Bitcoin: Strengths and Vulnerabilities

Jose Victor Lineros, PhD
CIA, CPA, CISA, CFE, CRISC, MCTS
Department of Accounting
University of North Texas
2019

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Learning Objectives:

Review the history of blockchain

Gain an understanding of common blockchain terminology and technology

Understand the differences between permissioned and permission-less distributed networks

Review some of the current, and potential future applications

Understand some blockchain weaknesses and vulnerabilities…

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

A few early opinions:

"…Blockchain offers a sweeping vista of opportunity to reimagine how the financial system can and should work in the Internet era…"
(Marc Andreesen, 2014)

"Blockchain technology will revolution far more than money: it will change your life."
(Dominic Frisby, 2016)

"Blockchain technology is the most significant invention since the Internet and electricity"
(Mark Metry, 2017)

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

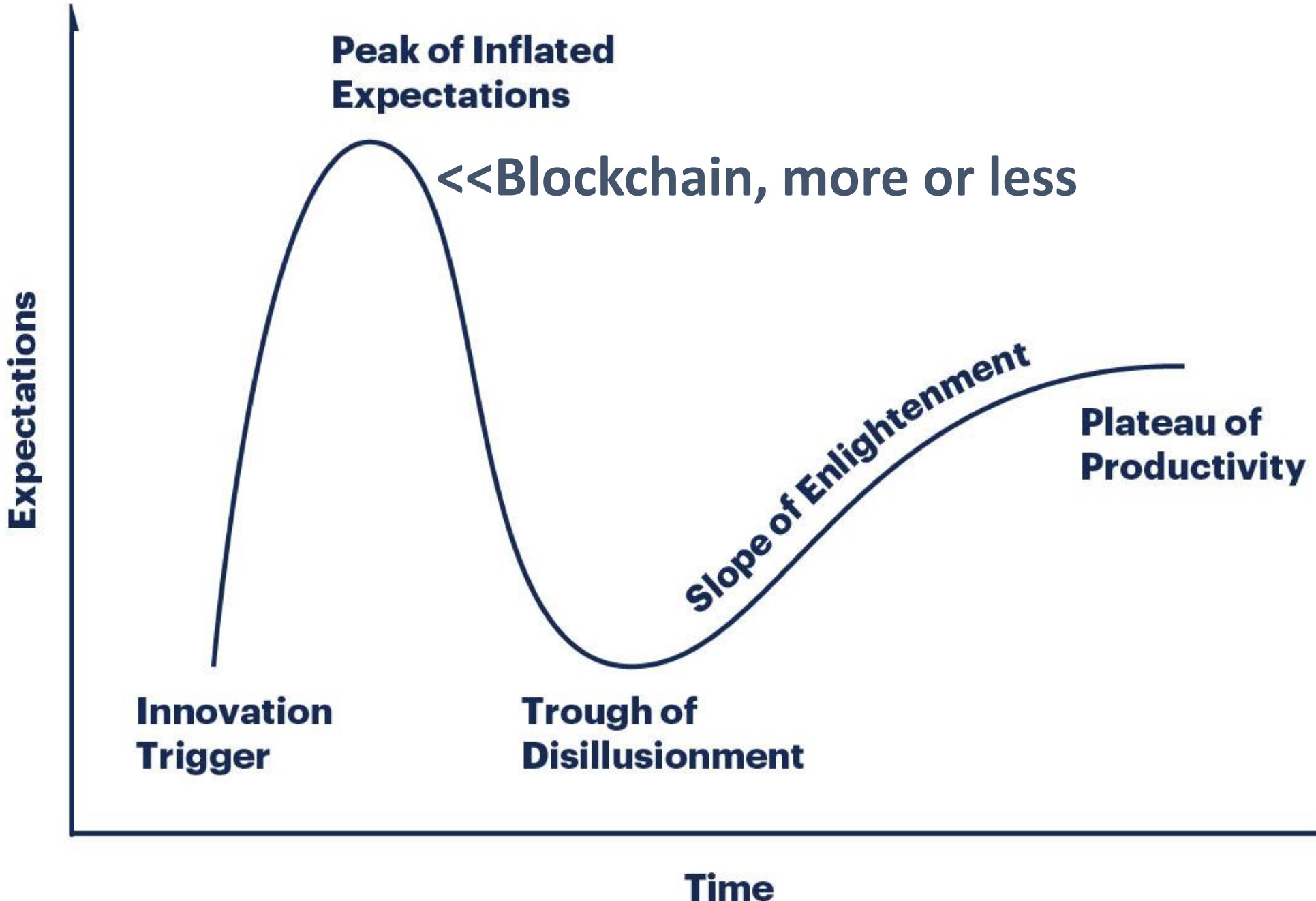
A few early opinions:

“There are no good uses for Blockchain” (Kai Stinchcombe, 2018)

“One of the most overhyped technologies ever” (NourielRobini, 2018)

“Maybe I’m just too old, but I’m going to let this <Blockchain> mania go on without me.”
Jeffrey Gundlach, DoubleLine Capital CEO and Chief Investment Officer

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890



DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

First, a brief history of "accounting for stuff"

- Born in 1447 in Italy
- He was a friar and a mathematician
- Most importantly, he wrote "*Summa de arithmetica, geometria. Proportioni et proportionalita*."

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Double-Entry Bookkeeping:

Cash $1,000
  Revenue $1,000
Seller's books

Inventory $1,000
  Cash $1,000
Buyer's books

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Notice a few things:

Everyone keeps their own books (version of the truth)

Redundancy is present

Mistakes on someone else's book are not readily apparent

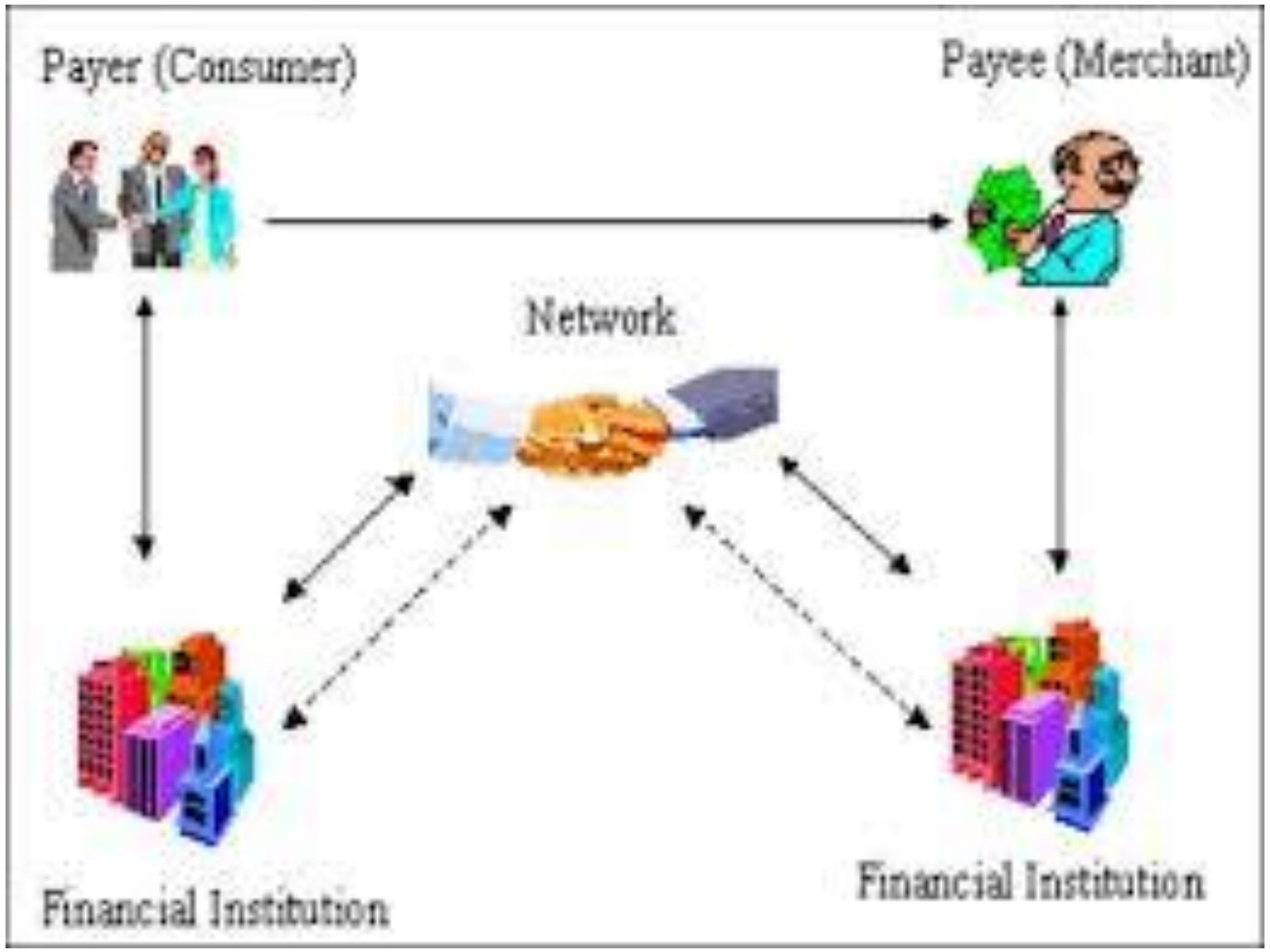
Someone could alter these records in relative isolation (low visibility)

How many parties are present here if you paid with ck?

Cash $1,000
Revenue $1,000
Seller's books

Inventory $1,000
Cash $1,000
Buyer's books

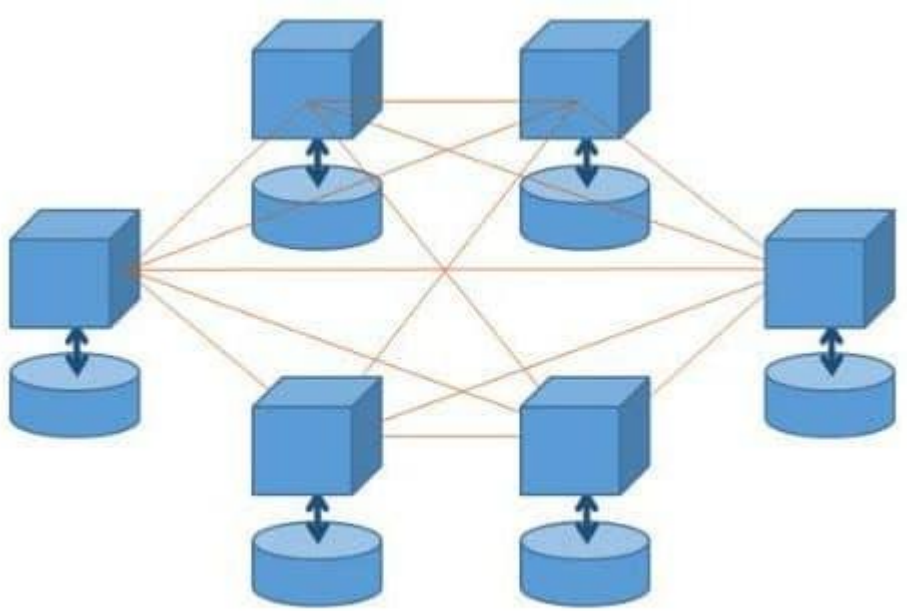
DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890



DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Blockchain eliminates intermediaries by each party selectively “sharing” the truth (books)

Everyone has a copy of the database (the truth)



Distributed blockchain

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Blockchain Benefits:

Greater transparency

Enhanced security

Provenance (end-to-end traceability)

Increased efficiency and speed

Reduced costs

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

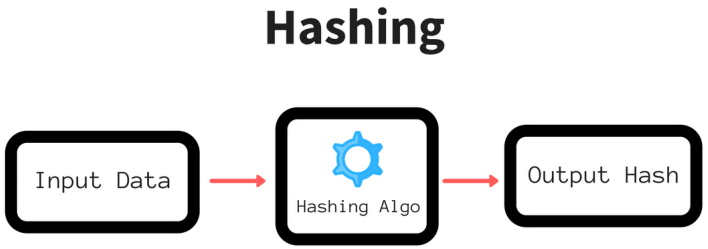
Downsides?

More on that at the end…

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

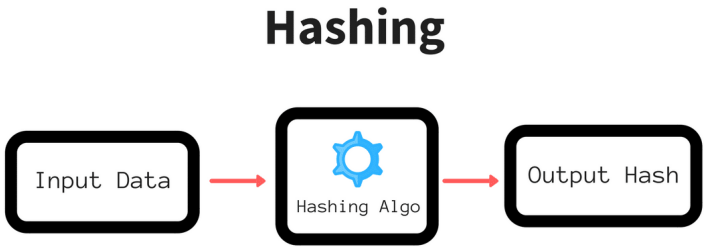
Background

- Blockchain architecture was born in the amniotic fluid of three other technologies:



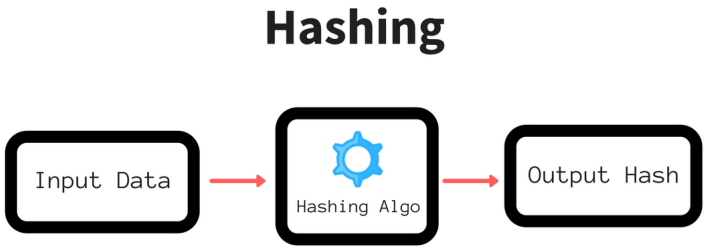
Background

- Blockchain architecture was born in the amniotic fluid of three other technologies:



Background

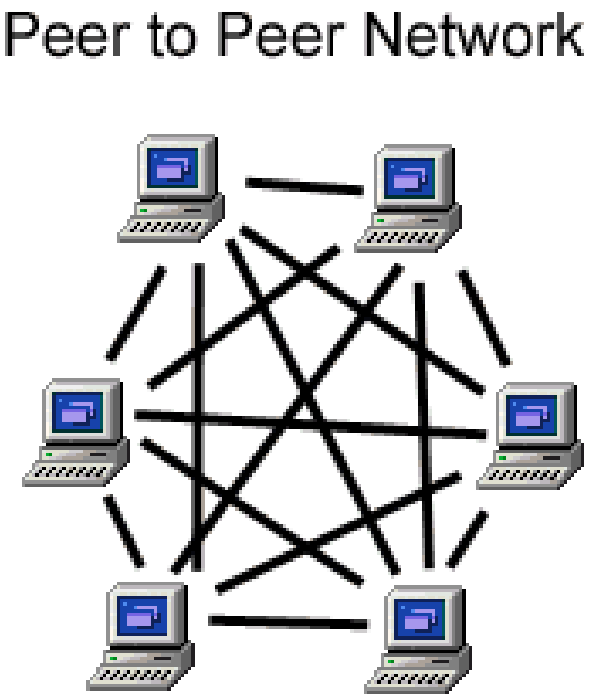
- Blockchain architecture was born in the amniotic fluid of three other technologies:



Let’s take these one-by-one

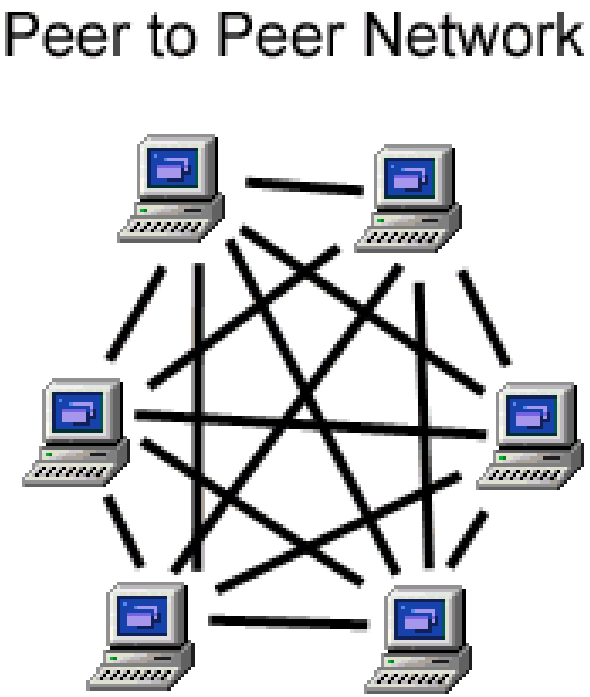
Peer-to-Peer Networking

- Involves the direct connection between computers without an intervening central authority. Became popular with Napster around 1999 and grew from there to current platforms such as BitTorrent, Kazaa, Gnutella, Freenet, etc.



Peer-to-Peer Networking

- In its purest form, it has no central authority and all nodes (or network contacts) are equal….



P-T-P networks are a distributed application architecture that partitions tasks or workloads between peers.

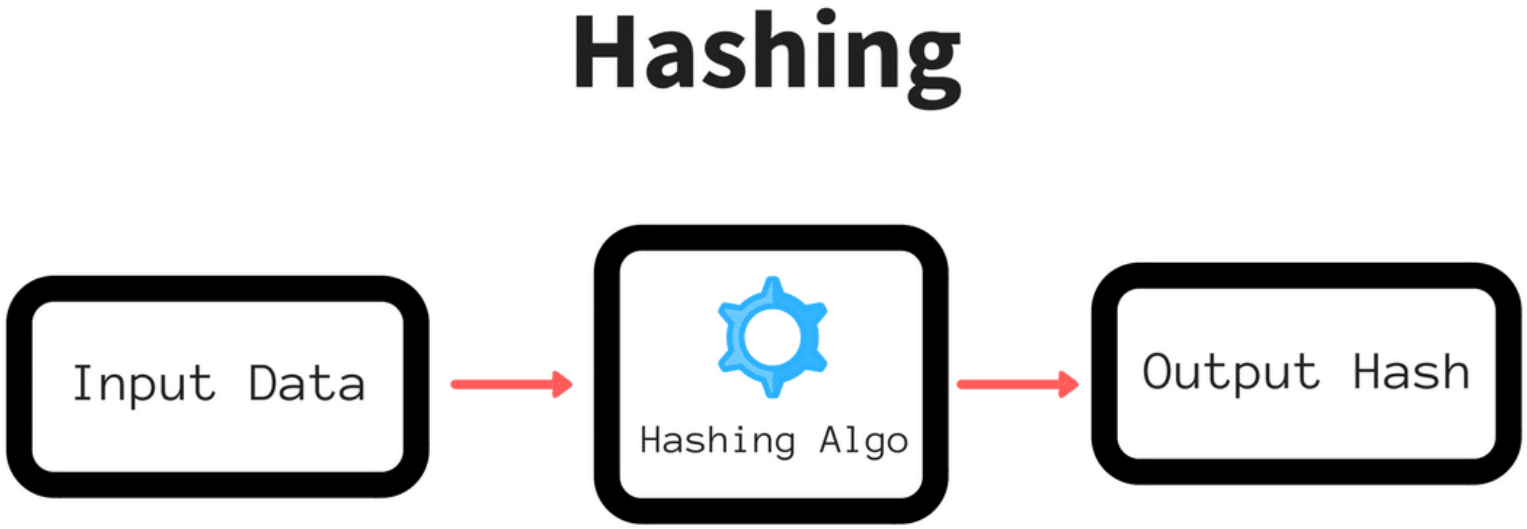
Peers are equally privileged, equipotent participants in the application.

No center, equal sharing of “the truth.”

More on this later….

Hashing

- The basis for digital signatures that are used to provide authenticity and non-repudiation services



Hashing

- Let's look at a quick example

Example of Hashing

	beginning hash	transaction id	sending payor id	receiving payee id	amount	ending hash	
block 1	0	000001	03000	04000	$45,000	52001	<<<<1 plus 3K plus 4000 plus 45K
block 2	52001	000002	04000	05000	$30,000	91003	<<<<52001+2 plus 4K plus 5K plus 30K
block 3	91003	000003	01000	03000	$10,000	105006	<<<<91003+3 plus 1K plus 3K plus 10K

Example of Hashing

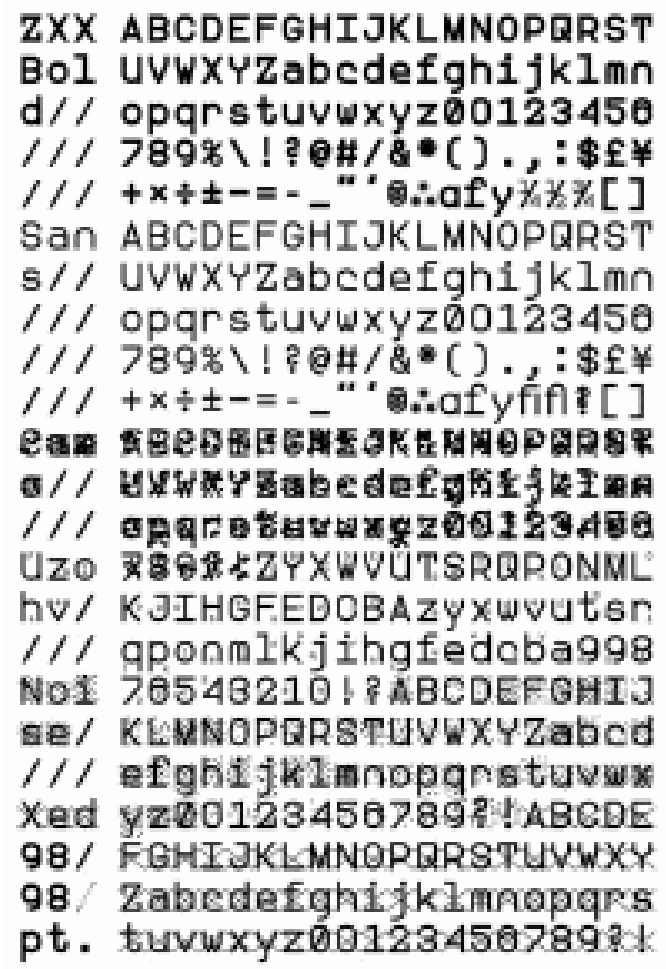
	beginning hash	transaction id	sending payor id	receiving payee id	amount	ending hash				
block 1	0	000001	03000	04000	$45,000	52001	<<<<1 plus 3K plus 4000 plus 45K			
block 2	52001	000002	04000	05000	$30,000	91003	<<<<52001+2 plus 4K plus 5K plus 30K			
block 3	91003	000003	01000	03000	$10,000	105006	<<<<91003+3 plus 1K plus 3K plus 10K			

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Example of Hashing

	beginning hash	transaction id	sending payor id	receiving payee id	amount	ending hash				
block 1	0	000001	03000	04000	$45,000	52001	<<<<1 plus 3K plus 4000 plus 45K			
block 2	52001	000002	04000	05000	$30,000	91003	<<<<52001+2 plus 4K plus 5K plus 30K			
block 3	91003	000003	01000	03000	$10,000	105006	<<<<91003+3 plus 1K plus 3K plus 10K			

Now let's talk about Encryption



Quick Test

- What does this mean?

D B U

Encryption

- Simply means that we can disguise data, for example the word CAT, through a plus one Caesar Cipher encryption protocol could be disguised as DBU (C+1=D, A+1=B, T+1=U).

Quick Test

- What does this mean?

More on encryption later…

Combining all of these, let's look at a another simple blockchain example

Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) contains:

CAB

Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) contains:

CAB

Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) contains:

CAB

Hash value = 6 (1+2+3)

Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) contains:

CAB

Hash value = 6 (1+2+3)

Word Document 2 (or block 2) contains:

HIGH

Hash value = 32 (8+9+7+8)

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) contains:

CAB

Hash value = 6 (1+2+3)

Word Document 2 (or block 2) contains:

HIGH

Hash value = 32 (8+9+7+8)

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Notice that each word document, or block, is independently hashed….

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

However, what if we "chained" one to the other, what would that look like?

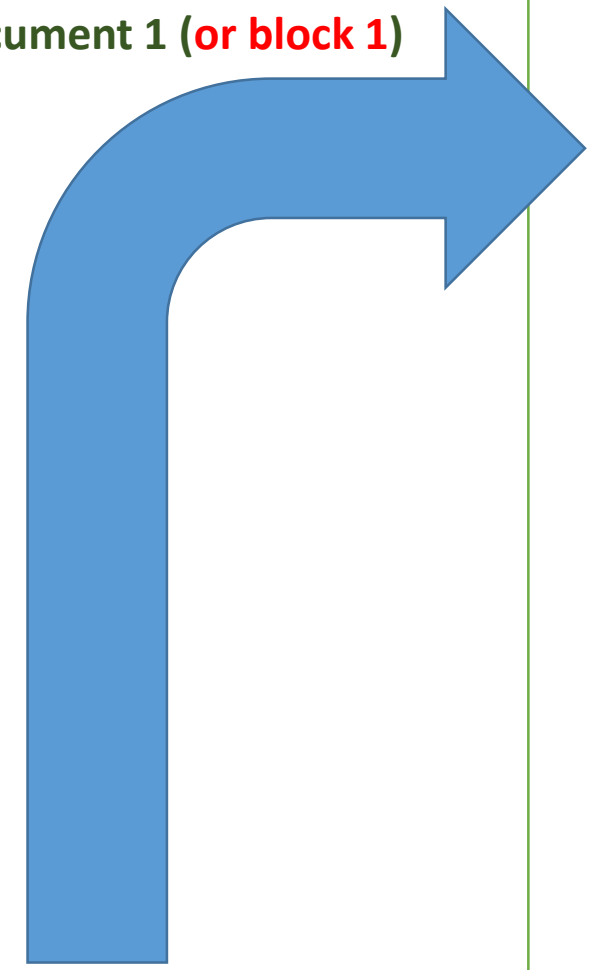
Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) contains:

CAB



Hash value = 6 (3+1+2)

Word Document 2 (or block 2) contains:

6

HIGH

Doc. 2 Doc. 1

Cumu. Hash value = 38 (8+9+7+8)+(6)

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) has:

CAB

Hash value = 6 (3+1+2)

Word Document 2 (or block 2) has:

HIGH

Doc. 2 Doc. 1

Cumu. Hash value = 38 (8+9+7+8)+(6)

<<<Block 1

<<<Block 2

Hashing

Hashing Algorithm

A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 has:

CAB

Hash value = 6 (3+1+2)

<<<Block 1

Word Document 2 has:

HIGH

Doc. 2 Doc. 1

Cumu. Hash value = 38 (8+9+7+8)+(6)

<<<Block 2

At this point, it should be noted that this blockchain example is known as – "Permissioned"

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890

Hashing

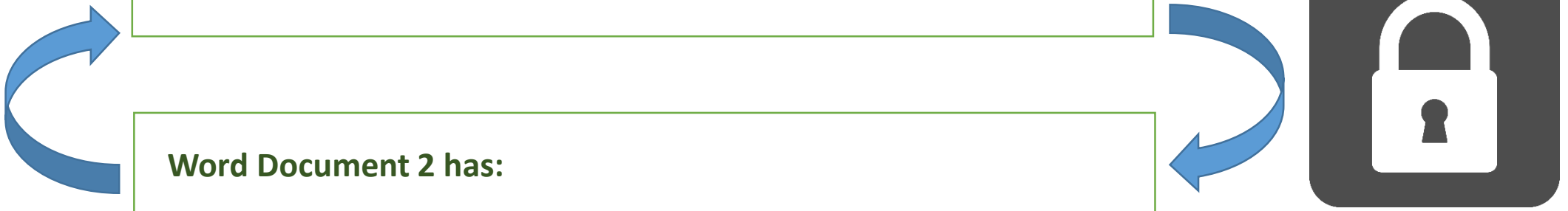
Hashing Algorithm
A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 has:

CAB

Hash value = 6 (3+1+2)

<<<Block 1



Word Document 2 has:

HIGH

Doc. 2 Doc. 1

Cumu. Hash value = 38 (8+9+7+8)+(6)

<<<Block 2

In a Permissionless – or public blockchain – "miners" would complicate the hash using a "nonce" and a "transaction id" in each block to ensure block uniqueness, non-reproducibility, and specific identification. To be covered later---

Now let's complicate the idea of a "hash" – yet…even…more…

Remember this hash?

Hashing

Hashing Algorithm
A = 1
B = 2
C = 3
D = 4
E = 5
F = 6
G = 7
H = 8
I = 9
J = 10
K = 11
L = 12
M = 13
N = 14
O = 15
P = 16
Q = 17
Etc…

Word Document 1 (or block 1) has:

CAB

Hash value = 6 (3+1+2)

<<<Block 1

Word Document 2 (or block 2) has:

HIGH

Doc. 2 Doc. 1

Cumu. Hash value = 38 (8+9+7+8)+(6)

<<<Block 2

In reality, this hash will continue to grow in size numerically (get bigger)

Also, it is somewhat simplistic…

Let's fix this with cryptography – I know – ugh

It's easy I promise….

Let’s introduce the idea of a semi-prime number:

These we know as prime numbers (2, 3, 5, 7, 11)

Less well known are semi-primes:

These are numbers divisible by themselves, 1, and only two other prime numbers…

For example,

These are semi-prime numbers divisible by themselves, 1, and two prime numbers

(15, 21, 22, 25, 26)

For example,

Let’s isolate the semi-prime number 15

It is divisible by 15, by 1, and by only two prime numbers?

5 and 3.

To participate in a Blockchain you need to have a public number, and a private key pair

In the case of semi-prime 15, the public number (or key) will be the number 15 – your identifier in the network

Your private key will be the two prime numbers 5 and 3, this will be your private key pair (or secret keys)

It should be noted that if you encrypt a message block with your public key, only the private keys can decrypt it.

Interestingly, if you encrypt a message block with your private keys, it can be decrypted with the public key (without revealing the private keys, nifty)…

Encryption

Enter your text below:

CAB <<<desired message

5, 3 <<<sender encrypts message with private key pair, this acts like our digital signature because when the receiver decrypts using the corresponding public key, it has to be me, only my private key pair (encryption) corresponds to my public key (decryption).

Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

☐ Treat each line as a separate string

SHA256 Hash of your string:

97A7E1CCB51F89A26A15D27403CF847039B0BAFD4351BFF5093DFE7182BDB726

Encryption

Enter your text below:

CAB <<<desired message

5, 3

<<<so, for example, CAB encrypted with +5 and then +3 might change the message above KIJ

Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

Treat each line as a separate string

SHA256 Hash of your string:

97A7E1CCB51F89A26A15D27403CF847039B0BAFD4351BFF5093DFE7182BDB726

Encryption

Enter your text below:

CAB <<<desired message

5, 3 <<<It does all of this without revealing our private key pair.

Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

Treat each line as a separate string

SHA256 Hash of your string:

97A7E1CCB51F89A26A15D27403CF847039B0BAFD4351BFF5093DFE7182BDB726

Hashing

Enter your text below:

CAB <<<desired message

5, 3

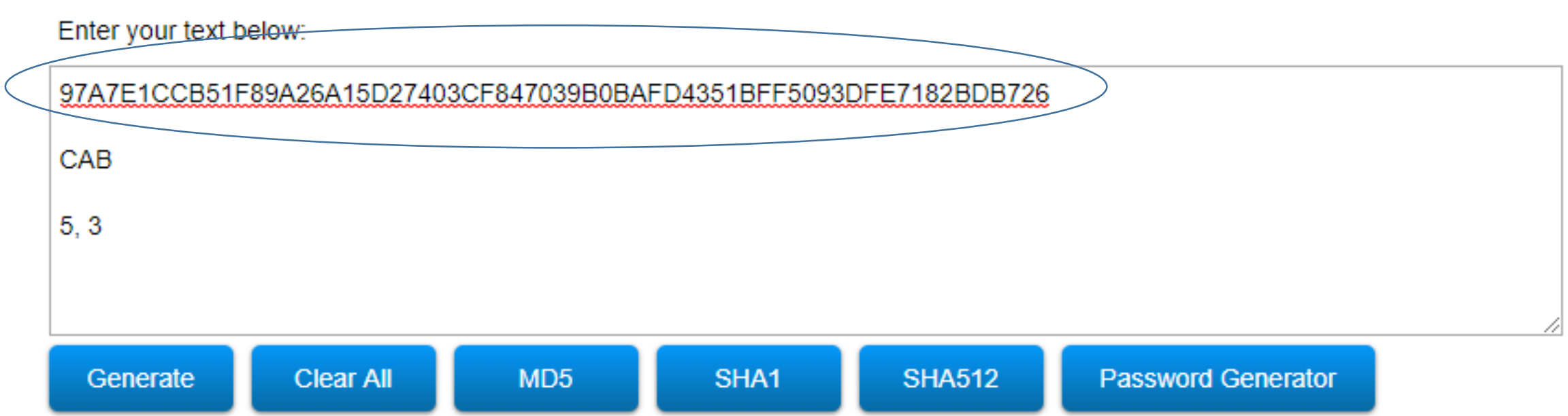
Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

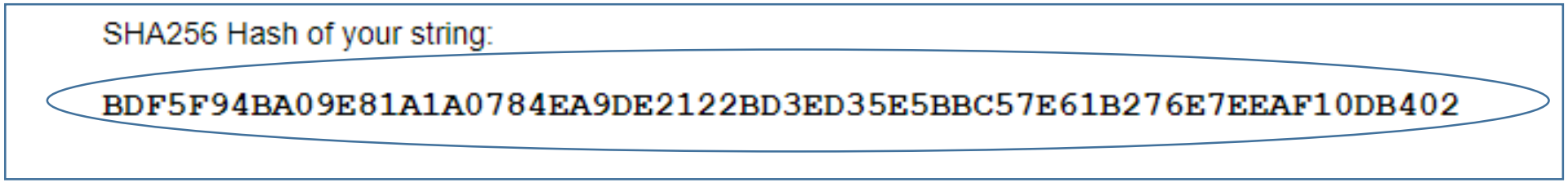
Treat each line as a separate string

SHA256 Hash of your string:

97A7E1CCB51F89A26A15D27403CF847039B0BAFD4351BFF5093DFE7182BDB726

Now let's talk about the funny numbers at the bottom, the cryptographic hash





If you'll notice, we use every previous hash as the beginning number of the next block

SHA256 was invented by the NSA (National Security Agency) and stands for Secure Hashing Algorithm

It is used to create a cryptographic hash (or digital signature)

A cryptographic hash represents a digital signature for each block.

Not only does it act as a signature for that block's state, but the actual message affects the hash, hence, any subsequent unauthorized changes break the hash and reveal tampering after you "sign it."

But wait, the semi-prime 15 (prime numbers 5, 3) are ridiculously easy to “crack” into its two prime numbers

Quick homework, what are the two prime numbers that make up this semi-prime?

944,871,836,856,450,000

944,871,836,856,450,000 <<public key

961,748,941 and 982,451,653<<private key pair

Semi-primes and their corresponding two prime numbers are the backbone of all security on the Internet

944,871,836,856,450,000<<public key

961,748,941 and 982,451,653<<private keys

In a blockchain, not only do you add blocks and hash them, but you also encrypt the message using your private key pair in the message to further alter the cryptographic hash.

15 public key
3 and 5 private key pairs

The beauty of this is that everyone can tell that your private keys were used to encrypt the message, they know that it is you because the altered hash programmatically ties to your public key (the one everyone can see).

But, they cannot "see" your private keys so they cannot impersonate you with your private keys, clever.

It's better than a physical signature, because they know you signed it, but cannot reproduce (i.e., trace/copy it).

What if they look at the visible public key and just try to "crack" the two private keys?

What if they look at the visible public key and just try to "crack" the two private keys?

Well it's a 256 bit key, so the possibilities are 2^256 or

$$2^{256} = 115792089237316195423570985008687907853269984665640564039457584007913129639936$$

What if they look at the visible public key and just try to "crack" the two private keys?

Well it's a 256 bit key, so the possibilities are 2^256 or

$$2^{256} = 115792089237316195423570985008687907853269984665640564039457584007913129639936$$

At modern supercomputer speeds (15 trillion tries / second), it would take about 650,000,000 years

So what three blockchain concepts have we learned:

1 – Hashing can be used to ensure that all the blocks are “chained” together to make them tamper evident.

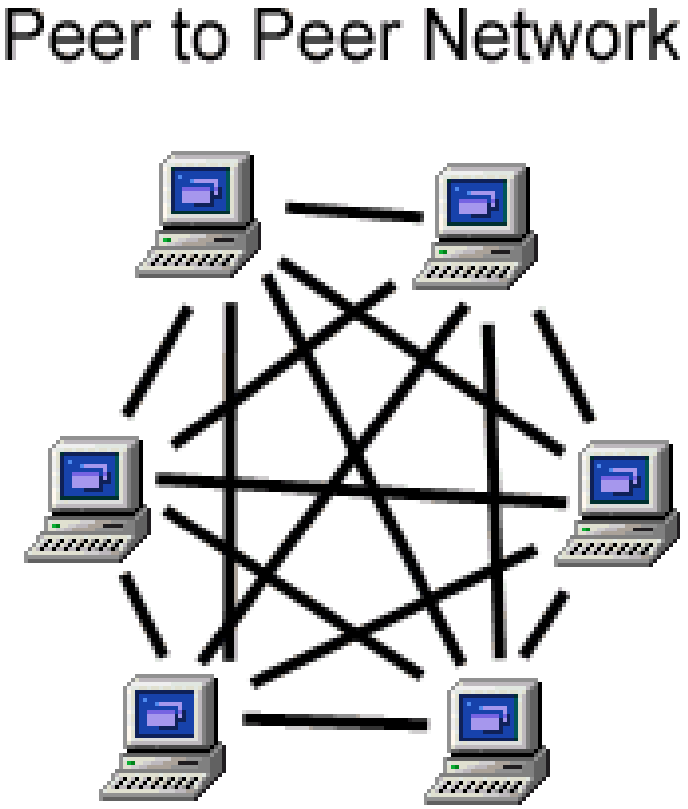
2 – Encryption can be used to “sign” those message blocks to authenticate that it is you to all blockchain participants

3 – Distributed ledger architecture ensures that everyone on the blockchain can have the same copy of the database (the truth).

So what?……

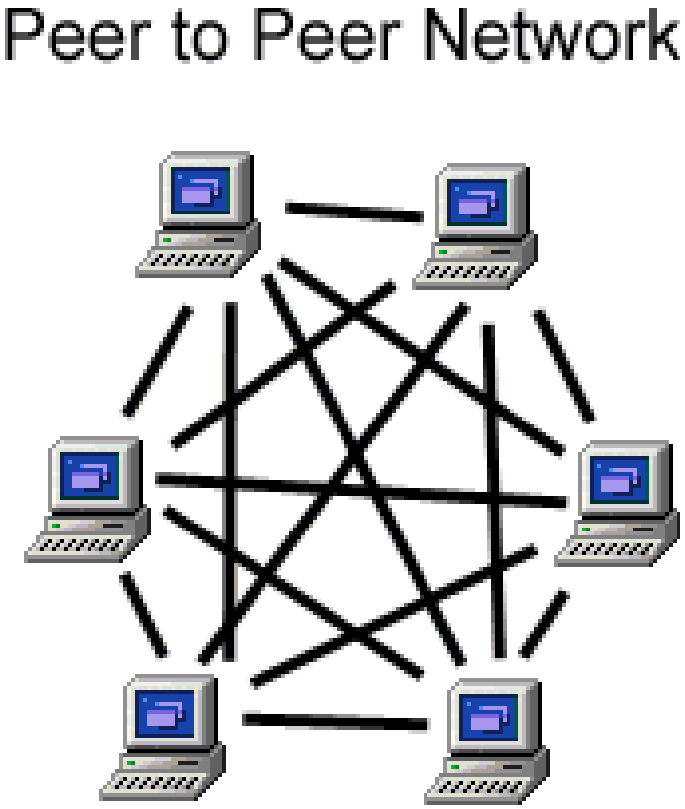
Why it matters

- For the first time we can record information in permission-less **public** blockchains (like Bitcoin) and selectively choose what we wish to reveal.



Why it matters

- For the first time we can record information in **permissioned private** blockchains and inherently govern an accounting system.



Applications

- In entertainment, Spotify uses it to collect listeners' music tracks in order to validate artists' royalties.

- In logistics, IBM, records the status and condition of every product in a supply chain from raw materials to finished goods

Applications

- In diamonds, DeBeers is using a blockchain ledger to trace diamonds from the mine to the final customer purchase.

DE BEERS

- In insurance, Accenture builds blockchain solutions for its insurance clients in order to translate key insurance industry processes into blockchain-ready procedures that embed trust.

accenture

And now a list of banks using blockchain

AEON Bank
Akbank
Akita Bank
ANZ (Australian and New Zealand Bank)
Aomori Bank
Al Rajhi Bank
Ashikaga Bank
ATB Financial
Axis Bank
Awa Bank

Banco Bilbao Vizcaya Argentaria (BBVA)
Bank Dhofar
Bank Of America
Bank Of America Merrill Lynch
Bank Of England
Bank Of Indonesia
Bank Of Iwate
Bank Of Leumi
Bank Of Nagoya
Bank Of Okinawa
Bank Of Thailand
Bank Of The Ryukyus

Accounting Firm Applications

- In 2014, Deloitte launched Rubix, a blockchain offering that provides advisory services and builds distributed applications for clients across sectors, including government.
- In April 2017, EY launched Ops Chain, a set of applications and services to facilitate the commercial use of blockchain technology across the enterprise.
- In November 2016, PwC launched Vulcan Digital Asset Services to enable digital assets to be used for everyday banking, commerce and other personal currency and asset-related services in collaboration with Bloq, Libra, and Netki.
- In September 2016, KPMG launched its Digital Ledger Services—a suite of services designed to help financial services companies realize the potential of blockchain.

Government Applications

- Dubai's government has made a bold move into blockchain and they track utility bills, passports, and shipping manifests with a cryptographic distributed ledger.

Applications

- But while all of these are permissioned private blockchains, the most (in)famous application of blockchain is Bitcoin

EXPLOSION OF ALTCOINS

Litecoin

ZCash

Stellar

Peercoin

Dogecoin

DASH

Monero

Ripple

Bitcoin has familiar precedents, for example:

Houses have PO boxes and mailbox keys

Emails have email accounts and passwords

Bitcoin has public keys and private key pairs

Bitcoin uses distributed ledgers, hashing, and encryption can enable a decentralized, software managed currency.

But, what can go wrong?

Cautions, especially with public blockchains

- The 51% (double spend problem): if any one miner is able to create a majority of the new blocks (takes huge computing power), they can fraudulently certify numerous blocks and get paid to do it.
- Transactional Malleability: if you create a block, and then change any information in that block, if due to a mining error, or hacking, the amended block is accepted first, then the original entry cannot be added and is not recognized. (Mt. Gox - $473 million)
- Blockchain mining code is subject to attacks if not adequately protected. Even if discovered through the distributed peer-to-peer ledger, it can halt all transactions until it is remediated.
- Change management is essential because all network nodes HAVE to be on the same software version.
- File size of the distributed public ledger can get unwieldy

Thank You:
Questions?

References:

- Akhtar, Nadir (2018). Blockchain at Berkeley

- Bougas, M. (2016). How distributed ledger technology is transforming the financial marketplace Retrieved from https://libproxy.library.unt.edu/login?url=https://search.proquest.com/docview/1864753381?accountid=7113
- Kuebler, R. G. (2018). Application of blockchain for authentication, verification of identity and cloud computing Retrieved from https://libproxy.library.unt.edu/login?url=https://search.proquest.com/docview/2038978132?accountid=7113O
- Wu, H. (2017). A distributed blockchain ledger for supply chain (Order No. 10615112). Available from ProQuest Dissertations & Theses Global. (1980717693). Retrieved from https://libproxy.library.unt.edu/login?url=https://search.proquest.com/docview/1980717693?accountid=7113

- YouTube IBM, Patreon - Blockchain

DEPARTMENT OF ACCOUNTING
College of Business
UNT
EST. 1890