0007

2009

2010

2011

2012

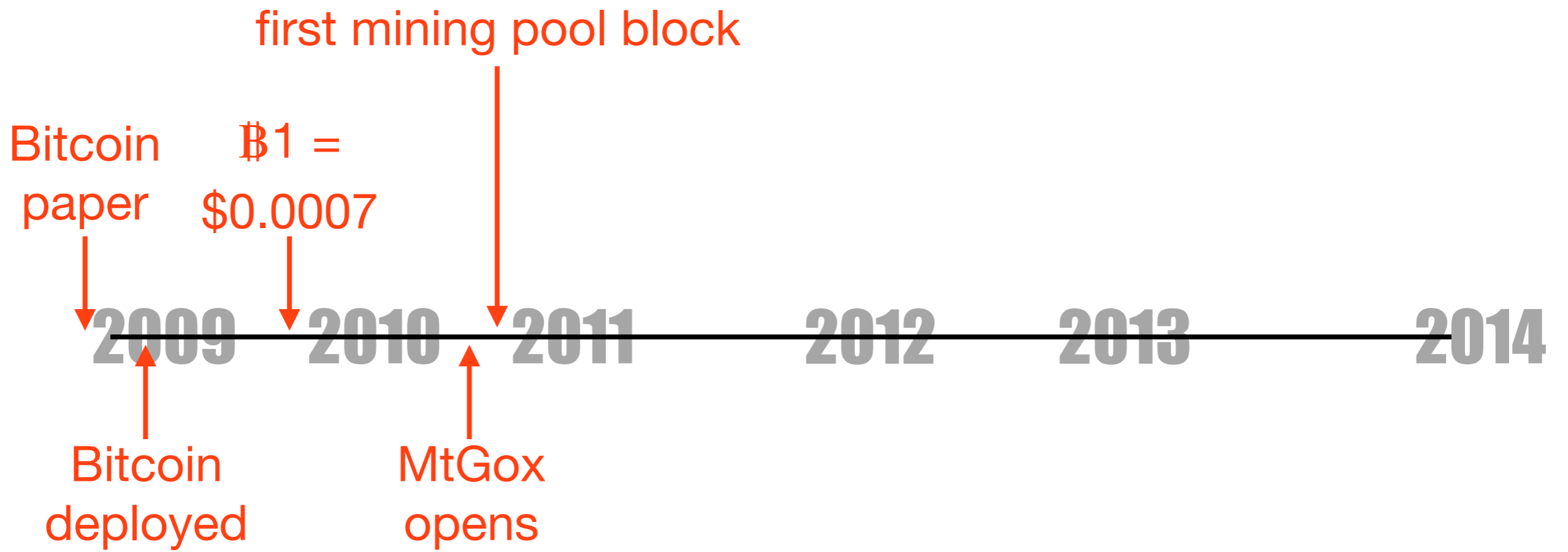
2013

2014

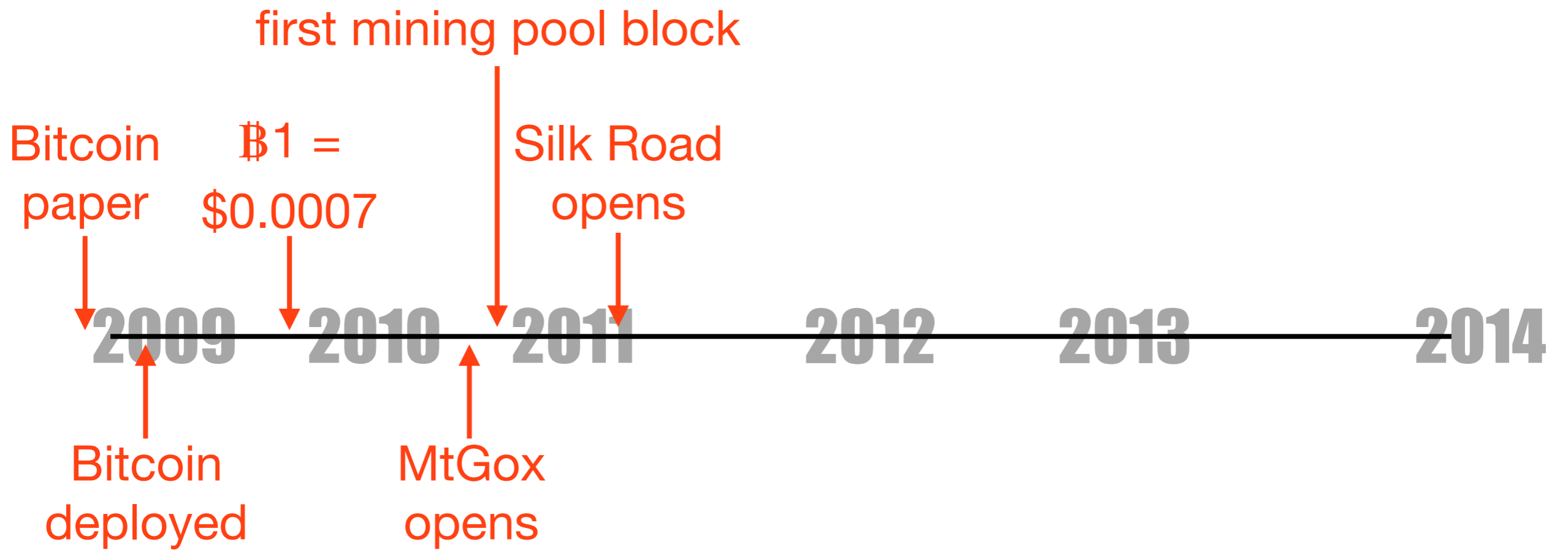
Bitcoin
deployed

MtGox
opens

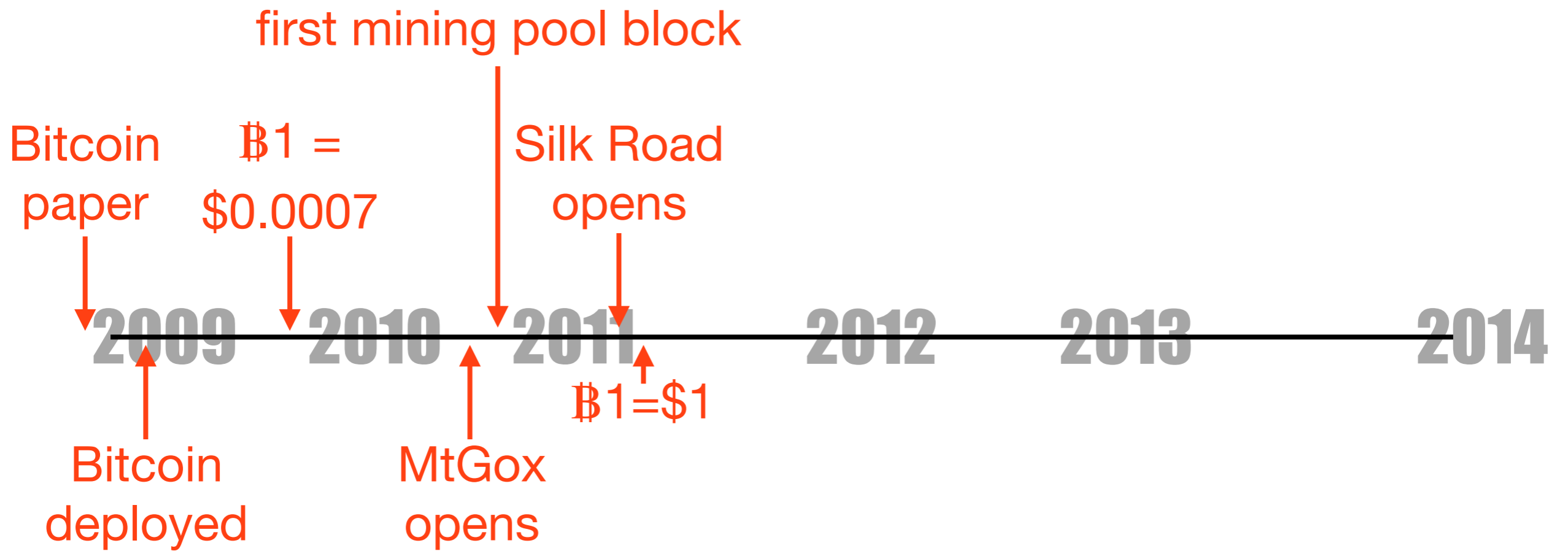
time



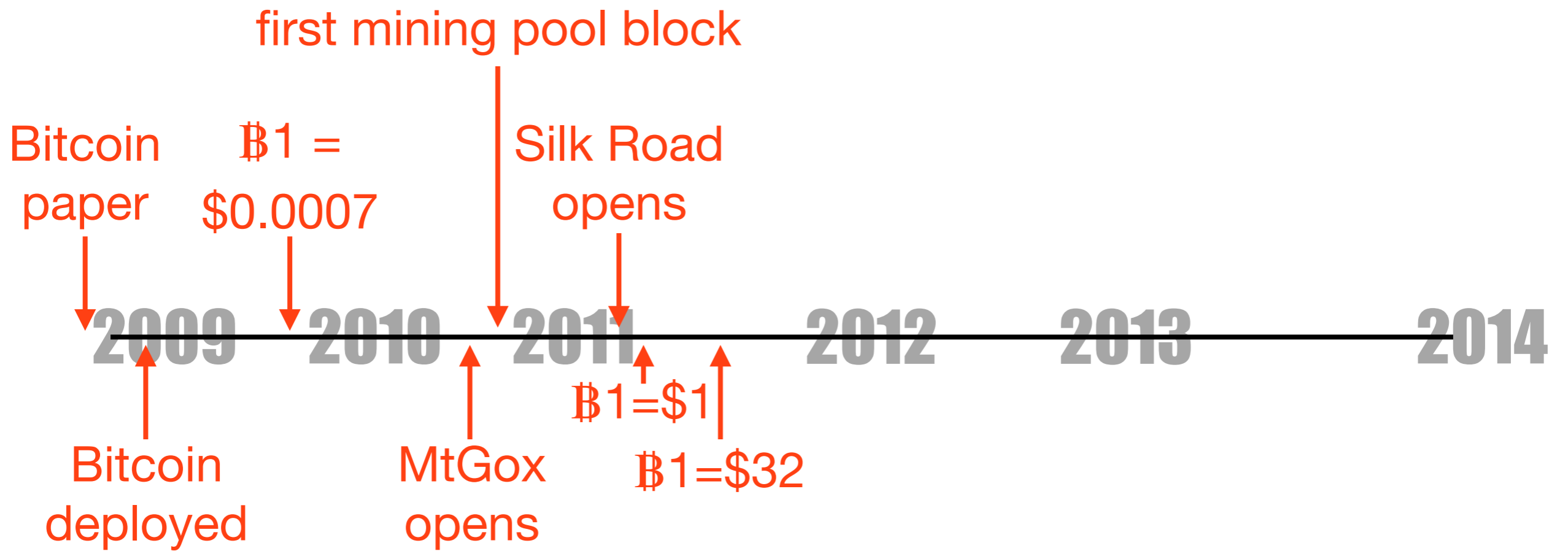
time →



time →

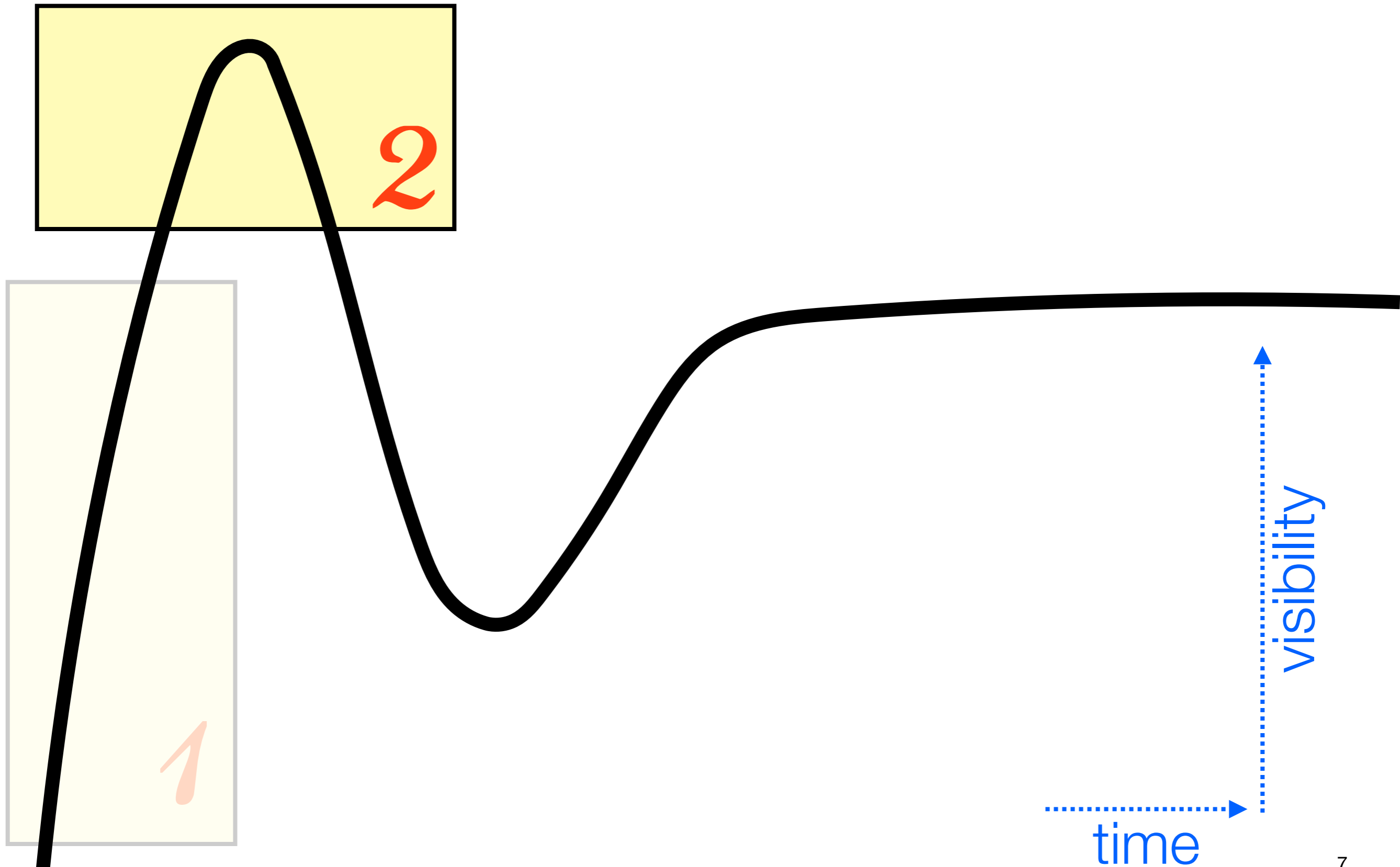


time →



time →

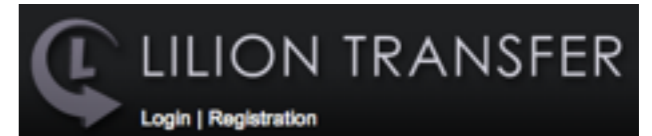
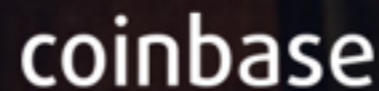
“peak of inflated expectations”



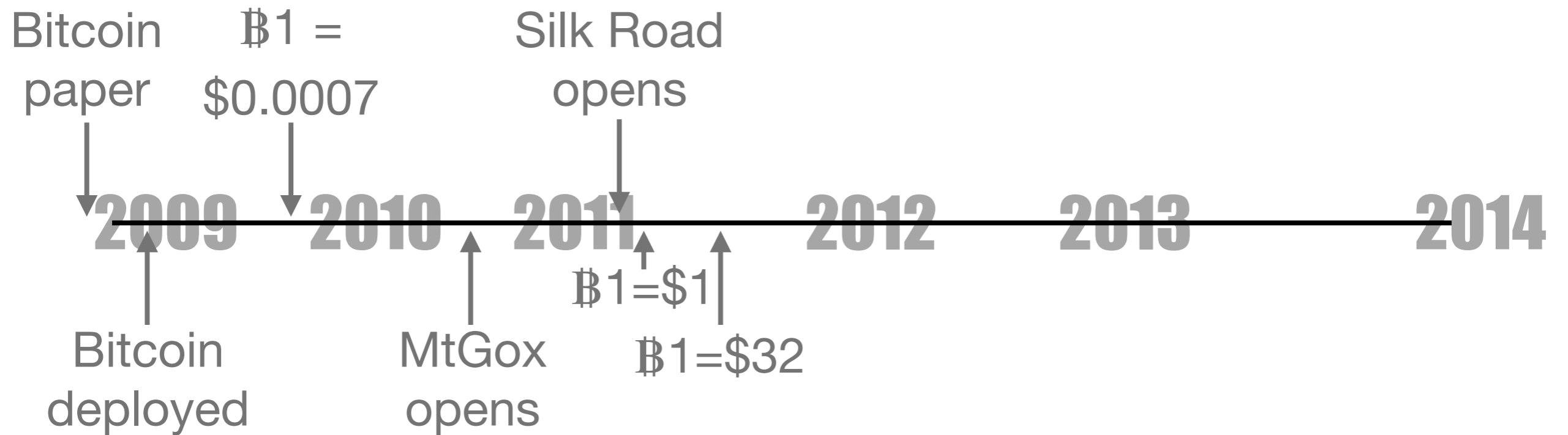
new businesses



new businesses

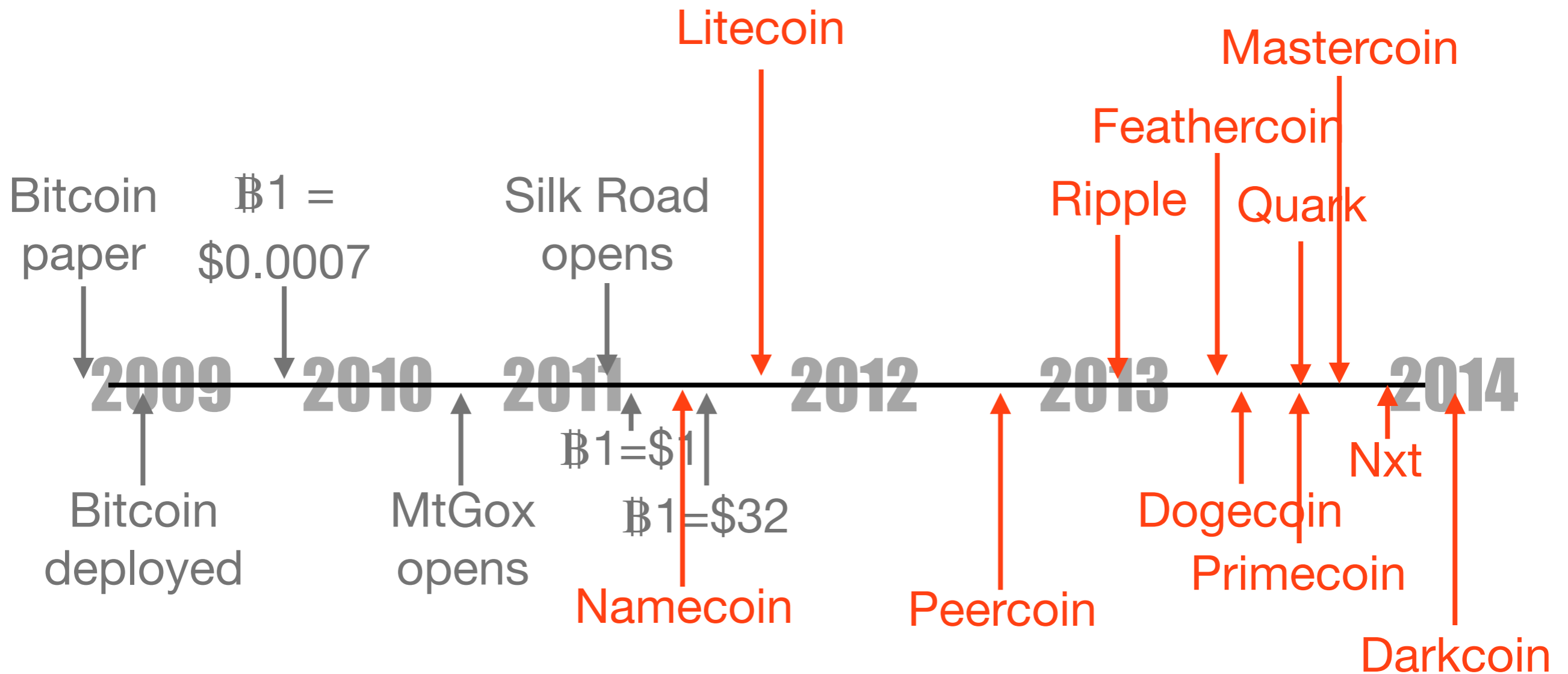


new cryptocurrencies (“altcoins”)





















.....→
time

new cryptocurrencies (“altcoins”)

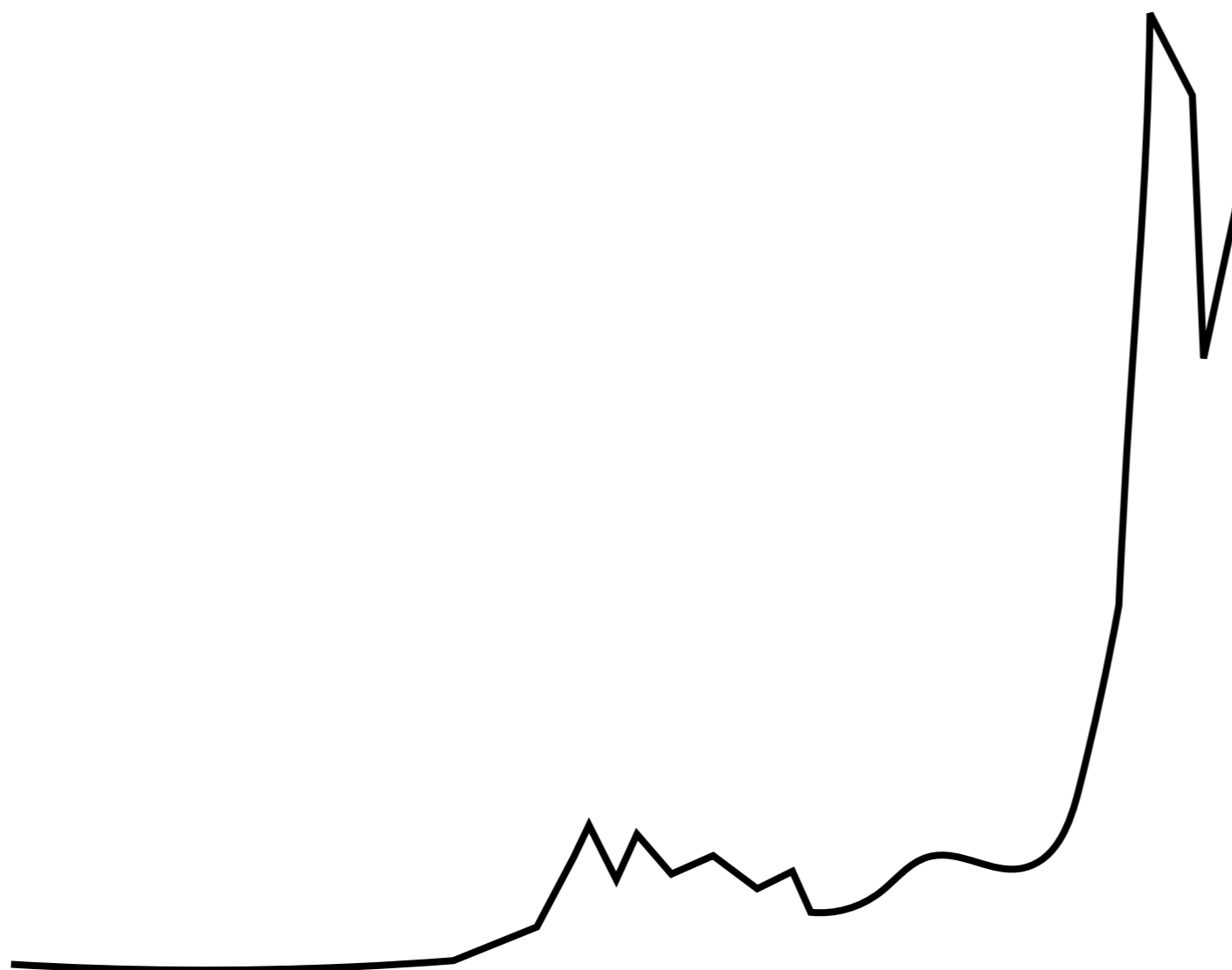


time →

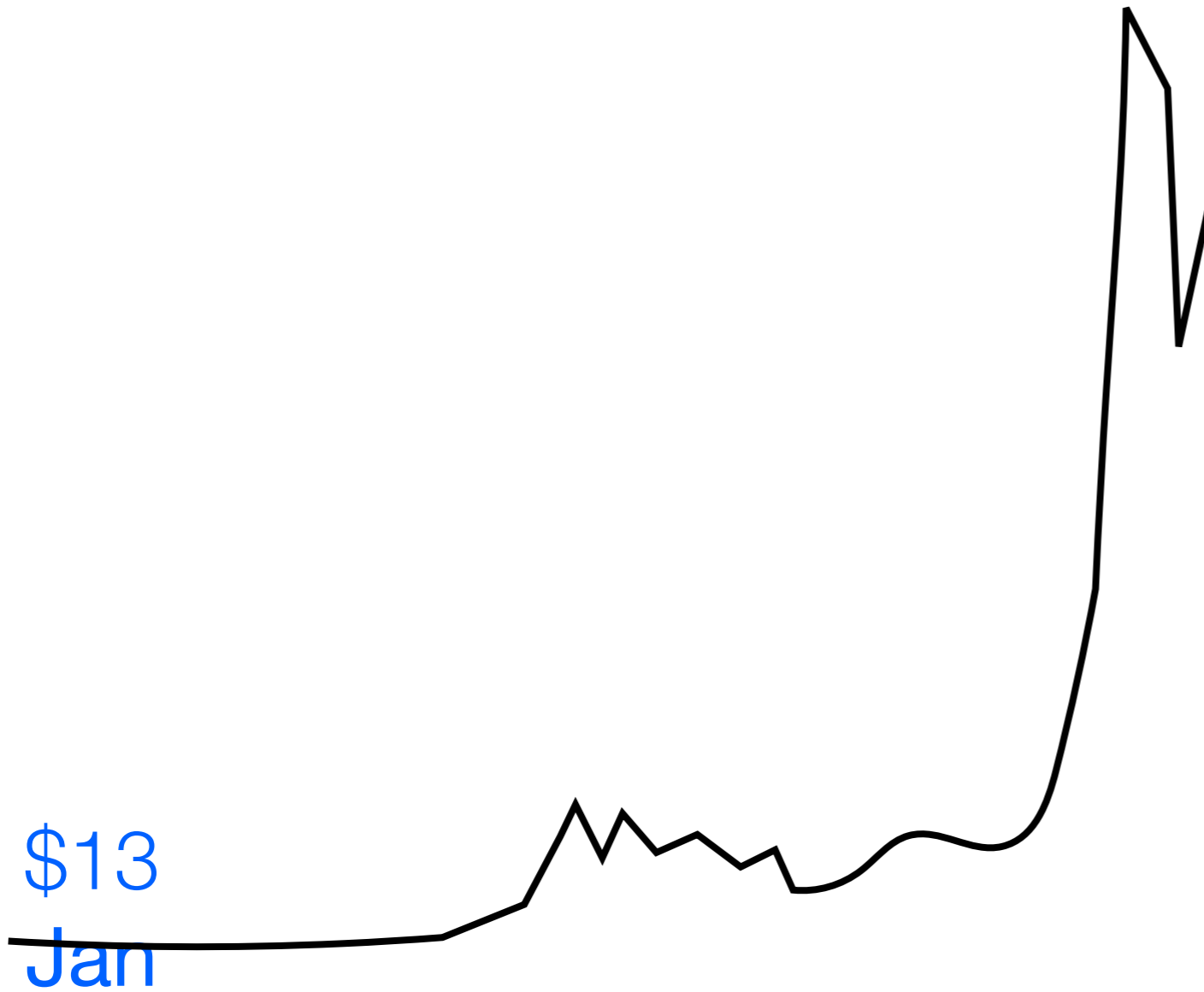
1	 Bitcoin	\$ 4,321,327,369	\$ 316.03	13,673,875 BTC
2	 Ripple	\$ 753,476,625	\$ 0.024323	30,978,075,200 XRP *
3	 PayCoin	\$ 100,507,953	\$ 8.15	12,325,837 XPY **
4	 Litecoin	\$ 95,072,164	\$ 2.70	35,218,304 LTC
5	 BitShares	\$ 40,746,199	\$ 0.016312	2,497,973,773 BTS *
6	 MaidSafeCoin	\$ 23,192,451	\$ 0.051248	452,552,412 MAID *
7	 Stellar	\$ 19,533,919	\$ 0.005492	3,557,060,725 STR *
8	 Dogecoin	\$ 17,889,012	\$ 0.000184	97,204,400,153 DOGE
9	 Nxt	\$ 17,504,849	\$ 0.017505	999,997,096 NXT *

28	 Quark	\$ 1,324,931	\$ 0.005331	248,529,548 QRK
29	 CoinoUSD	\$ 1,208,710	\$ 1.05	1,154,584 COINO *
30	 InstantDEX	\$ 1,208,630	\$ 1.21	1,000,000 DEX *
31	 DNotes	\$ 1,140,315	\$ 0.012011	94,940,826 NOTE
32	 Pangea Poker	\$ 1,102,710	\$ 1.10	999,402 PANGEA *
33	 Feathercoin	\$ 1,051,275	\$ 0.015819	66,455,200 FTC
34	 ReddCoin	\$ 1,042,389	\$ 0.000038	27,310,972,002 RDD
35	 BitUSD	\$ 917,585	\$ 1.05	873,433 BITUSD *
36	 Primecoin	\$ 823,269	\$ 0.097423	8,450,498 XPM

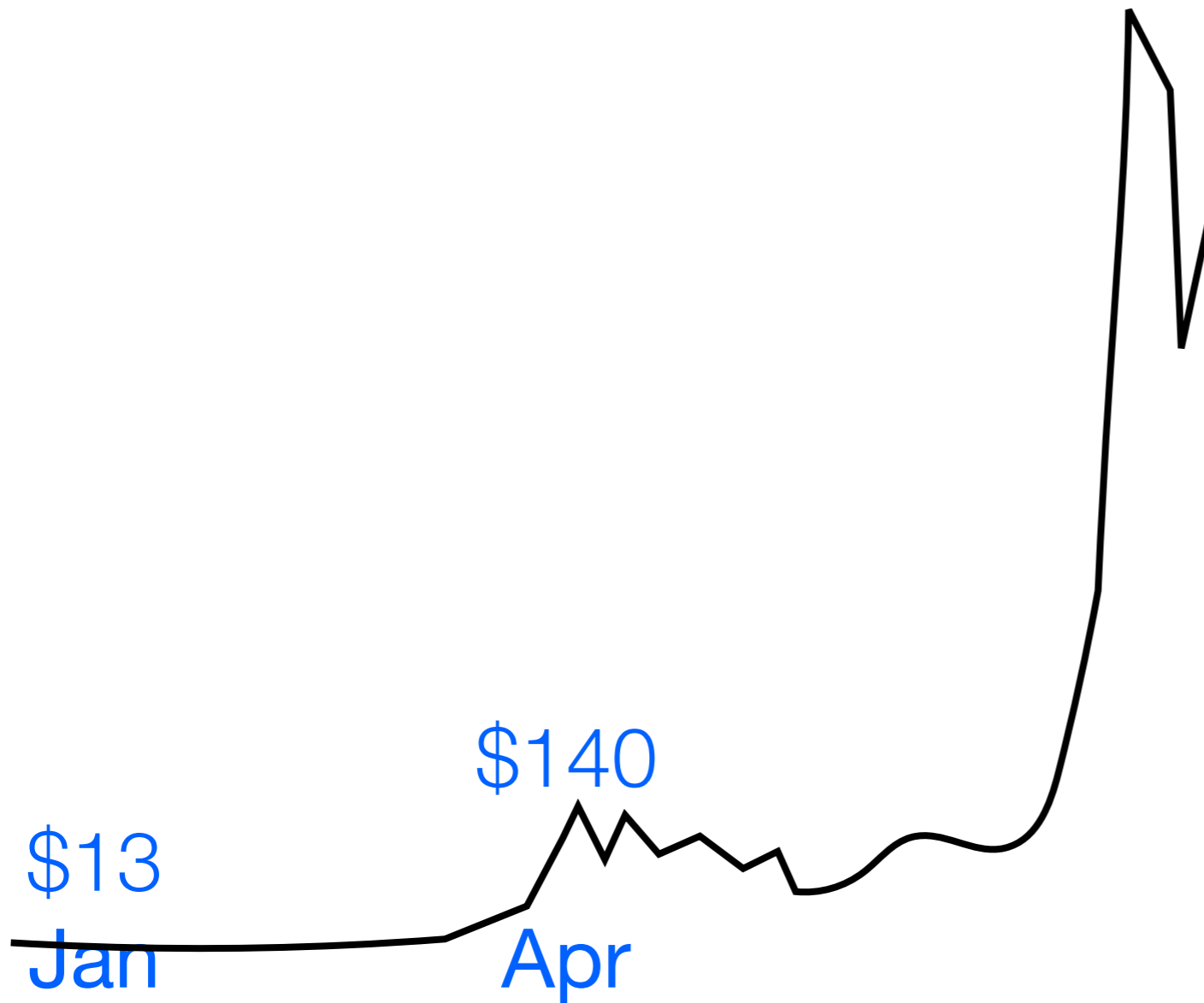
soaring exchange rate



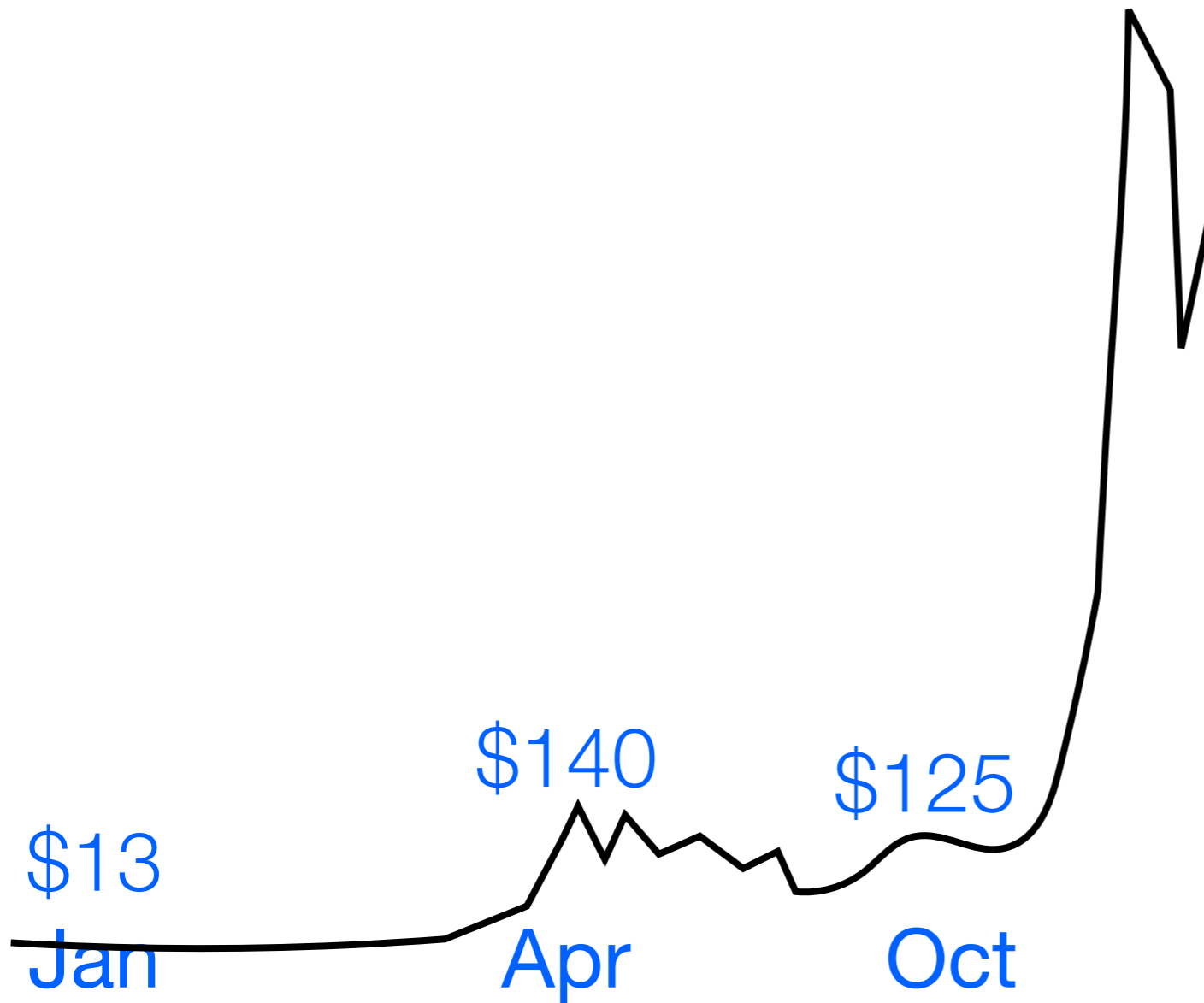
soaring exchange rate



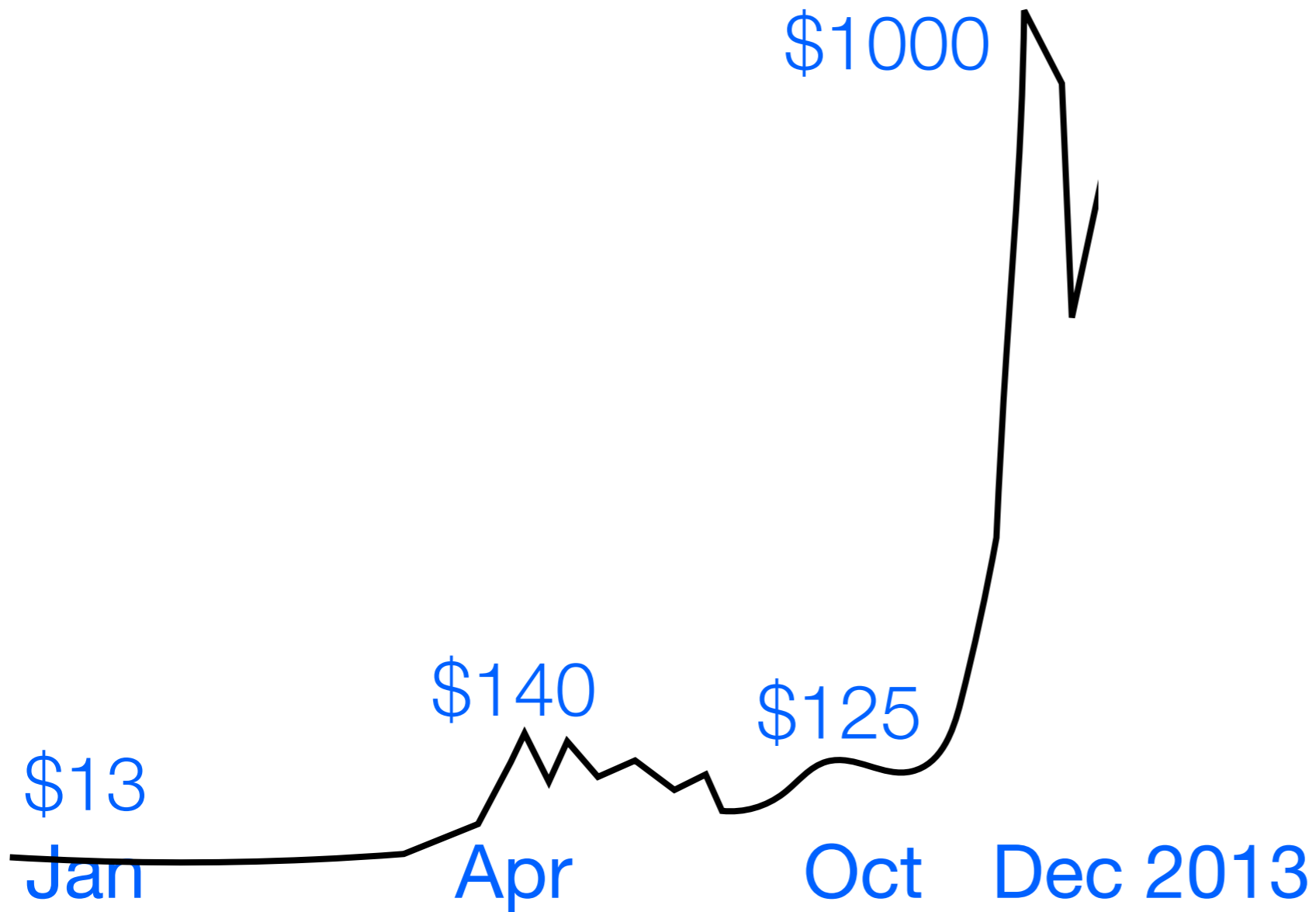
soaring exchange rate



soaring exchange rate



soaring exchange rate



regulatory interest

Bitcoin.de and Fidor Bank AG Agree on Large-Scale Partnership

Bitcoin-Central becomes first Bitcoin exchange licensed to operate like a bank

New Money Laundering Guidelines Are A Positive Sign For Bitcoin

This Senate hearing is a Bitcoin lovefest

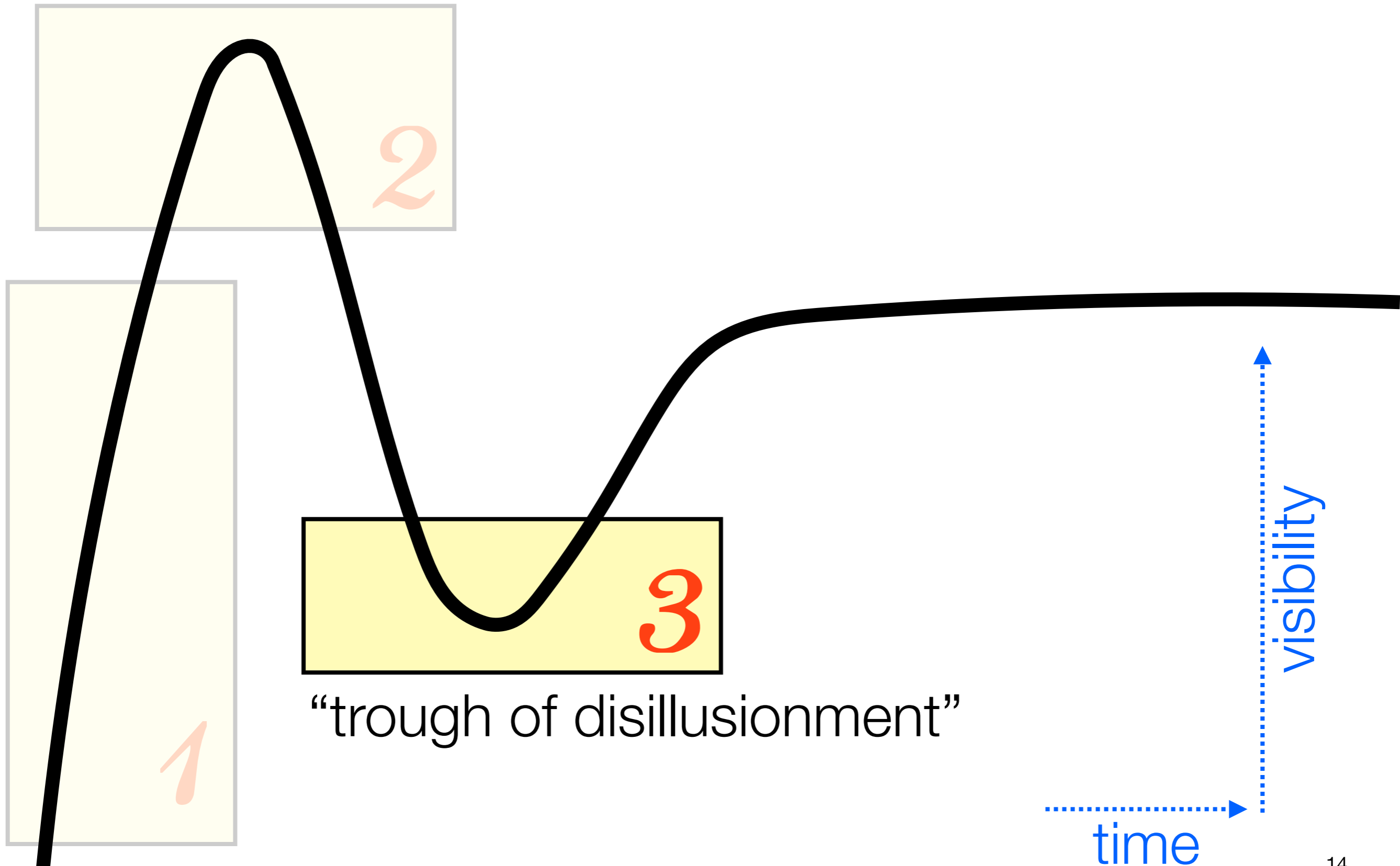
news media

YC-Backed Buttercoin Uses Bitcoin To Attack The \$500B-A-Year Remittances Economy

Silicon Valley catches Bitcoin fever

2013: Year Of The Bitcoin

Why Bitcoin Is Poised To Change Society Much More Than The Internet Did



Bitcoin might not be as as we hoped.

Bitcoin might not be as **decentralized** as we hoped.

Bitcoin might not be as **decentralized** as we hoped.

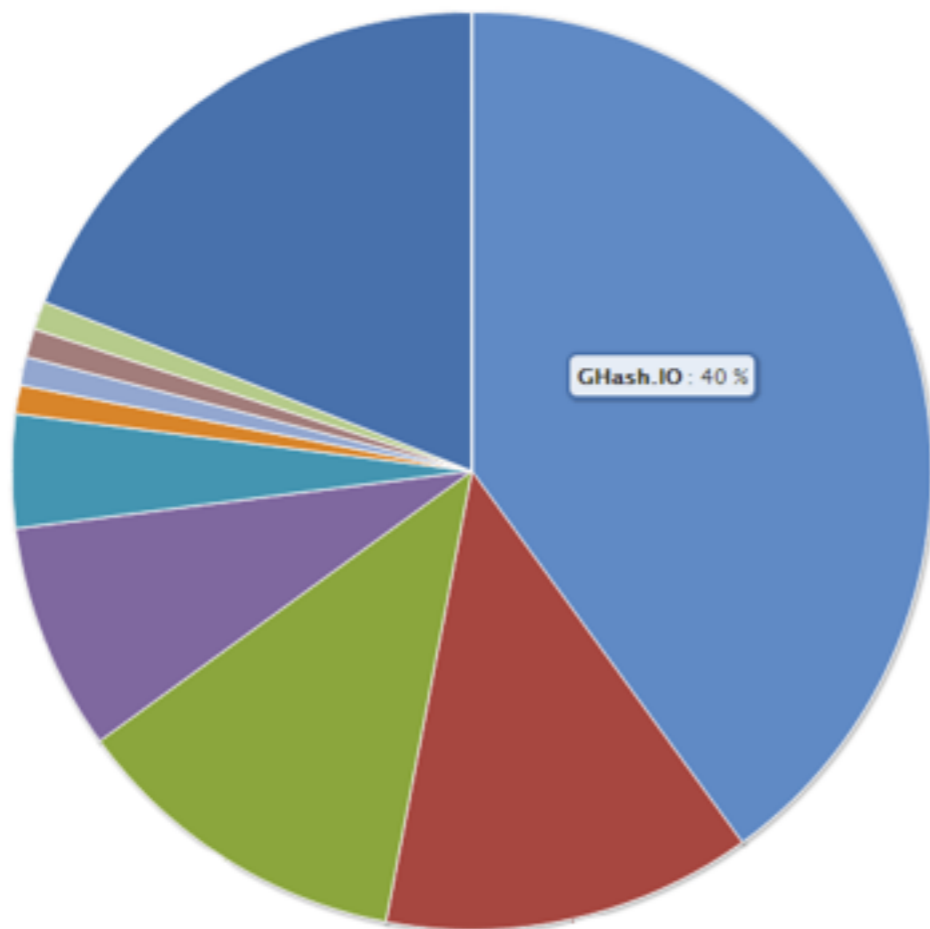
**Majority is not Enough:
Bitcoin Mining is Vulnerable**

Ittay Eyal and Emin Gün Sirer

Bitcoin might not be as **decentralized** as we hoped.

**Majority is not Enough:
Bitcoin Mining is Vulnerable**

Ittay Eyal and Emin Gün Sirer

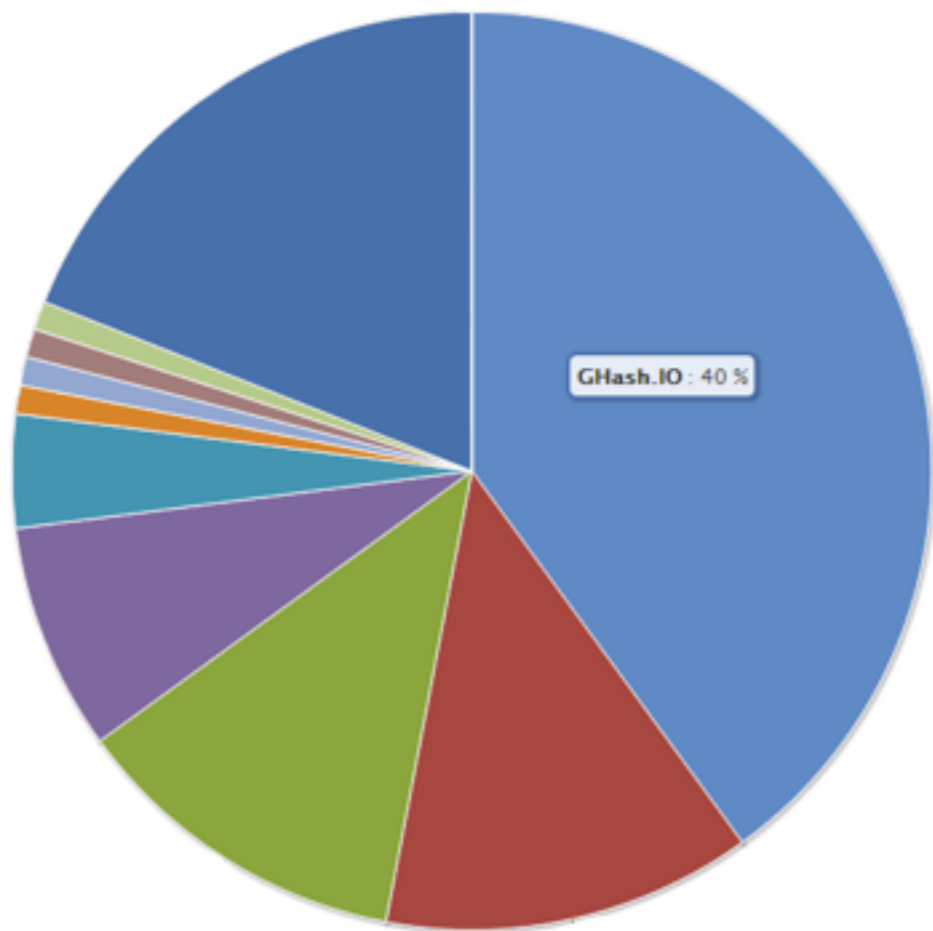


June 2014

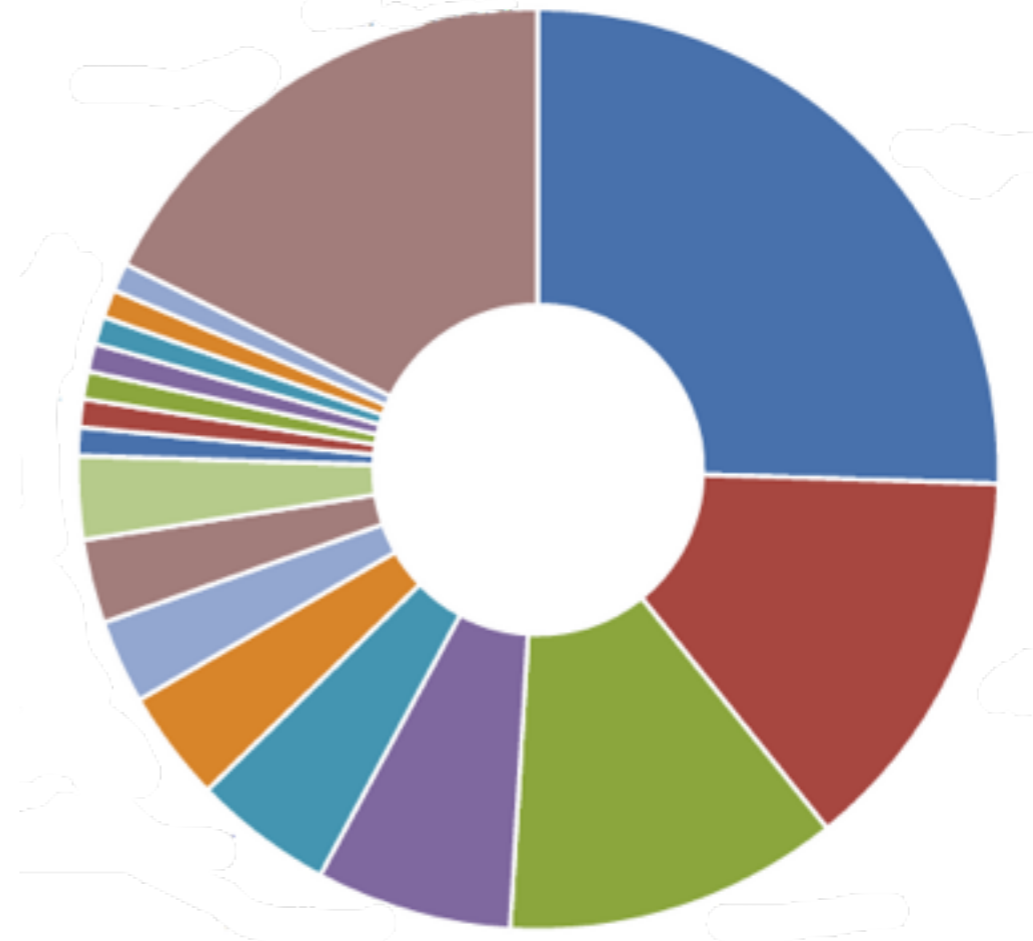
Bitcoin might not be as **decentralized** as we hoped.

**Majority is not Enough:
Bitcoin Mining is Vulnerable**

Ittay Eyal and Emin Gün Sirer



June 2014



today

Bitcoin might not be as **secure** as we hoped.
decentralized

Elliptic Curve Cryptography in Practice

Joppe W. Bos¹, J. Alex Halderman², Nadia Heninger³, Jonathan Moore, Michael Naehrig¹,
and Eric Wustrow²

Android bug batters Bitcoin wallets

Bitcoin might not be as **secure** as we hoped.
decentralized

Elliptic Curve Cryptography in Practice

Joppe W. Bos¹, J. Alex Halderman², Nadia Heninger³, Jonathan Moore, Michael Naehrig¹,
and Eric Wustrow²

Android bug batters Bitcoin wallets

Deterministic Wallets, Their Advantages and their Understated Flaws

Bitcoin might not be as **secure** as we hoped.
decentralized

Elliptic Curve Cryptography in Practice

Joppe W. Bos¹, J. Alex Halderman², Nadia Heninger³, Jonathan Moore, Michael Naehrig¹,
and Eric Wustrow²

Android bug batters Bitcoin wallets

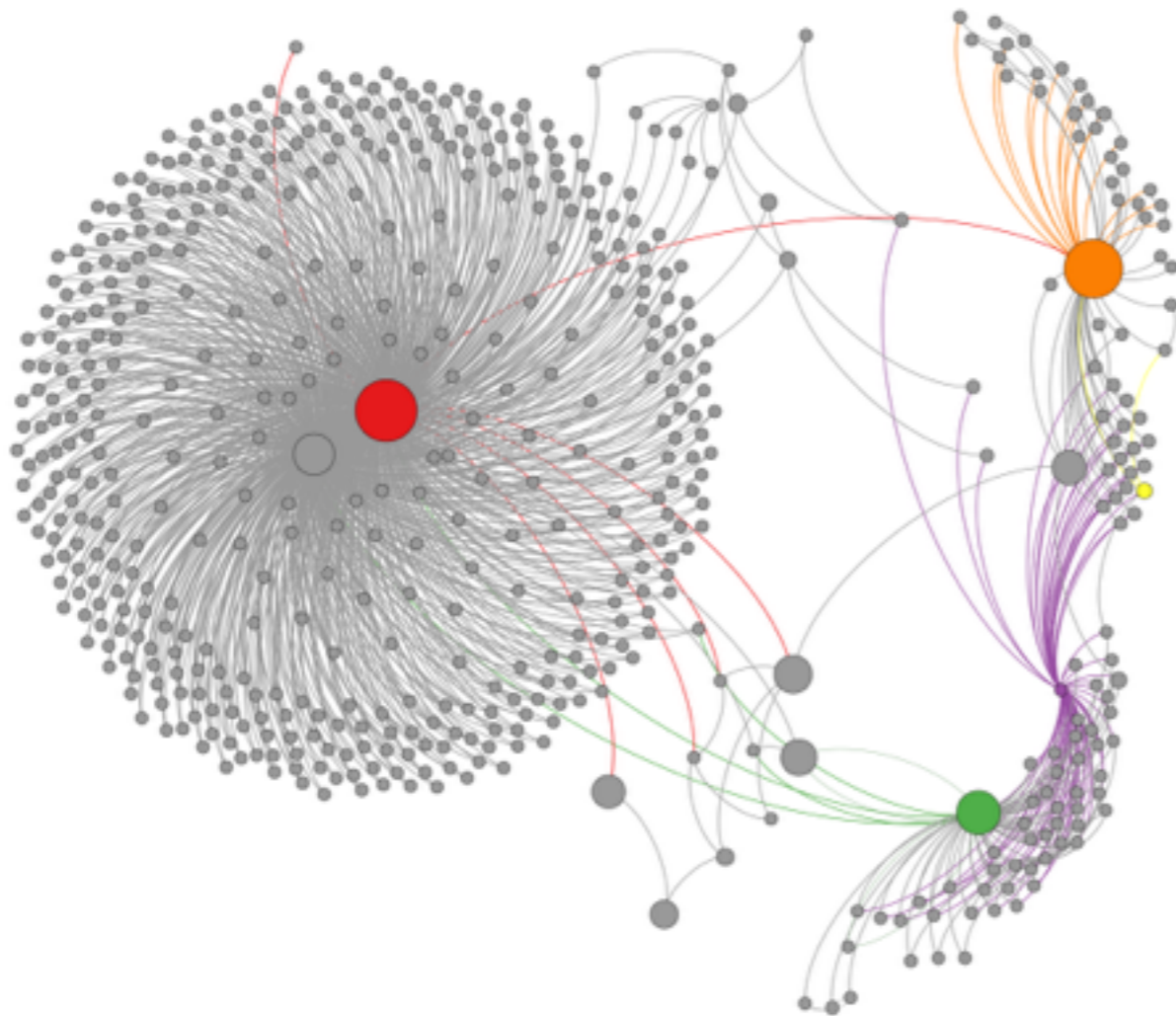
Deterministic Wallets, Their Advantages and their Understated Flaws

Bitcoin “Brainwallets” and why they are a bad idea

Bitcoin might not be as **anonymous** as we hoped.

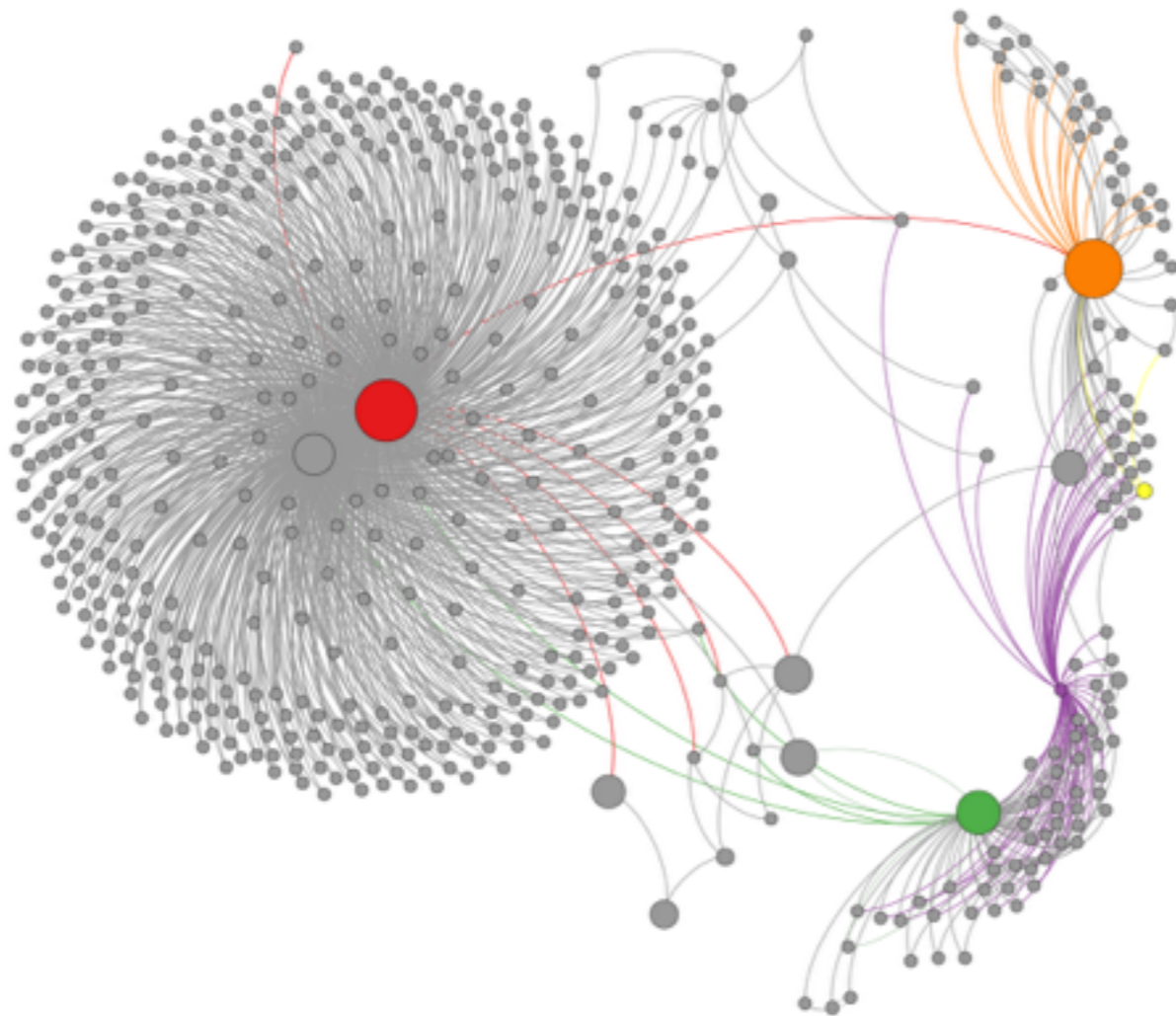
decentralized
secure





Bitcoin might not be as **anonymous** as we hoped.
decentralized
secure



[RH,RS,A+,**M+**,M13,SMZ14]

Bitcoin might not be as **anonymous** as we hoped.
decentralized
secure



	9	3
7		
5		1

[RH,RS,A+,**M+**,M13,SMZ14]

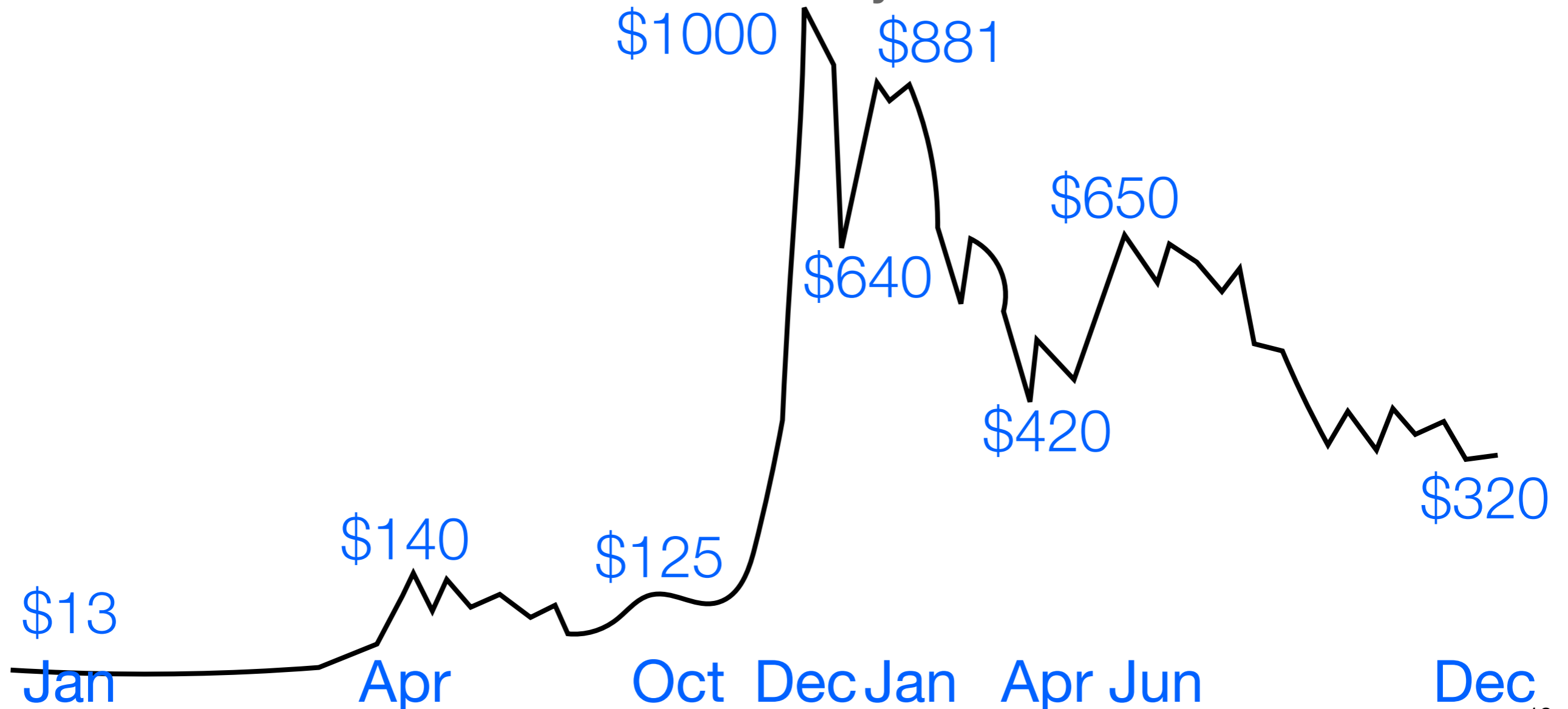
[A14,**MO**15]

Bitcoin might not be as **stable** as we hoped.

decentralized
secure
anonymous

Bitcoin might not be as **stable** as we hoped.

decentralized
secure
anonymous



Bitcoin might not be as **useful** as we hoped.

decentralized
secure
anonymous
stable

Bitcoin might not be as **useful** as we hoped.

decentralized
secure
anonymous
stable

The 'Killer Bitcoin App' Has Yet To Arrive

Bitcoin Is Still Adrift

**CoinSummit Venture Capitalists Seek
'Killer' Bitcoin App**

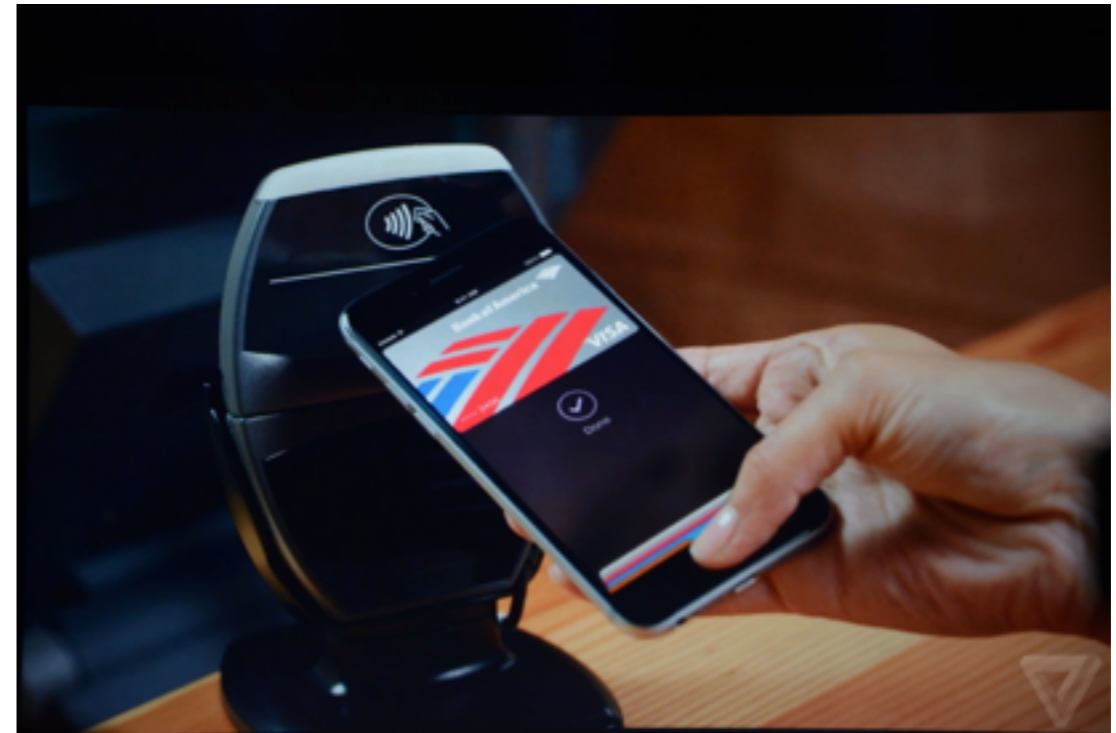
Bitcoin might not be as **useful** as we hoped.

decentralized
secure
anonymous
stable

The 'Killer Bitcoin App' Has Yet To Arrive

Bitcoin Is Still Adrift

**CoinSummit Venture Capitalists Seek
'Killer' Bitcoin App**



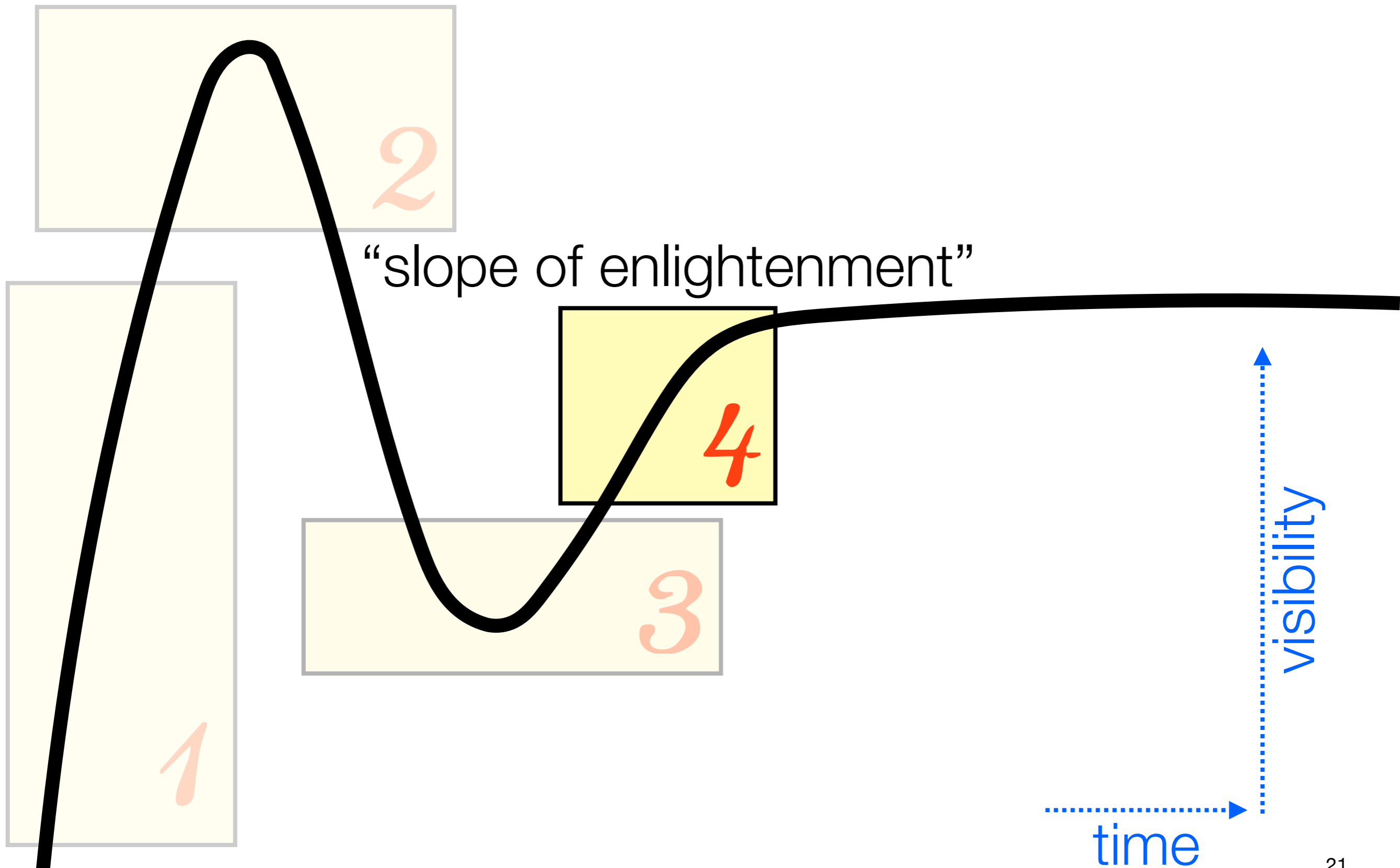
Is Apple Pay a bitcoin killer?

Bitcoin might not be as **useful** as we hoped.

decentralized
secure
anonymous
stable

IN-DEPTH: BANGLADESH BANS BITCOIN

Russia Proposes Monetary Penalties for Bitcoin Use and Promotion



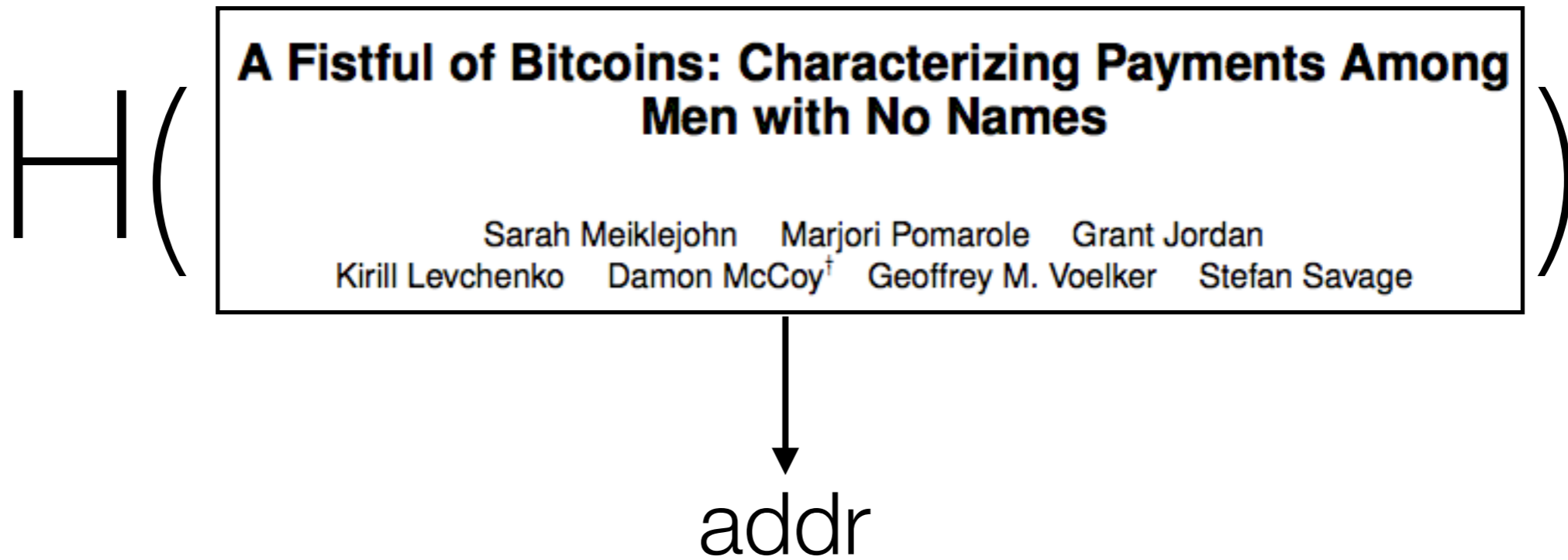
how to **timestamp**

how to **timestamp**

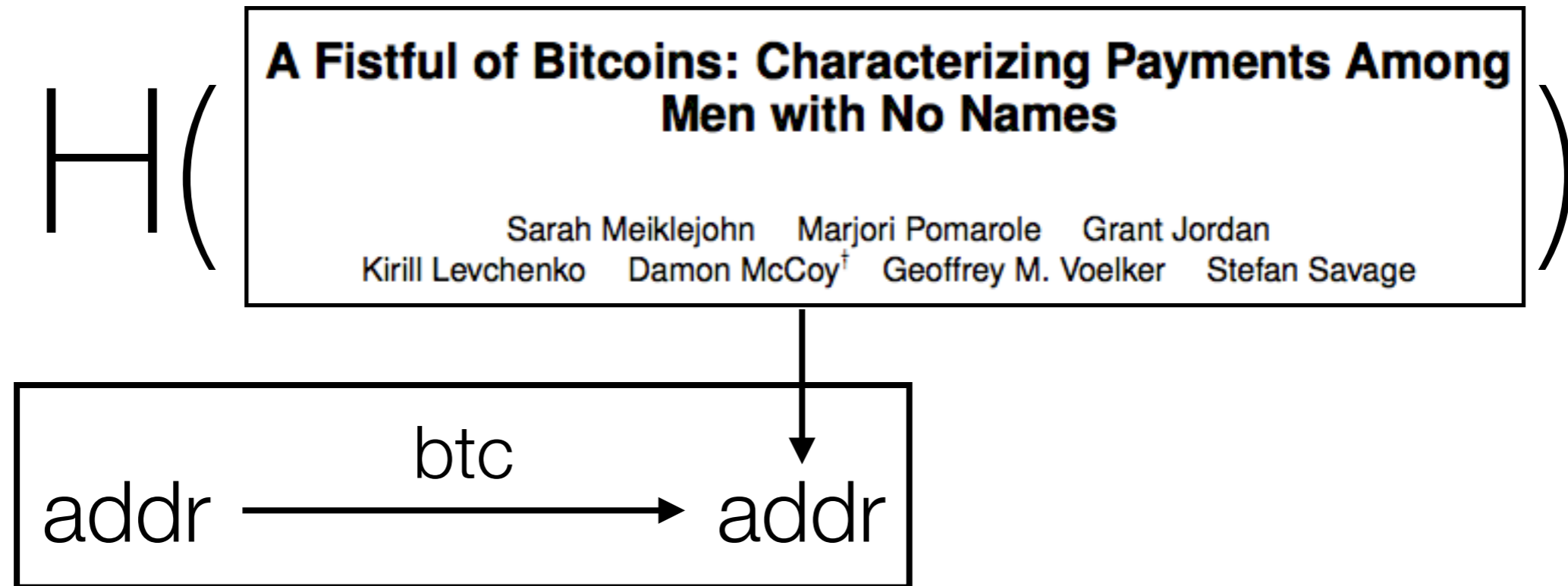
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

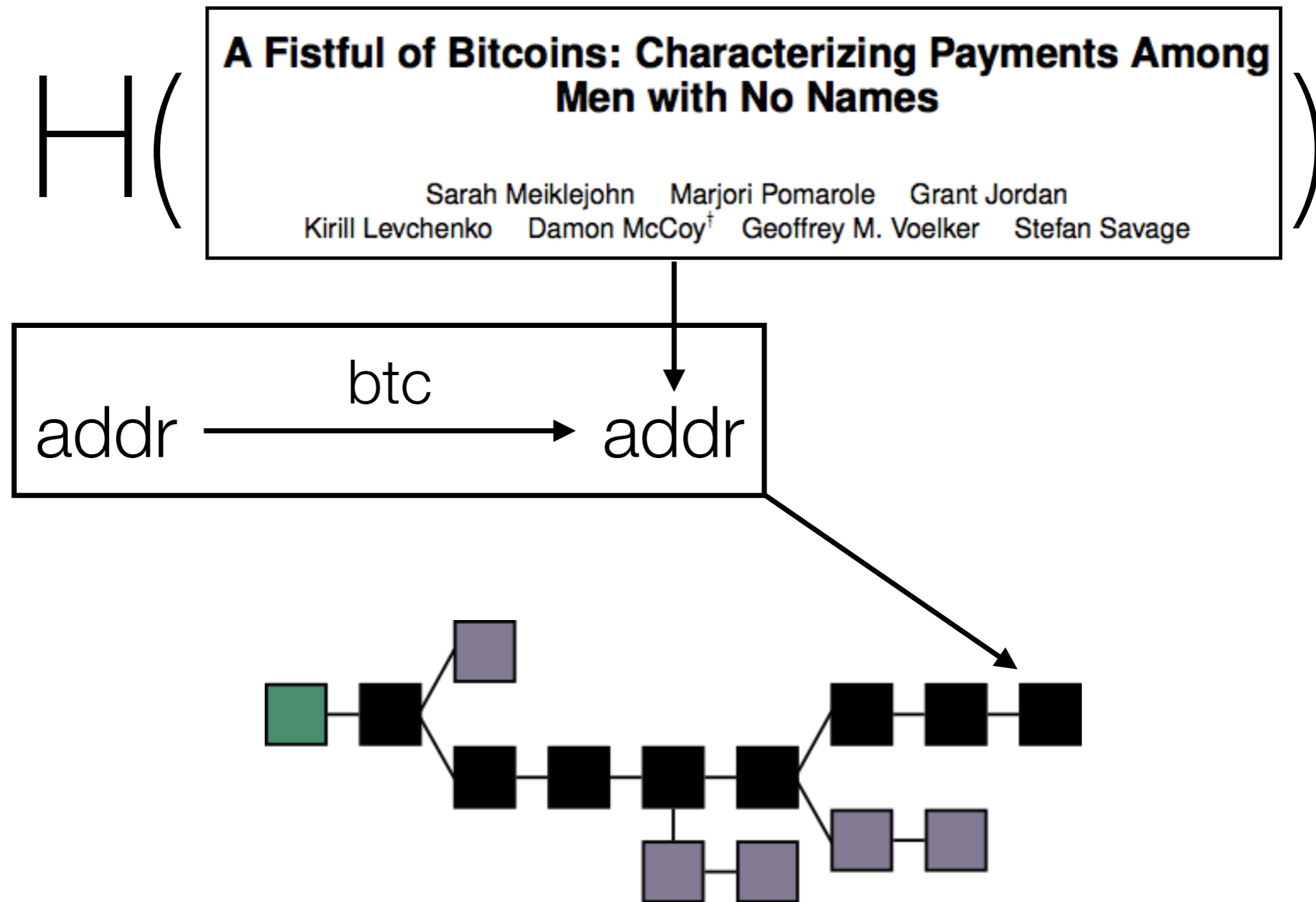
how to **timestamp**



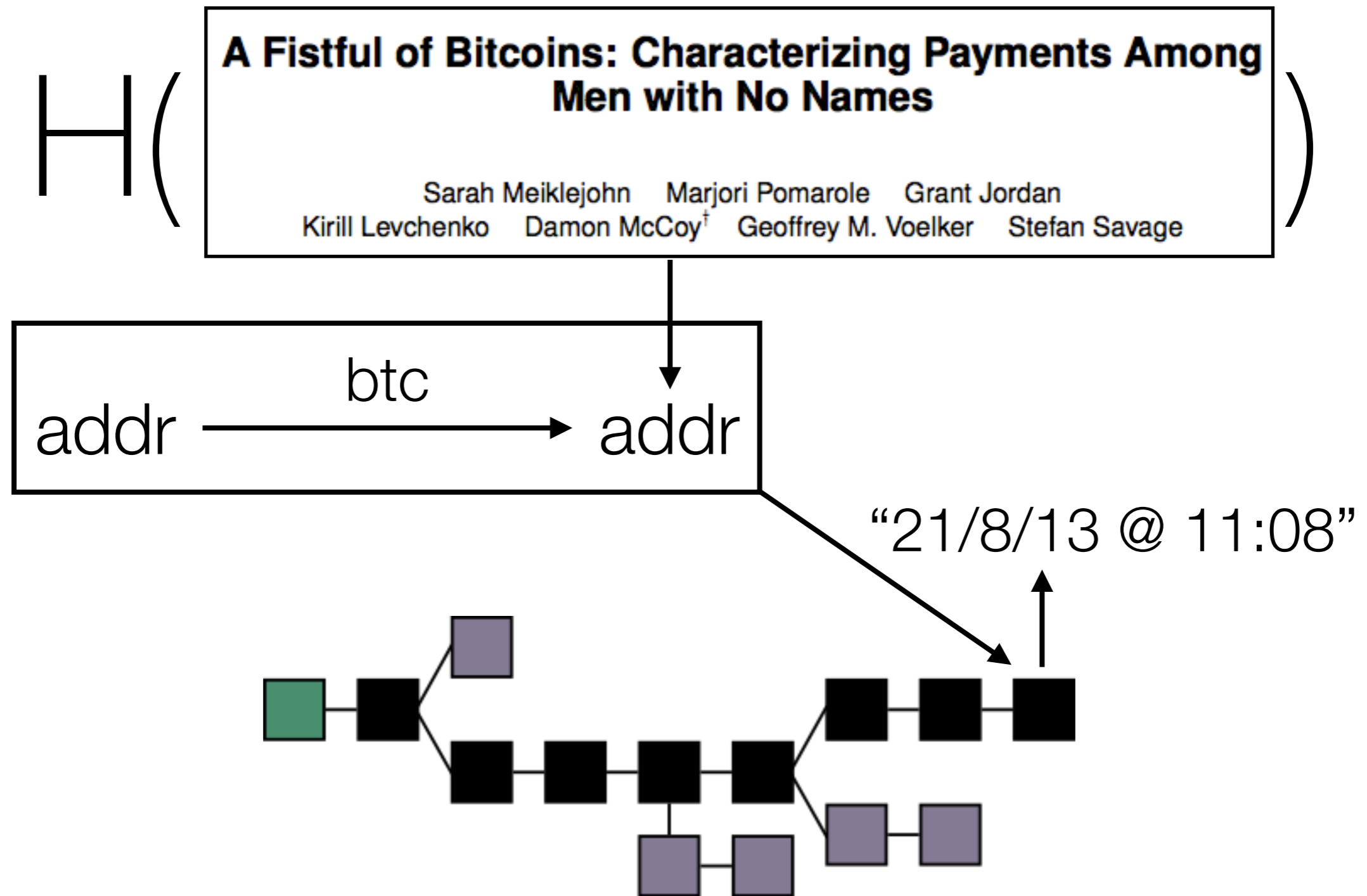
how to **timestamp**



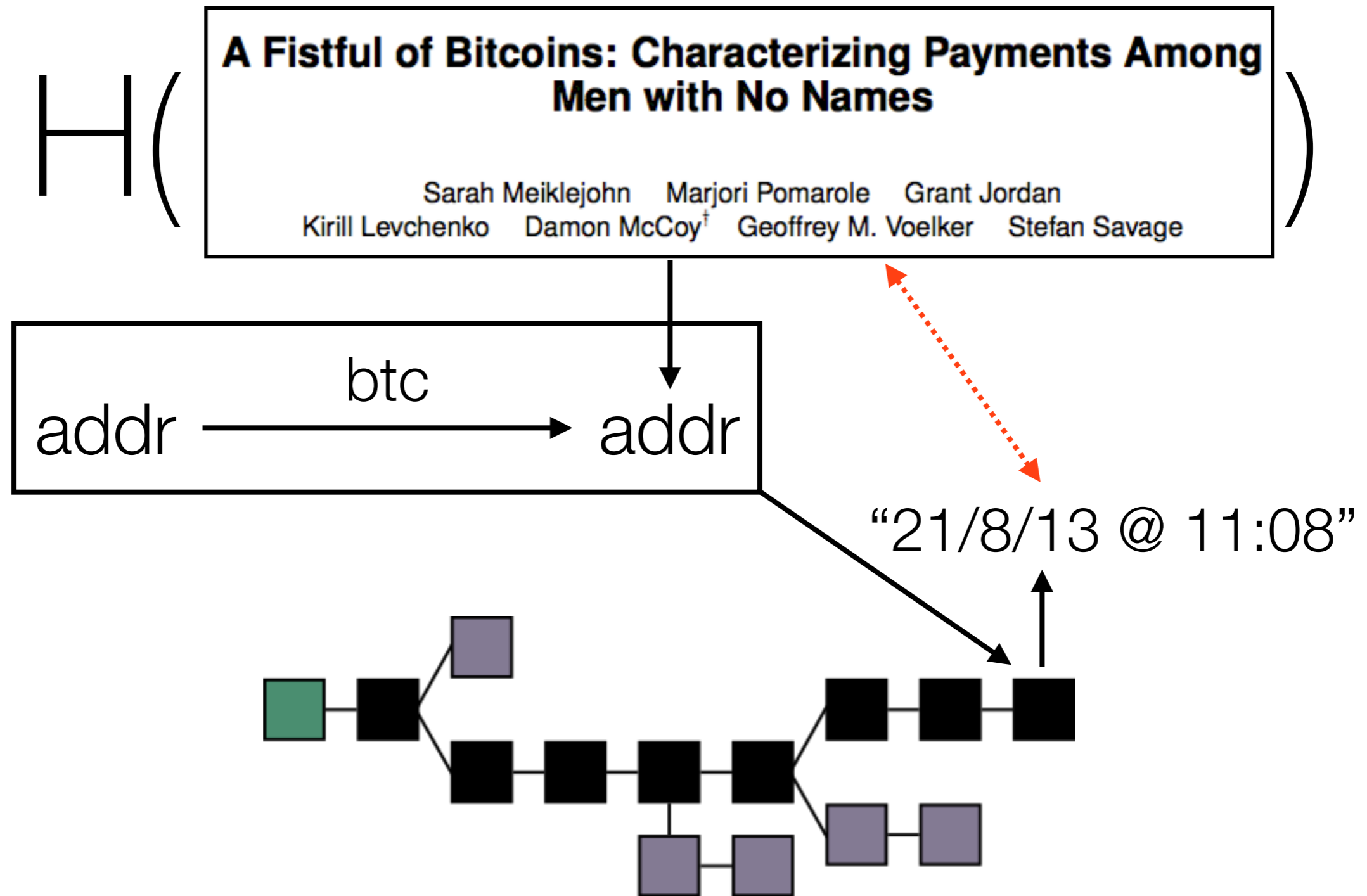
how to **timestamp**



how to **timestamp**



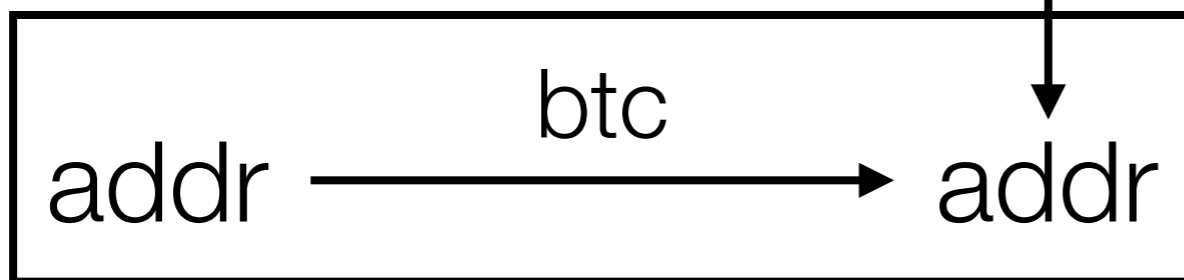
how to **timestamp**



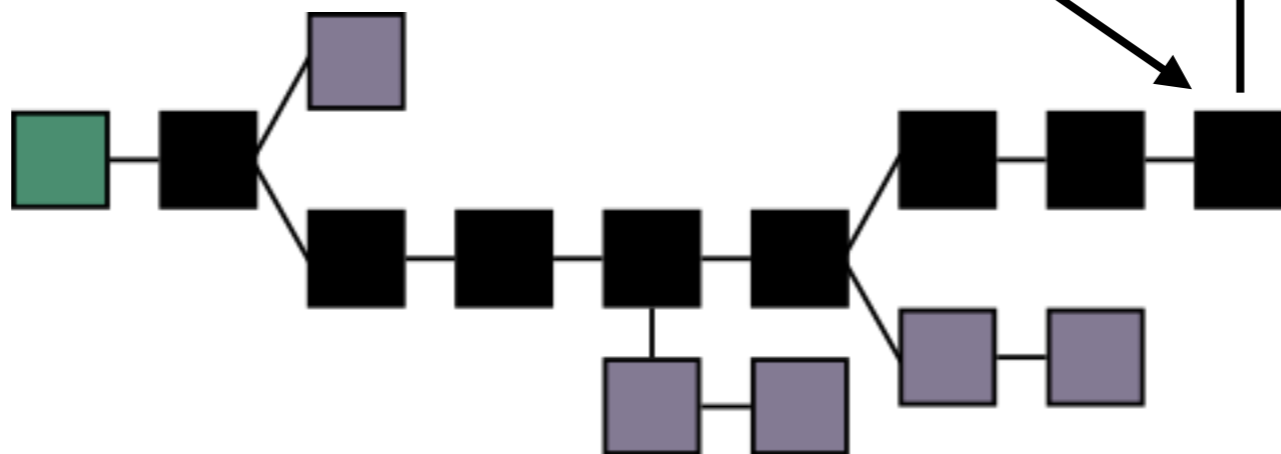
H(



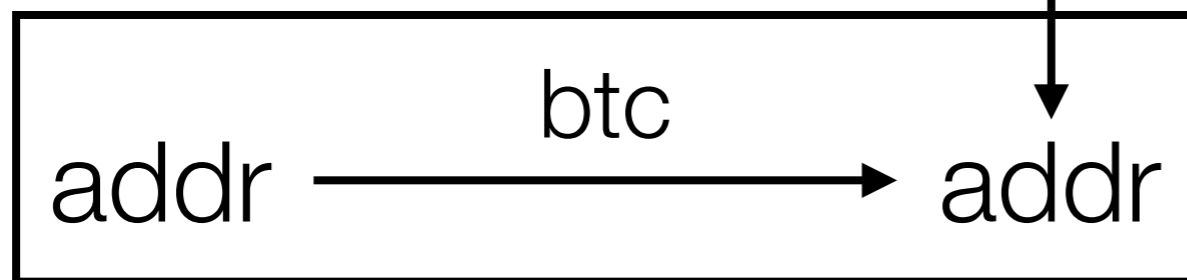
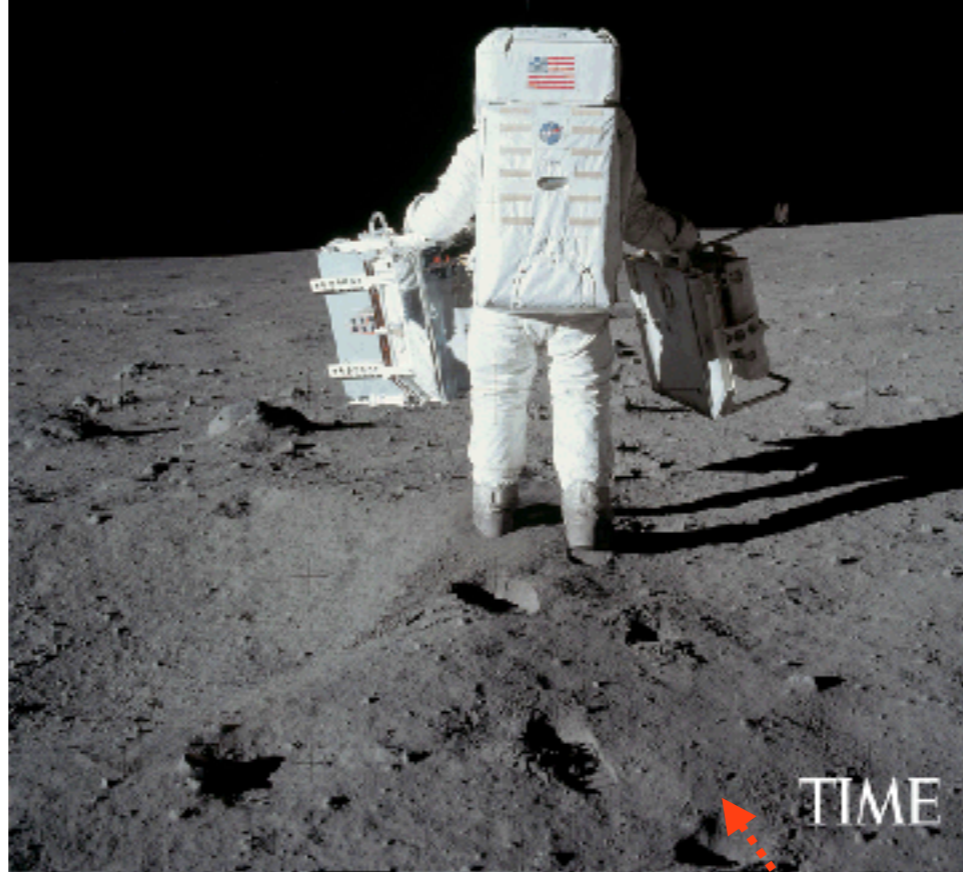
)



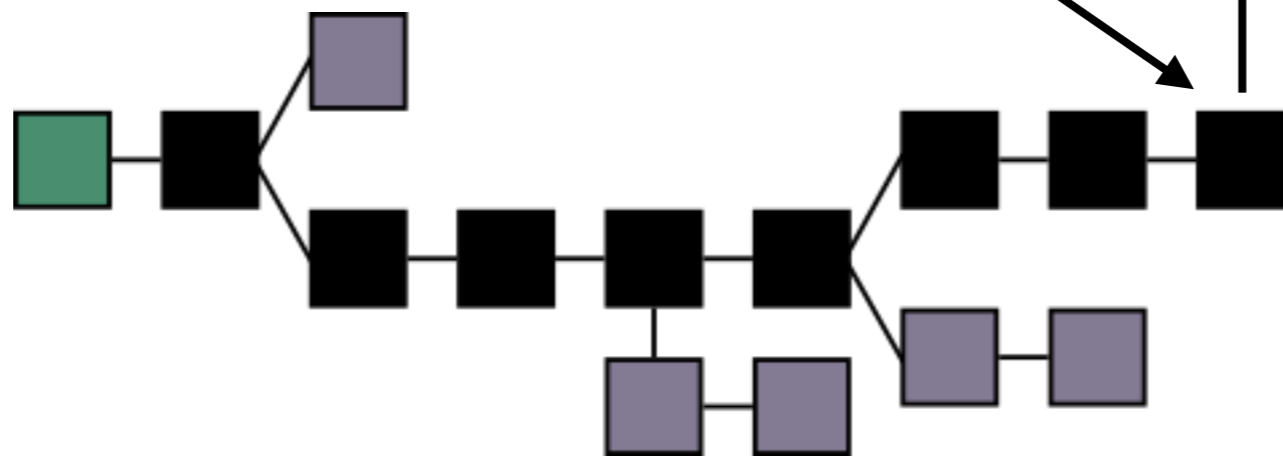
“21/8/13 @ 11:08”



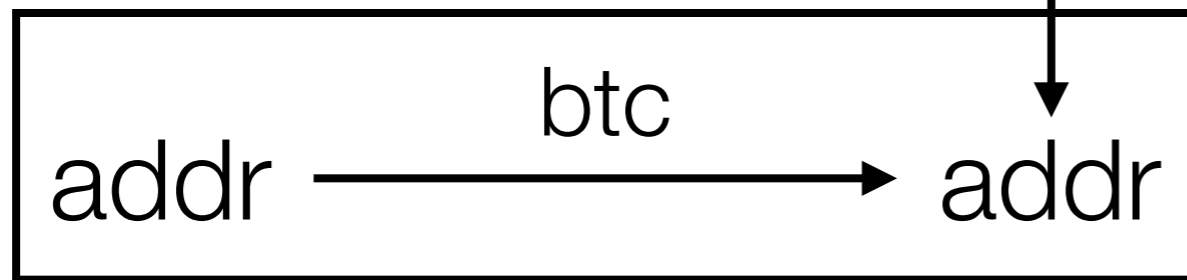
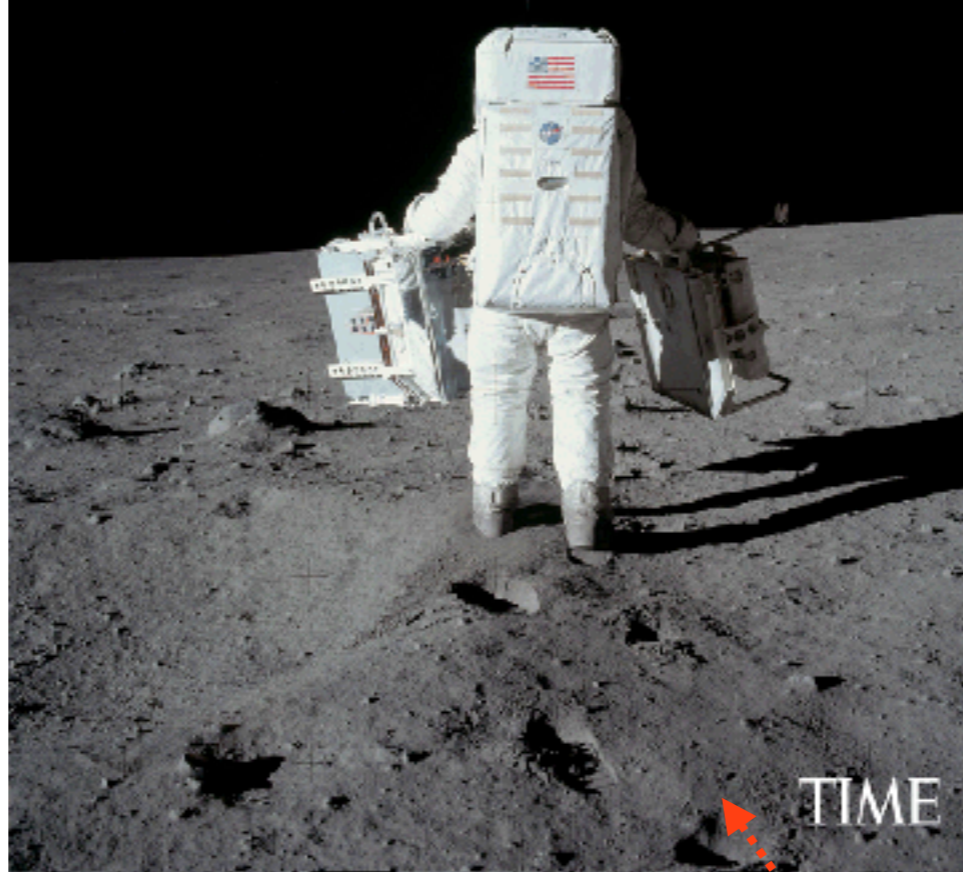
H()



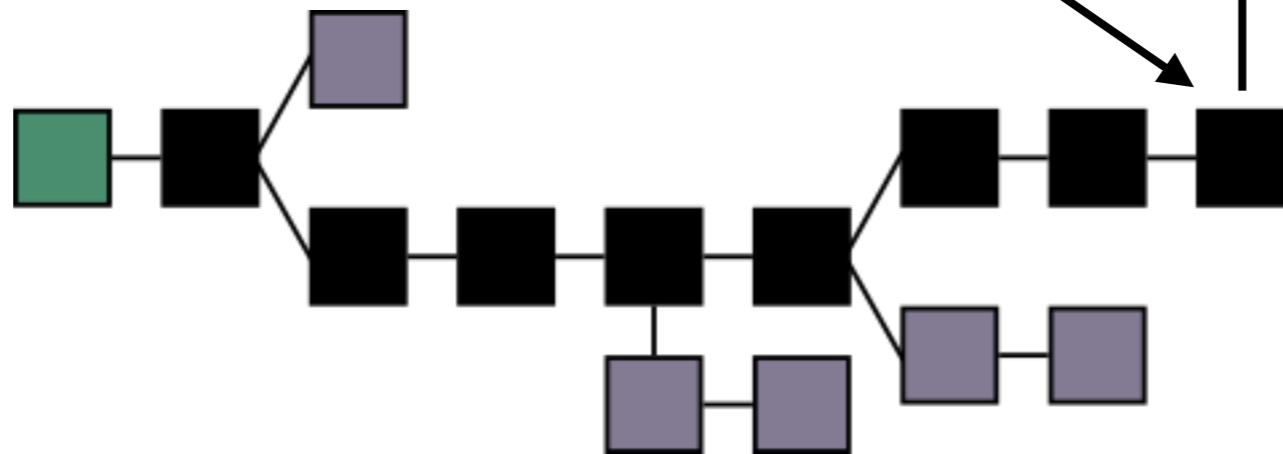
“20/7/69 @ 20:18”



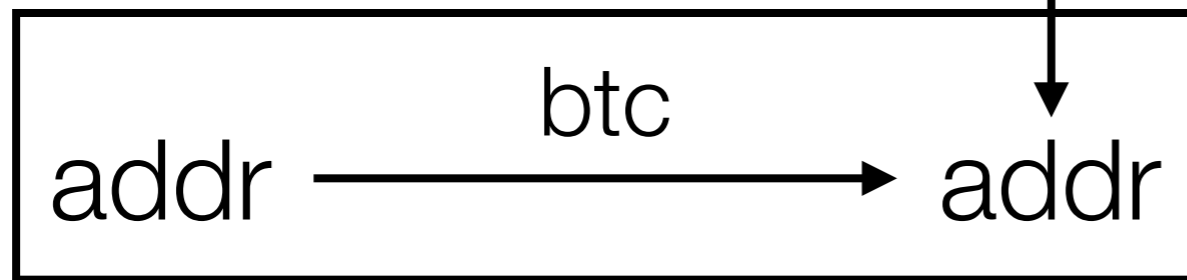
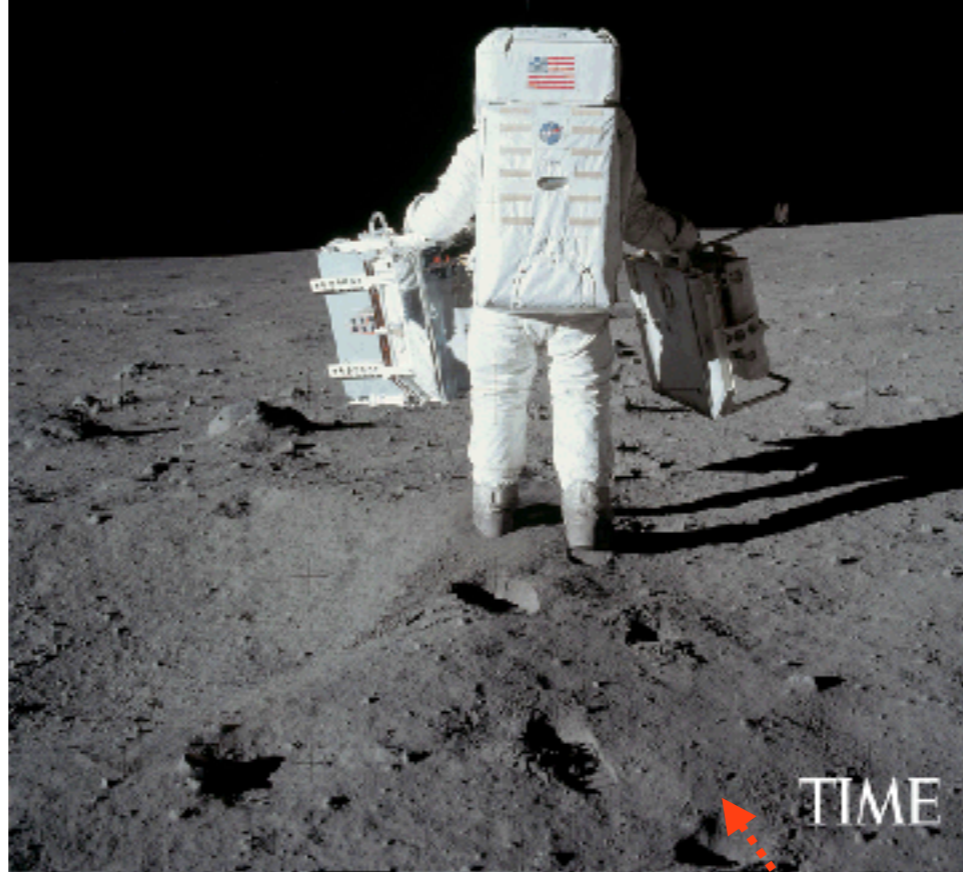
H()



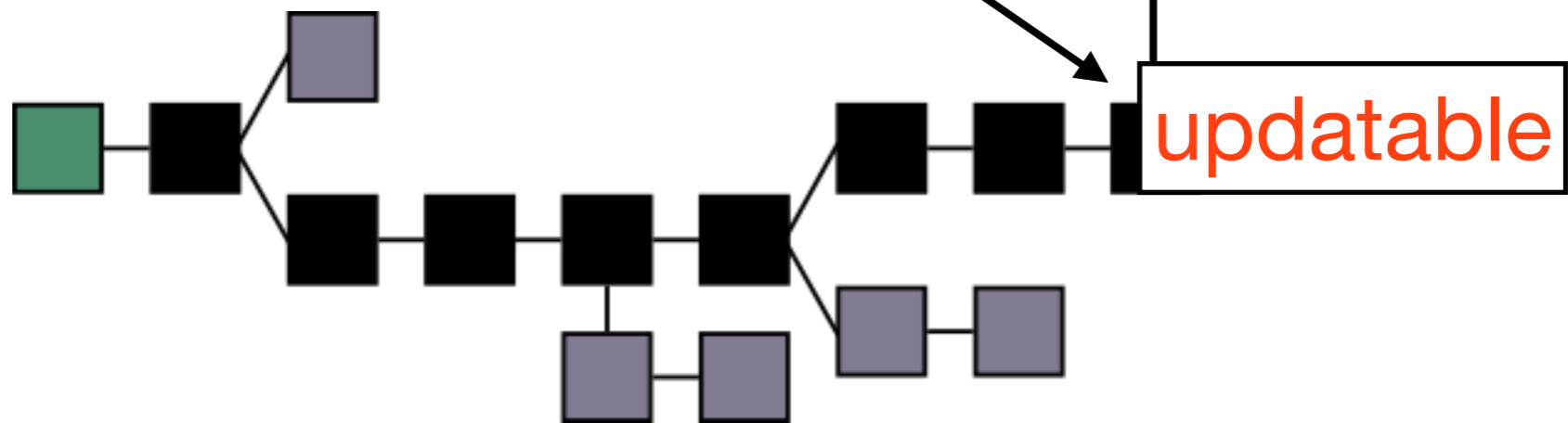
“20/7/69 @ 20:18”



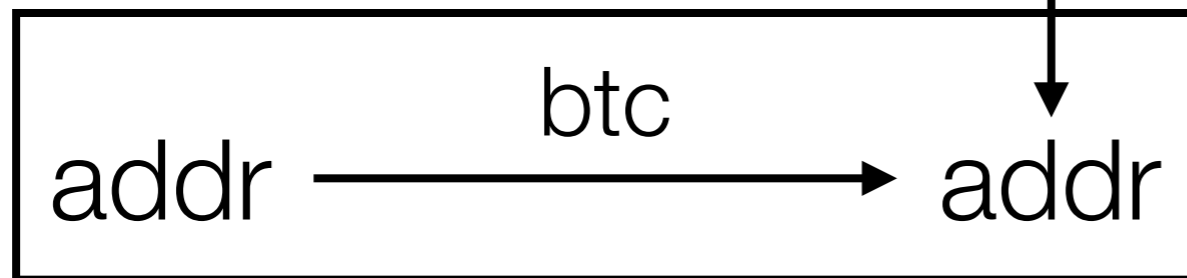
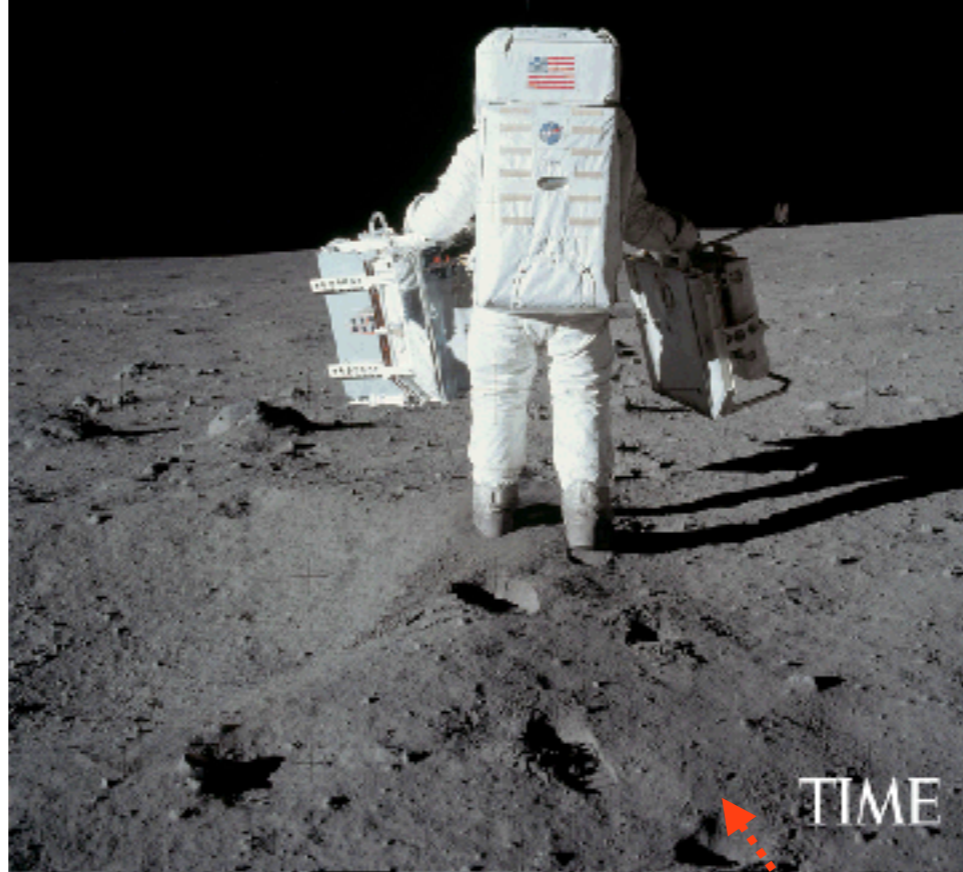
H()



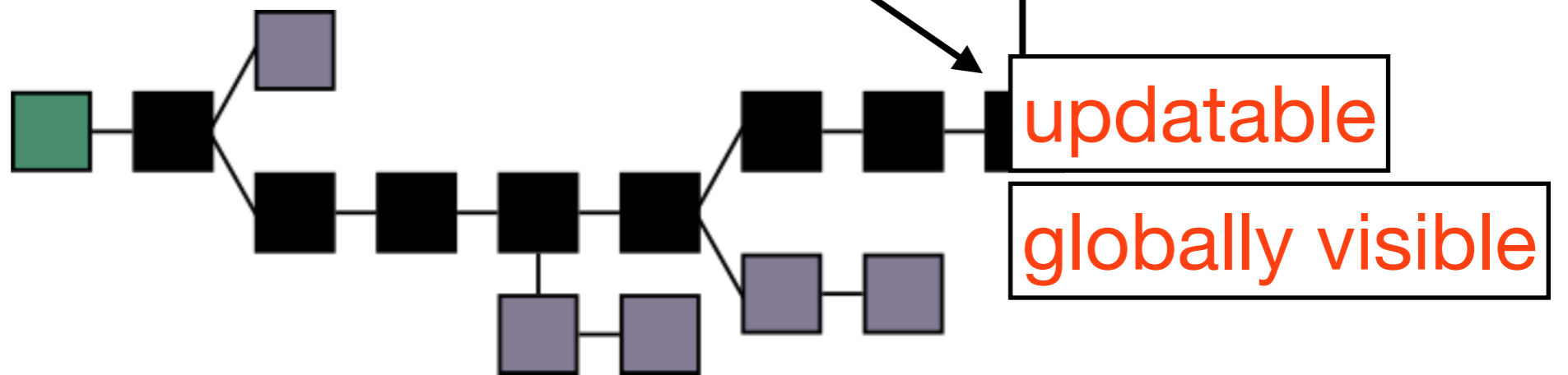
“20/7/69 @ 20:18”



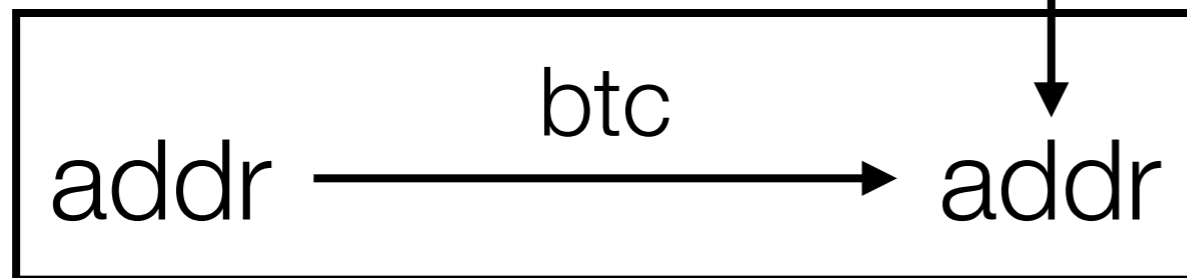
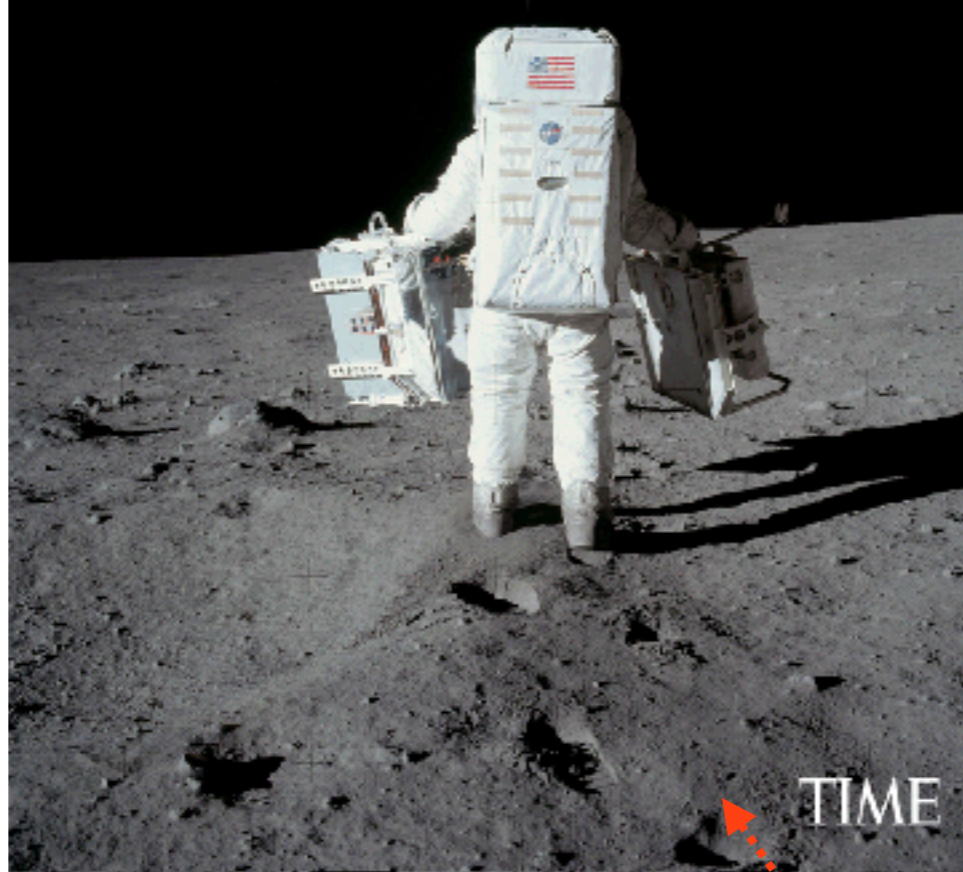
H()



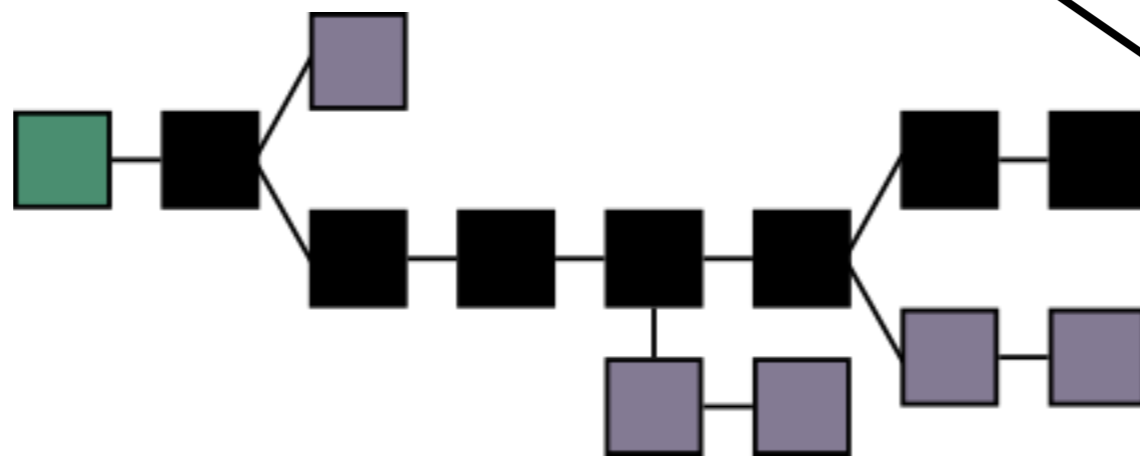
“20/7/69 @ 20:18”



H()



“20/7/69 @ 20:18”



- updatable
- globally visible
- immutable

notary publics

Select a document and have it certified in the Bitcoin blockchain [What?](#)

Click here or drag and drop your document in the box.

The file will **NOT** be uploaded. The cryptographic proof is calculated client-side.



Sign a document

Upload a document and sign it or
get it signed.



Verify a document

Check the authenticity of a
document signed on BlockSign.

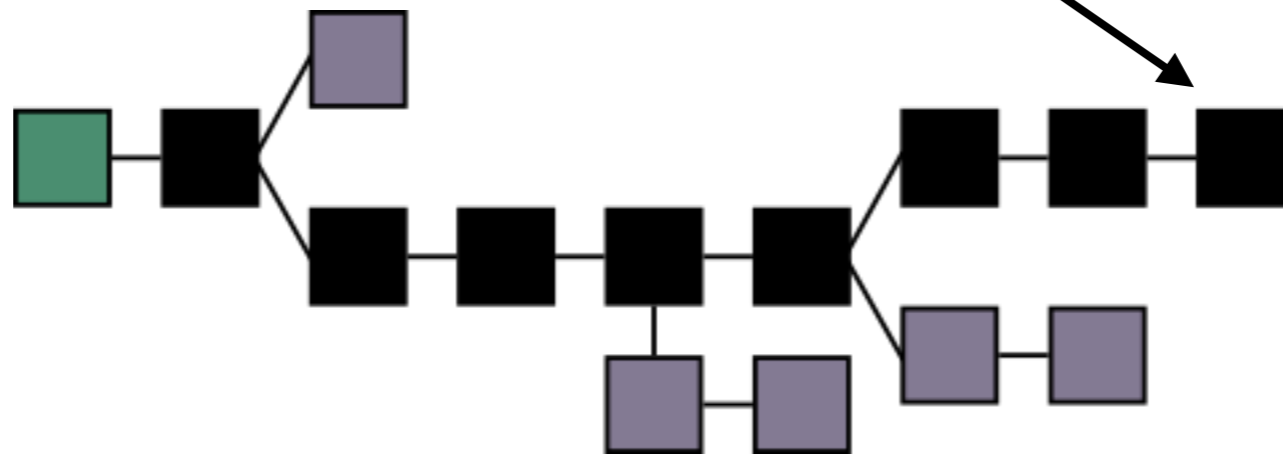
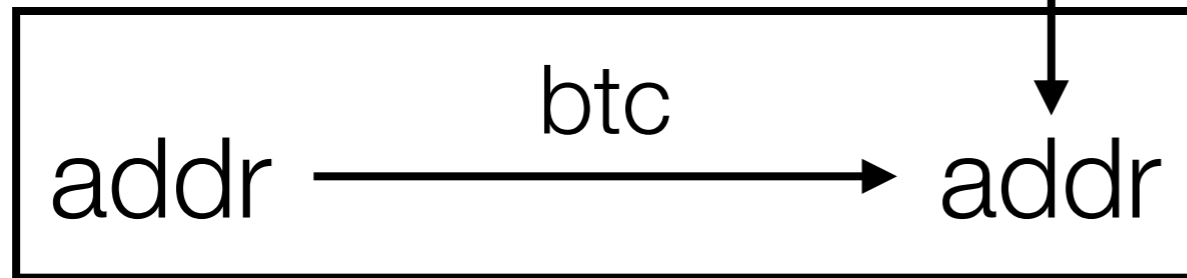
how to **claim ownership**



H (

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage



how to **claim ownership**

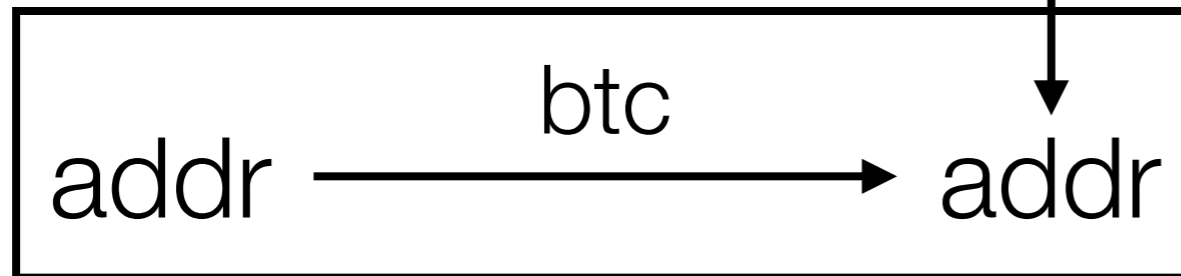


H (

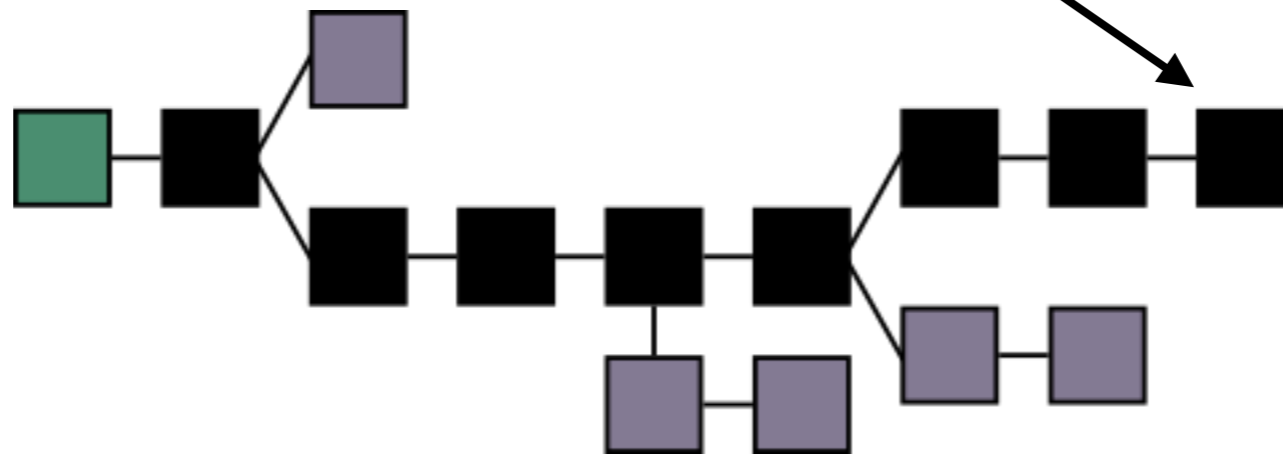
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

)



eprint



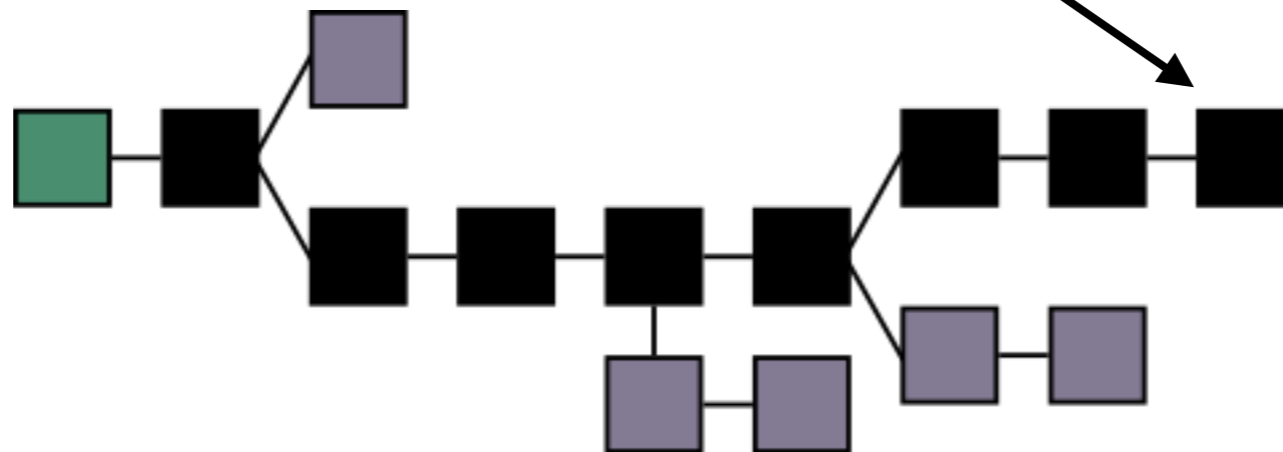
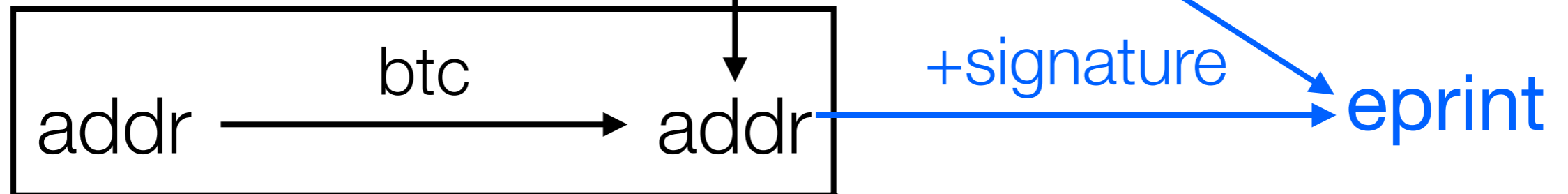
how to **claim ownership**



H (

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage



how to **claim ownership**



H (

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

how to **claim ownership**



H (

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

)

addr

+signature

eprint



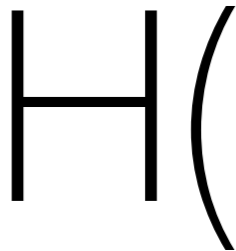
H (

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

)

how to **claim ownership**



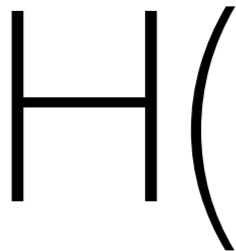
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

addr

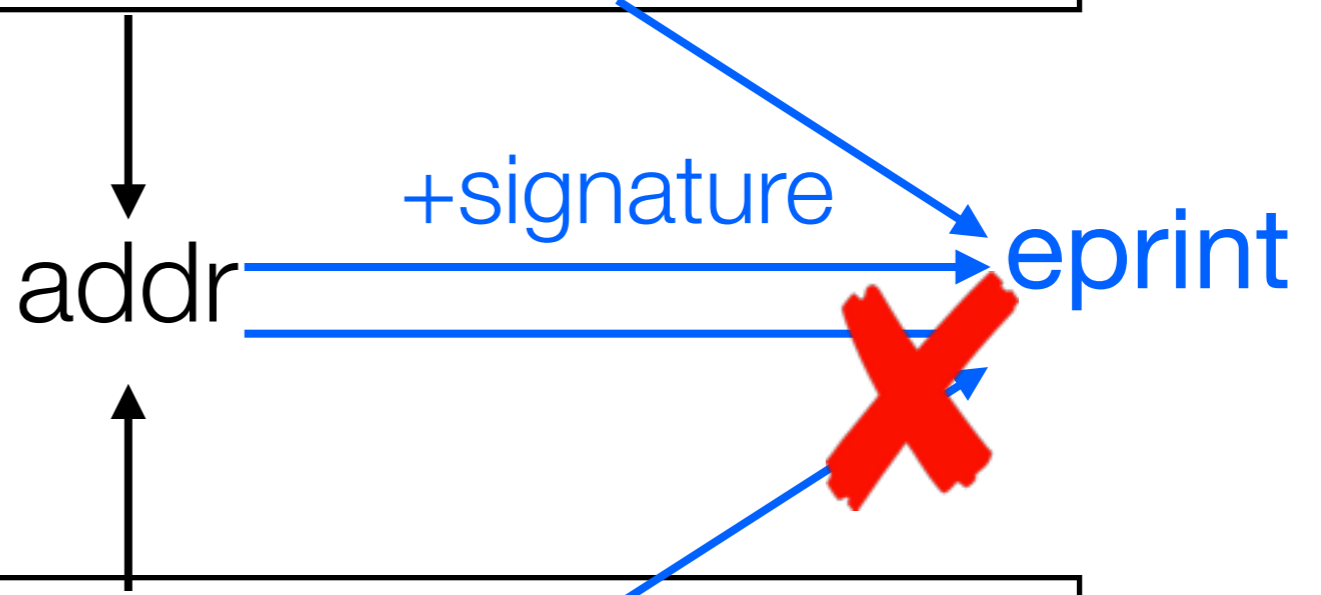
+signature

eprint



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage



MONOGRAPH_



`{"file":"http://static.mccoyspace.com/gifs/cars.gif", "post":"https://twitter.com/mccoyspace/status/462455439930966016", "hash":"f3969884355163f4d336fdef318d671d1d12616e60bb1dcb6be67f3a177a63d4", "title":"I hereby assert title to the file at the URL listed. It was originally published at the post URL. The file whose SHA265 hash is as indicated herein is the file in question. Title to file transfers to whoever controls this blockchain entry"}`

MONEGRAPH_



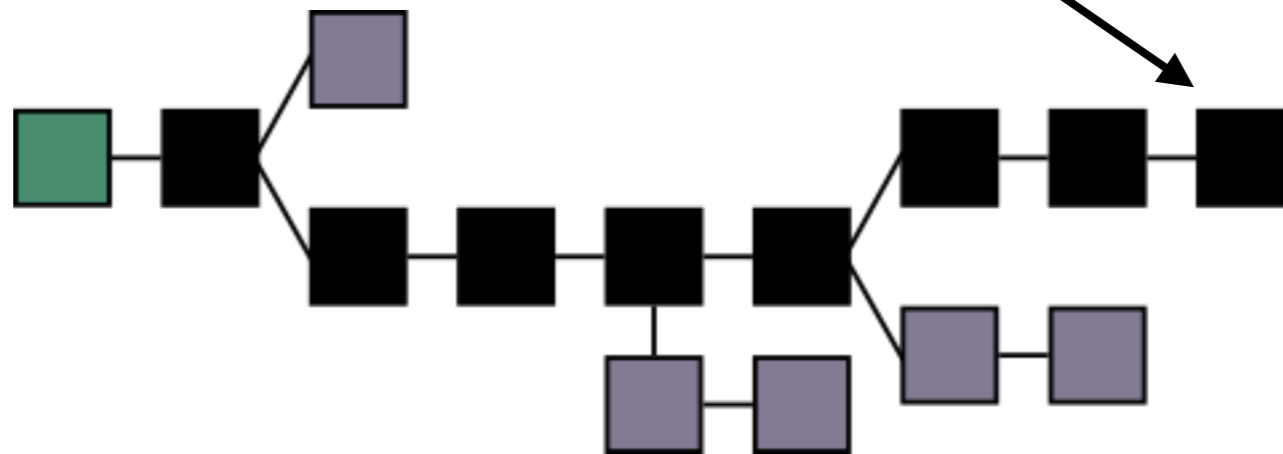
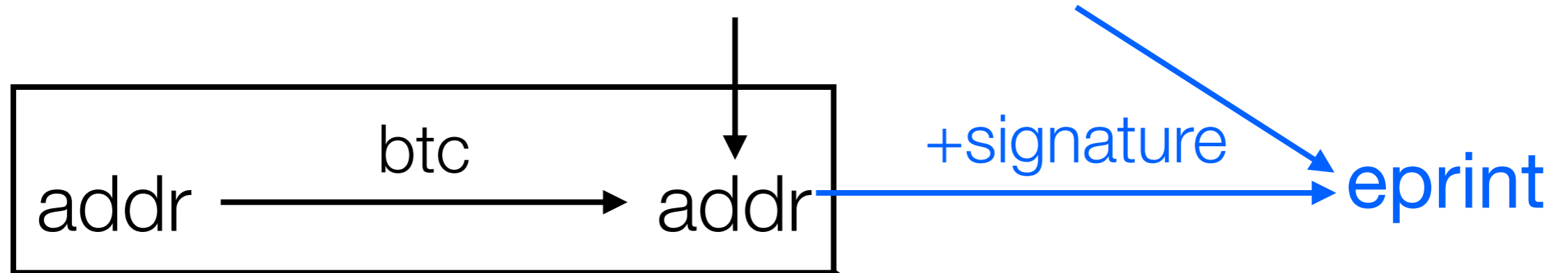
`{"file":"http://static.mccoyspace.com/gifs/cars.gif", "post":"https://twitter.com/mccoyspace/status/462455439930966016", "hash":"f3969884355163f4d336fdef318d671d1d12616e60bb1dcb6be67f3a177a63d4", "title":"I hereby assert title to the file at the URL listed. It was originally published at the post URL. The file whose SHA265 hash is as indicated herein is the file in question. Title to file transfers to whoever controls this blockchain entry"}`

how to **prove** history



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage



how to **prove history**

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage



how to **prove history**



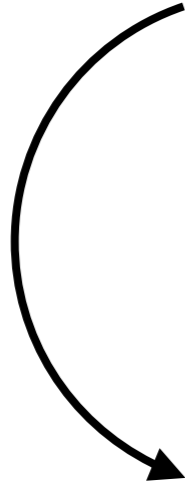
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

Characterising

A Fistful of Bitcoins: ~~Characterizing~~ Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage



how to **prove history**

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

Characterising

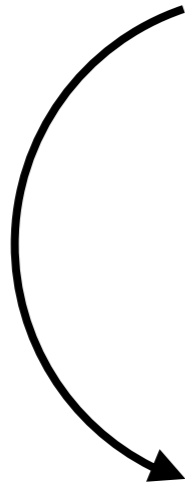
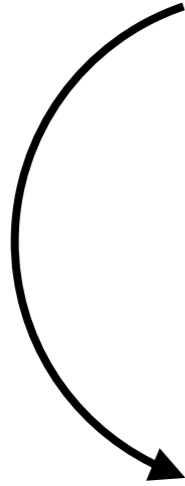
A Fistful of Bitcoins: ~~Characterizing~~ Payments Among Men with No Names

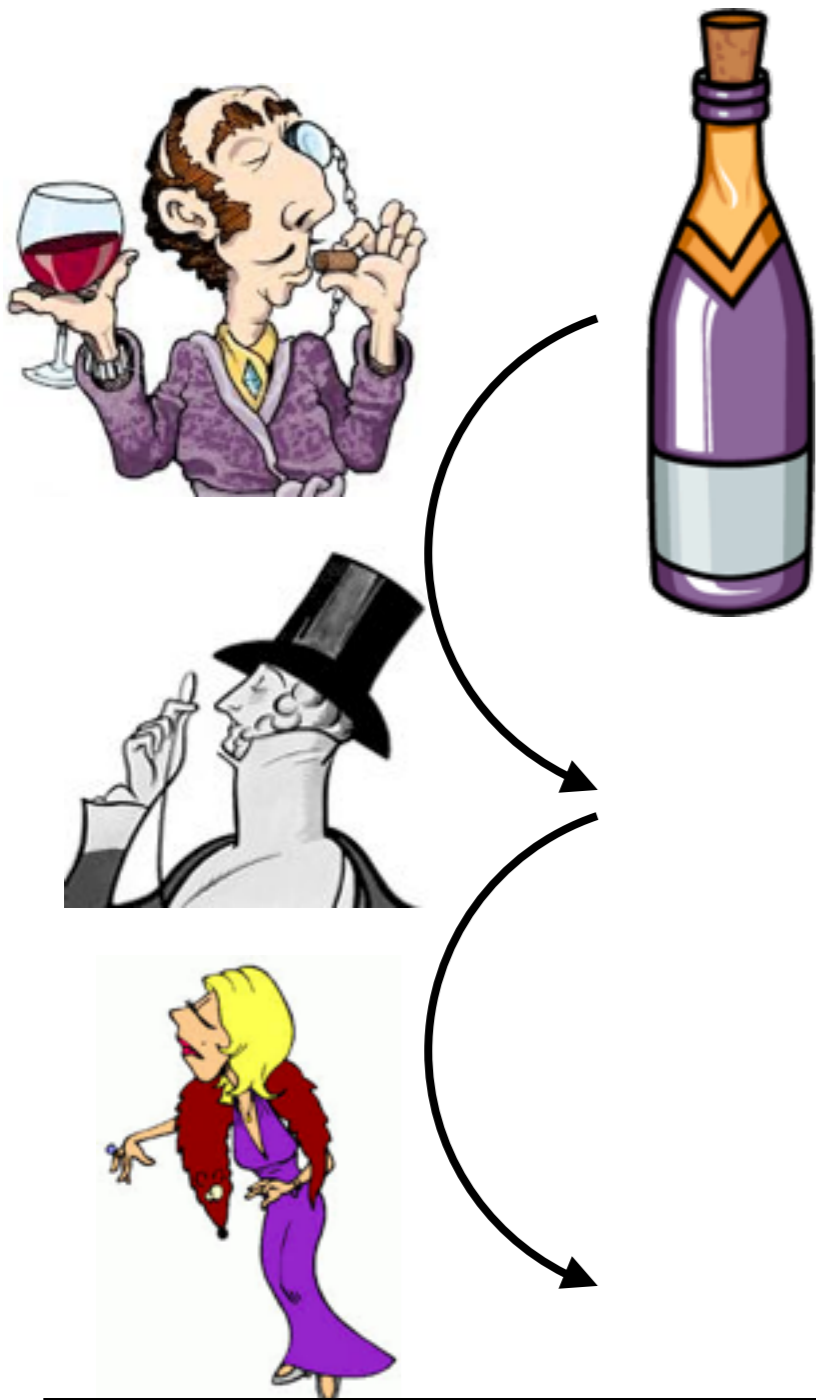
Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

Characterising

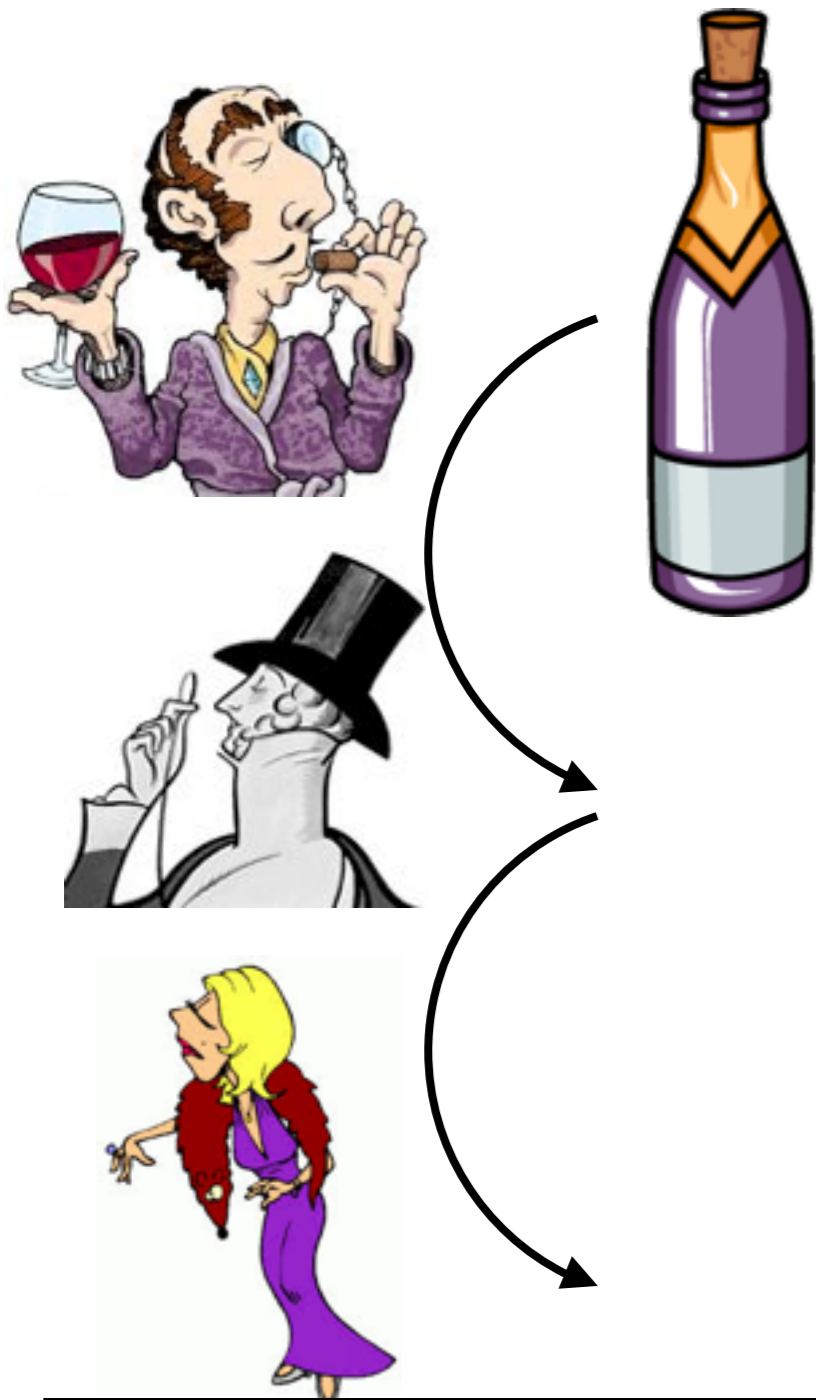
A Fistful of Bitcoins: ~~Characterizing~~ Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage





**The Future of Wine Provenance
Is Bitcoin**



**The Future of Wine Provenance
Is Bitcoin**

no blood diamonds!



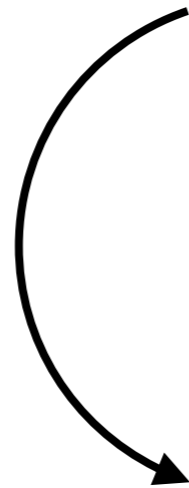
belonged to a queen!



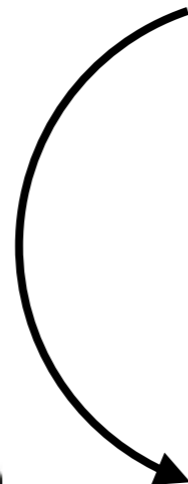
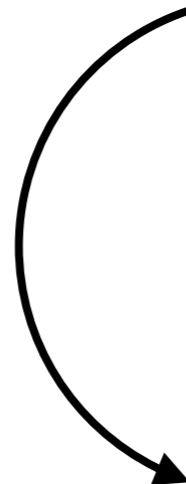
county records office / land registry



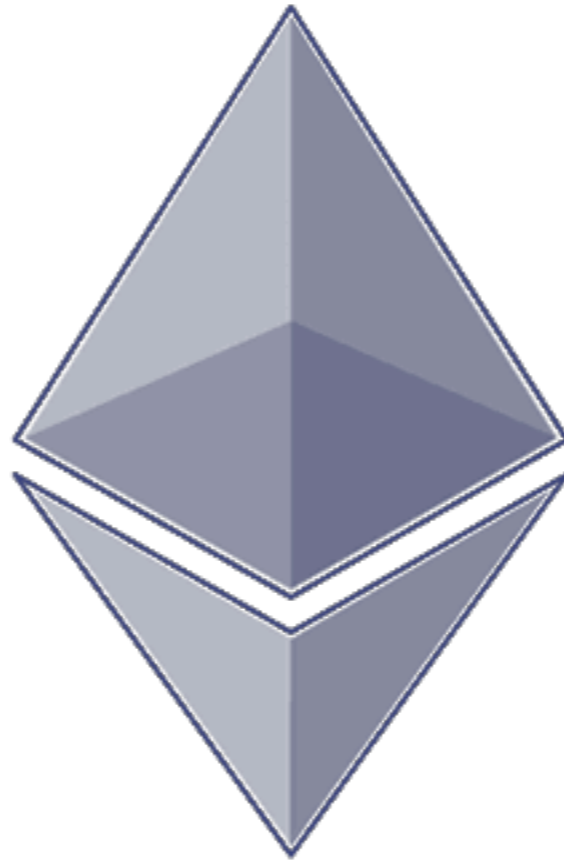
county records office / land registry



county records office / land registry



ethereum



proof of existence

proof of ownership
proof of existence

proof of history
proof of ownership
proof of existence

proof of history
proof of ownership
proof of existence

updatable

globally visible

immutable

Bitcoin might not be as as we hoped.

decentralized
secure
anonymous
stable
useful

proof of history
proof of ownership
proof of existence

updatable

globally visible

immutable

Bitcoin might not be as as we hoped.

decentralized

secure

[anonymous
stable
useful]

proof of history
proof of ownership
proof of existence

updatable

globally visible

immutable

Bitcoin might not be as as we hoped.

decentralized

secure

[anonymous
stable
useful]

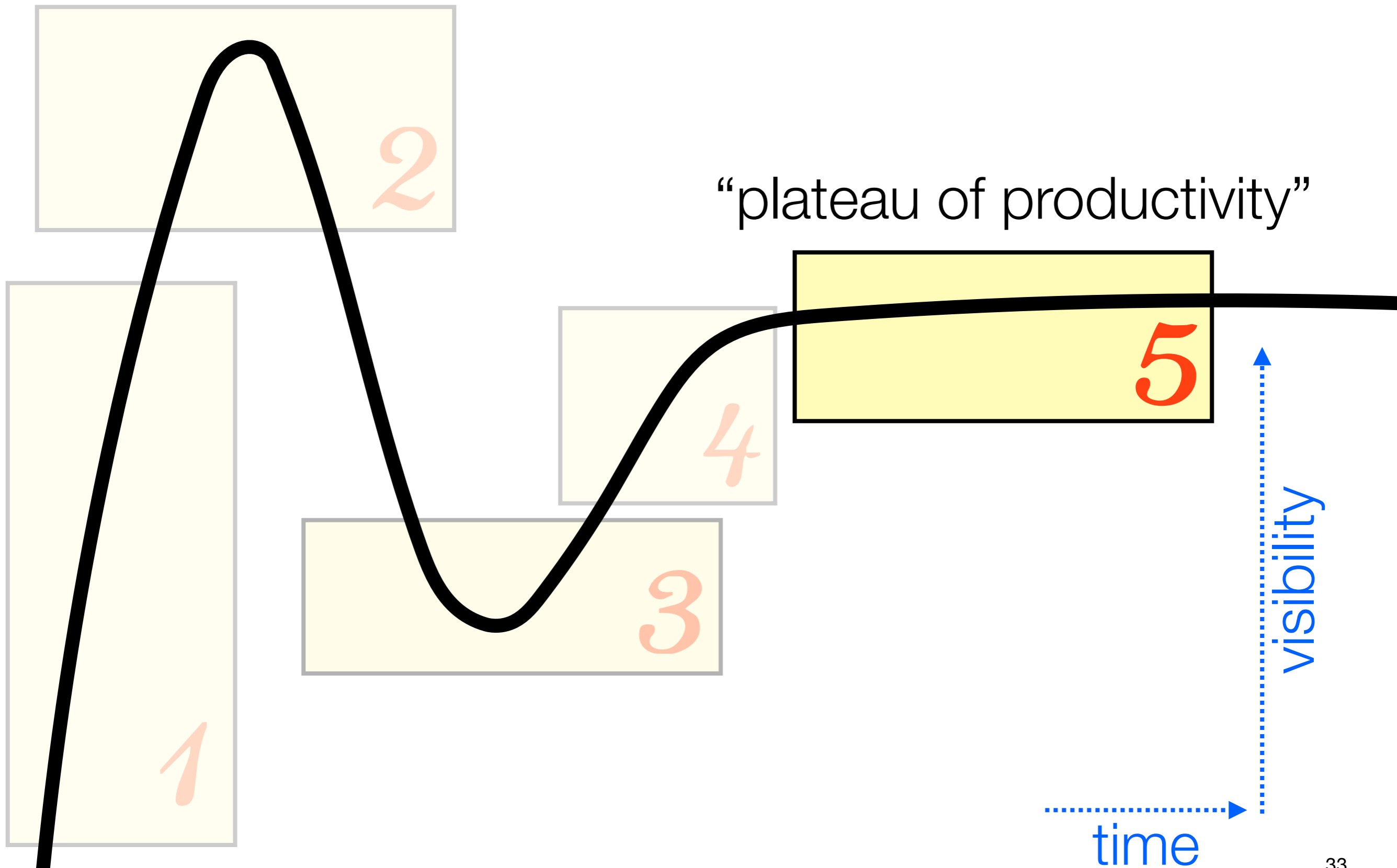
Less crucial in these contexts?

proof of history
proof of ownership
proof of existence

updatable

globally visible

immutable



what can real world cryptographers do?

what can real world cryptographers do?

increase **usability** to improve **security**

what can real world cryptographers do?

increase **usability** to improve **security**

enforce **decentralization**

what can real world cryptographers do?

increase **usability** to improve **security**

enforce **decentralization**

(solutions for **burn transactions**
solutions for **bloat problem**)

what can real world cryptographers do?

increase **usability** to improve **security**

enforce **decentralization**

(solutions for **burn transactions**
solutions for **bloat problem**)

audit software

what can real world cryptographers do?

increase **usability** to improve **security**

enforce **decentralization**

(solutions for **burn transactions**
solutions for **bloat problem**)

audit software

apply **proofs of history/ownership** to crypto

