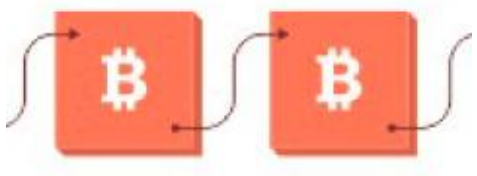
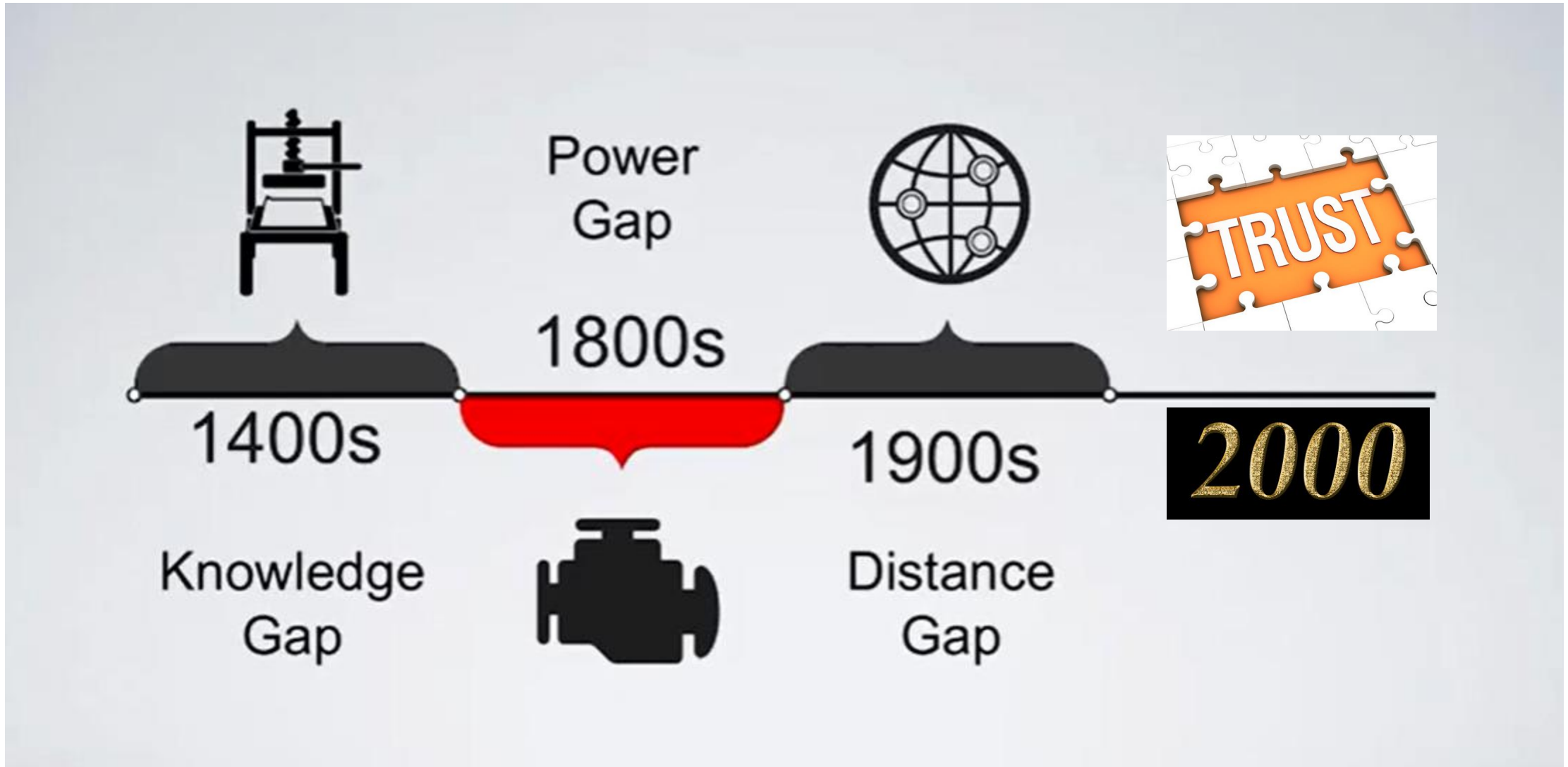
Why are we here today?

Bitcoin



Blockchain

Encryption, Authentication, Hashing, Digital signatures, Problems with current currency system, Trust and trusted parties


Power
Gap
TRUST
1800s
1400s
1900s
2000
Knowledge
Gap
Distance
Gap

I am going to give away USD $10 to everyone in this room! *

I am going to wire transfer USD $10 to everyone who is attending remotely **

* **Can you process my credit card in next 5 minutes?**

** **as long as you cover all the bank transaction fees**

May be something wrong with USD $ currency..

So how about a different currency?

656 Indian Rupees (~USD $10)

No ATM locally dispenses Indian Rupees

No bank branch locally stocks Indian Rupees

Do you think?

President Trump could make $100 bill invalid effective tomorrow?

Nov 2016, Indian Govt. cancelled all 500 and 1,000 rupees bills

Do you think?

The money you have in your bank can lose its value by half?

2007 inflation rate was 231 million percent

Do you think?

You can do the following transactions?

-- Send $10,000 to your mom in North Korea
-- $10,000 to your son in Iran and
-- $2,500 to a charity in Syria

Simple transaction

Offer
Acceptance
Payment

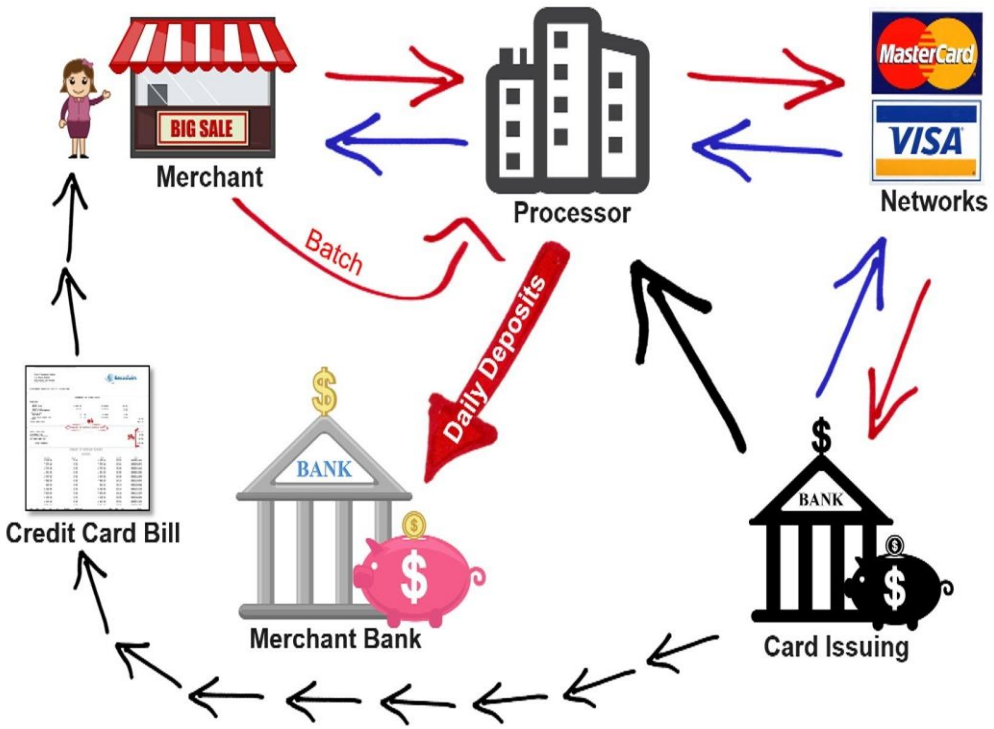
Quick, Fast and Easy!

Anyone can participate
No Middleman
Zero Transaction Cost

No PII info sharing

Nothing is simple anymore!

Complete reliance on Trusting parties, Middleman Controlled by Banks, Master/Visa, PayPal, Clearing networks



Full PII info must
Not open to everyone
Transactions can be restricted

Very Efficient

Bank overdraft fees	$33.3 billion in 2016
Credit Card Fees	$94.3 billion in 2015
Credit Card Interest	$70.4 billion in 2015

“Normalized” DBA team often goes for lunch to Monica’s.

But there is nothing normal about it!

Typical DBA lunch event

Brock left his checkbook at his desk

Phil left his platinum card at a fancy restaurant last night

Jack gave a big tip to a pizza delivery guy yesterday so he has no cash

Davinder is not willing to keep his promise of expensing lunch

John pays and "**Trusts**" his team to pay him back

There has to a better way!

DBA's simple solution

Ledger
Brock pays John $20.02
John Pays Jack $3.45
Phil Pays Brock $3.40
Phil Pays John $200.00
Jack pays Brock $12.75
……

- Accounting concept dating back over 7,000 years in Mesopotamia
- Transaction Log to keep record
- Kept near DBA area where they sit
- Anyone can add an entry
- Settle every month

Problems with DBA's simple solution

Ledger
Brock pays John $20.02
John Pays Jack $3.45
Phil Pays Brock $3.40 Phl pays John $20.00
Phil Pays John $200.00
Jack pays Brock $12.75
…… **Someone accidently shreds the notebook!**

Relies on complete Trust in each other

How do remote folks participate?

Anyone can add an entry!

Settlement Issues?

Intentional or un-intentional damage

Solutions to problems

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
~~John Pays Jack $3.45~~	Rgee
Phil Pays Brock $3.40	Phil
~~Phl pays John $20.00~~	Phil
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack
…… Someone accidently shreds the notebook!	

How do remote folks participate?
Intentional or un-intentional damage

~~Put it on internet/common trusted location~~
Let everyone have a copy!
Encrypted/secure peer to peer distribution

Relies on complete Trust on each other
Anyone can add an entry!

Digital Signatures and Authentication
Use Block chain (with Cryptography Hash) to link blocks

Settlement Issues?

Implement no overspend rule (double spend)
No transaction can be reversed (immutable)
Use software to eliminate Trusted parties!
“proof of work” concept and “longest chain wins” rule

Encryption

Encryption is a mechanism for hiding information by turning readable text into a stream of gibberish in such a way that someone with the proper key can make it readable again.

Public key cryptography, or asymmetrical cryptography, is any cryptographic system that uses pairs of keys:

Public keys which may be disseminated widely

Private keys which are known only to the owner.

Public key

Private Key

Anything encrypted with Private key can be decrypted by Public key.

Anything encrypted with Public key can be decrypted by Private key.

Encryption and authentication

Anything encrypted with Private key can be decrypted by Public key.
Anything encrypted with Public key can be decrypted by Private key.

How can John send an encrypted message to Brock?

Clear Message:
ADW Database admin password is Password12~

Brock's Public key

Encrypted Message
01010011010111111111111
11101111111000010011110
11011001100010110110
00100111110100110000

Brock's Private key

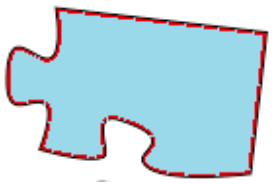
Clear Message:
ADW Database admin password is Password12~

Encryption Authentication

How can Brock be sure that John sent that message?

Clear Message:
ADW Database admin password is Password12~

John's Private key

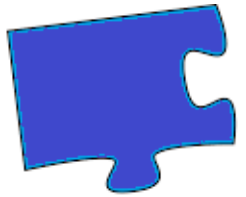


Brock's Public key

Encrypted Message
11111110100110101111111
11111111011111110000010
01110110110011000101111
01100001111101001100000

Brock's Private key

John's Public key

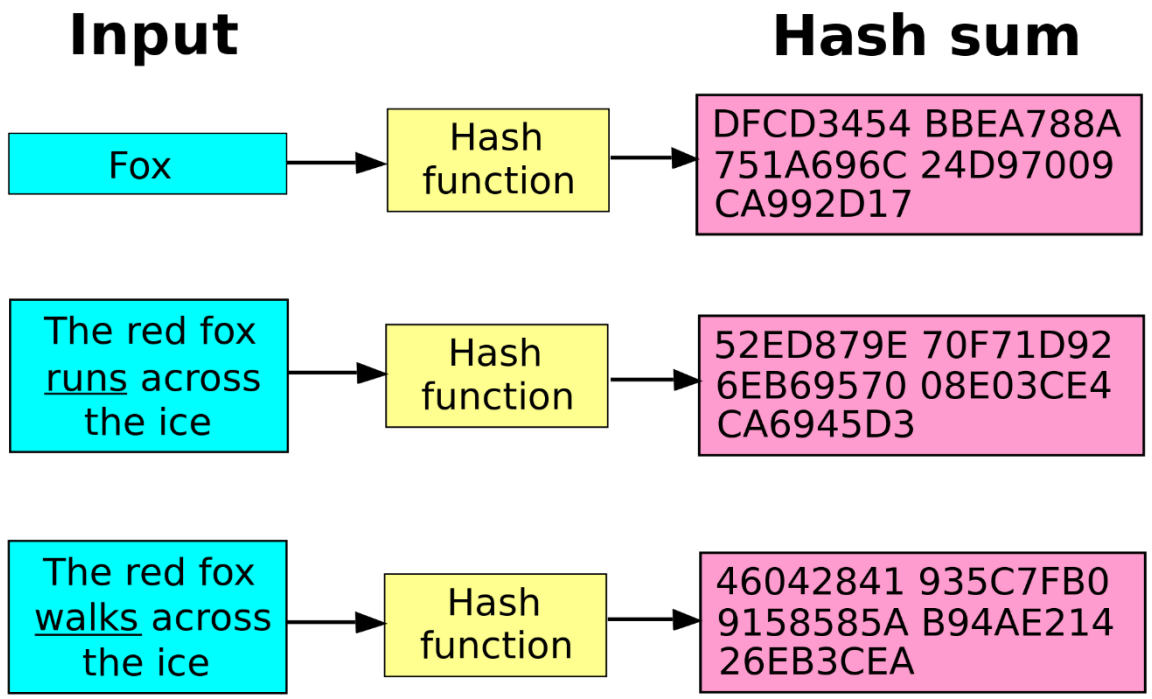


Clear Message:
ADW Database admin password is Password12~

Encryption Authentication

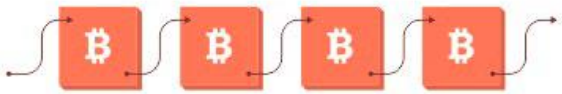
Hash Function

1. Same message = Same hash
2. Different messages ≠ Same hash
3. Quick Computation
4. Small change to a message should result in extensive uncorrelated hash value change
5. it is infeasible to generate a message from its hash value except by trying all possible messages



Applications: Digital Signatures, Password storage, Checksum/Data Integrity, fast look-up of a data in a hash table etc.

What's Blockchain?



Blocks in a chain refer to previous blocks, like page numbers in a book

BOOK ORDERING	BLOCK ORDERING
Page 1, 2, 3, 4, 5	Block n58uf0 built on 84n855, Block 90fk5n built on n58uf0, Block 8n6d7j built on 90fk5n.
Implicit that the page builds on the page whose number is one less. eg Page 5 builds on page 4 (5 minus 1).	84n855, n58uf0, 90fk5n, 8n6d7j represent fingerprints or hashes of the blocks.

Page by page. With books, predictable page numbers make it easy to know the order of the pages. If you ripped out all the pages and shuffled them, it would be easy to put them back into the correct order where the story makes sense.

Block by block. With block chains, each block references the previous block, not by 'block number', but by the block's fingerprint, which is cleverer than a page number because the fingerprint itself is determined by the contents of the block

Images reproduced *from publication "A Gentle Introduction to Blockchain Technology" by Antony Lewis*

Internal consistency. By using a fingerprint instead of a timestamp or a numerical sequence, you also get a nice way of validating the data. In any blockchain, you can generate the block fingerprints yourself by using certain algorithms. If the fingerprints are consistent with the data, and the fingerprints join up in a chain, then you can be sure that the blockchain is internally consistent. If anyone wants to meddle with any of the data, they have to regenerate all the fingerprints from that point forwards and the blockchain will look different.

This means that if it is difficult or slow to create this fingerprint, then it can also be difficult or slow to re-write a blockchain.

Images reproduced *from publication "A Gentle Introduction to Blockchain Technology" by Antony Lewis*

Encryption, Authentication, Cryptographic Hashing, Digital signatures, Blockchain, Immutability, Decentralized, Distributed (P2P), Secure, Anyone, Anywhere can join, Open Border

How to process new transactions without Trusted parties and still have trust? Double payment Problem?

Brock's Copy (Delhi)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil

John's Copy (Iowa)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays B	
Phil Pays Jo	
Jack pays B	

Barry's Copy (London)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

New Transactions	Signature
Jack pays Janet $32.75	Jack
Phil pays John $38.89	Phil
Brock pays John $10.00	Brock
Phil Pays John $20.00	Phil
Jack pays Brock $32.75	Jack
.. .. ..	
.. ..	
.. ..	

Kiran's Copy (India)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

Janet's Copy (Dallas)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

Phil's Copy (Northbrook)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

Start broadcasting every transaction to everyone
Transactions may be received in different order (Latency etc.)
A set of transactions is "Block"
One Block can only have 1 transaction from one person (**Double payment solution**)
Anyone can process transactions (called "miners")

"**Proof of work**" concept, Game theory
Difficult and time consuming task (minimum xx minutes to solve)
Should be quick and easy to validate the work
Adjust the difficulty of problem in real time.
e.g. DBA's get difficult Query to tune or
Miners get a difficult hashing/encryption problem to solve

Monetary award for work
Miner who provides the "proof of work" for the block, adds the block to blockchain and broadcasts the information to everyone on network
Longest blockchain wins.

Brock's Copy (Delhi)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil

John's Copy (Iowa)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays B	
Phil Pays Jo	
Jack pays B	

Barry's Copy (London)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil e
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

New Transactions	Signature
Jack pays Janet $32.75	Jack
Phil pays John $38.89	Phil
Brock pays John $10.00	Brock
Phil Pays John $20.00	Phil
Jack pays Brock $32.75	Jack
.. .. ..	
.. ..	
.. ..	

Kiran's Copy (India)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil e
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

Janet's Copy (Dallas)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil e
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

Phil's Copy (Northbrook)

Ledger	Signature
Brock Starts with $400	Brock
John Starts with $400	John
Phil Starts with $400	Phil
Jack Starts with $400	Jack
Jack pays $100	Jack
Phil pays John $300	Phil
Brock pays John $20.02	Brock
Phil Pays Brock $3.40	Phil e
Phil Pays John $200.00	Phil
Jack pays Brock $12.75	Jack

Phil

Difficult hashing/encryption problem

New Block	
Previous Block HASH	0101001101011111111111111011111 1000010011110110110011000101101 0010011111010011000010010011011 0110001110010101011000001010001 1010101001010010001111001100101 0000101100000000110000101110011 0110110011111100111001011100010 0010110011110011011110100010110
Jack pays Janet $32.75	Jack
Phil pays John $38.89	Phil
.. .. ..	
System pays Miner 0.01	
Hash Key Seed/Variable	1

SHA256 HASH ➔

101100101000110110101100110001010
111000001011101110110011000011100
100111101010110100010111110100110
000001011000000001000101111110001
011010010001001101100100110001000
101111111101000001100110010010000
101010101001101110000000011000110
001001101100011110010100100101000

New Block	
Previous Block HASH	0101001101011111111111111011111 1000010011110110110011000101101 0010011111010011000010010011011 0110001110010101011000001010001 1010101001010010001111001100101 0000101100000000110000101110011 0110110011111100111001011100010 0010110011110011011110100010110
Jack pays Janet $32.75	Jack
Phil pays John $38.89	Phil
.. .. ..	
System pays Miner 0.01	
Hash Key Seed/Variable	2

SHA256 HASH ➔

111111100100000100100100111011101
100111010100010101111111100101010
101101001101100001111100000000000
101001110000000001010110000010000
100110100011001010010100101101100
011011101100001101100010111100100
011011010111010001111001000111100
010100011011100101101100010000010

Phil

Difficult hashing/encryption problem

Finding the magic number (“proof of work”) will take about numerous tries (billion in this case to look for 30 leading zeroes in hash output)

But verification is simple (1 try) by using the same HASH function.

New Block	
Previous Block HASH	0101001101011111111111111011111 1000010011110110110011000101101 1 0010011111010011000010010011011 1 0110001110010101011000001010001 1 1010101001010010001111001100101 0 0000101100000000110000101110011 0 0110110011111100111001011100010 1 0010110011110011011110100010110 0
Jack pays Janet $32.75	Jack
Phil pays John $38.89	Phil
.. .. ..	
System pays Miner 0.01	
Hash Key Seed/Variable	3456789065

SHA256 HASH ➔

000000000000000000000000000000010
100111010100010101111111001010101
011010011011000011111000000000000
101001110000000010101100000100000
100110100011001010010100101101100
011011110110000110110001011110010
011011010111010001111001000111100
010100011011100101101100010000010

System dynamically changes the complexity of puzzle to ensure it takes about 10 minutes to be successful

Proof of work

Why make it difficult hashing/encryption?

- People generally don’t value the things they get for free
- People value what they pay for
- If everyone started getting dollars for free and no work, do you think will have any value in commerce?
- This scheme “Proof of work” was created with concept in mind that you will have to spend Hardware/Compute power, Electricity and Time to earn Bitcoin rewards.

Hardware Innovations

CPU

In the beginning, mining with a CPU was the only way to mine bitcoins and was done using the original Satoshi client. You might mine for decades using your laptop without earning a single coin.

GPU (Graphical Processing Unit)

About year and a half after, The massively parallel nature of some GPUs allowed for a 50x to 100x increase in bitcoin mining power while using far less power per unit of work.

FPGA (Field Programmable Gate Array)

Butterfly Labs FPGA 'Single', the bitcoin mining hardware landscape gave way to specially manufactured hardware dedicated to mining bitcoins. While the FPGAs didn't enjoy a 50x - 100x increase in mining speed as was seen with the transition from CPUs to GPUs, they provided a benefit through power efficiency and ease of use. A typical 600 MH/s graphics card consumed upwards of 400w of power, whereas a typical FPGA mining device would provide a hashrate of 826 MH/s at 80w of power. That 5x improvement allowed the first large bitcoin mining farms to be constructed at an operational profit. The bitcoin mining industry was born

ASIC (Application Specific Integrated Circuit)

An ASIC is a chip designed specifically to do one thing and one thing only. Unlike FPGAs, an ASIC cannot be repurposed to perform other tasks. An ASIC designed to mine bitcoins can only mine bitcoins and will only ever mine bitcoins. The inflexibility of an ASIC is offset by the fact that it offers a 100x increase in hashing power while reducing power consumption compared to all the previous technologies.

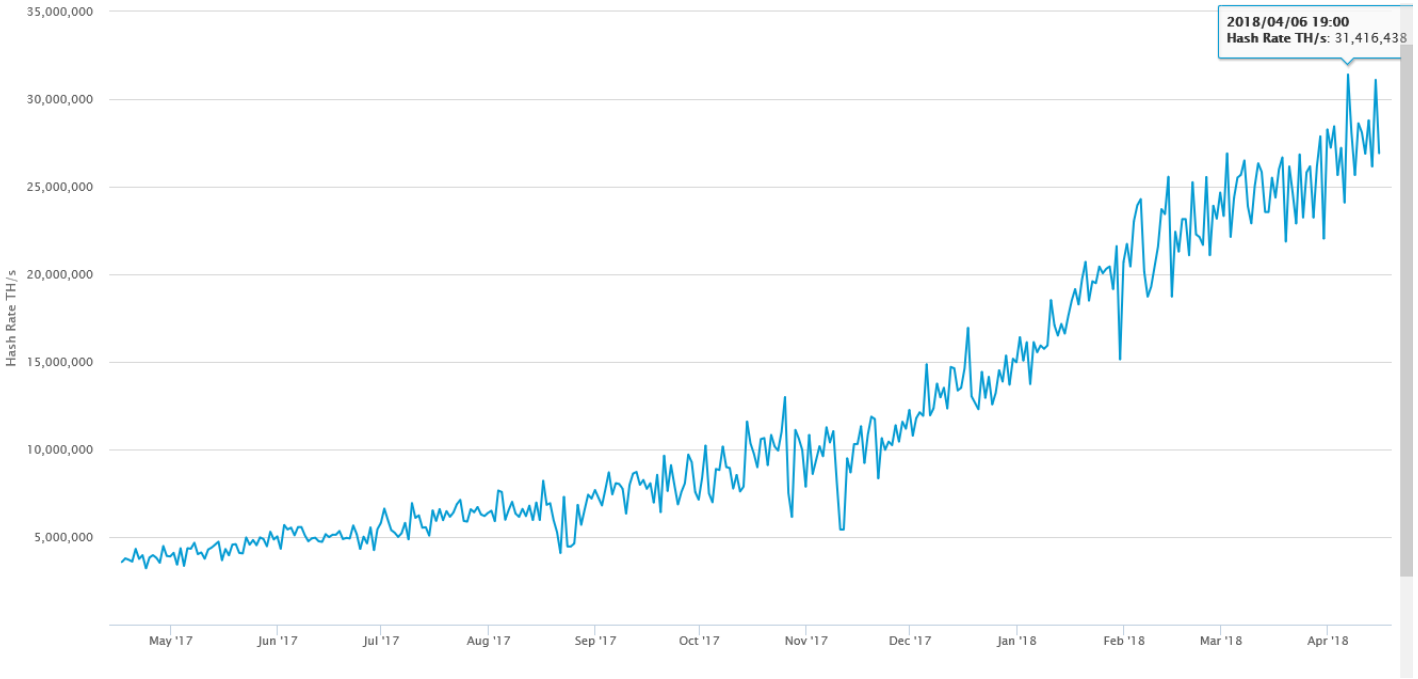
Bitcoin network Hash Rate.

Number of Tera hashes per second (trillions of hashes per second)

31,416,438 Trillions of hashes/second

30,680 Peta Hashes/Second (on Apr 06, 2018)

11,329 Peta Hashes/Second (on Oct 14, 2017)



June 2017: Fastest supercomputer is 93 peta FLOPS (floating point operations per second)

Total Power of top 500 supercomputers = 748 Petaflop/s

Network Hash Rate data/image from https://blockchain.info/charts/hash-rate

Questions?