Blockchain, Institutions and Technology

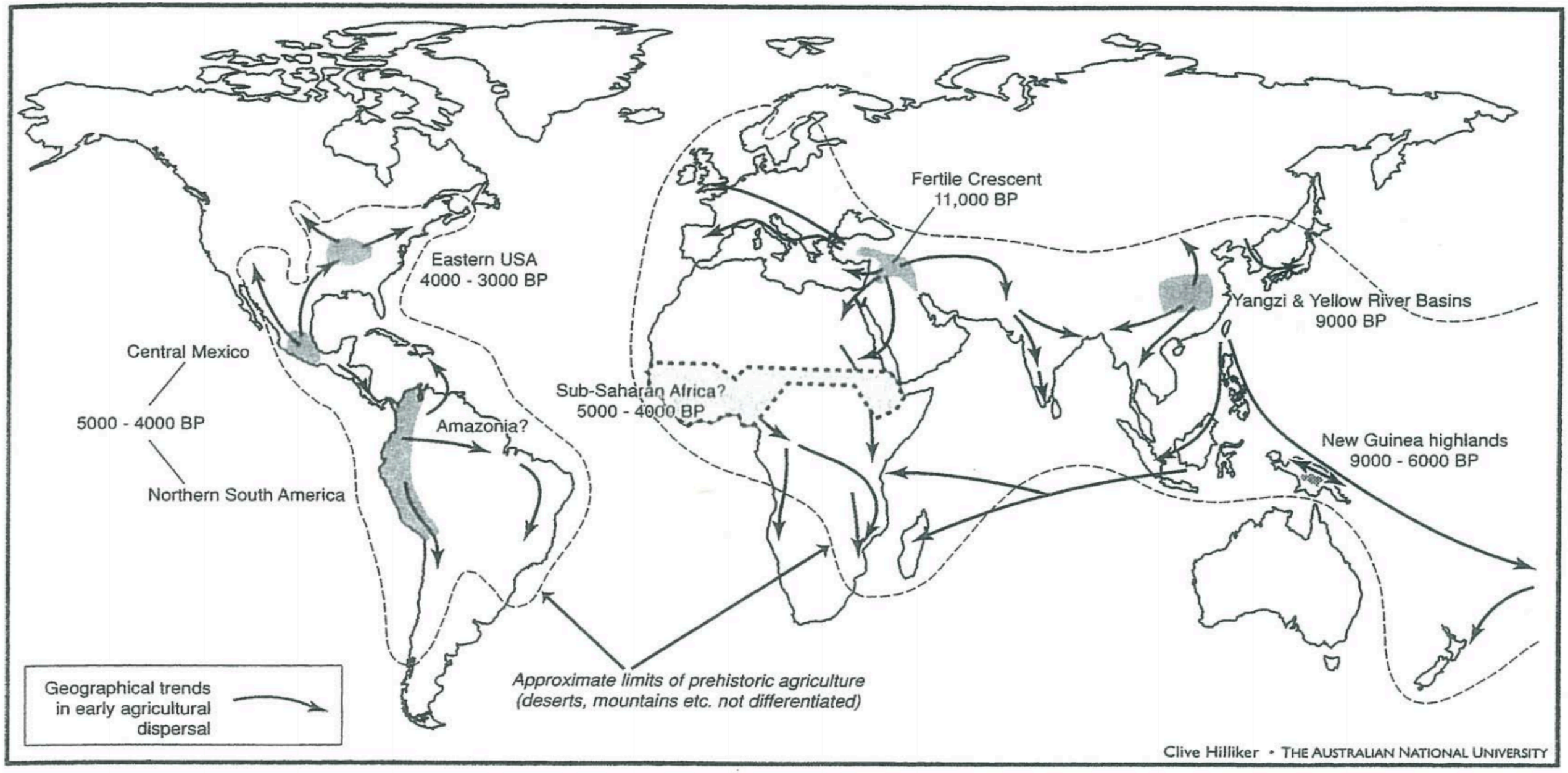
Lawrence R. De Geest

Spring 2018

hunter-gathering: 95% of biological history

egalitarian, resource-sharing, coinsurance

communal property



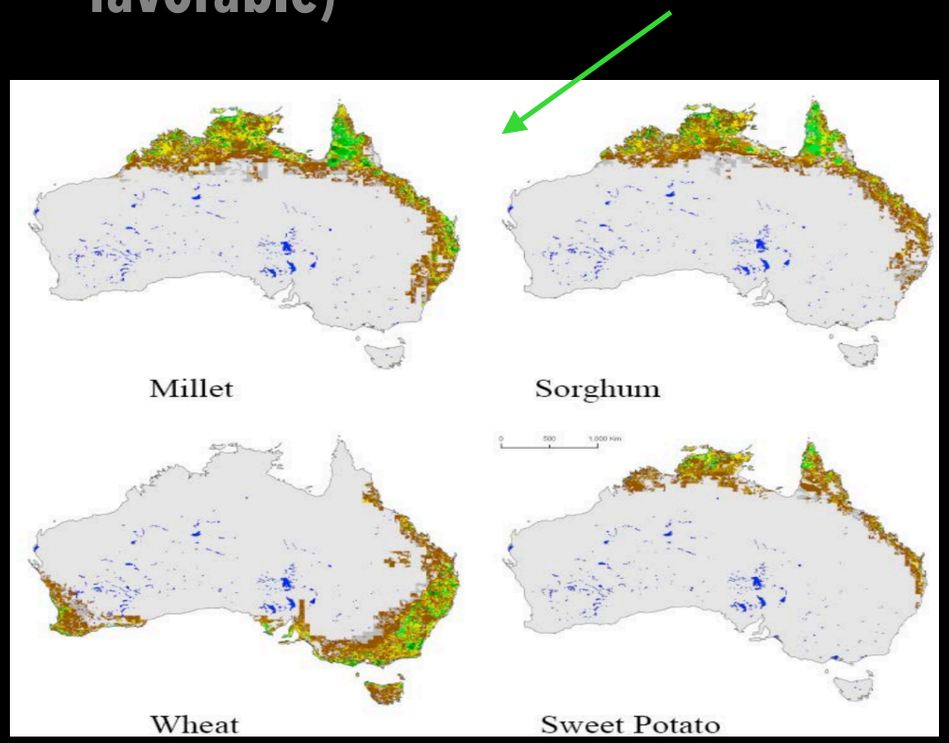
Suddenly, farming

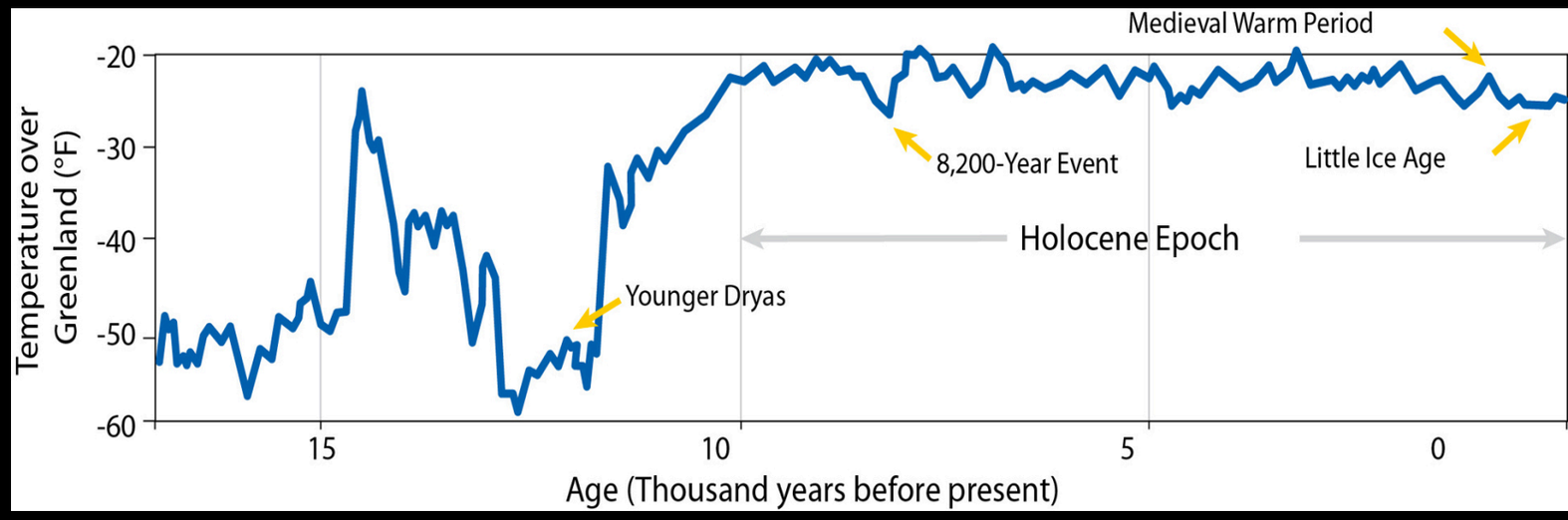
~~**communal property**~~ **private property**

But which came first: technology (farming) or institution (private property)?

Was it because climate conditions improved?

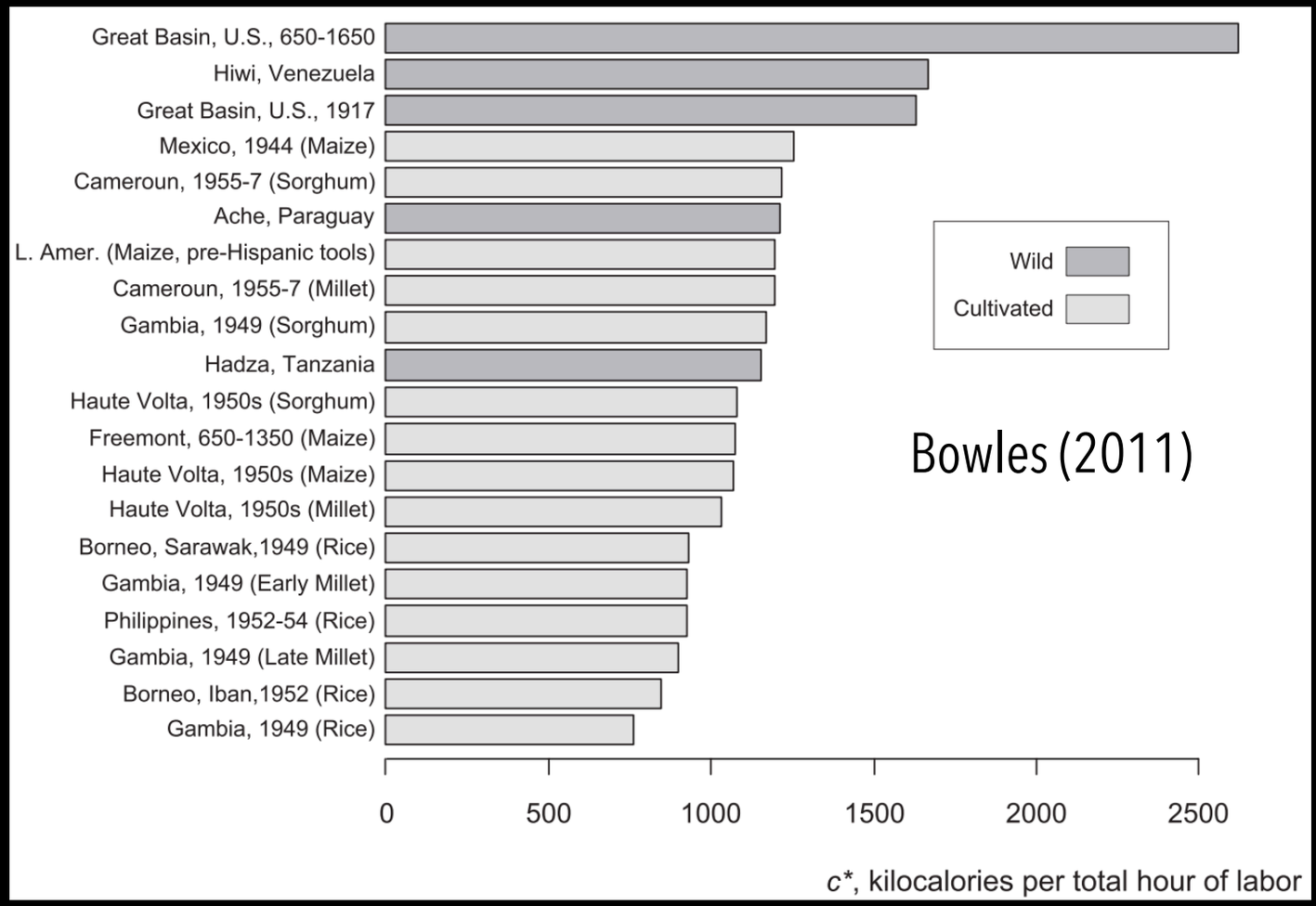
- That helped - but why then was adoption not uniform?
- The dog that did not bark: no Holocene revolution in certain places like Australia **(even though conditions were favorable)**





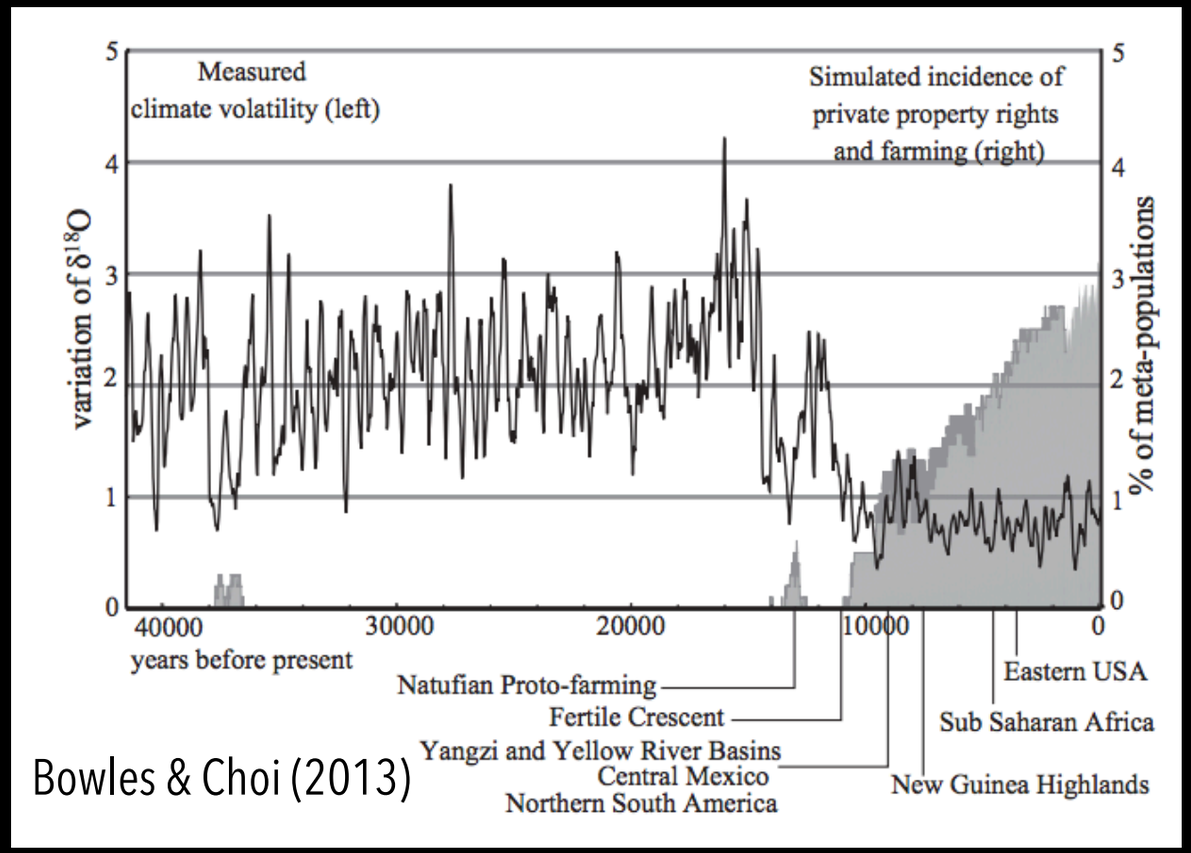
Was it because farming was *more productive?*

Probably not!



a one-way causal model is probably wrong

more likely: **co-emergence** of farming and private property



Bowles & Choi (2013)

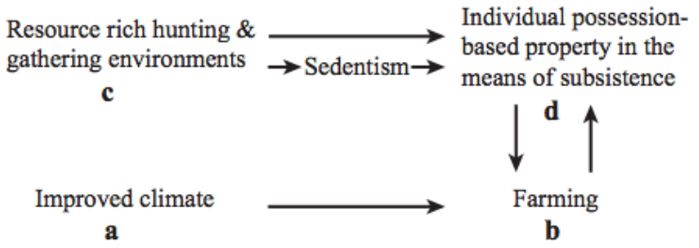
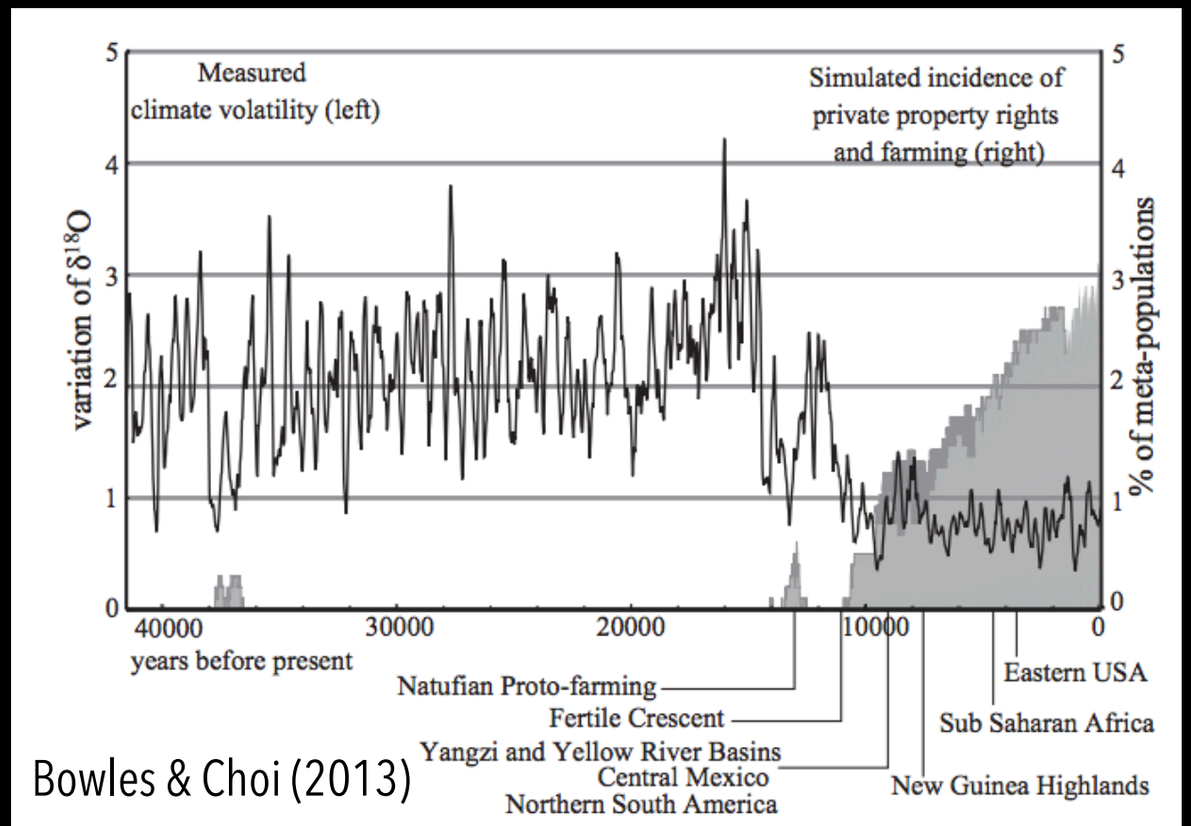


Fig. 1. Holocene coevolution of farming and private property. A conventional causal sequence is that **a** is a sufficient condition for **b**, which is then followed by **d**. Our model and simulations suggest a coevolutionary scenario: In the absence of farming, **c** is a necessary condition for **d**, which in conjunction with **a** provided the necessary but not sufficient conditions for **b**.

a one-way causal model is probably wrong

more likely: **co-emergence** of farming and private property



Bowles & Choi (2013)

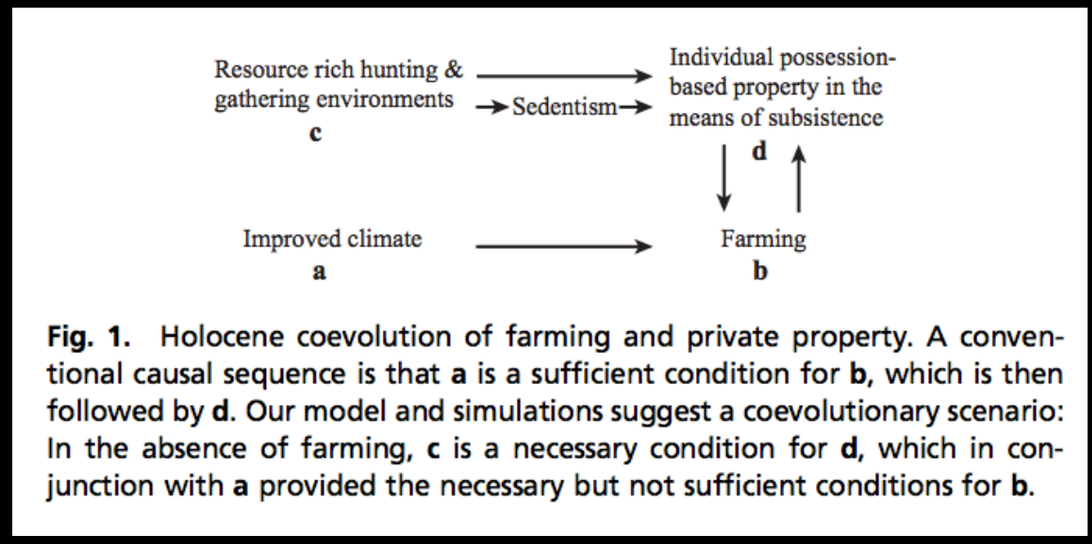


Fig. 1. Holocene coevolution of farming and private property. A conventional causal sequence is that **a** is a sufficient condition for **b**, which is then followed by **d**. Our model and simulations suggest a coevolutionary scenario: In the absence of farming, **c** is a necessary condition for **d**, which in conjunction with **a** provided the necessary but not sufficient conditions for **b**.

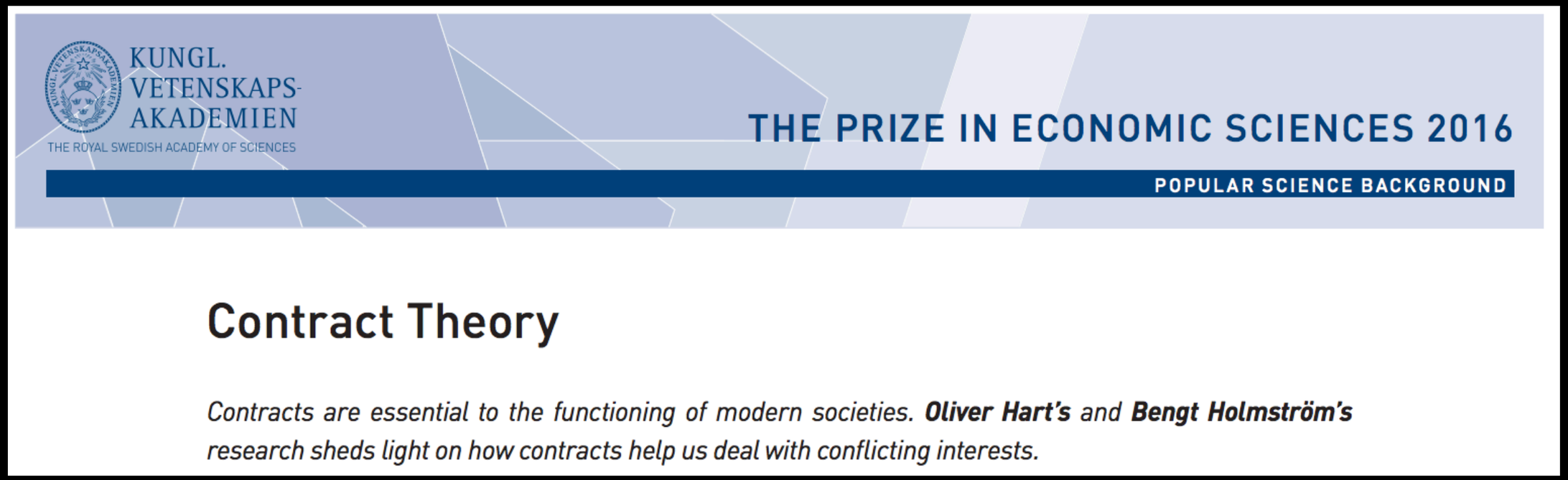
Key idea: institutions emerge to solve problems

property rights regimes determine access to resources
who can use it? who can be excluded?

benefit of private property regimes: individuals can more easily design **contracts** and **trade** **(e.g. maize for millet). this was revolutionary! all roads point to trade as the biggest reason humans are rich**

farming was probably adopted because it opened up new avenues for economic activity

we will look at **blockchain** in a similar way.
like farming, we can ask: what problem is blockchain solving?

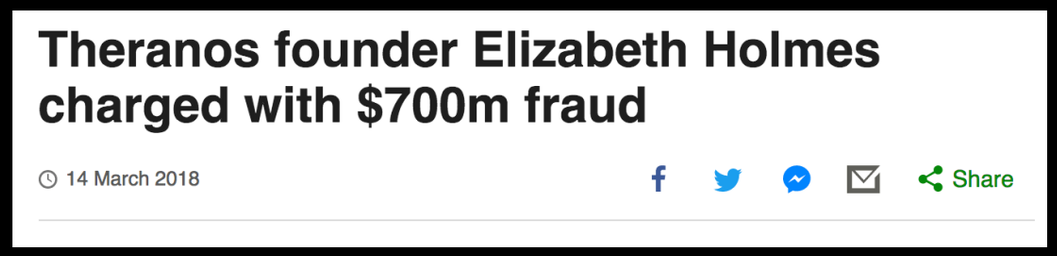


Contracts specify the transfer of private property

As we will see, blockchain **increases the contract space**
(the number/type of contracts people can enter)

why? because a major problem is that contracts are often **incomplete**
(hard to write down what to do in every possible contingency)

leads to **transaction costs** (costs associated with doing business) like enforcement
explains why we have the SEC and other centralized authorities regulating trade
trade relies on trust, and trust is expensive



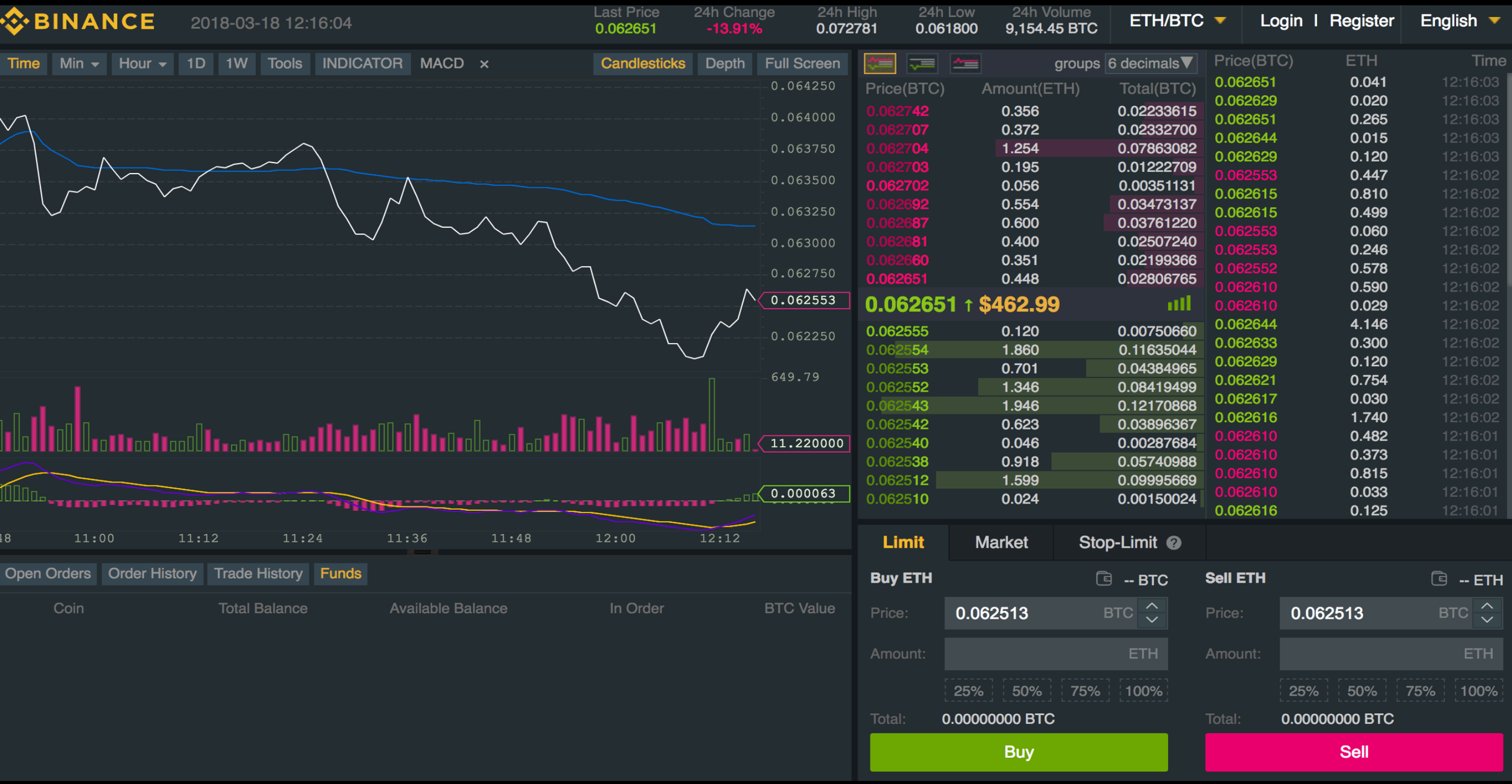
incomplete contracts can **crowd-out** trade

blockchain makes it possible to (somewhat) substitute trust with **smart contracts**
(roll the terms of trade and execution of trade and enforcement into one)

applications? look for any setting where incomplete contracts significantly crowd-out exchange
"How much more exchange would there have been if contracts were complete?"
(e.g. governance, intellectual property, tracking asset ownership, public records)

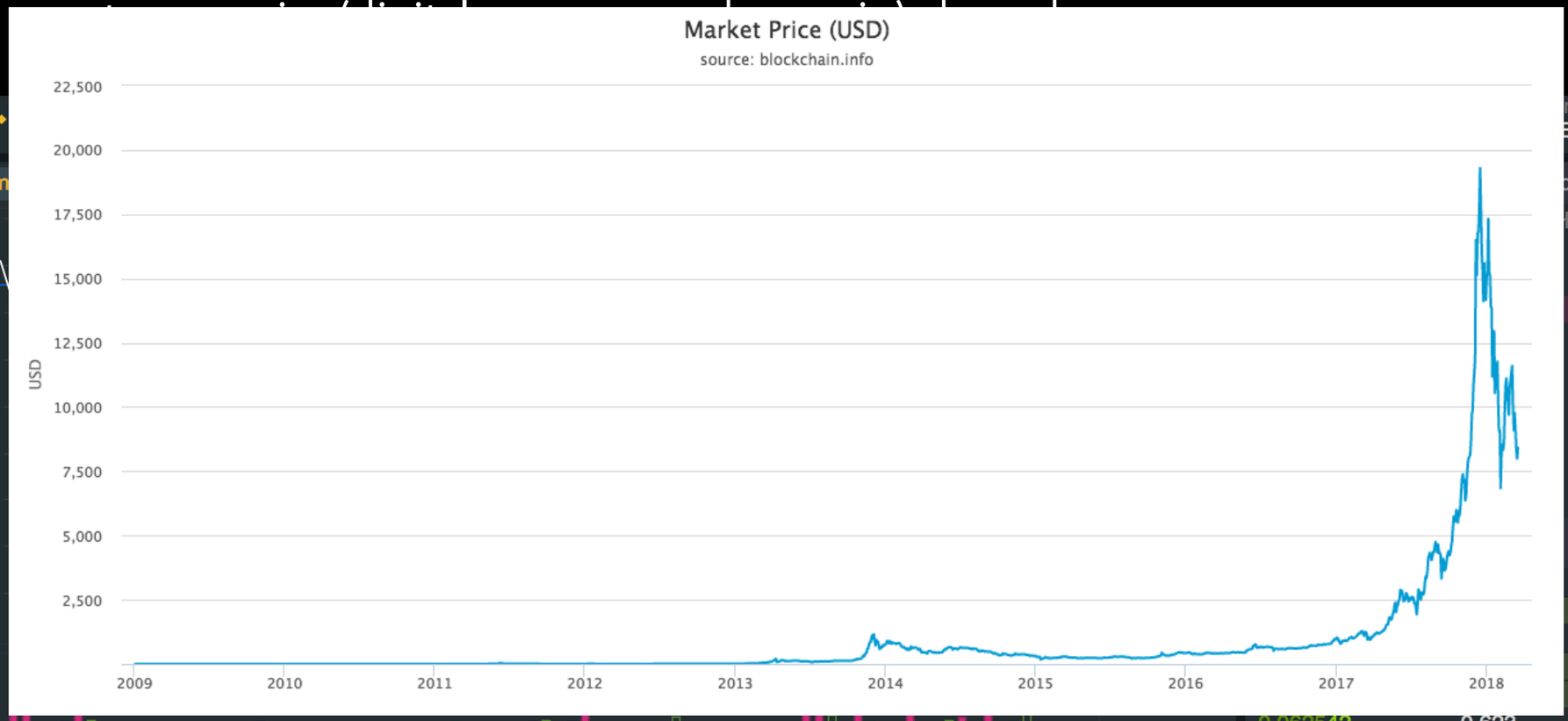
key question: will it remove the need for central authority (e.g. central banks)? *do we want that?*

cryptocurrencies (digital currency - code as coin) abound



focus less on the currency market and more on *what the currency is:* ***a means for participating in a blockchain***

why? **b/c if a blockchain is valuable, the currency is valuable**



ETH/BTC | Login | Register | English

Price(BTC)	ETH	Time
0.062651	0.041	12:16:03
0.062629	0.020	12:16:03
0.062651	0.265	12:16:03
0.062644	0.015	12:16:03
0.062629	0.120	12:16:03
0.062553	0.447	12:16:02
0.062615	0.810	12:16:02
0.062615	0.499	12:16:02
0.062553	0.060	12:16:02
0.062553	0.246	12:16:02
0.062552	0.578	12:16:02
0.062610	0.590	12:16:02
0.062610	0.029	12:16:02
0.062644	4.146	12:16:02
0.062633	0.300	12:16:02
0.062629	0.120	12:16:02
0.062621	0.754	12:16:02
0.062617	0.030	12:16:02
0.062616	1.740	12:16:02
0.062610	0.482	12:16:01
	0.373	12:16:01
		12:16:01
		12:16:01
		12:16:01

Total(BTC)
0.02233615
0.02332700
0.07863082
0.01222709
0.00351131
0.03473137
0.03761220
0.02507240
0.02199366
0.02806765
0.00750660
0.11635044
0.04384965
0.08419499
0.12170868
0.03896367
0.00287684

11.220000

0.062542 0.623
0.062540 0.046

11:00 11:12 11:24 11:36 11:48 12:00

Open Orders | Order History | Trade History | Funds

Coin	Total Balance	Available Balance	In Order

-- ETH
BTC
ETH
100%

focus less on the currency market and more on *what the cu*

why? **b/c if a blockchain is valuable, the currency is**

'Virgin Mary' toast fetches $28,000

A decade-old toasted cheese sandwich said to bear an image of the Virgin Mary has sold on the eBay auction website for $28,000.

The toast is not intended for consumption

An internet casino confirmed it had purchased the sandwich, saying it had become a "part of pop culture".

Goldenpalace.com says it will take the sandwich on world tour before selling it and donating the money to charity.

Diane Duyser, from Florida, says the sandwich has never gone mouldy since she made it 10 years ago.

ETH/BTC | Login | Register | English

Price(BTC) ETH Time

Price(BTC)	ETH	Time
0.062651	0.041	12:16:03
0.062629	0.020	12:16:03
0.062651	0.265	12:16:03
0.062644	0.015	12:16:03
0.062629	0.120	12:16:03
0.062553	0.447	12:16:02
0.062615	0.810	12:16:02
0.062615	0.499	12:16:02
0.062553	0.060	12:16:02
0.062553	0.246	12:16:02
0.062552	0.578	12:16:02
0.062610	0.590	12:16:02
0.062610	0.029	12:16:02
0.062644	4.146	12:16:02
0.062633	0.300	12:16:02
0.062629	0.120	12:16:02
0.062621	0.754	12:16:02
0.062617	0.030	12:16:02
0.062616	1.740	12:16:02
0.062610	0.482	12:16:01
	0.373	12:16:01
		12:16:01
		12:16:01
		12:16:01

Total(BTC)

Total(BTC)
0.02233615
0.02332700
0.07863082
0.01222709
0.00351131
0.03473137
0.03761220
0.02507240
0.02199366
0.02806765
0.00750660
0.11635044
0.04384965
0.08419499
0.12170868
0.03896367
0.00287684

11.220000

0.062542 0.623
0.062540 0.046

11:00 11:12 12:00

Open Orders | Order History | Tr

Coin | In Order

-- ETH
BTC
ETH
100%

focus less on the ... *what the cu*

why? **b/c if a blockchain is valuable, the currency is**

'Virgin Mary' toast fetches $28,000

A decade-old toasted cheese sandwich said to bear an image of the Virgin Mary has sold on the eBay auction website for $28,000.

An internet casino confirmed it had purchased the sandwich, saying it had become a "part of pop culture".

Goldenpalace.com says it will take the sandwich on world tour before selling it and donating the money to charity.

The toast is not intended for consumption

Diane Duyser, from Florida, says the sandwich has never gone mouldy since she made it 10 years ago.

markets facilitate voluntary trade between buyers and sellers

markets facilitate voluntary trade between buyers and sellers

a buyer and seller enter into a contract

markets facilitate voluntary trade between buyers and sellers

a buyer and seller enter into a contract

for the contract to be **executed**, attributes of the trade need to verified
e.g. the quality of the good, authenticity of payment. trivial if trade happens in person.
the only intermediary is the central backing the currency used in the trade

markets facilitate voluntary trade between buyers and sellers

a buyer and seller enter into a contract

for the contract to be **executed**, attributes of the trade need to verified
e.g. the quality of the good, authenticity of payment. trivial if trade happens in person.
the only intermediary is the central backing the currency used in the trade

What about online trade? Intermediaries reduce information asymmetry by providing 3rd party verification, becoming more important when markets scale. The intermediary charges a fee for this service. Thus the cost of transaction increases.

e.g. Ebay, Amazon, banks

markets facilitate voluntary trade between buyers and sellers

a buyer and seller enter into a contract

for the contract to be **executed**, attributes of the trade need to verified
e.g. the quality of the good, authenticity of payment. trivial if trade happens in person.
the only intermediary is the central backing the currency used in the trade

What about online trade? Intermediaries reduce information asymmetry by providing 3rd party verification, becoming more important when markets scale. The intermediary charges a fee for this service. Thus the cost of transaction increases.
e.g. Ebay, Amazon, banks

Major drawback of centralized systems is that they have unique points of failure
e.g. the 2008-2009 financial crisis

markets facilitate voluntary trade between buyers and sellers

a buyer and seller enter into a contract

for the contract to be **executed**, attributes of the trade need to verified
e.g. the quality of the good, authenticity of payment. trivial if trade happens in person.
the only intermediary is the central backing the currency used in the trade

What about online trade? Intermediaries reduce information asymmetry by providing 3rd party verification, becoming more important when markets scale. The intermediary charges a fee for this service. Thus the cost of transaction increases.
e.g. Ebay, Amazon, banks

Major drawback of centralized systems is that they have unique points of failure
e.g. the 2008-2009 financial crisis

3rd party verification relies on monitoring users and enforcing contracts.
a big part of this is collecting **information** above and beyond what is needed if contracts were complete.
what if this information leaks?
e.g. credit card data, social security numbers
leakages: information could be sold by intermediary, or it could be stolen

markets facilitate voluntary trade between buyers and sellers

a buyer and seller enter into a contract

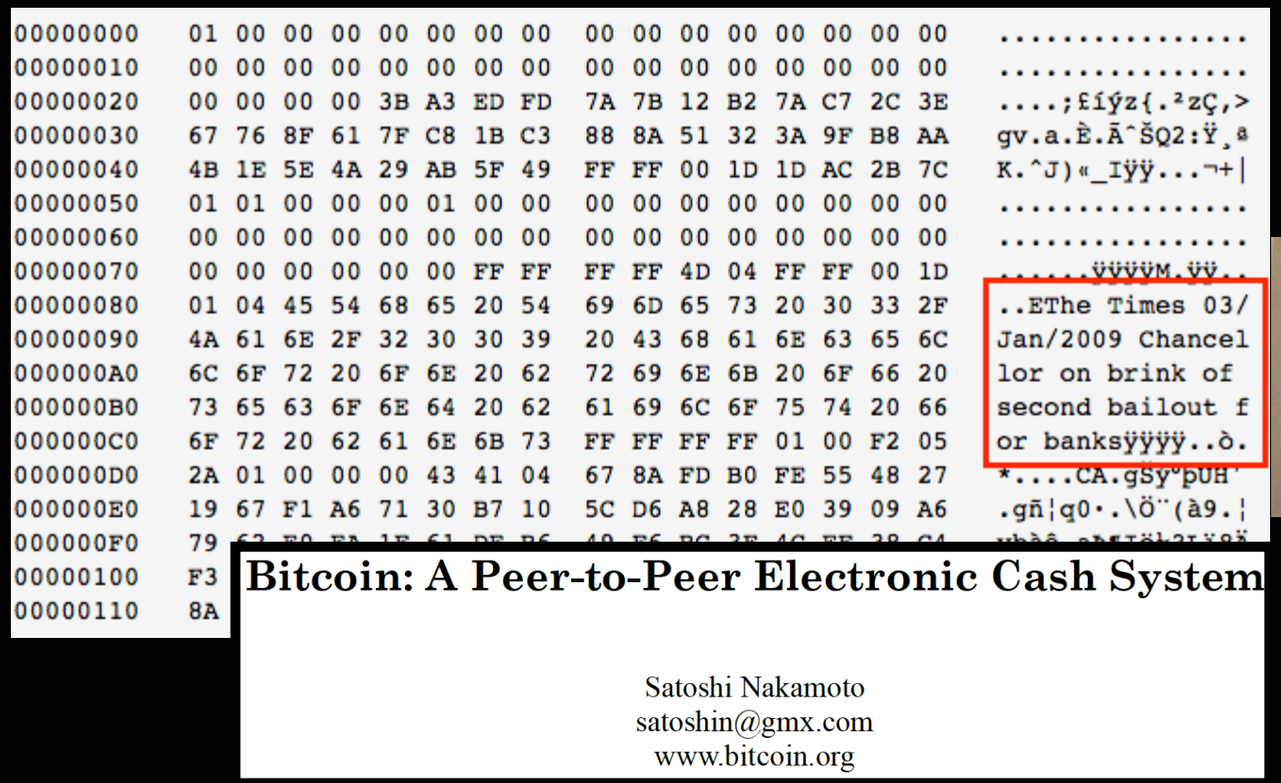
for the contract to be **executed**, attributes of the trade need to verified
e.g. the quality of the good, authenticity of payment. trivial if trade happens in person.
the only intermediary is the central backing the currency used in the trade

What about online trade? Intermediaries reduce information asymmetry by providing 3rd party verification, becoming more important when markets scale. The intermediary charges a fee for this service. Thus the cost of transaction increases.

e.g. Ebay, Amazon, banks

Major drawback of centralized systems is that they have unique points of failure
e.g. the 2008-2009 financial crisis

3rd party verification relies on monitoring users and enforcing
a big part of this is collecting **information** above and beyond
what if this information leaks?
e.g. credit card data, social security numbers
leakages: information could be sold by intermediary,



```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 F0 EA 1E 61 DE B6   49 F6 BC 3E 4C FF 38 C4   ybðê.aÞ¶Iö¼>Lÿ8Ä
00000100   F3
00000110   8A
```

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

*"**We define an electronic coin as a chain of digital signatures**. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership."*

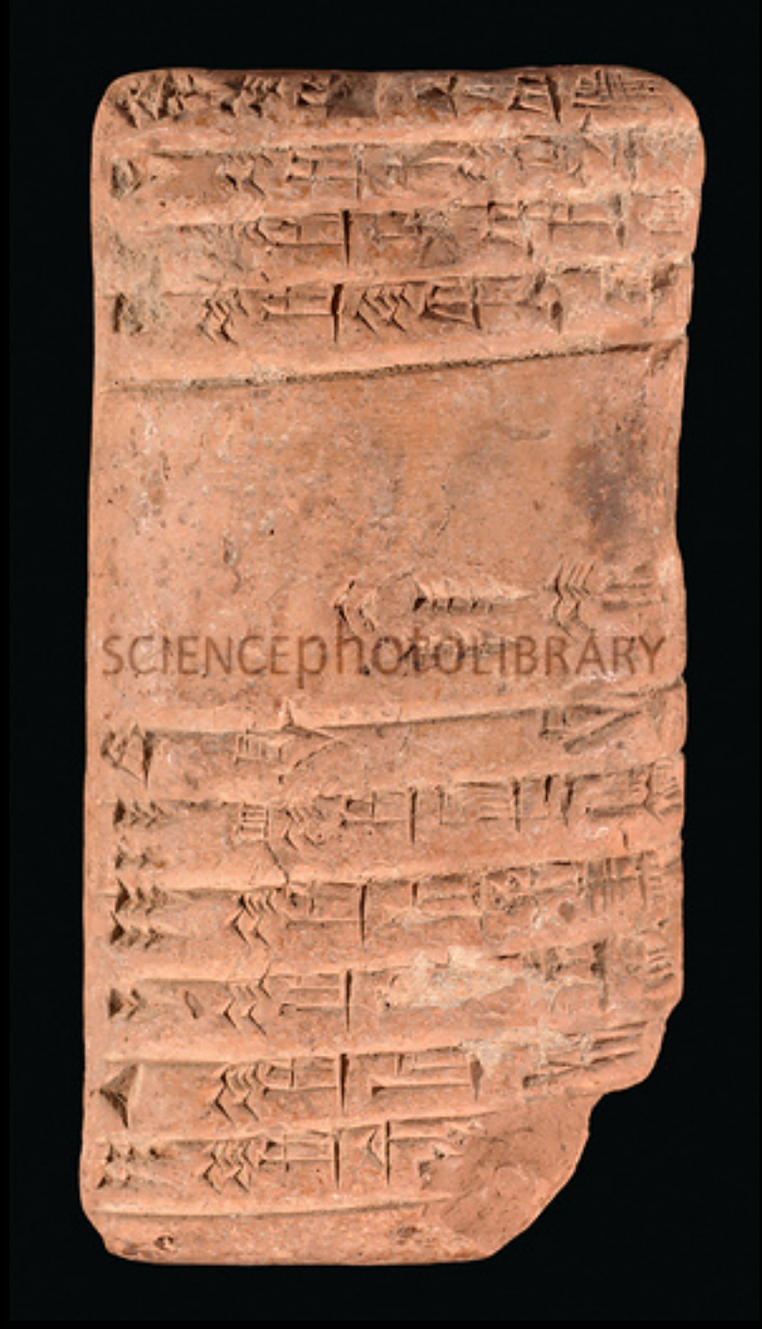
Amazon and Ebay are *centralized markets*
transactions are verified and executed by the intermediary

what if you could substitute trust in intermediary with trust in code?

information about the buyer/seller and/or the good can be digitized

it can then be stored on a "distributed ledger" *that can be viewed by a decentralized market*

the market can then verify transactions by agreeing on the true state of the ledger - **crowed-sourced verification**



Height	Time	Relayed By	Hash	Size (kB)
514134 (Main Chain)	2018-03-18 19:56:50	ViaBTC	0000000000000000003523b6696867f90c7e946020b5d91975620c9afe3d8eb3	1,112.12
514133 (Main Chain)	2018-03-18 19:18:28	BTC.TOP	0000000000000000000270d96fa1763a0cbf8b45fc3ad35352fc813a8bf90ee7b	1,166.45
514132 (Main Chain)	2018-03-18 19:02:28	AntPool	0000000000000000000421f2ec02f8a0d20ca050fc1acb8c1a209a70638de352c	122.05
514131 (Main Chain)	2018-03-18 19:00:48	ViaBTC	0000000000000000000c5db329c4eb6781f80539bc1c32d28c38ec8fc18a727c	1,266.83
514130 (Main Chain)	2018-03-18 18:59:12	AntPool	0000000000000000003fa30b5d5157af623d3db0122cf22da2ef14f7cfbdf729	279.85
514129 (Main Chain)	2018-03-18 18:56:11	Bitcoin.com	0000000000000000002481c4bd3c61ce4c571ee365650af63512ac7265a99803	111.26
514128 (Main Chain)	2018-03-18 18:52:14	AntPool	0000000000000000003d75e0f3036e0dd1f703264daed3a9d2bf8888d889a554	1,077.95
514127 (Main Chain)	2018-03-18 18:38:56	F2Pool	0000000000000000004a01d058296d9c0fe2b51665d051daf132ab7d5e793c76	163.63
514126 (Main Chain)	2018-03-18 18:36:49	BTC.com	0000000000000000014dd997b8bbd7c1c154d89159bf33c25f6391d03f2cc59	620.78
514125 (Main Chain)	2018-03-18 18:29:55	SlushPool	0000000000000000004da3f10312a139123d82891fa719175dba64fd570035f3	182.93

Suppose I want to buy your used car with a Bitcoin
Problem: what if I already spent it? How do you confirm I'm not "double-spending"?
Traditionally this is the domain of a central authority.

"The only way to confirm the absence of a transaction is to be aware of all transactions…To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received."

Suppose I want to buy your used car with a Bitcoin
Problem: what if I already spent it? How do you confirm I'm not "double-spending"?
Traditionally this is the domain of a central authority.

"The only way to confirm the absence of a transaction is to be aware of all transactions…To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received."

That system is **blockchain:** a sequential database secured with cryptography

The idea of "chains of blocks" has been around since Haber and Stornett (1991)

a "block" is a bundle of data (e.g. transactions, property rights)
it is computationally cheaper to authorize a block of transactions than each transaction alone

by "chaining" blocks you can deter fraud

Suppose I want to buy your used car with a Bitcoin
Problem: what if I already spent it? How do you confirm I'm not "double-spending"?
Traditionally this is the domain of a central authority.

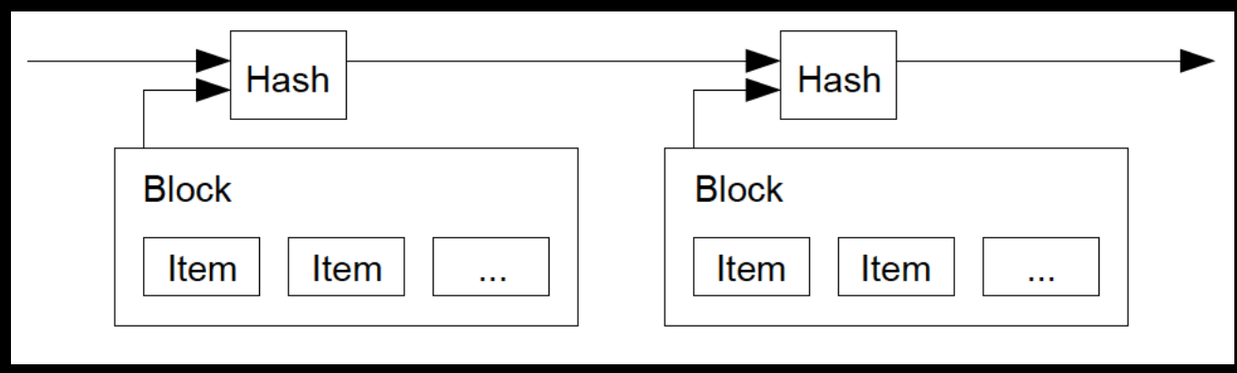
"The only way to confirm the absence of a transaction is to be aware of all transactions…To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received."

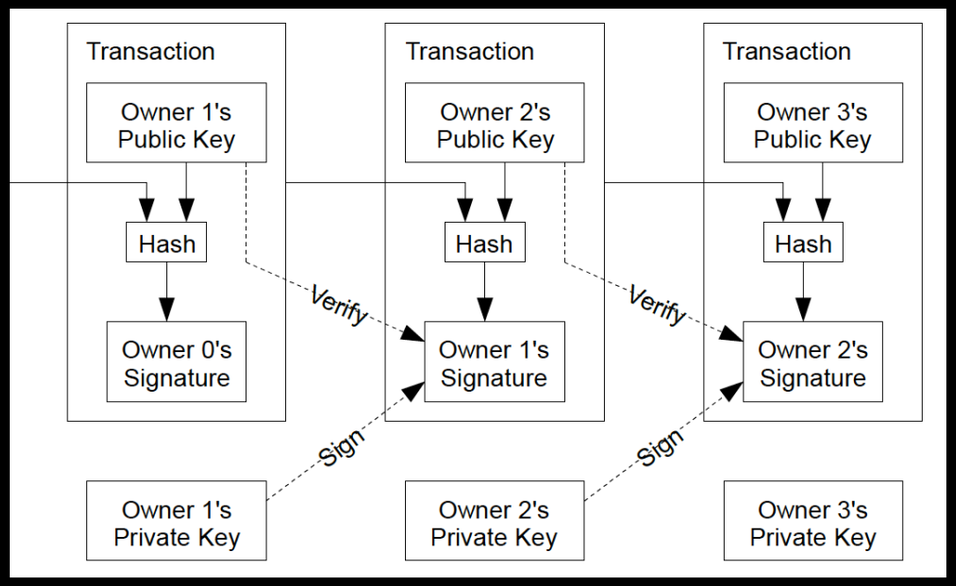
That system is **blockchain:** a sequential database secured with cryptography

The idea of "chains of blocks" has been around since Haber and Stornett (1991)

a "block" is a bundle of data (e.g. transactions, property rights)
it is computationally cheaper to authorize a block of transactions than each transaction alone

by "chaining" blocks you can deter fraud





What makes Bitcoin so interesting is how it combines three technologies to create a blockchain:

1. private key cryptography

   digital signature = private key + public key

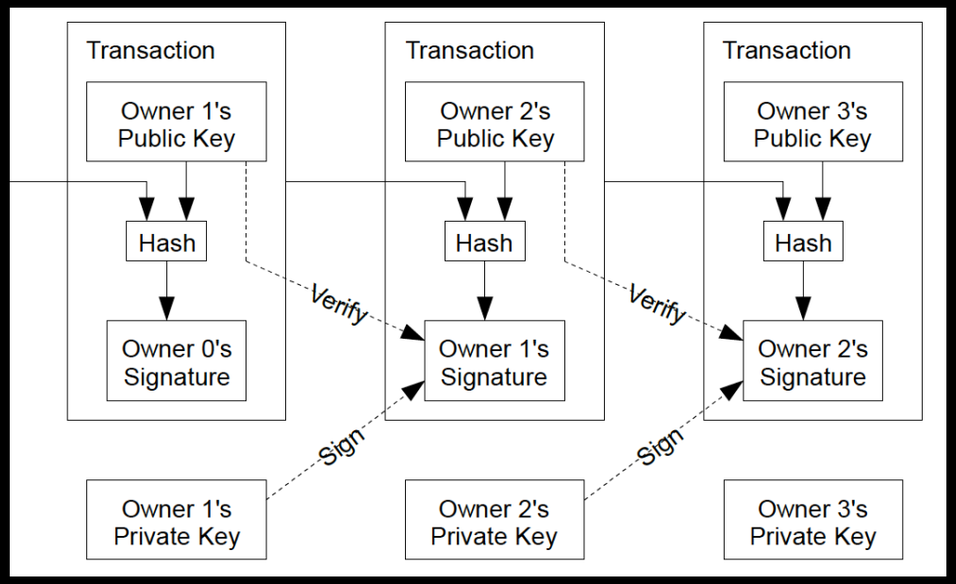
2. a decentralized P2P network (the internet)
3. a **protocol** (rules of the game) based on time-stamped **hashes** to authenticate transactions

   hash = function that takes variable-length input and produces a fixed-length hexadecimal output

   3 desiderata:

   1. small changes in input should lead to totally different output
   2. knowledge of output does not lead you to input
   3. no collisions

   Bitcoin uses SHA-256:



What makes Bitcoin so interesting is how it combines three technologies to create a blockchain:

1. private key cryptography

   digital signature = private key + public key

2. a decentralized P2P network (the internet)
3. a **protocol** (rules of the game) based on time-stamped **hashes** to authenticate transactions

   hash = function that takes variable-length input and produces a fixed-length hexadecimal output

   3 desiderata:

   1. small changes in input should lead to totally different output
   2. knowledge of output does not lead you to input
   3. no collisions

Bitcoin uses SHA-256:

```
> library(digest)
> hash1 <- digest("This lecture is awesome", algo = "sha256")
> hash2 <- digest("This lecture is boring", algo = "sha256")
> hash3 <- digest("What is this lecture even about and why am I here", algo = "sha256")
> print(hash1)
[1] "2f34fee999b59b3576b4f770ae8b6e7ad7327f78e4154830bbe71034acbe1961"
> print(hash2)
[1] "42007a45779ab7f48fc1a4294c0ad7fc40c31d7e5fca5426cf38adea77a2a14a"
> print(hash3)
[1] "6f3b84ef48729e72ffde574339e298934ef9a8859805ea3535ed5d99187a07af"
> nchar(hash1); nchar(hash2); nchar(hash3)
[1] 64
[1] 64
[1] 64
```

Kocherlakota (1998) “money is memory”

a bitcoin is valuable b/c it stores the memory of pervious transactions

Kocherlakota (1998) “money is memory”

a bitcoin is valuable b/c it stores the memory of pervious transactions

Let’s look at how blockchains work

We will use the Bitcoin version as an example

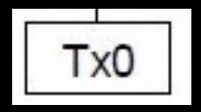
(Remember: Bitcoin is just the token used to participate in the blockchain)

The blockchain should have three key features:

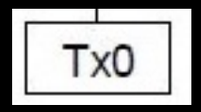
1. a way for the network of users to authorize transactions
2. an incentive for users to
3. a way to deter fraud

You decided to sell me your used car

We make a transaction – let's call it "Tx0"



You decided to sell me your used car

We make a transaction – let's call it "Tx0" 

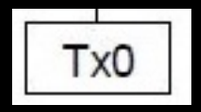
That transaction is broadcast to the "network" (all the computers in the world running the Bitcoin software) **(a "node" in this network is a computer)**

Our transaction needs to be verified

Who will verify it? The network.

How? **Mining.**

You decided to sell me your used car

We make a transaction – let's call it "Tx0" 

That transaction is broadcast to the "network" (all the computers in the world running the Bitcoin software) **(a "node" in this network is a computer)**

Our transaction needs to be verified

Who will verify it? The network.

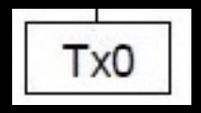
How? **Mining.**

Some nodes are "miners"

They collect a bunch of transactions (including ours) into a block

Then they race to find the **block header**

You decided to sell me your used car

We make a transaction – let's call it "Tx0" 

That transaction is broadcast to the "network" (all the computers in the world running the Bitcoin software) **(a "node" in this network is a computer)**

Our transaction needs to be verified

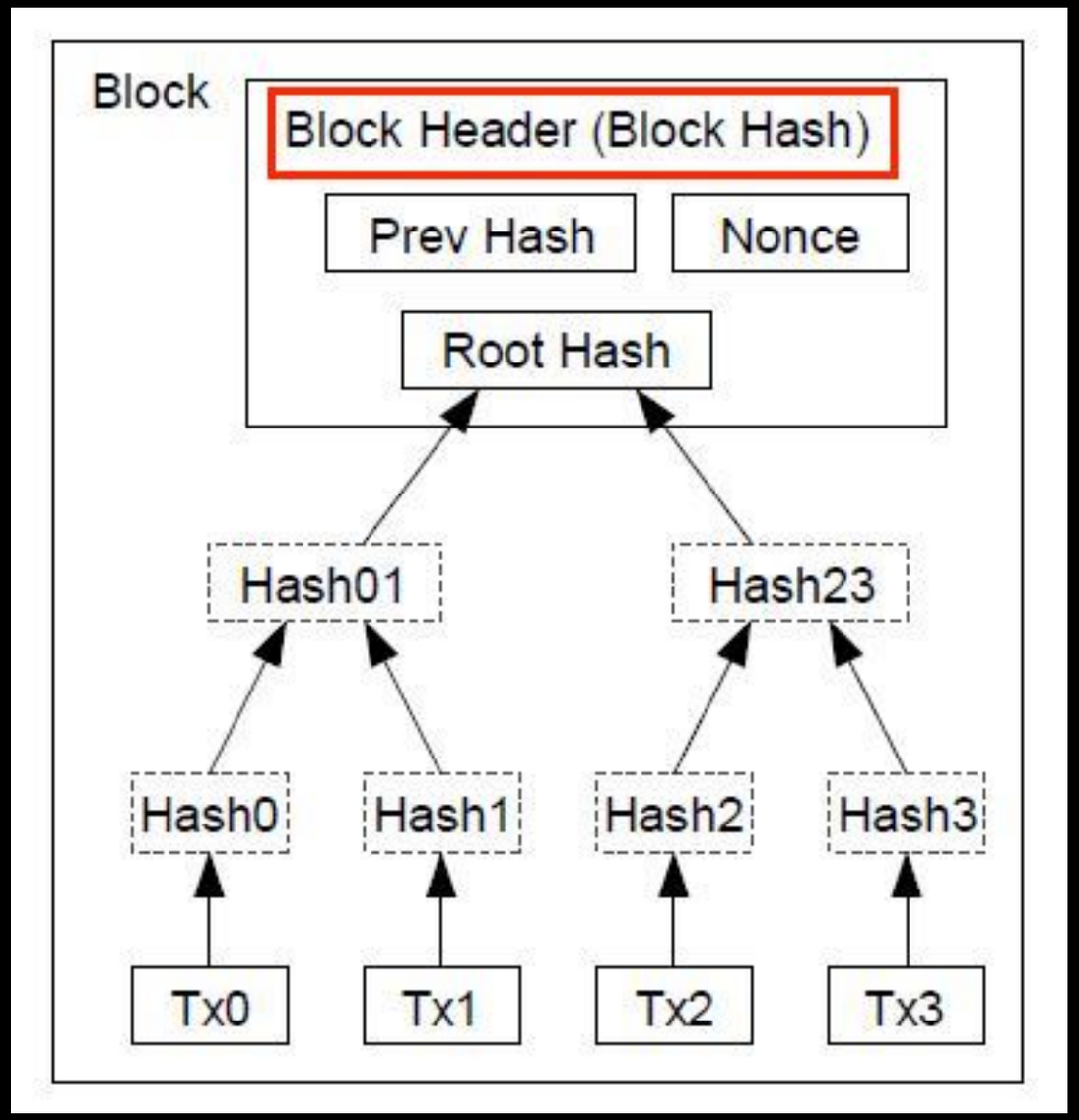
Who will verify it? The network.

How? **Mining.**

Some nodes are "miners"

They collect a bunch of transactions (including ours) into a block

Then they race to find the **block header**



How do you find the block header?

How do you find the block header?

$$h(\cdot) : S \to S$$

$$m \in M$$

$$h(m^*) = h^*$$

How do you find the block header?

By solving this puzzle:
*Find a **number** that when combined with data in the block and passed* through a hash function produces a hexadecimal output (a "hash") within a certain **range**

$$h(\cdot) : S \to S$$

$$m \in M$$

$$h(m^*) = h^*$$

This **number** is called a "**nonce**" (number used once)
What is the "**range**"? A number of leading zeros in the hash.

How do you find the block header?

By solving this puzzle:
*Find a **number** that when combined with data in the block and passed* through a hash function produces a hexadecimal output (a "hash") within a certain **range**

$$h(\cdot) : S \to S$$

$$m \in M$$

$$h(m^*) = h^*$$

This **number** is called a "**nonce**" (number used once)
What is the "**range**"? A number of leading zeros in the hash.

Suppose the range is a hexadecimal with at least 3 zeros.
What you do is re-hash the block over and over again, changing the nonce each time:

How do you find the block header?

By solving this puzzle:
*Find a **number** that when combined with data in the block and passed* through a hash function produces a hexadecimal output (a "hash") within a certain **range**

$$h(\cdot) : S \to S$$

$$m \in M$$

$$h(m^*) = h^*$$

This **number** is called a "**nonce**" (number used once)
What is the "**range**"? A number of leading zeros in the hash.

Suppose the range is a hexadecimal with at least 3 zeros.
What you do is re-hash the block over and over again, changing the nonce each time:

```
2   block+0 => "1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64"
3   block+1 => "e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8"
4   block+2 => "ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7"
5   ...
6   block+998 => "6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965"
7   block+999 => "c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6"
8   block+1000 => "0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9"
```

How do you find the block header?

By solving this puzzle:
*Find a **number** that when combined with data in the block and passed* through a hash function produces a hexadecimal output (a "hash") within a certain **range**

$$h(\cdot) : S \to S$$

$$m \in M$$

$$h(m^*) = h^*$$

This **number** is called a "**nonce**" (number used once)
What is the "**range**"? A number of leading zeros in the hash.

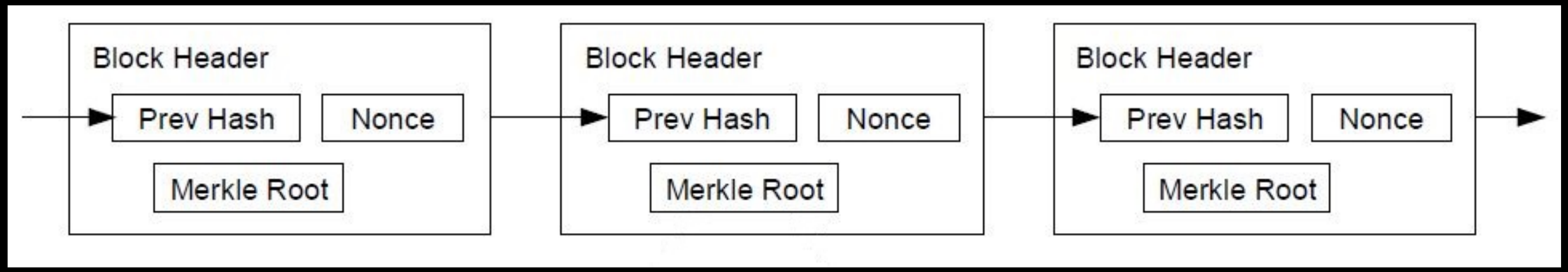
Suppose the range is a hexadecimal with at least 3 zeros.
What you do is re-hash the block over and over again, changing the nonce each time:

```
2   block+0 => "1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64"
3   block+1 => "e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8"
4   block+2 => "ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7"
5   ...
6   block+998 => "6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965"
7   block+999 => "c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6"
8   block+1000 => "0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9"
```

In this example it took 1000 tries

In general, a winning hash can only be found through trial-and-error

Now what? You broadcast your block to network. Other nodes verify it and then add it to the chain



The whole song-and-dance is a "proof of work"

Why do it? Because if you find a winning hash, you "mine" Bitcoin for yourself

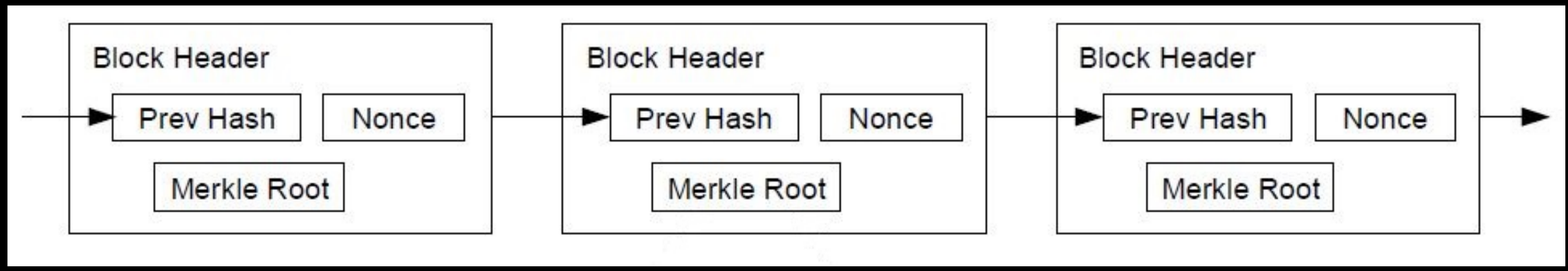
This is the incentive for contributing your computing resources to the verification process
Takes the place of the fee a central authority would charge

So miners compete for the right to add the next block to the chain

What is going is decentralized consensus over the "ledger" (the transaction history)
The network "agrees" on the "true state of the ledger" by "voting"
with their CPUs
Accepting blocks by working on the next one, ignoring blocks by refusing to work on them

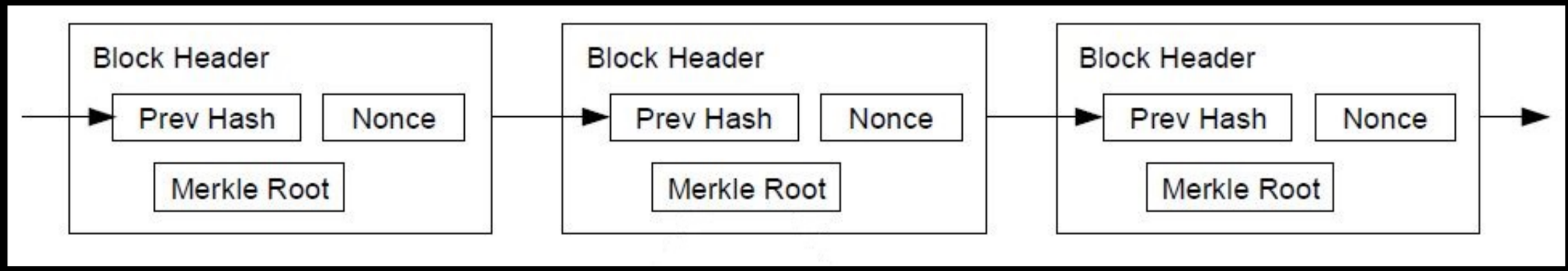
Why does proof of work deter fraud? Why can't somebody cook the books?

Notice how each block contains info from the previous block, specifically the hash:



Why does proof of work deter fraud? Why can't somebody cook the books?

Notice how each block contains info from the previous block, specifically the hash:



Since each block "remembers" the previous block, if you change the previous block (e.g. alter or delete a transaction), then by definition you change the current block .

The chain is immutable.

You can't just adjust a single block - you have to adjust the entire chain!

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24

Suppose the network is working on block 24

an attacker wants to change a transaction in block 17

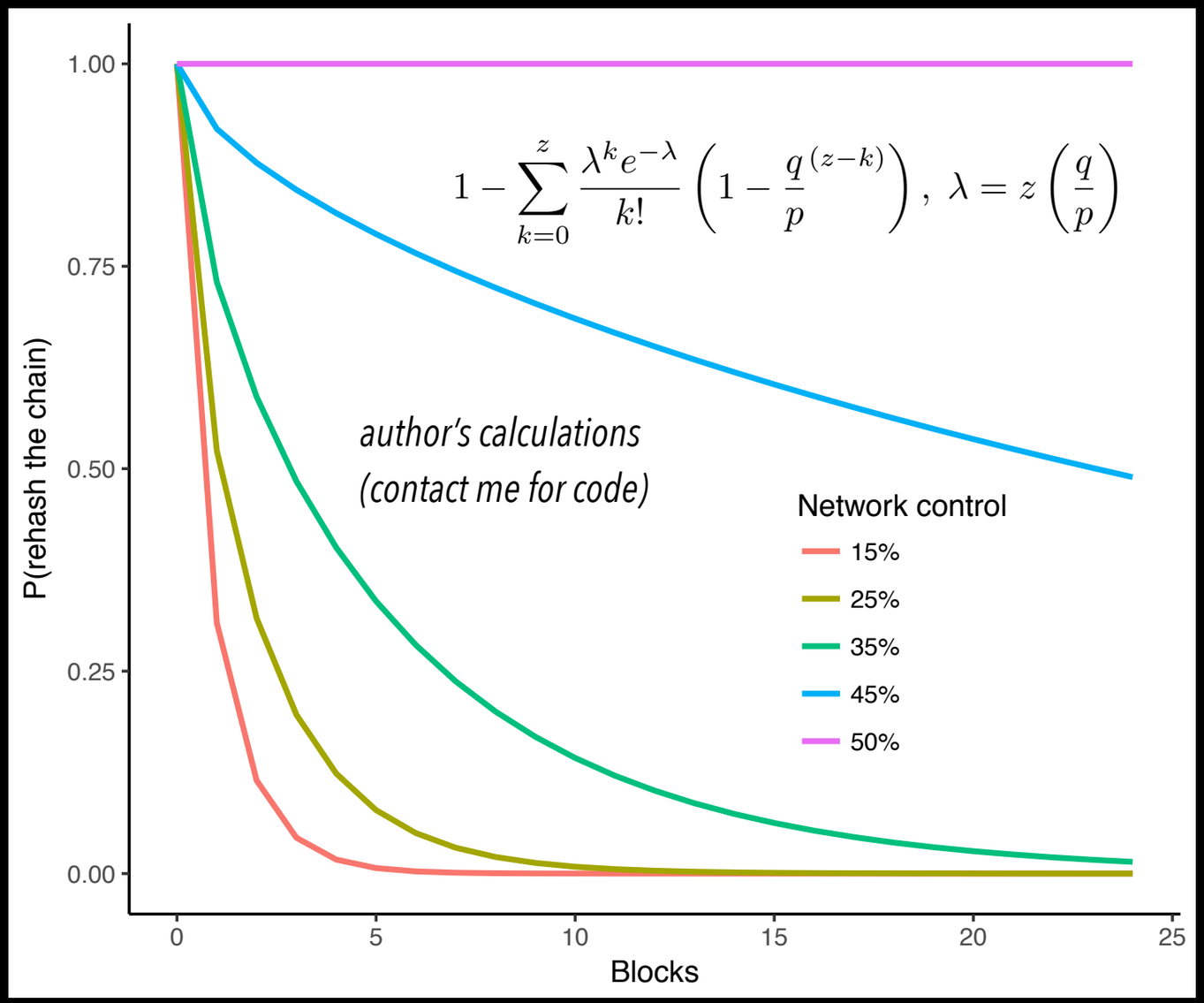
the attacker would have to then change blocks 18 to 23,
before the network completes block 24!

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24

Suppose the network is working on block 24

an attacker wants to change a transaction in block 17

the attacker would have to then change blocks 18 to 23,
before the network completes block 24!



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24

The only way an attacker could alter the chain is if it had at least half the network's total computing power

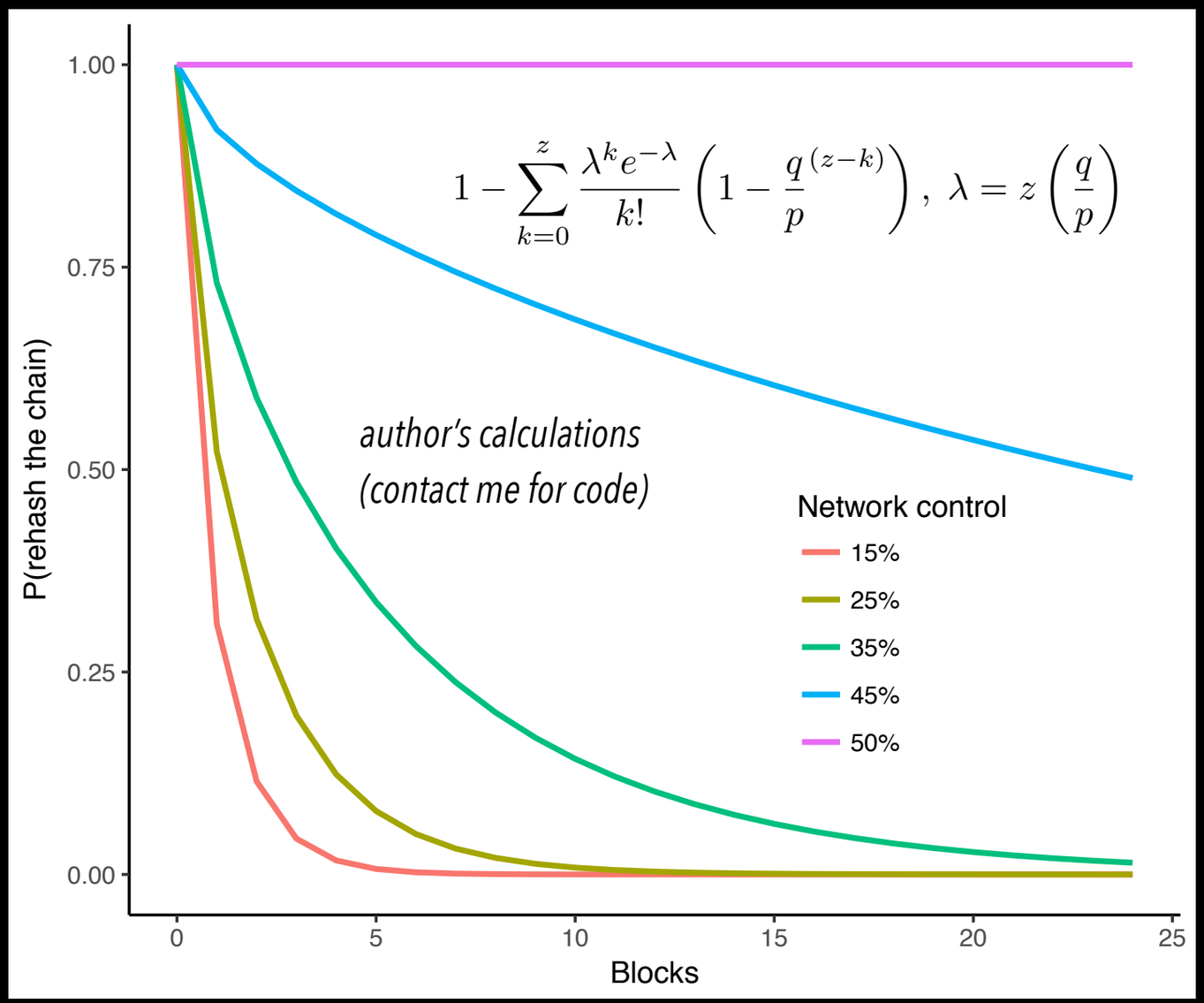
But even if it did, then it would be better off using that computing power for mining

The work is expensive
Proving the work done is cheap

Suppose the network is working on block 24

an attacker wants to change a transaction in block 17

the attacker would have to then change blocks 18 to 23, *before the network completes block 24!*

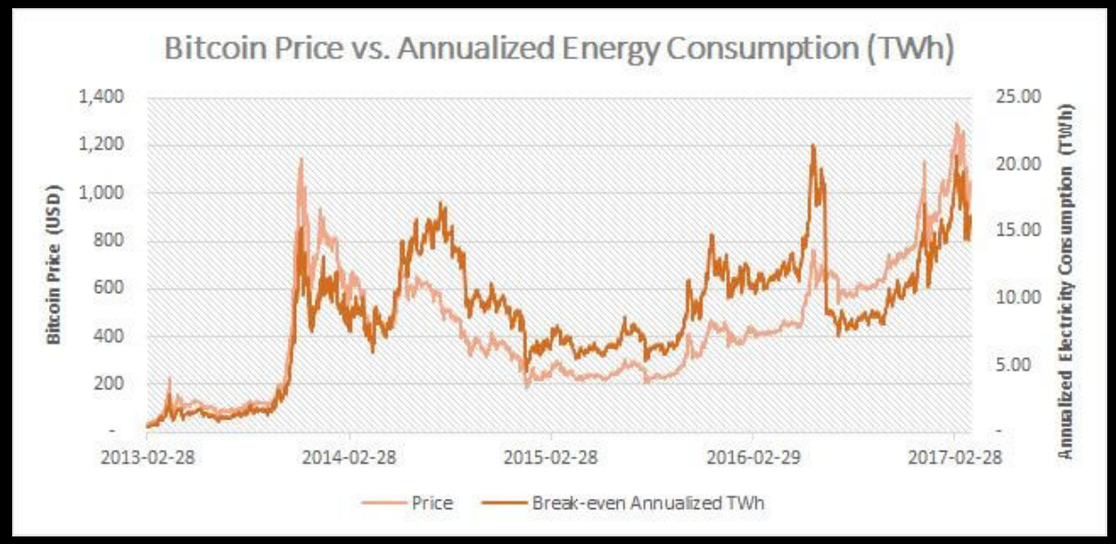


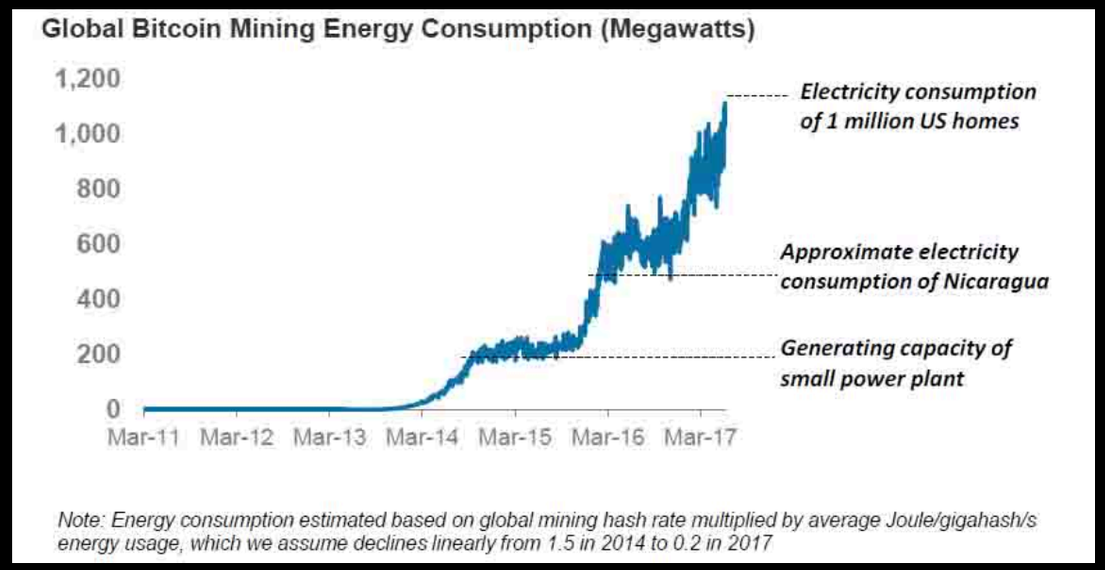
A blockchain is only as secure as its computing power
Network effects play a large role

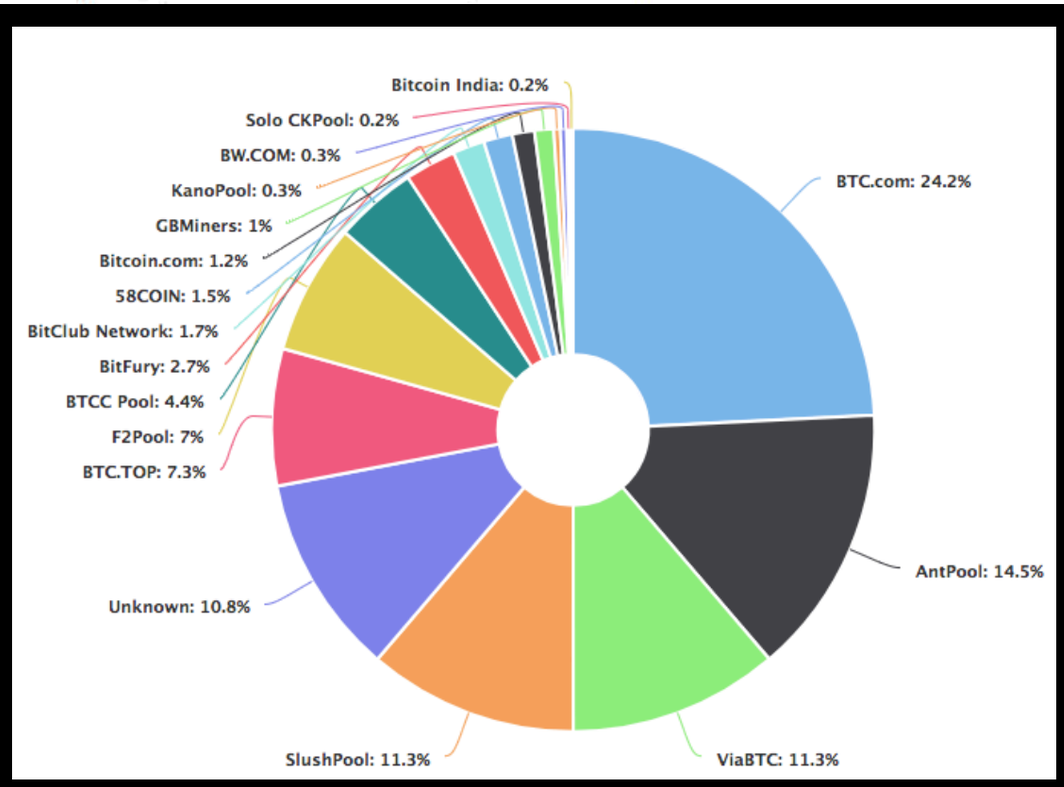
Unfortunately proof of work is very wasteful
Jan '18: mining consumes 40.64 TWh
More than Hungary

And economies of scale in mining mean that as the blockchain becomes more valuable, it also becomes *less decentralized*
Concerns about **market power**

The Bitcoin blockchain is also very slow
VISA: ~57k transactions per second
BTC: ~ 7 transactions per second







Key point: since there are tradeoffs to blockchain design, *no single blockchain will suit every transaction type*

What are these tradeoffs?

1. Security
2. Privacy
3. Transaction size (e.g. Litecoin vs Bitcoin)
4. Nature of the transaction (e.g. exchange of value, executing a legal contract, etc)
5. **Permissionless vs. permissioned**

e.g. Australian Securities Exchange

despite issues, bitcoin shows how blockchain can reduce:

1. cost of **verification**
2. cost of **networking**

also shows that we probably won't eliminate intermediaries – just change their nature

as we saw, farming was not adopted because it was immediately better, but because it increased the scope of feasible economic activity

Earlier we said "look for where contracts are incomplete"

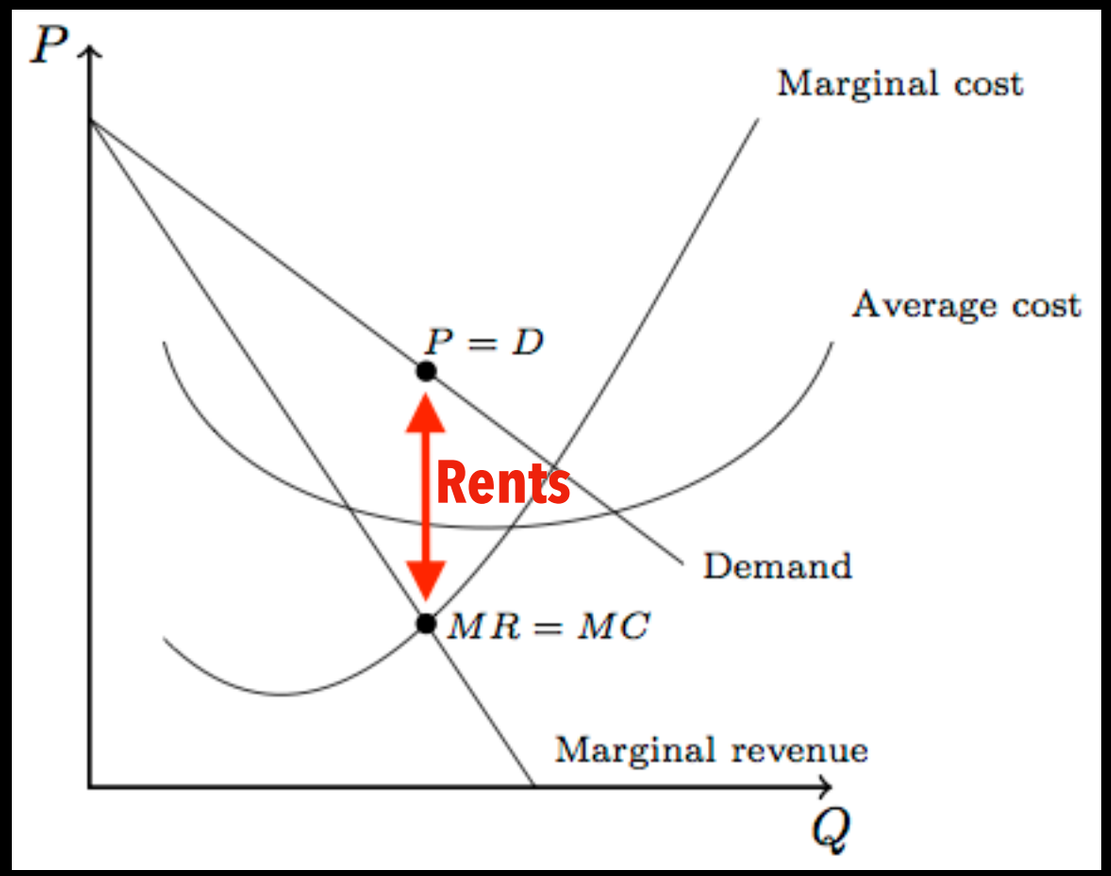
Now we can be more specific

Look for where:

verification costs are high

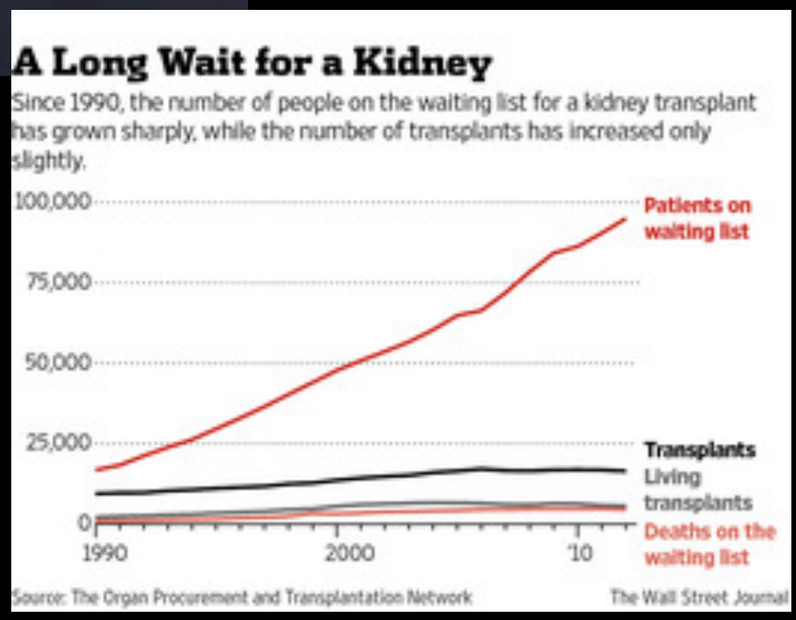
platform operators enjoy uncompetitive rents

privacy / censorship risk is high



Blockchains can efficiently deliver digital goods/services that were previously tough to contract on

Blockchains can efficiently deliver digital goods/services that were previously tough to contract on



Blockchain revived the old(ish) notion of **smart contracts**

> *"**Smart contracts** are digital contracts allowing terms contingent on decentralized consensus that are self-enforcing and tamper-proof through automated execution."*
> **(Cong & He 2018)**

> *"A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine."*
> **(Szabo 1996)**

Many contracts are incomplete b/c they rely on **contingencies** (stuff that may or may not happen in the future)
Delivery, performance, weather…

As a result they can be costly to enforce

The idea of a smart contract is to roll the contract and its execution (and thus its enforcement) all in one

Blockchains can also deliver **attributes** of *non-digital* goods/services (e.g **property rights**)

Blockchains can also deliver **attributes** of *non-digital* goods/services (e.g **property rights**)

Spotify®

mediachain

Music/Arts

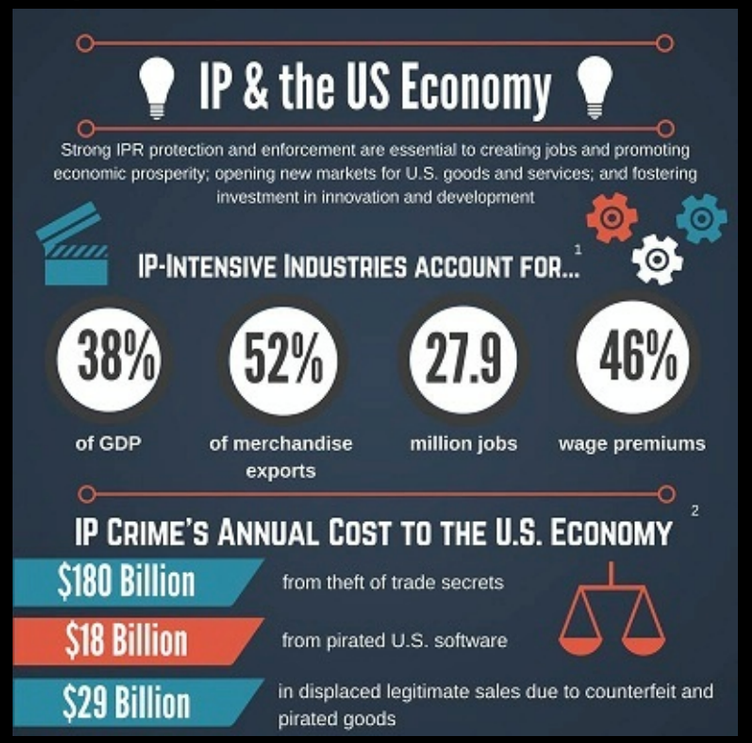
Blockchains can also deliver **attributes** of *non-digital* goods/services (e.g **property rights**)

Spotify®

mediachain

Music/Arts

Could intellectual property be replaced with blockchain?



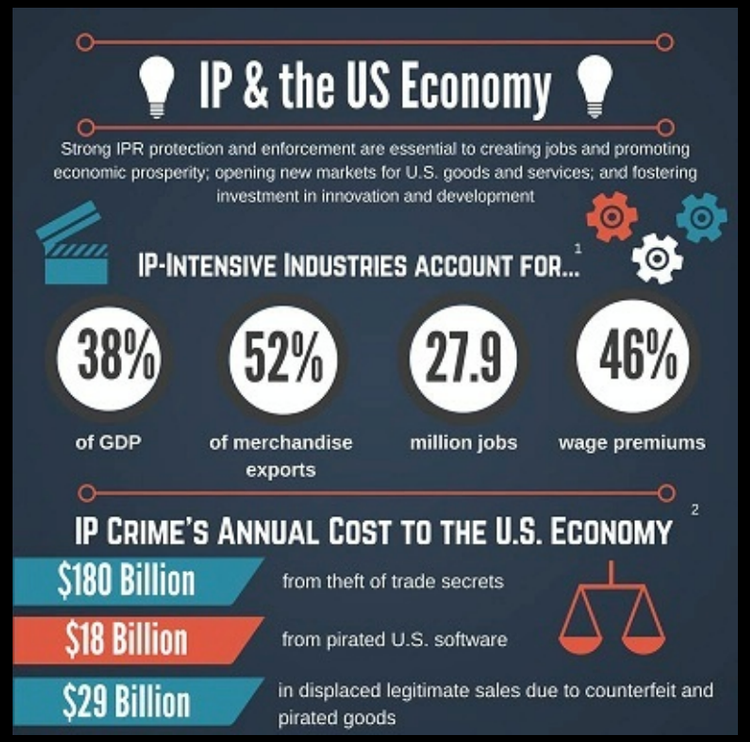
Blockchains can also deliver **attributes** of *non-digital* goods/services (e.g **property rights**)

Spotify®

mediachain

Music/Arts

Could intellectual property be replaced with blockchain?



Identification / electronic medical records?

Would people license their privacy?

Tracking food production

Walmart + IBM

Reputation

Self-driving cars buying/selling lane space?

Blockchain is good for **auditing** / **tracking** / **time stamping / consensus**

Many applications to **finance** and **management:**

Transparently reward contributions to financial prediction models. (Numerai)

Corporate governance
Reduce incentive for strategic default

Fewer lawyers / instant settlements

Exercising options in derivatives
$65b-$85b: cost of clearing, settling, and managing the post-trade processes in securities

Instant transfer of collateral in event of default / Instant compensation if performance goals are met

Trade finance (especially cross-border trade)

Blockchain is good for **auditing** / **tracking** / **time stamping / consensus**

Many applications to **finance** and **management:**

Transparently reward contributions to financial prediction models. (Numerai)

Corporate governance
Reduce incentive for strategic default

Fewer lawyers / instant settlements

Exercising options in derivatives
$65b-$85b: cost of clearing, settling, and managing the post-trade processes in securities

Instant transfer of collateral in event of default / Instant compensation if performance goals are met

Trade finance (especially cross-border trade)

Largest gain may be in ***signaling*** benefits
Firm willing to write smart contracts is credible signal of quality

The big question is whether digital currency will *replace* central authority

Bitcoin created to compete with central banks
algorithmic vs discretionary monetary policy

If central bank loses monopoly power, then supply and demand will drive which money is used as a medium of exchange.

Is more competition in currency better?

Yes: more flexibility for contracting parties to choose settlement terms

No:

- could lead to credit constraints
- harder to conduct any kind of monetary policy
- licensing laws make it easier to regular threat from competition currencies, thus easier to combat tax evasion and money laundering

Option 1: central bank issues digital currency ("FedCoin")

Allow citizens to deposit directly to central bank

When you spend a FedCoin, you transfer it over a blockchain.

CB would have exclusive right to modify or add or delete transactions.

Blockchain would not be transparent. (Is this a blockchain at all?)

Exploits low cost of verification, but not networking

Since you deal directly with CB, it would end fractional reserve banking

Commit to algorithmic money creation

Smart contracts that alter algorithm based on future contingencies

CB has better understanding of financial system, thus improve interventions

Reduce interest rates below zero

Option 1: central bank issues digital currency ("FedCoin")

Allow citizens to deposit directly to central bank

When you spend a FedCoin, you transfer it over a blockchain.

CB would have exclusive right to modify or add or delete transactions.

Blockchain would not be transparent. (Is this a blockchain at all?)

Exploits low cost of verification, but not networking

Since you deal directly with CB, it would end fractional reserve banking

Commit to algorithmic money creation

Smart contracts that alter algorithm based on future contingencies

CB has better understanding of financial system, thus improve interventions

Reduce interest rates below zero

But: You still have a single point of failure

Option 1: central bank issues digital currency ("FedCoin")

Allow citizens to deposit directly to central bank

When you spend a FedCoin, you transfer it over a blockchain.

CB would have exclusive right to modify or add or delete transactions.

Blockchain would not be transparent. (Is this a blockchain at all?)

Exploits low cost of verification, but not networking

Since you deal directly with CB, it would end fractional reserve banking

Commit to algorithmic money creation

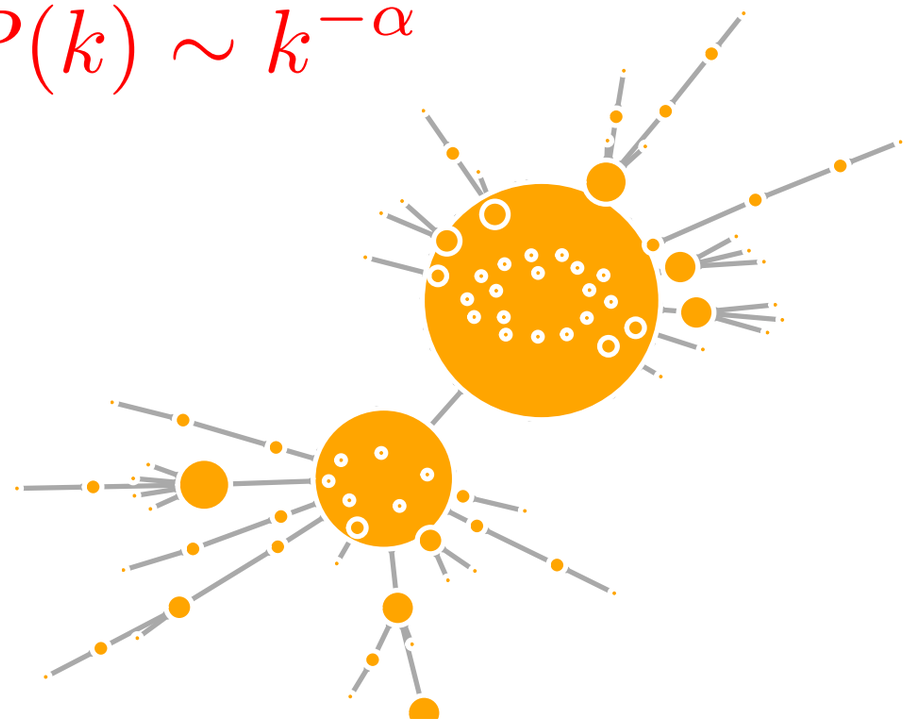
Smart contracts that alter algorithm based on future contingencies

CB has better understanding of financial system, thus improve interventions

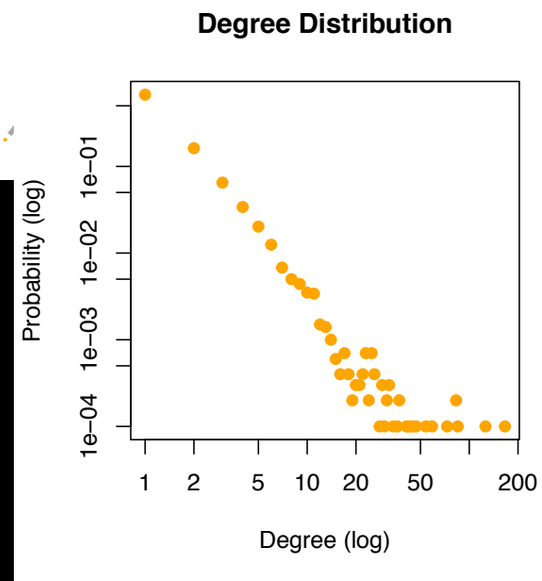
Reduce interest rates below zero

But: You still have a single point of failure

$$P(k) \sim k^{-\alpha}$$



(contact me for code)



Option 2: Blockchain only

Allow CB to move money more reliably and cheaply between depositors
Estimating savings in processing and bookkeeping costs are 50–80%.
Average cost of a money transfer was 7.37% worldwide (2015) and take several days and many layers of verification

Allow CB to more directly monitor depositor banks, easier to identify money laundering and tax evasion and general fraud
(Hopefully) Inspire confidence in banking system

We saw that two revolutionary advancements, **property rights** and **farming** co-evolved

Does blochain + digital currency present a new and important co-evolution?

It depends on our ability to identify the size of the marginal gains
Not every market needs blockchain

We saw that two revolutionary advancements, **property rights** and **farming** co-evolved

Does blochain + digital currency present a new and important co-evolution?

It depends on our ability to identify the size of the marginal gains
Not every market needs blockchain

What tradeoffs is a society willing to make?
Imagine if elections were conducted on blockchain
Imagine if professors administered classes on blockchain

"Blockchain and smart contracts can sustain market equilibria with a larger range of economic outcomes." (Cong & He 2018)

WIT Computational Finance Club
Wednesdays 7-8pm

```python
import matplotlib
import pandas as pd
from binance.enums import *
from binance.client import Client
import json
import matplotlib.pyplot as plt
keys = json.load(open('keys.json'))
client = Client(keys['public'], keys['private'])
prices = client.get_all_tickers()
client.get_recent_trades(symbol = "POWRETH")
depth = client.get_order_book(symbol = S)
df = pd.DataFrame(depth)
df['asks_min'] = df['asks'].str[0]
df['asks_max'] = df['asks'].str[1]
df['bids_min'] = df['bids'].str[0]
df['bids_max'] = df['bids'].str[1]
df = df.drop(df.columns[[0,1]], axis=1)
df.loc[:,'asks_min':'bids_max'] = df.loc[:,'asks_min':'bids_max'].apply(pd.to_numeric)
```

Email: degeestl@wit.edu

Web: lrdegeest.github.io

References

Bowles, Samuel. "Cultivation of cereals by the first farmers was not more productive than foraging." Proceedings of the National Academy of Sciences 108, no. 12 (2011): 4760-4765.

Bowles, Samuel, and Jung-Kyoo Choi. "Coevolution of farming and private property during the early Holocene." Proceedings of the National Academy of Sciences 110, no. 22 (2013): 8830-8835.

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

Cong, Lin William, and Zhiguo He. Blockchain Disruption and Smart Contracts. No. w24399. National Bureau of Economic Research, 2018.

Yermack, David. "Corporate governance and blockchains." Review of Finance 21, no. 1 (2017): 7-31.

Raskin, Max, and David Yermack. Digital currencies, decentralized ledgers, and the future of central banking. No. w22238. National Bureau of Economic Research, 2016.

Catalini, Christian, and Joshua S. Gans. Some simple economics of the blockchain. No. w22952. National Bureau of Economic Research, 2016.

Ma, June, Joshua S. Gans, and Rabee Tourky. Market structure in bitcoin mining. No. w24242. National Bureau of Economic Research, 2018.

Albert, Réka, Hawoong Jeong, and Albert-László Barabási. "Error and attack tolerance of complex networks." nature 406, no. 6794 (2000): 378.