МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

MONGOLIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

MN CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

BLOCKCHAIN TECHNOLOGY & CRYPTOCURRENCY

MNSEC-2017

DASHZEVEG Gadbadrakh

Department of Network and Information Security

SICT, MUST

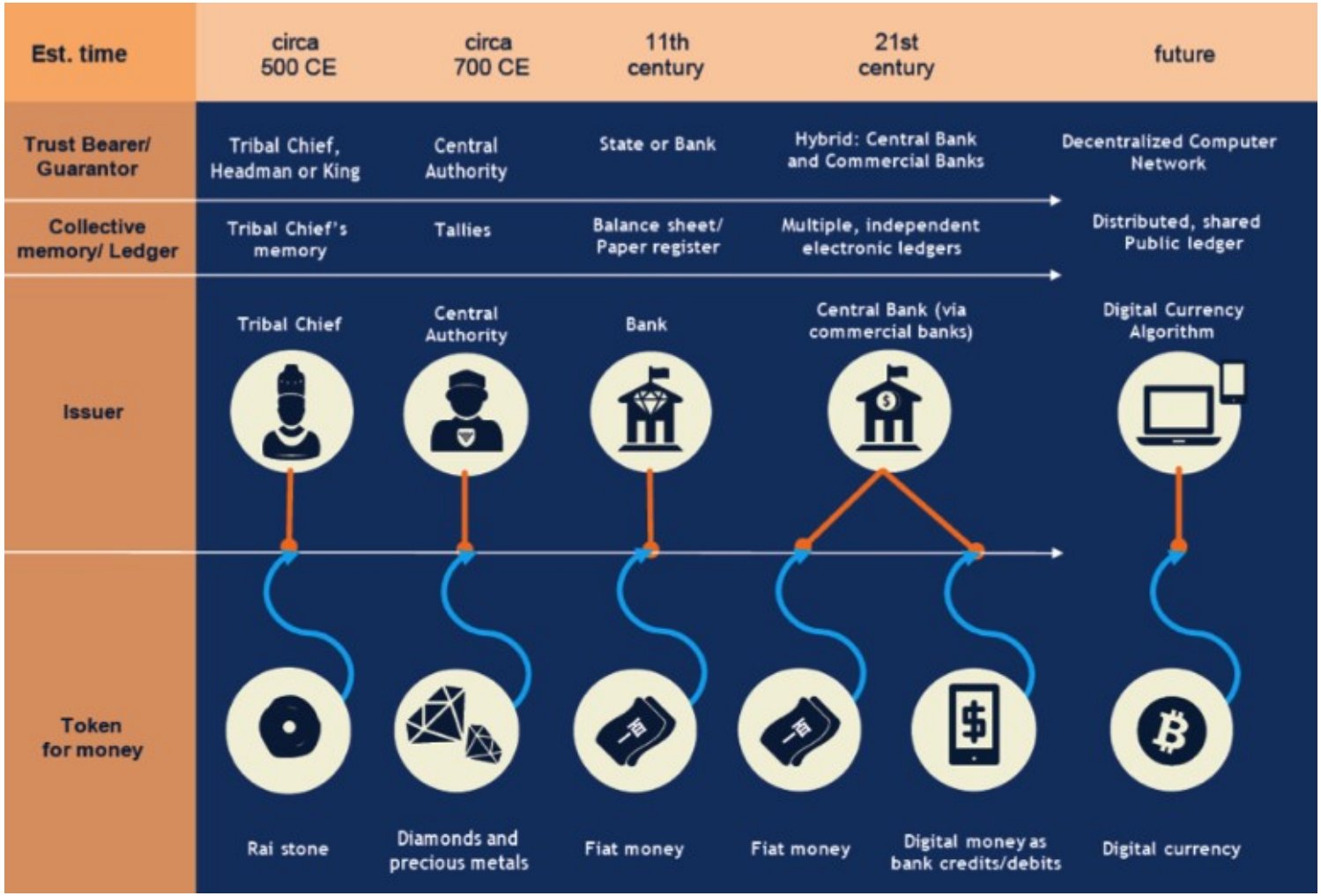
Ulaanbaatar, MN

Content

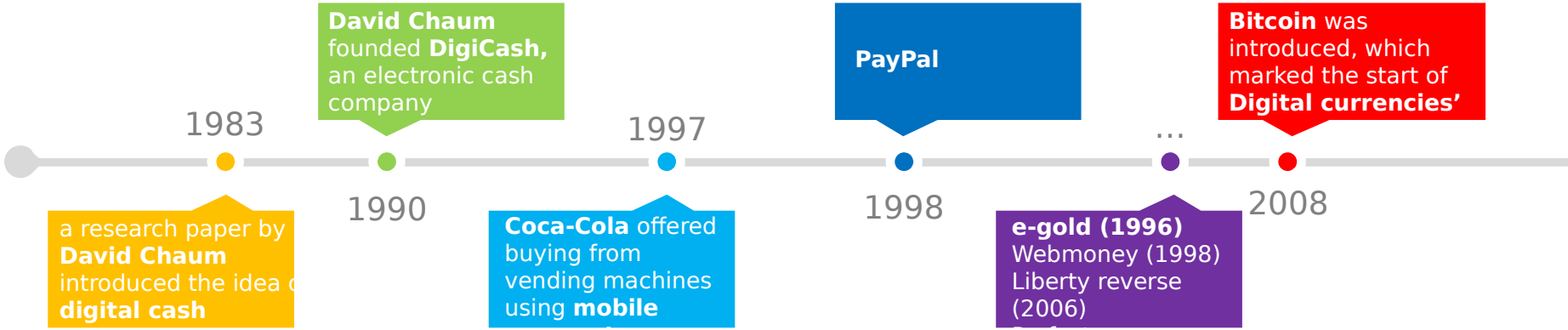
Money vs Currency

Money	Currency
Money is a store of value and maintains its purchasing power over a long period of time plus:	Currency is what most people think money is!
medium of exchange	medium of exchange.
unit of account.	unit of account. (it’s got numbers on it!).
portable	portable
durable (it never changes from one century to the next).	durable
divisible	divisible
interchangeable	interchangeable
• **Silver and gold have intrinsic value!**	• Currency is simply paper. This paper money is a tool for trading your time. • **Currency has no intrinsic value!**

Exchange methods



Digital currency



Cryptocurrency

Cryptocurrency

870
Currencies

249
Assets

5539
Markets

$136,583,460,780
Market Cap

$3,946,593,519
24h Vol

48.2%
BTC Dominance

Cryptocurrencies by Market Cap

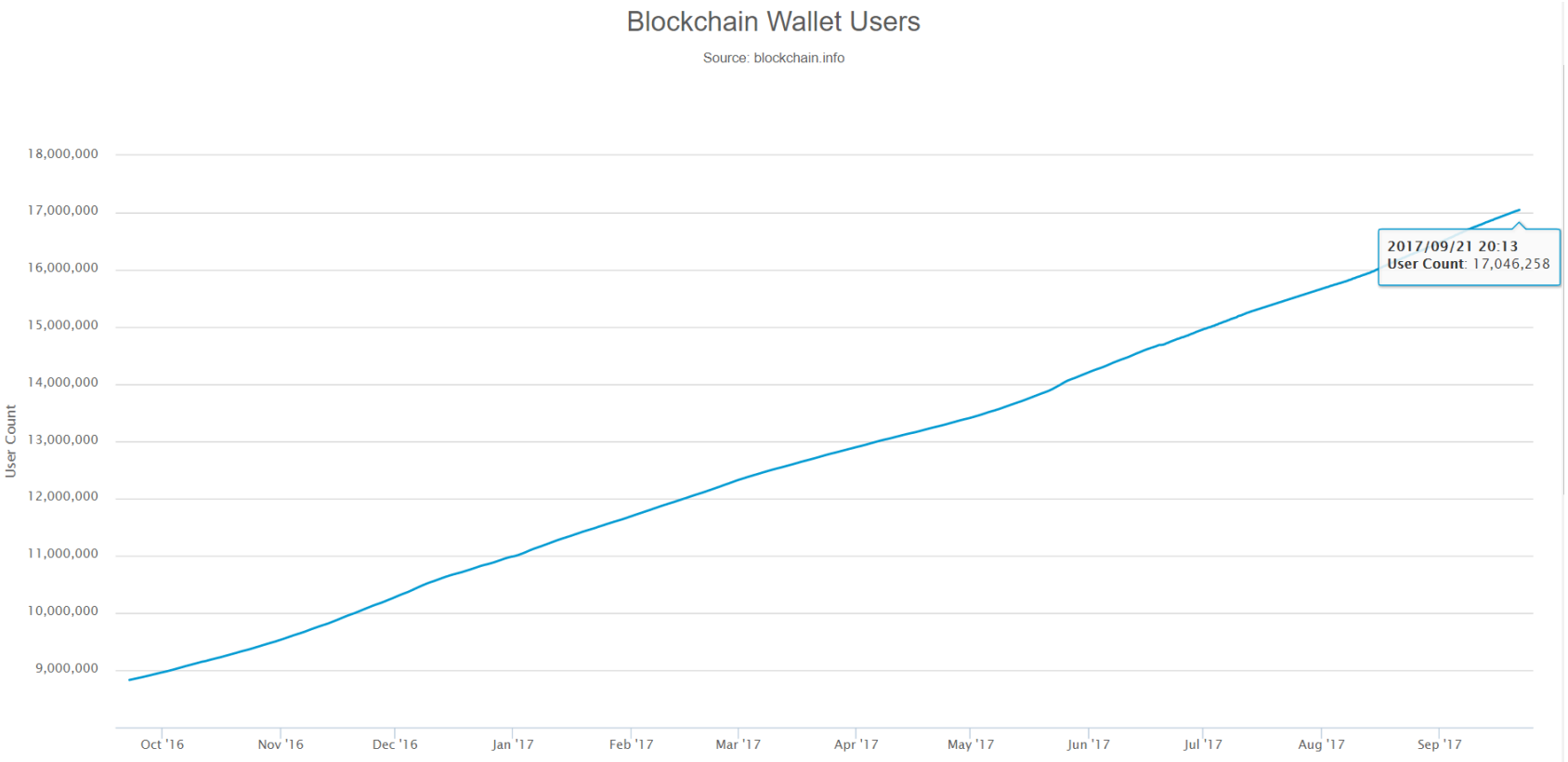
#	Name	Market Cap (USD)	Unit Price (USD)
1	Bitcoin	$65,890,246,635.00	$3975.21000000
2	Ethereum	$27,028,213,792.00	$285.37500000
3	Bitcoin Cash	$7,738,989,490.00	$466.35800000
4	Ripple	$7,055,458,626.00	$0.18400500
5	Litecoin	$2,871,000,431.00	$54.16810000
6	Dash	$2,446,364,642.00	$323.30200000
7	NEM	$2,187,702,000.00	$0.24307800
8	IOTA	$1,585,243,947.00	$0.57032800
9	Monero	$1,455,674,378.00	$96.37650000
10	Ethereum Classic	$1,099,002,428.00	$11.48830000
11	NEO	$1,068,115,000.00	$21.36230000
12	OmiseGo	$1,011,876,507.00	$10.29250000
13	bcc	$803,962,113.00	$119.34900000

Info of Bitcoin

Total Bitcoins in circulation:	16,580,963
Total Bitcoins to ever be produced:	21,000,000
Percentage of total Bitcoins mined:	78.96%
Total Bitcoins left to mine:	4,419,038
Total Bitcoins left to mine until next blockhalf:	1,794,038
Bitcoin price (USD):	$3,589.60
Market capitalization (USD):	$59,519,022,990.00
Bitcoins generated per day:	1,800
Bitcoin inflation rate per annum:	4.04%
Bitcoin inflation rate per annum at next block halving event:	1.80%
Bitcoin inflation per day (USD):	$6,461,280
Bitcoin inflation until next blockhalf event based on current price (USD):	$6,439,877,010
Total blocks:	486,477
Blocks until mining reward is halved:	143,523
Total number of block reward halvings:	2
Approximate block generation time:	10.00 minutes
Block reward	12.5
Approximate blocks generated per day:	144
Difficulty:	1,103,400,932,964
Hash rate:	8.90 Exahashes/s

1 USD = 100 cents
1 BTC = 100,000,000 satosh

Blockchain Wallet Users



Richest addresses

Richest addresses

	Address	Balance
1	1CLnjM8wMfATK7gseWgcnfBshEgexCXEXL	121,403.03942934 BTC
2	1NGvjF6XbeoxWybkbtGeYCRJ7C46WSvbQn	94,348.3264714 BTC
3	16rCmCmbuWDhPjWTrpQGaU3EPdZF7MTdUk	91,203.00212323 BTC
4	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	79,957.16305325 BTC
5	18rnfoQgGo1HqvVQaAN4QnxjYE7Sez9eca	70,000.00152157 BTC
6	1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx	69,370.10718311 BTC
7	1PnMfRF2enSZnR6JSexxBHuQnxG8Vo5FVK	66,452.06642179 BTC
8	1AhTjUMztCihiTyA4K6E3QEpobjWLwKhkR	66,378.80979283 BTC
9	1DiHDQMPFu4p84rkLn6Majj2LCZZZRQUaa	66,235.82443862 BTC
10	1EBHA1ckUWzNKN7BMfDwGTx6GKEbADUozX	66,233.75706908 BTC
11	1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC	53,880.05753422 BTC
12	1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy	53,000.00684844 BTC
13	12QwMGnW6vhZoNNKJNEZeJjgySw2eSvqJz	48,288.95915154 BTC
14	1EfBMK9q6rGFZazeF7jyNdTgqGYgcDgRE5	47,550.37250986 BTC
15	16cou7Ht6WjTzuFyDBnht9hmvXytg6XdVT	44,998.00024657 BTC

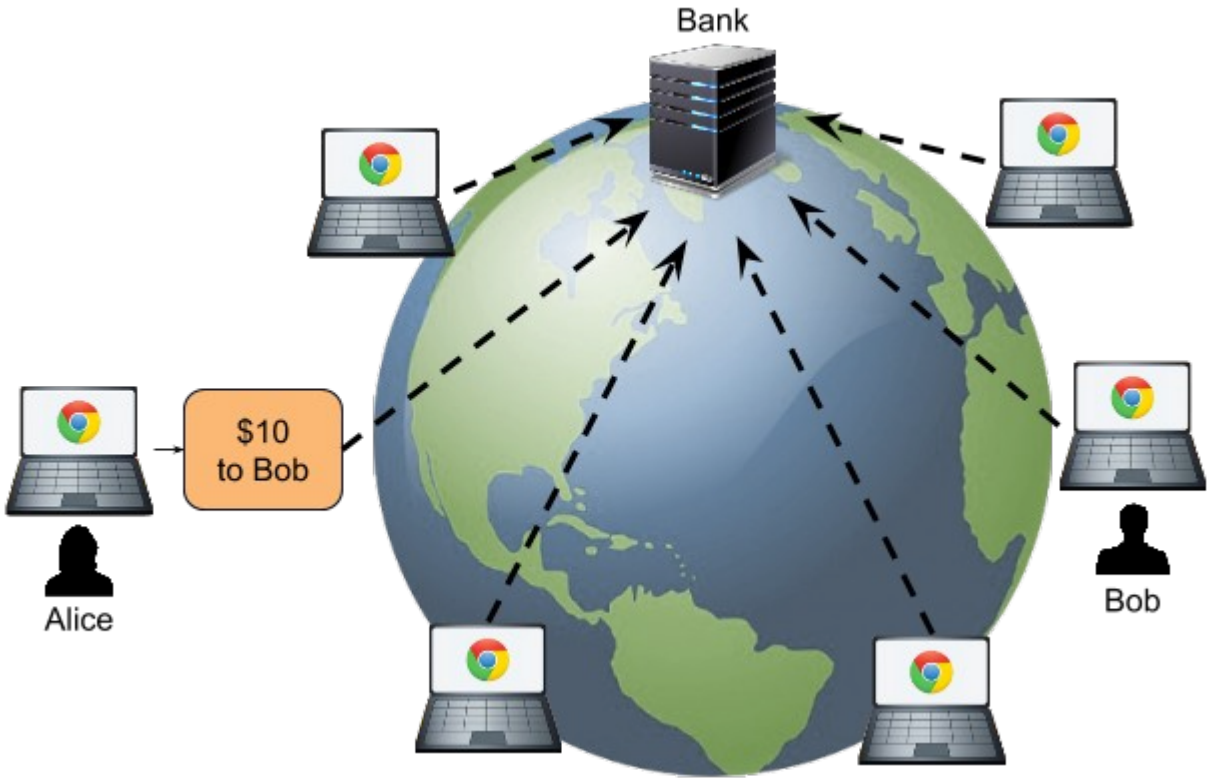
$ 485,612,120 = 121403.03 * 40

Bank Ledger vs Bitcoin Ledger

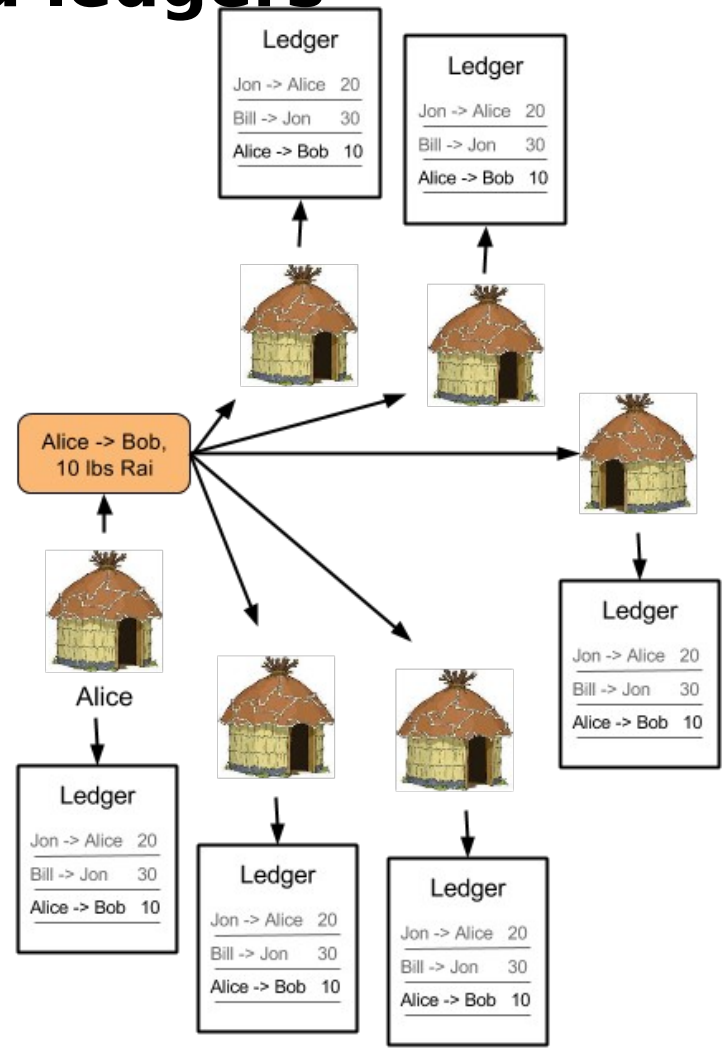
BANK LEDGER	
20 Aug	Acc #12345678 pays $100 to Acc #32121054
20 Aug	Acc #88812345 pays $150 to Acc #32121054
21 Aug	Acc #88812345 pays $100 to Acc #3234567

BITCOIN LEDGER	
17 Aug	Bitcoin address xxx pays 0.5 BTC to bitcoin address yyy
18 Aug	Bitcoin address xxx pays 2 BTC to bitcoin address zzz
18 Aug	Bitcoin address zzz pays 0.002 BTC to bitcoin address xxx

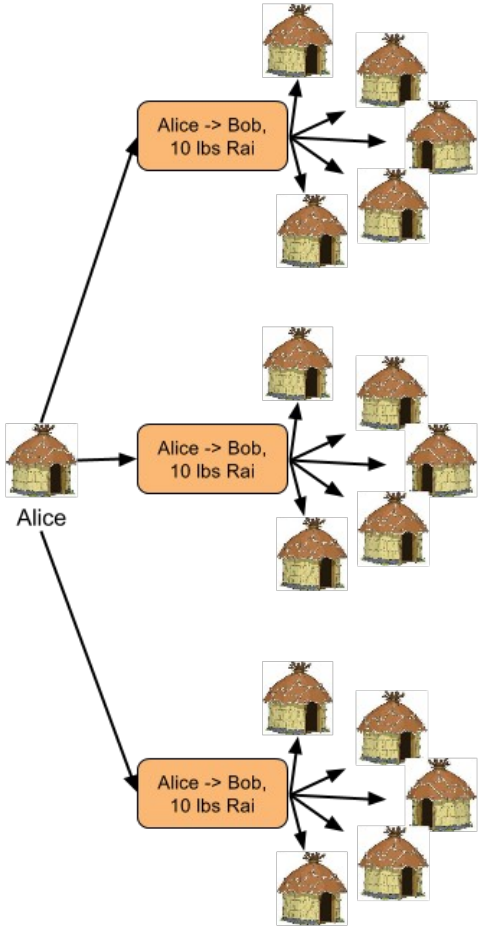
Centralized ledgers



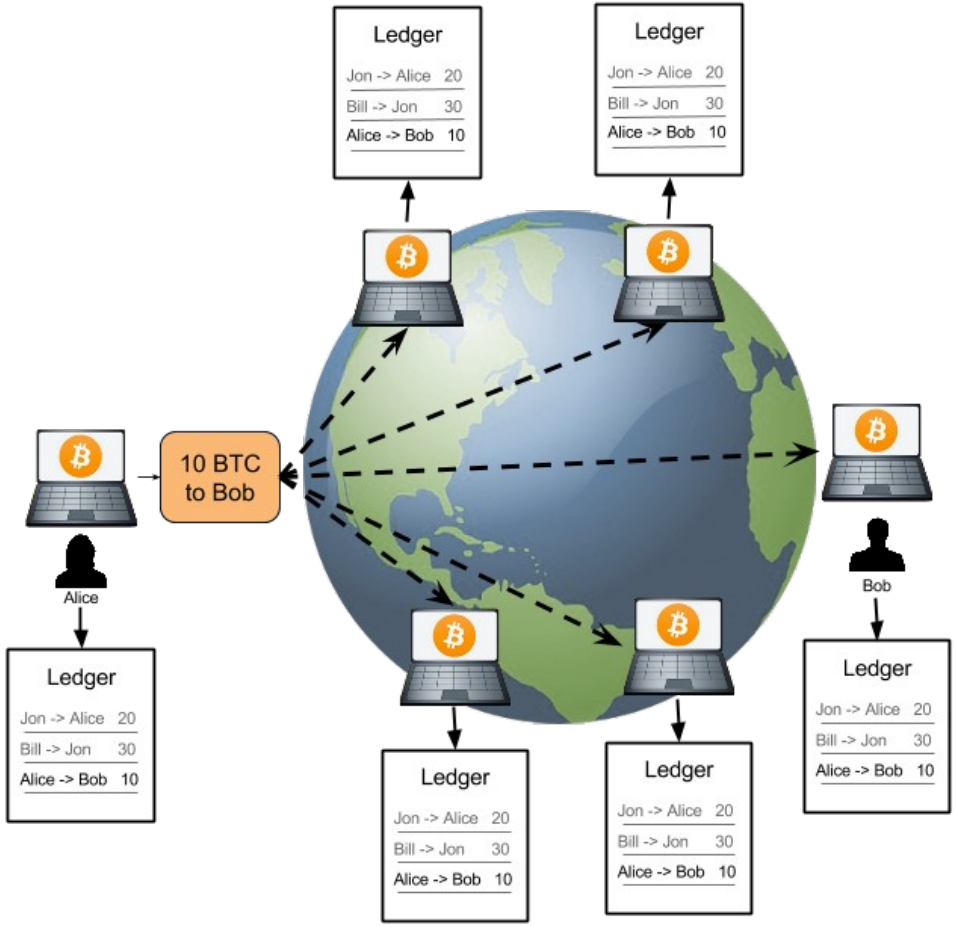
Decentralized ledgers



Decentralized ledgers



Decentralized ledgers



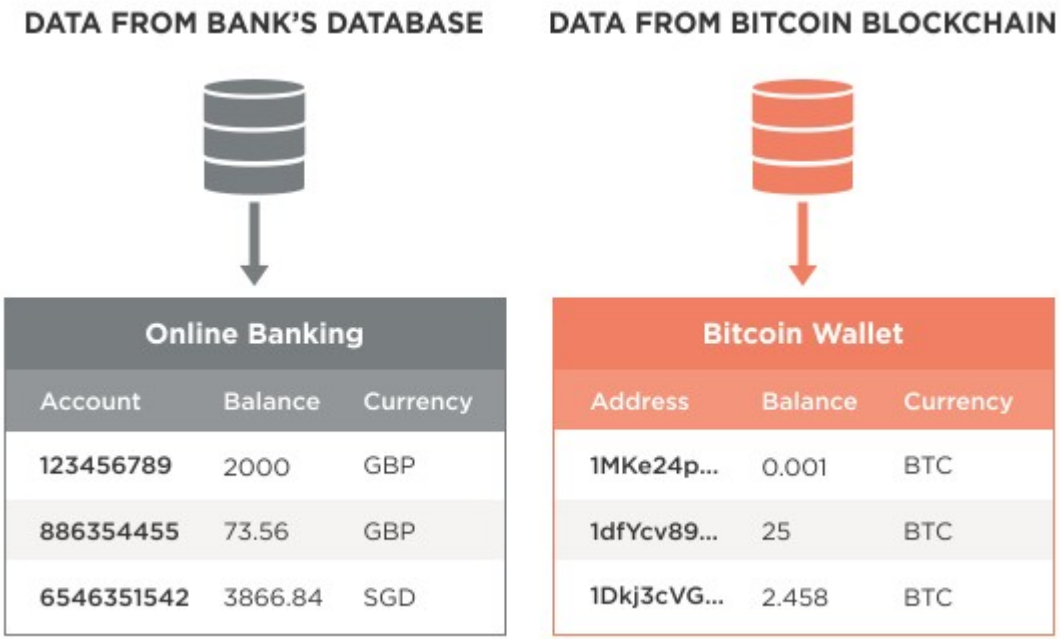
Bitcoin accounts: addresses

Bitcoin accounts: addresses

There are currently two address formats in common use:

- Common P2PKH (Pay to Pubkey Hash) which begin with the number 1, eg: **1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2**.
- Newer P2SH (Pay to Script Hash) type starting with the number 3, eg: **3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy**.

Bitcoin wallets



How are bitcoins sent?
Payments, or bitcoin transactions

BITCOIN WALLET	
Address	Private Key (usually hidden from screen)
1KrieA3KyYVrLJbSynkML9rriBLZpkPvDR	5J7ZWKWJE1fMSjQSTyeBqD4cxickKKA7xFdYHZDeXVbmoPBLrey
1KKGgesMtkWW52SEyd88kBkSijhVps7nJJ	5JwGTvMJumhMtxNBSj5QdYZVSck5W8PqAC5mtEUnRA1xHpL9g5x
14wKRvadKMq6Lthg9HAic5iebKWGSY2w75	5JphsyRvz3Goves7GVzntJ4bVpTWnmExXsjK3fHe6zhRqrgZoDT

Wallet types

Cold wallets and Hot wallets

- Desktop wallets
- Mobile wallets
- Online web wallets
- Physical wallets (Paper wallets, ...)
- Bitcoin Clients
- Hardware Wallets

5 Ways to Participate in the Bitcoin Revolution

1. **Acquire bitcoins.**
   a.) **Accepting bitcoin payments**
   b.) **Mining bitcoins**
   c.) **Purchasing bitcoins**
2. **Engage in services for bitcoin.**
   a.) **Digital or hardware wallet services**:
   b.) **Bitcoin payment processors**:
3. **Provide solutions for bitcoin acceptance.**
4. **Leverage blockchain technology.**
5. **Invest in bitcoin.**

Who controls the Bitcoin network?

There are currently **9141*** nodes running on the Bitcoin network.

6685 Bitcoin Core nodes

809 Bitcoin-ABC nodes

666 Bitcoin Unlimited nodes

437 Bitcoin UASF nodes

184 btc1 nodes

132 Bitcore nodes

95 Bitcoin Classic nodes

47 Bitcoin Knots nodes

26 bcoin nodes

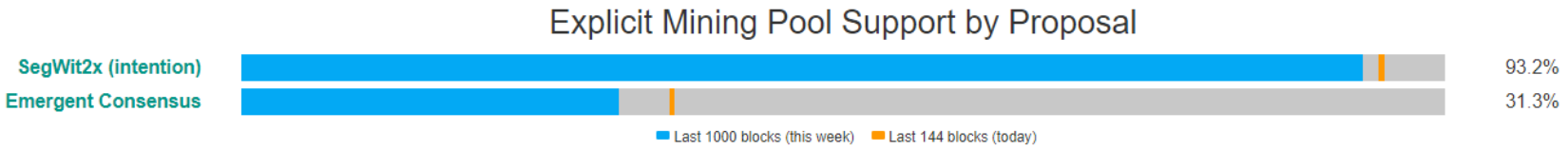
25 btcd nodes

19 Bitcoin XT nodes

11 TRB nodes

5 libbitcoin nodes

Who controls the Bitcoin network?



bitcoin

2017-07-23

$62B

$7B

1 BTC = $3768.96

1 BCC = $426.80

bitcoin cash

ethereum

2016-07-23

$26B

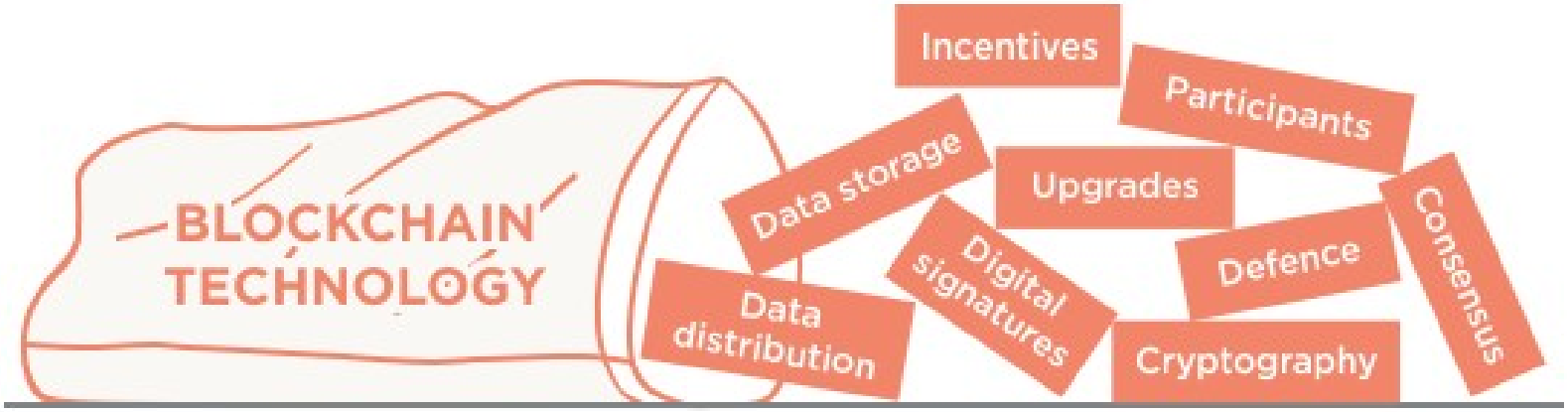
$1B

1 ETH = $277.50

1 ETC = $10.67

ethereum classic

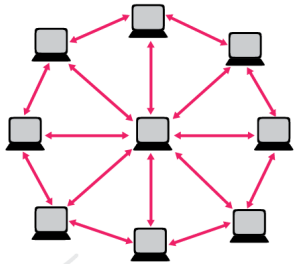
What is Blockchain Technology?



Blockchains are built from 3 technologies		
1. Private Key Cryptography	**2. P2P Network**	**3. Program (the blockchain's protocol)**
Cash vs. Plastic	Tree falls in a forest	Tragedy of the commons
Identity	**System of Record**	**Platform**

Bitcoin transaction

Someone requests a transaction.



The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.

Validation

The network of nodes validates the transaction and the user's status using known algorithms.

A verified transaction can involve **cryptocurrency**, contracts, records, or other information.

cryptocurrency

Has no intrinsic value in that is not redeemable for another commodity such as gold.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger,

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

DATA STORAGE: What is a blockchain?

A blockchain is just a file.

Blocks in a chain = pages in a book

For analogy, a book is a chain of pages. Each page in a book contains:

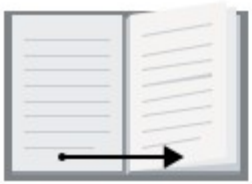
the text: for example the story

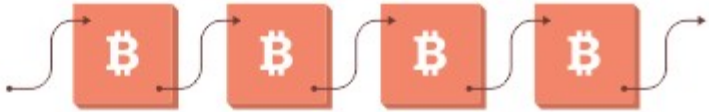
information about itself: at the top of the page there is usually the title of the book and sometimes the chapter number or title; at the bottom is usually the page number which tells you where you are in the book. This ‘data about data’ is called meta-data.

Similarly in a blockchain block, each block has:

the contents of the block, for example in bitcoin is it the bitcoin transactions, and the miner incentive reward (currently 25 BTC).

a ‘header’ which contains the data about the block. In bitcoin, the header includes some technical information about the block, a reference to the previous block, and a fingerprint (hash) of the data contained in this block, among other things. This hash is important for ordering





Keeping track of payments: The Bitcoin Blockchain

Name	Date Modified	Size	Kind
Bitcoin	Today 9:33 pm	--	Folder
bitcoind.pid	13 Aug 2015 10:15 pm	4 bytes	Document
blocks	Today 8:15 am	--	Folder
blk00000.dat	16 Dec 2014 12:23 pm	134.2 MB	Document
blk00001.dat	16 Dec 2014 12:27 pm	134.2 MB	Document
blk00002.dat	16 Dec 2014 12:32 pm	134.2 MB	Document
blk00003.dat	16 Dec 2014 12:36 pm	134.2 MB	Document
blk00004.dat	16 Dec 2014 12:40 pm	134.2 MB	Document
blk00005.dat	16 Dec 2014 12:52 pm	134.2 MB	Document
blk00006.dat	16 Dec 2014 12:56 pm	134.2 MB	Document
blk00007.dat	16 Dec 2014 1:01 pm	134.2 MB	Document
blk00008.dat	16 Dec 2014 1:05 pm	134.2 MB	Document
blk00009.dat	16 Dec 2014 2:48 pm	134.2 MB	Document
blk00010.dat	16 Dec 2014 2:51 pm	134 MB	Document
blk00011.dat	16 Dec 2014 2:56 pm	134 MB	Document

As of **2014**, A screenshot of The Bitcoin Blockchain files on my computer. Here you can see The Bitcoin Blockchain split into files, each 134MB big, and the total is about 50GB at time of writing.

Block ordering in a blockchain

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 blockchains, 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.

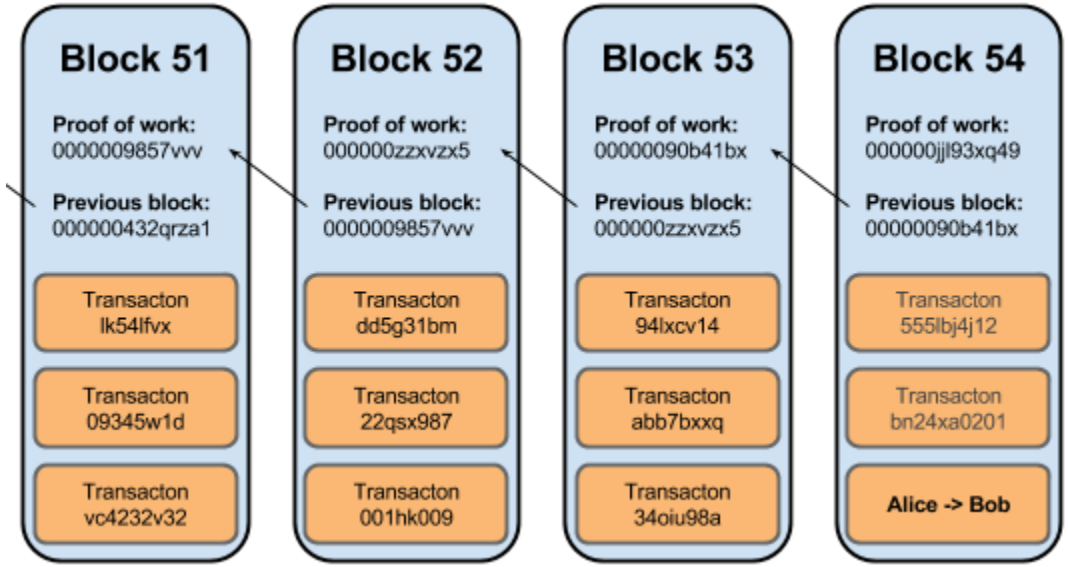
BOOK ORDERING	BLOCK ORDERING
Page 1, 2, 3, 4, 5	Block n58uf0 built on 84n855, Block 90fk5n built on n58uf0, Block 8n6d7j built on 90fk5n.
Implicit that the page builds on the page whose number is one less. eg Page 5 builds on page 4 (5 minus 1).	84n855, n58uf0, 90fk5n, 8n6d7j represent fingerprints or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

Internal consistency

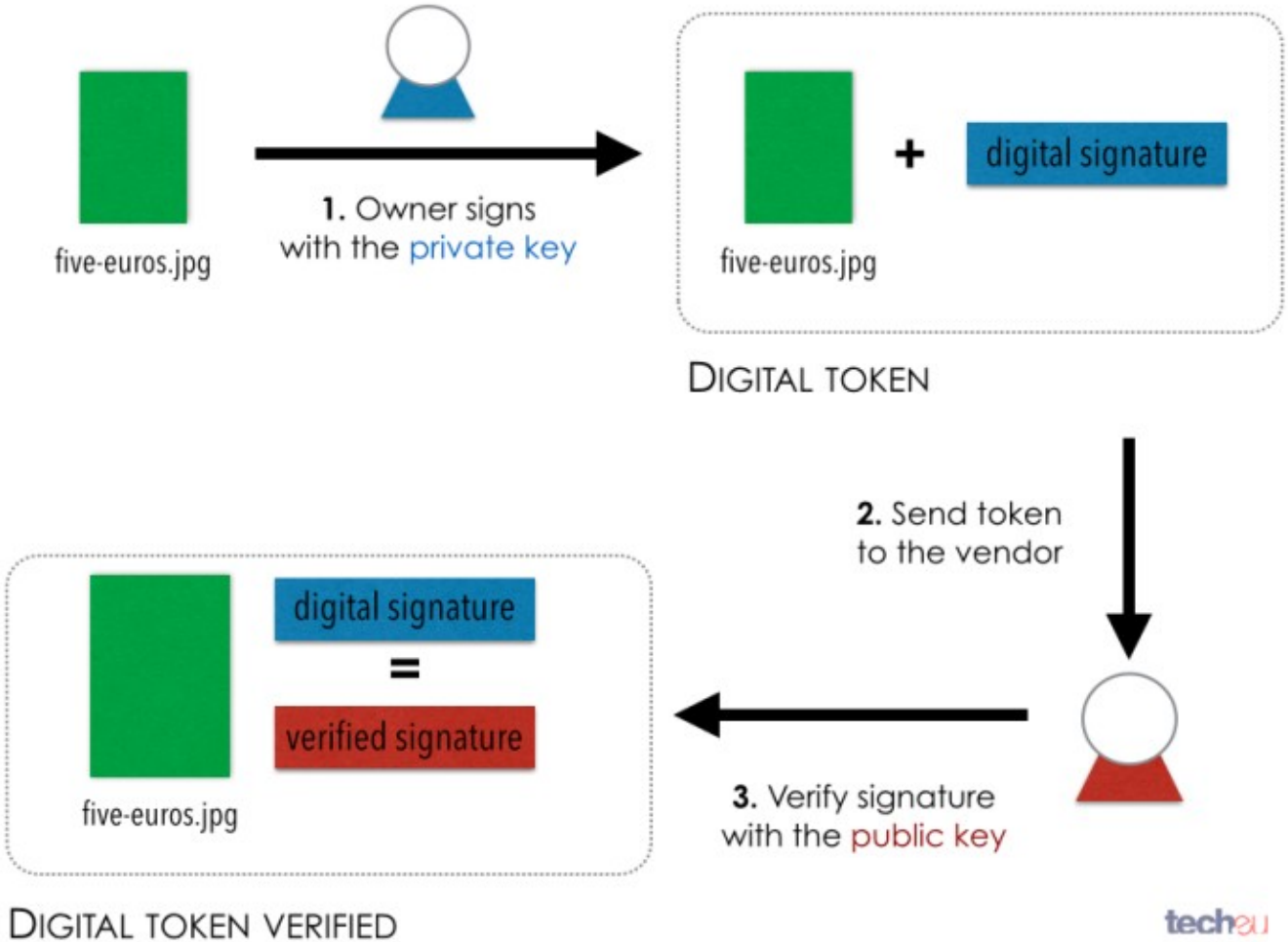
Structure of Bitcoin Block

Field	Description	Size
Magic no	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes
transactions	the (non empty) list of transactions	<Transaction counter>-many transactions

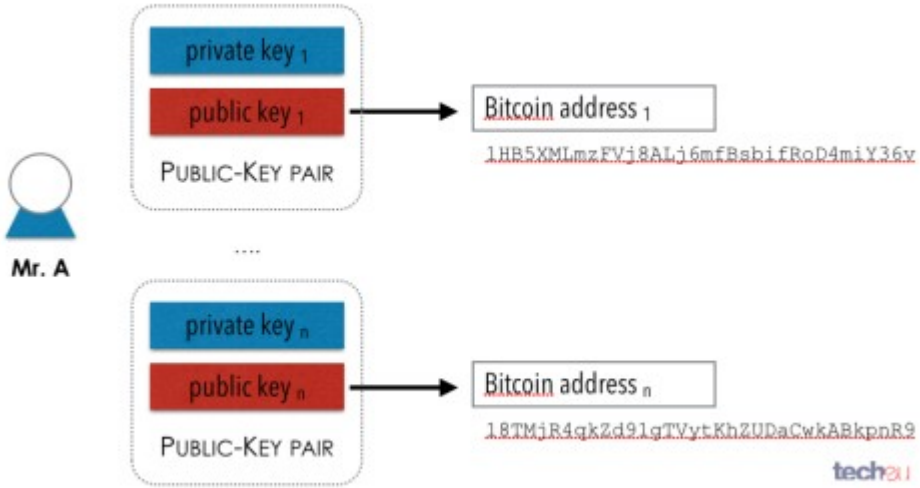
Structure of Bitcoin Blockchain



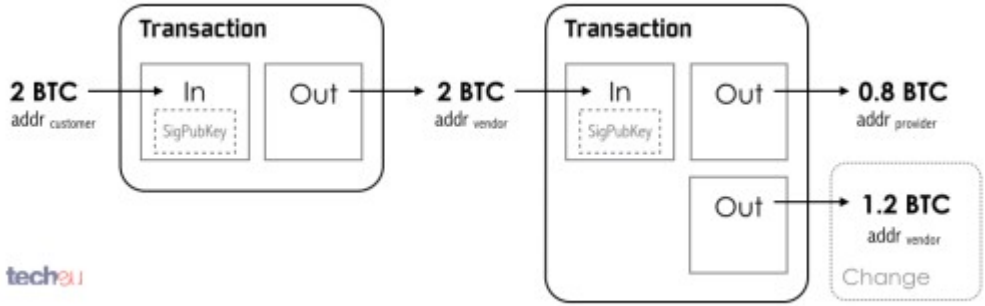
How digital signature algorithms can be used to verify ownership of a digital token



What exactly is Bitcoin?

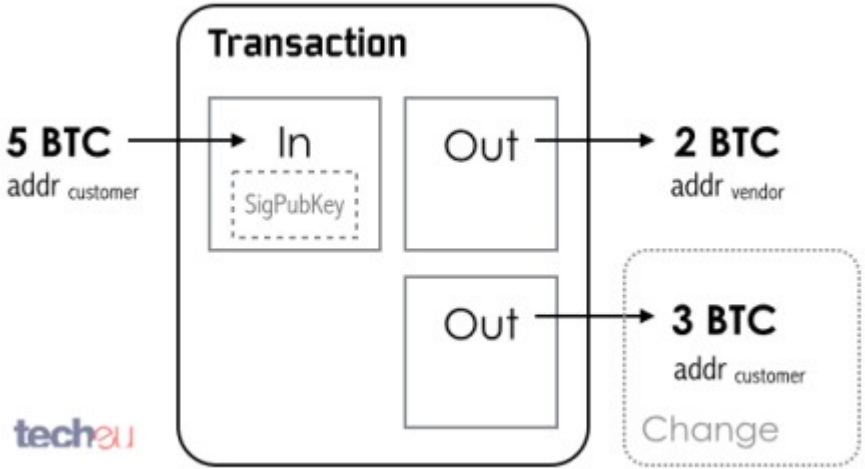


An example of two linked transactions

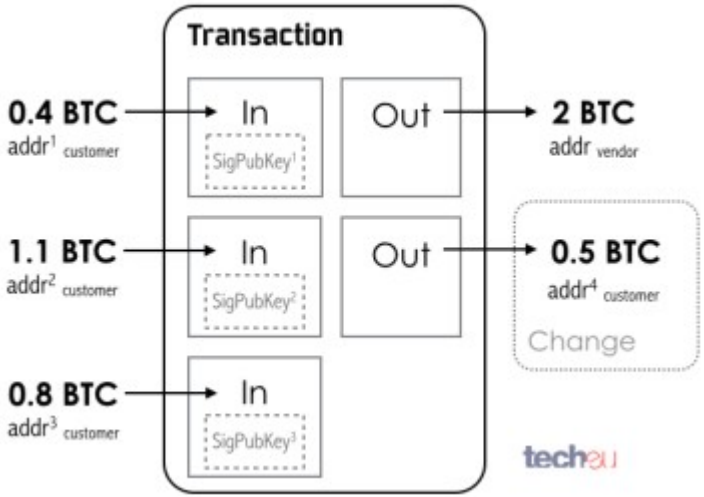


The Bitcoin transactions stored in the Blockchain can be very simple (above), or become very complex with multiple input and output sources (below).

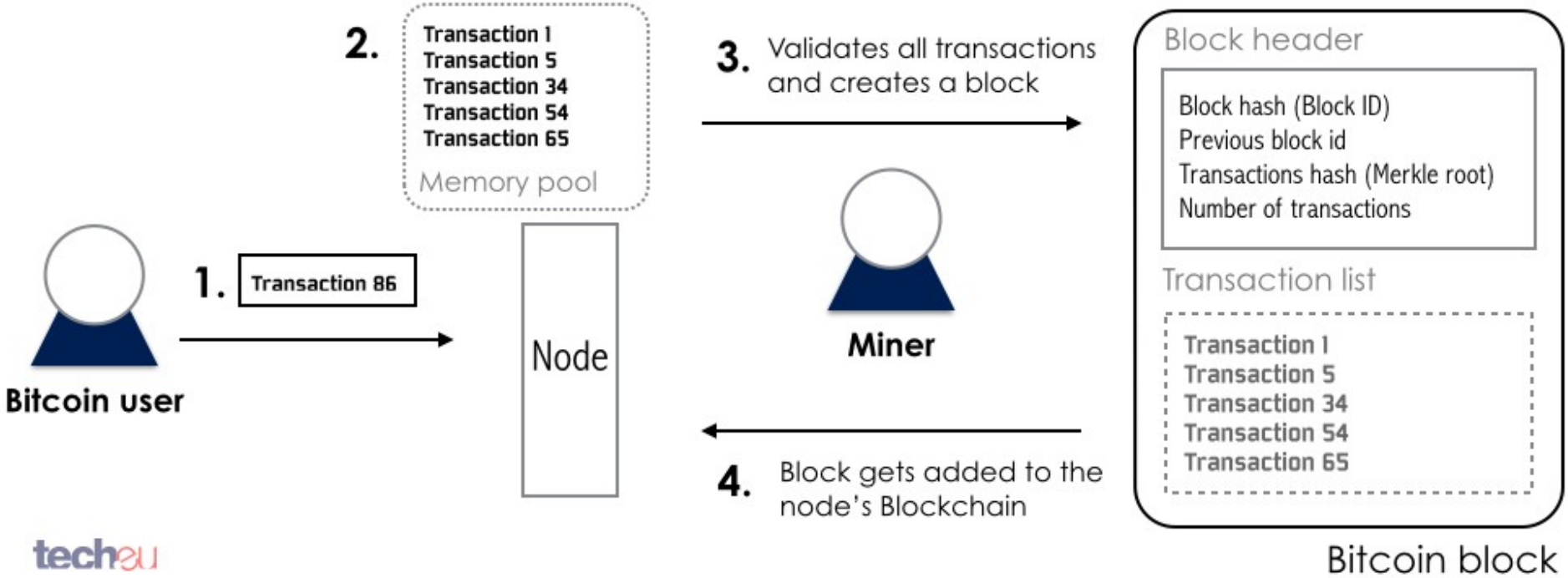
A single input-multiple output Bitcoin transaction



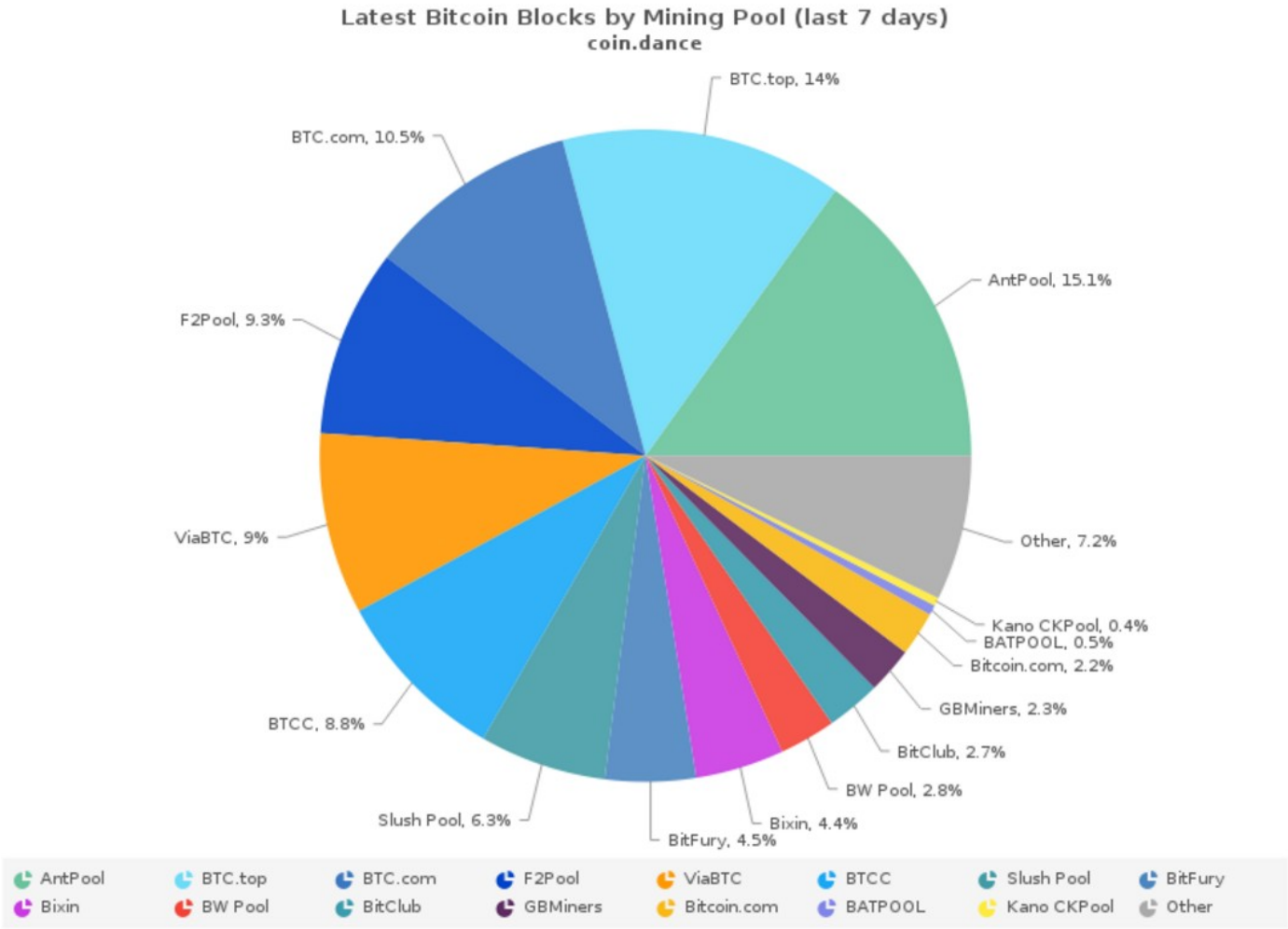
A multiple input-multiple output Bitcoin transaction



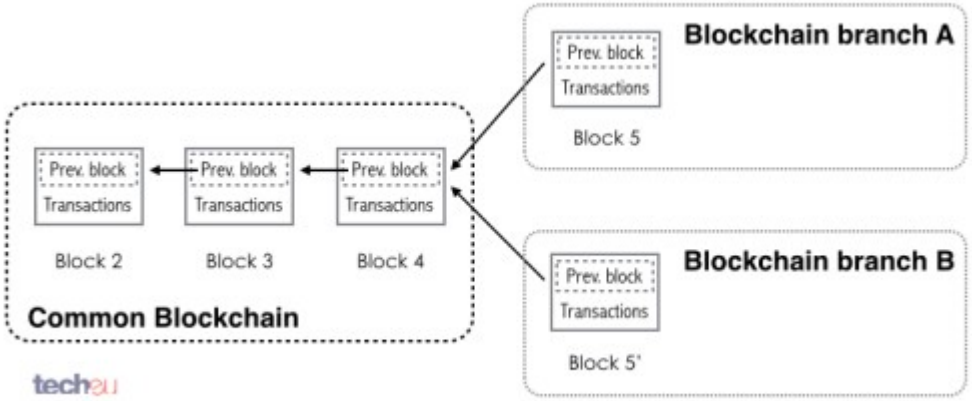
Create a block

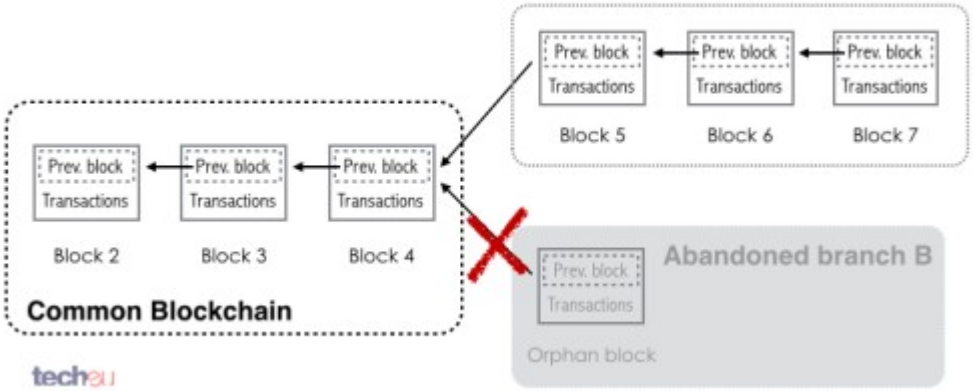


Latest Bitcoin Blocks by Mining Pool



Bitcoin Blockchain fork





Transaction confirmations

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	12yxzhUNfQSPWeDrmwKrWKCxQW2Cz36v3B
Hash 160	15be2967d0e0b0f5ae59b8e66e84dcfc3126cf89
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	0.0029 BTC
Final Balance	0.0029 BTC

Request Payment | Donation Button

Transactions (Oldest First) Filter

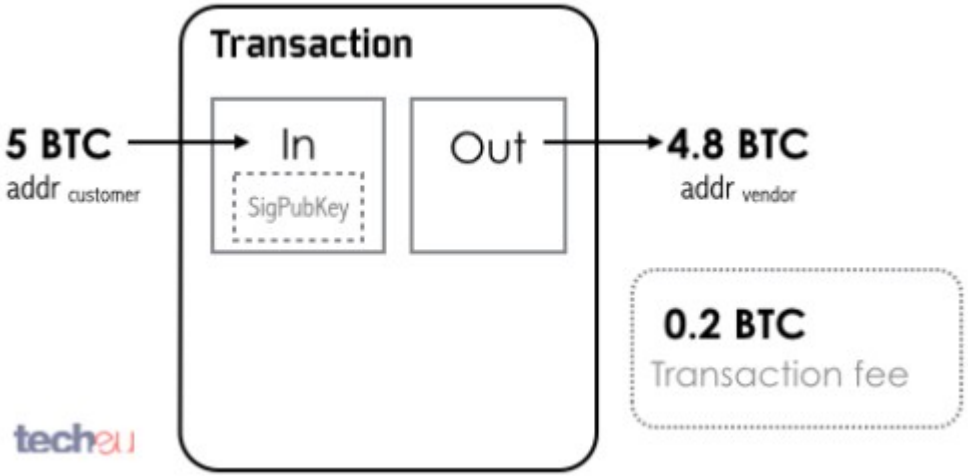
1061b3e85dbe4e6985a6ba650f8222bacc267cd7b5678560e50ee235aba070fa (Fee: 0.0001 BTC - Size: 192 bytes) 2014-05-06 11:40:11

1C8jj1cY2abXmW3LrDoCq8ywPbXEKmyHhz (0.003 BTC - Output) → 12yxzhUNfQSPWeDrmwKrWKCxQW2Cz36v3B - (Unspent) 0.0029 BTC

44 Confirmations | 0.0029 BTC

The reason is that, as seen before, the blockchain might have **a fork**. If we **accept a transaction** before waiting for **at least six confirmations**, it might happen that the network **drops that branch**, effectively rendering the transaction **void**, exposing us to **a fraud situation** or **double spending**.

Transaction fees



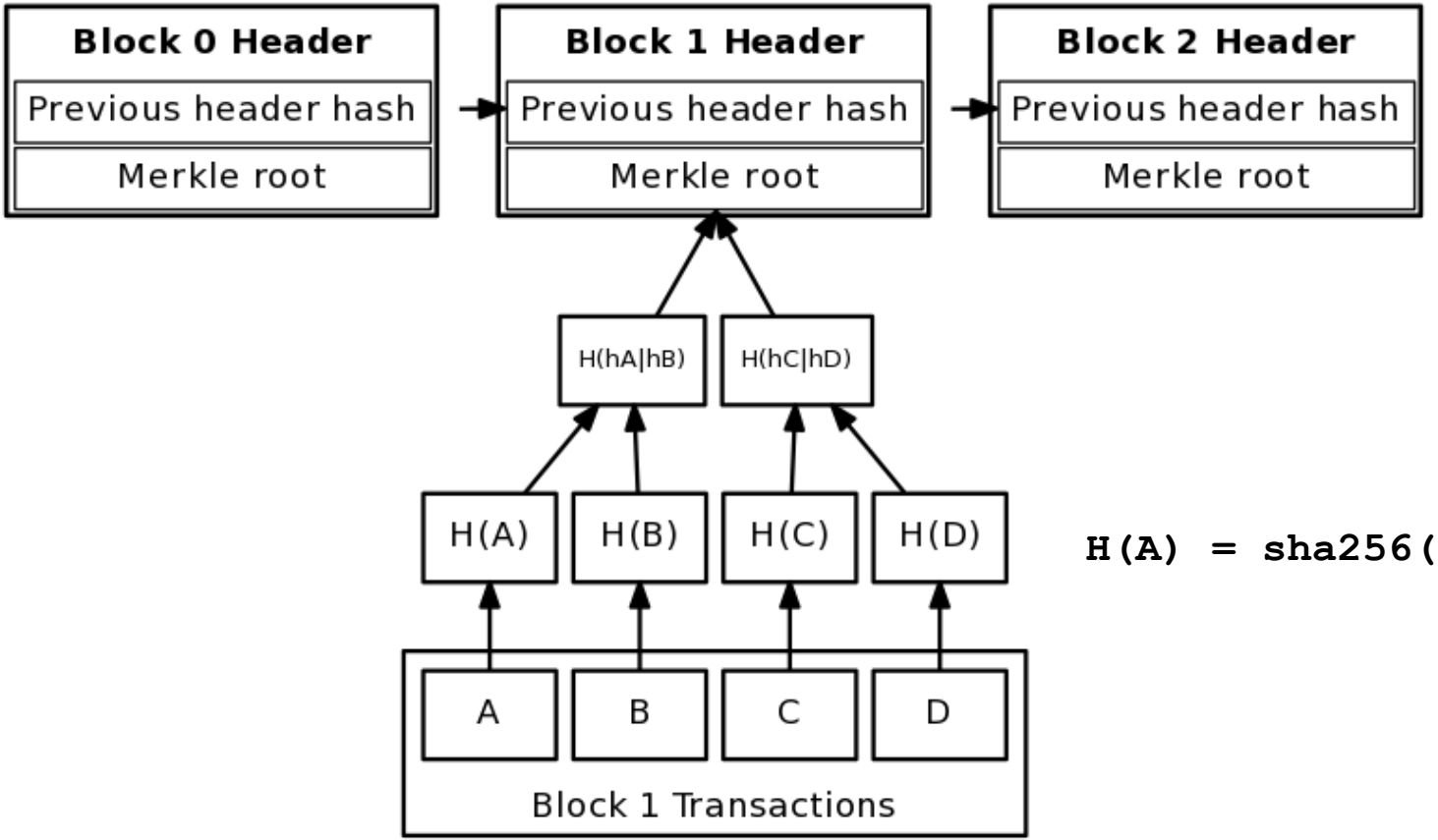
- In theory, every transaction is processed for free.
- However, Bitcoin allows its users to ‘tip’ the miners for validating their transaction.

Types of Proof

- **Proof of Work**
- Proof of Stake
- Proof of Importance
- …

```
payload = <some data related to things happening on the Bitcoin network>
nonce = 1
hash = SHA2( SHA2( payload + nonce ) )
```

Transaction verify: Merkle Tree




```
H(A) = sha256( sha256(A) )
```

Merkle tree connecting block transactions to block header merkle root

What is Bitcoin mining?

payload = <some data related to things happening on the Bitcoin network>

nonce = 1

hash = SHA2(SHA2(payload + nonce))

hash => Target

For example:

Our target is a value beginning with '000'.

"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7

...

"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965

"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6

"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Difficulty and Target

Target represents a number of leading zeroes

Difficulty represents how difficult the current target makes it to find a block

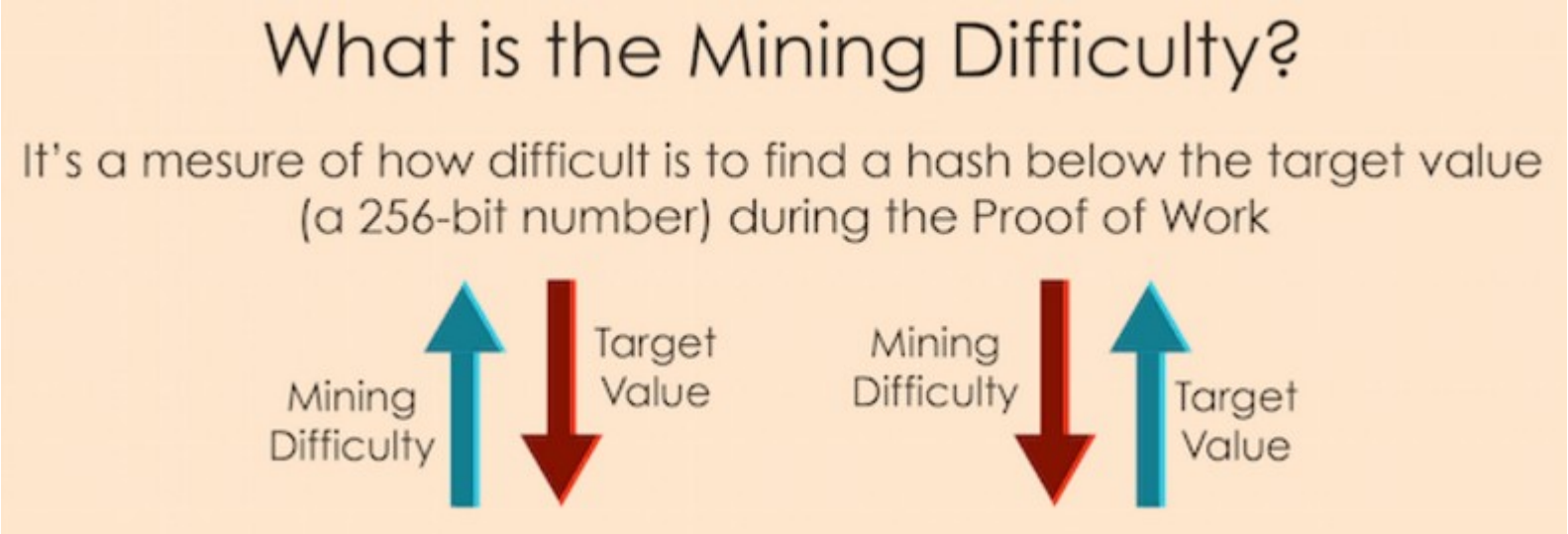
Current difficulty = 1,103,400,932,964 (2017-09-22)

hash = SHA2(SHA2(payload + nonce))

Every 2016th blocks:

- The target is change (re-target).

Difficulty and Target



Difficulty and Target

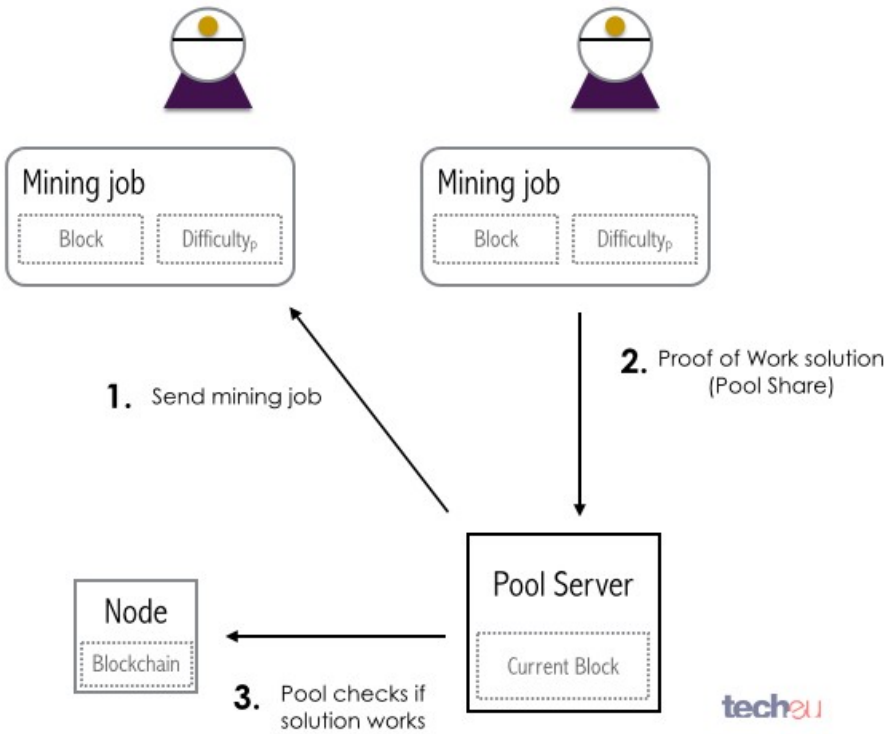
ANTPOOL Home Statistics Coinbase Hashnest Help EN

Block History Solo Ranking

HASHNEST PACMIC V5 Release! 0.45 Satoshi/Secor

Block Height	Time	Block Hash	Value	Status	Duration	Luck	Hashrate	Total Shares
486468	2017-09-22 19:19:24	0000000000000000000362acb1...	13.19513735	6/120	1h 25m 38s	77.89%	1184.05 PH/s	1,416,463,979,234
486461	2017-09-22 17:53:46	0000000000000000000043824bb...	12.52966299	13/120	1h 54m 10s	58.79%	1176.70 PH/s	1,876,711,152,568
486447	2017-09-22 15:59:36	0000000000000000001ec5884...	12.72549537	27/120	2h 43m 29s	41.25%	1171.41 PH/s	2,675,310,805,412
486431	2017-09-22 13:16:07	0000000000000000000071ba706...	12.56043987	43/120	19m 59s	333.36%	1185.75 PH/s	331,017,605,002
486428	2017-09-22 12:56:08	0000000000000000009d6d7ec...	12.65949899	46/120	41m 17s	145.22%	1317.52 PH/s	759,843,098,986
486423	2017-09-22 12:14:51	0000000000000000000e945f85...	13.18348594	51/120	28m 5s	208.72%	1347.52 PH/s	528,660,494,288
486418	2017-09-22 11:46:46	0000000000000000000bd4659e...	14.40516547	56/120	2h 10m 57s	42.73%	1411.49 PH/s	2,582,107,603,496
486405	2017-09-22 09:35:49	0000000000000000000bb6a692...	12.54927704	69/120	22m 8s	203.24%	1755.57 PH/s	542,821,075,202
486401	2017-09-22 09:13:41	0000000000000000002f34ffb...	13.22148771	73/120	10m 7s	394.23%	1980.49 PH/s	279,899,780,754
486400	2017-09-22 09:03:34	0000000000000000000d92b7e8...	13.82759412	74/120	1h 6m 42s	65.37%	1811.31 PH/s	1,687,759,760,634
486395	2017-09-22 07:56:52	0000000000000000000020aac59...	13.02740839	79/120	18m 46s	254.88%	1651.00 PH/s	432,838,834,706
486392	2017-09-22 07:38:06	0000000000000000004a8a1ad...	12.79347552	82/120	46m 58s	90.49%	1858.61 PH/s	1,219,464,624,518
486387	2017-09-22 06:51:08	0000000000000000008e30b98...	12.65165809	87/120	55m 5s	82.18%	1744.80 PH/s	1,342,635,437,546
486381	2017-09-22 05:56:03	0000000000000000000ad2840e...	12.86529619	93/120	45m 15s	100.52%	1736.64 PH/s	1,097,790,961,320

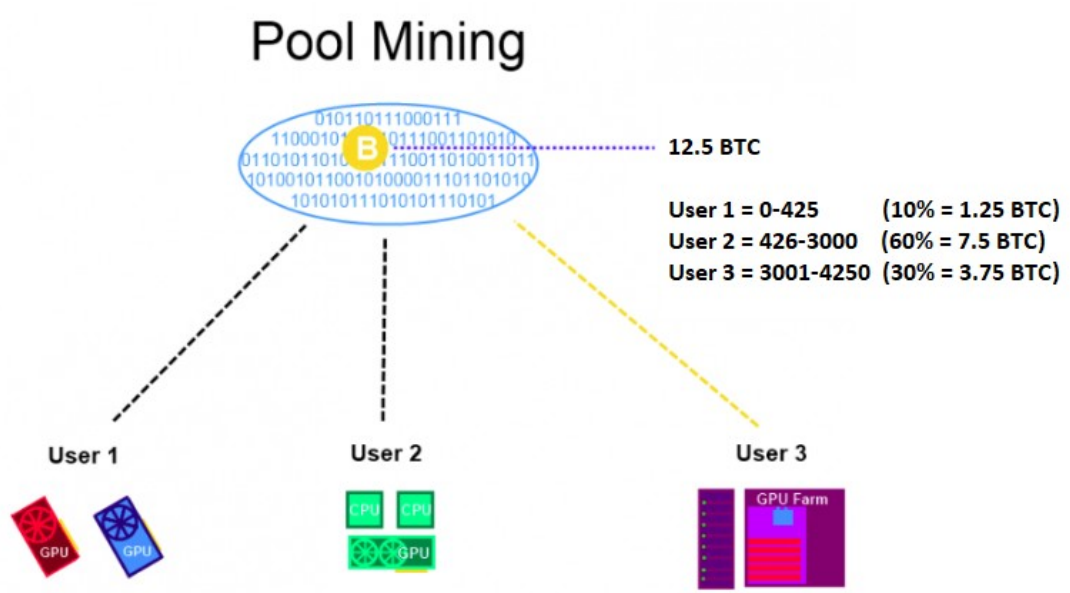
What is a Mining Pool?



1. Taking the pool members hashes
2. Looking for block rewards
3. Recording how much work all the participants are doing
4. Assigning block rewards proportionally to participants

What is a Mining Pool?

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```



Cryptocurrency Mining Types

Types of Mining:

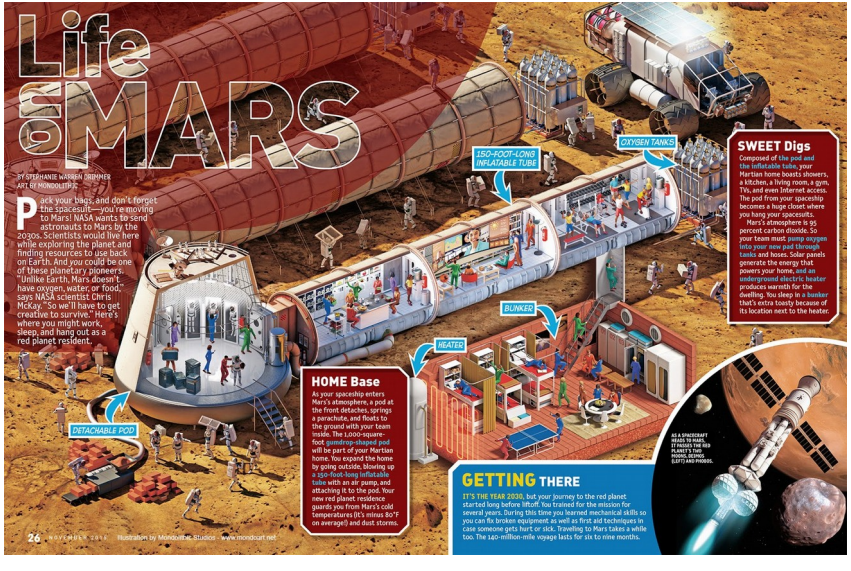
- ASIC Mining
- GPU Mining
- Mining services (Cloud mining)
- HDD Mining
- CPU Mining
- FPGA Mining

Daily electric cost of whole cryptocurrency mining **~ $2,593,721** (2017-09-21)

The value and The future

12.5 cents

20-25% cost: ~ $1000



Bitcoin ATM map

Bitcoin ATM map.

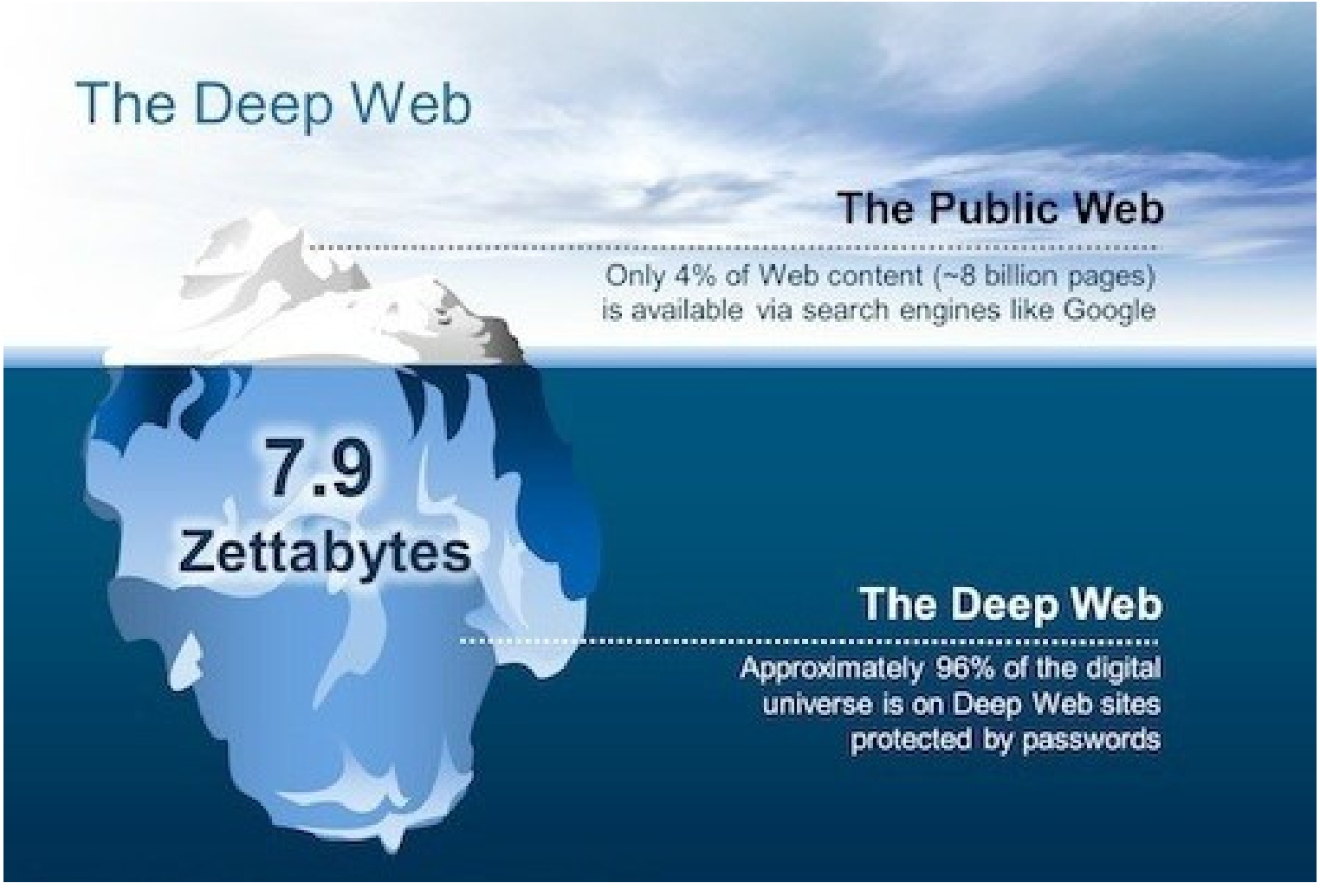
Use our map to find bitcoin or other cryptocurrency ATM locations as well as various alternative crypto-cash exchange services.

1567	40275	59	21	265
Bitcoin ATMs	Other services	Countries	Producers	Operators

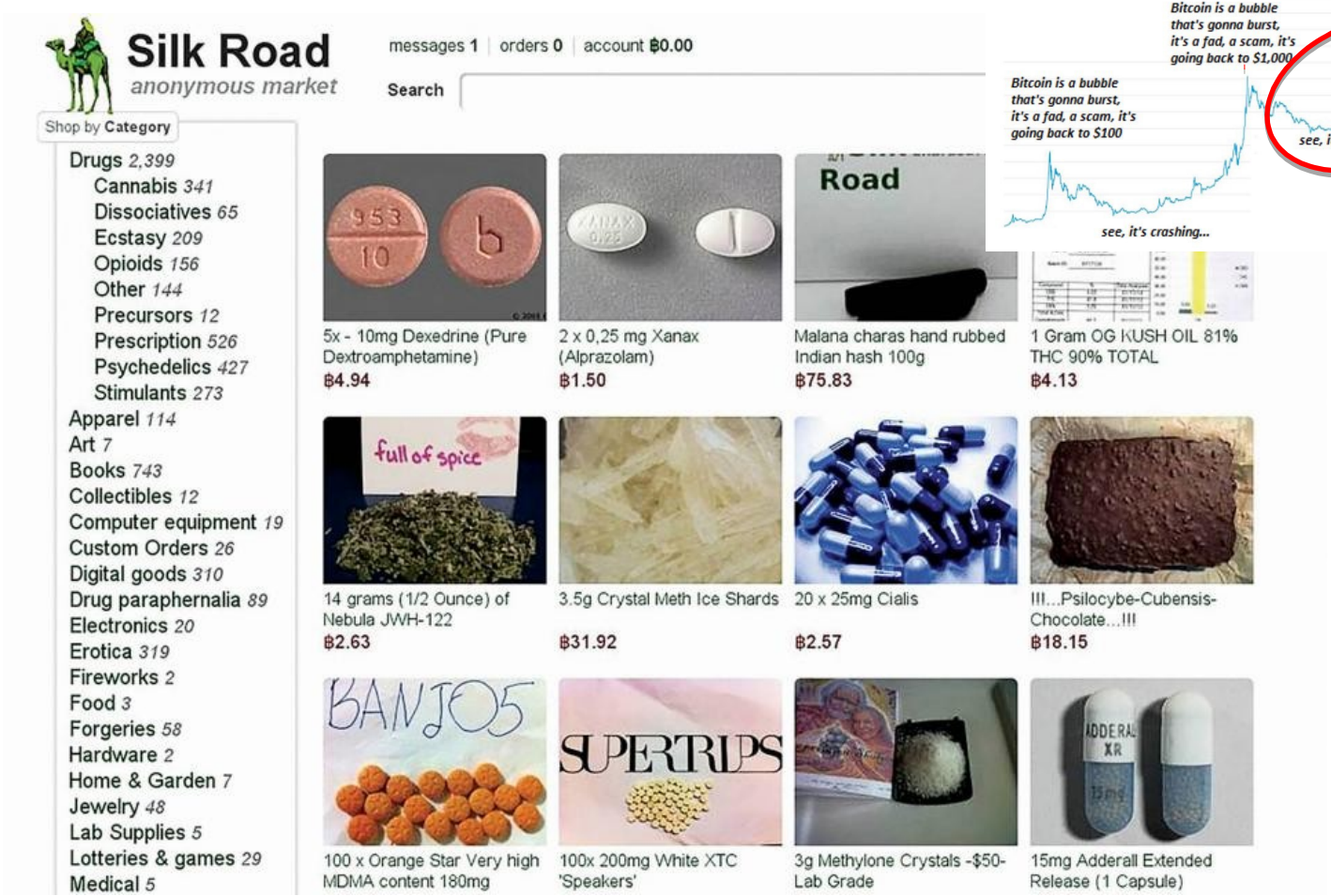
Bitcoin ATM map

Depression of Bitcoin

Depression of Bitcoin



Depression of Bitcoin



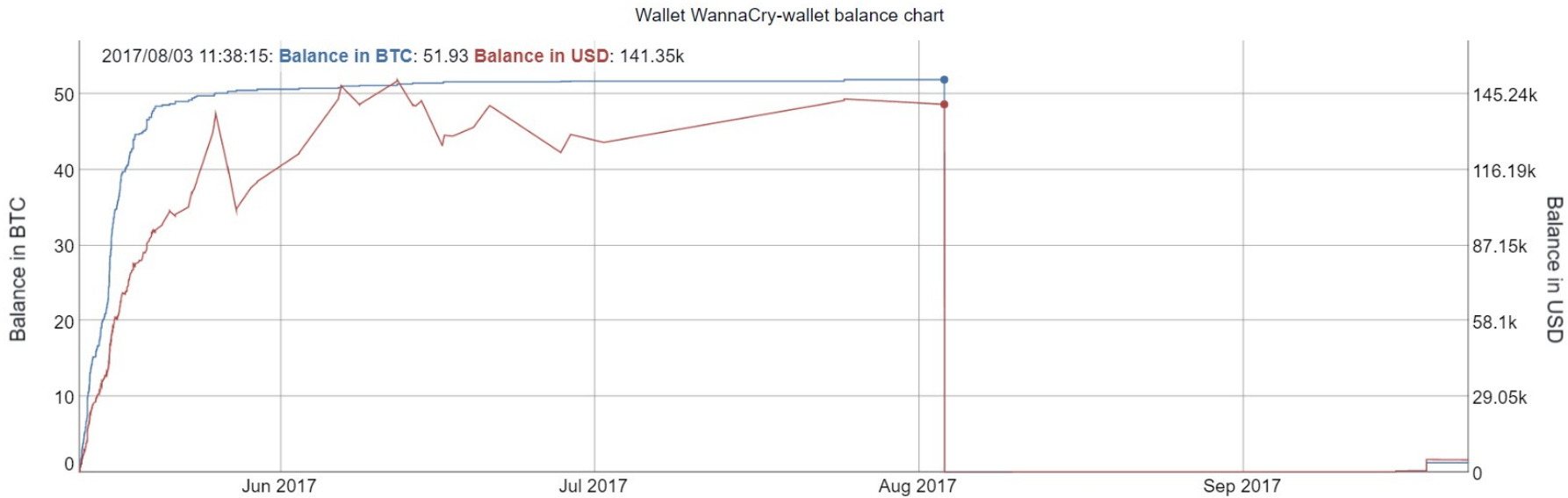
Depression of Bitcoin

Depression of Bitcoin

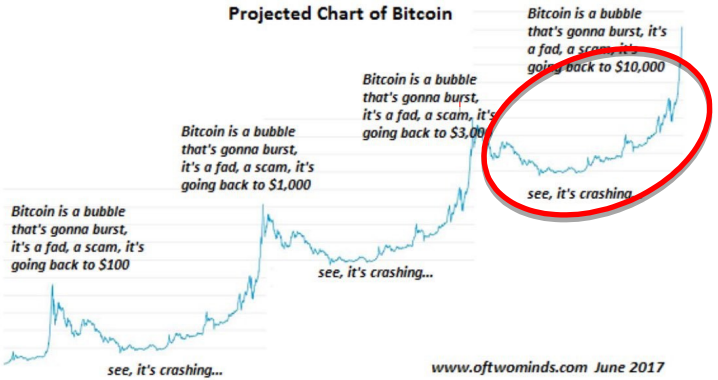
1.28658268 BTC			0.0000078% of all coins
Balance: 4,816.09 USD			
Received	count: 355	first: 2017-05-12 19:08:21	last: 2017-09-18 12:56:09
Sent	count: 352	first: 2017-08-03 11:39:15	last: 2017-08-03 12:41:34
Unspent	count: 3		

.com June 2017

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn



Depression of Bitcoin



Maybe come other reasons!!

FinTech: Global FinTech Survey 2017

Source: https://www.pwc.com/gx/en/advisory-services/FinTech/pwc-fintech-global-report.pdf

What is Blockchain Technology?

1991

by **Stuart Haber and W. Scott Stornetta**, The first work on a cryptographically secured chain of blocks was described.

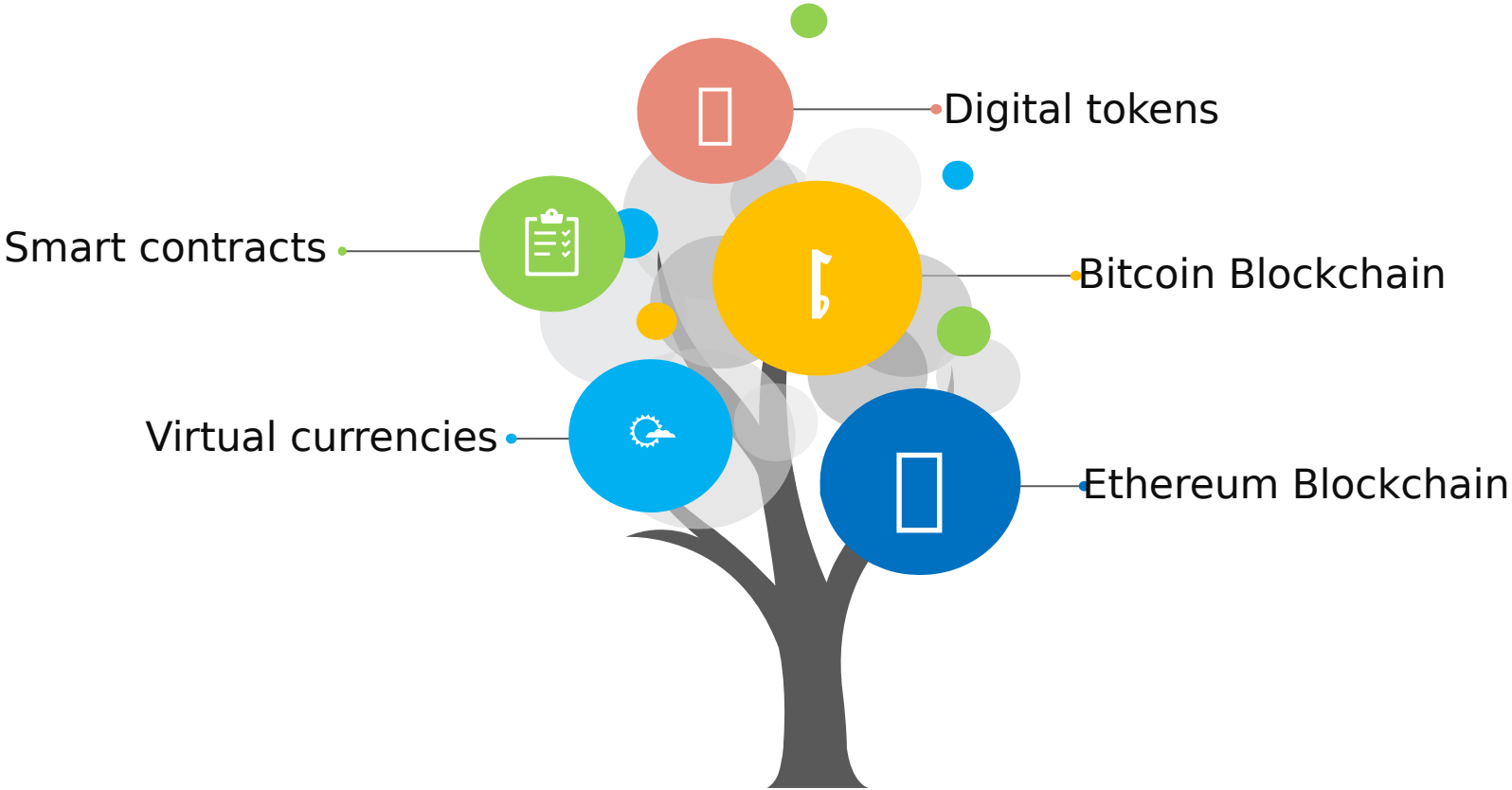
1992

Bayer, Haber and Stornetta, incorporated **Merkle trees** to the **blockchain** as an efficiency improvement to be able to collect several documents into one block.

2008

Satoshi Nakamoto, The **first distributed blockchain** was then **conceptualised** and **implemented** the following year as a core component of the digital currency bitcoin, where it serves as the public ledger for all transactions.

What is Blockchain Technology?



about **distributed ledgers / replicated database**

What is Blockchain Technology?

The common themes seem to be a **data store** which:

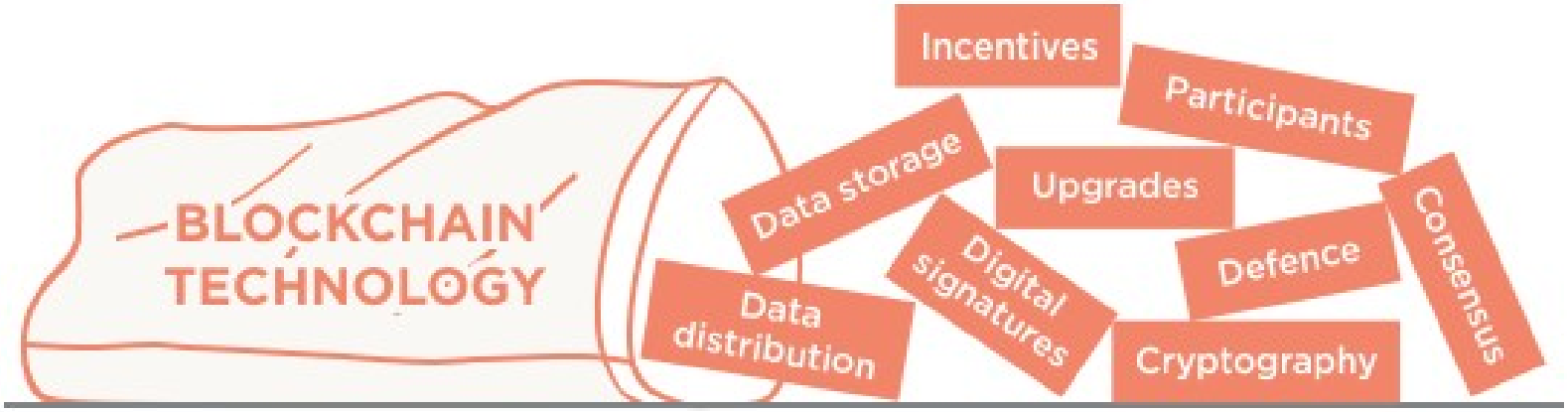
- usually contains **financial transactions**
- is replicated across **a number of systems** in almost **real-time**
- usually exists over a **peer-to-peer** network
- uses **cryptography** and **digital signatures** to prove identity, authenticity and enforce read/write access rights
- can be **written** by certain participants
- can be **read** by certain participants, maybe a wider audience, and
- has mechanisms to make it **hard to change historical records**, or at least make it easy to detect when someone is trying to do so

What is Blockchain Technology?

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

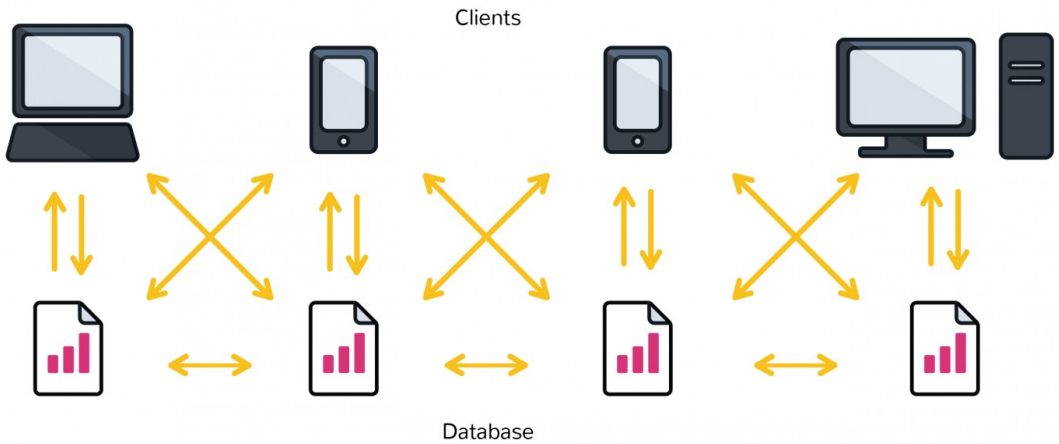
Don & Alex Tapscott, authors Blockchain Revolution (2016)

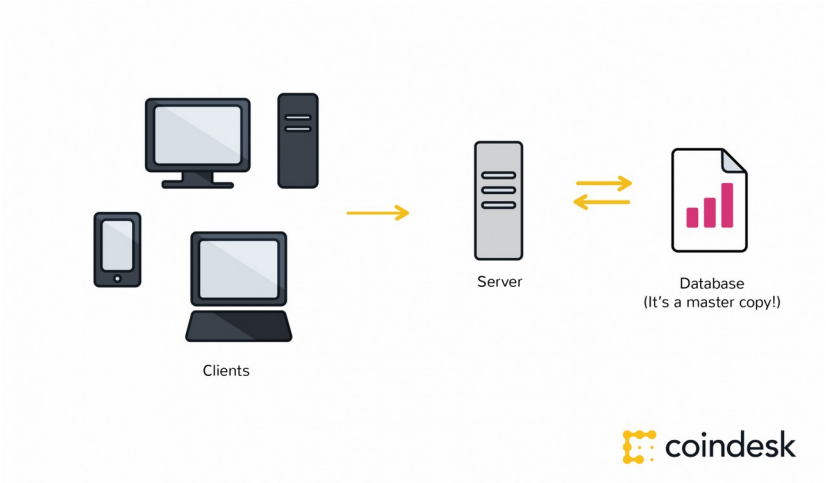
What is Blockchain Technology?



Blockchains are built from 3 technologies		
1. Private Key Cryptography	**2. P2P Network**	**3. Program (the blockchain's protocol)**
Cash vs. Plastic	Tree falls in a forest	Tragedy of the commons
Identity	**System of Record**	**Platform**

A distributed database





What is Blockchain Technology?

Public blockchains. Ledgers can be ‘public’ in two senses:

1. Anyone, without permission granted by another authority, can **write** data
2. Anyone, without permission granted by another authority, can **read** data

it needs

- ways of arbitrating discrepancies (there is no ‘boss’ to decide)
- defense mechanisms against attacks

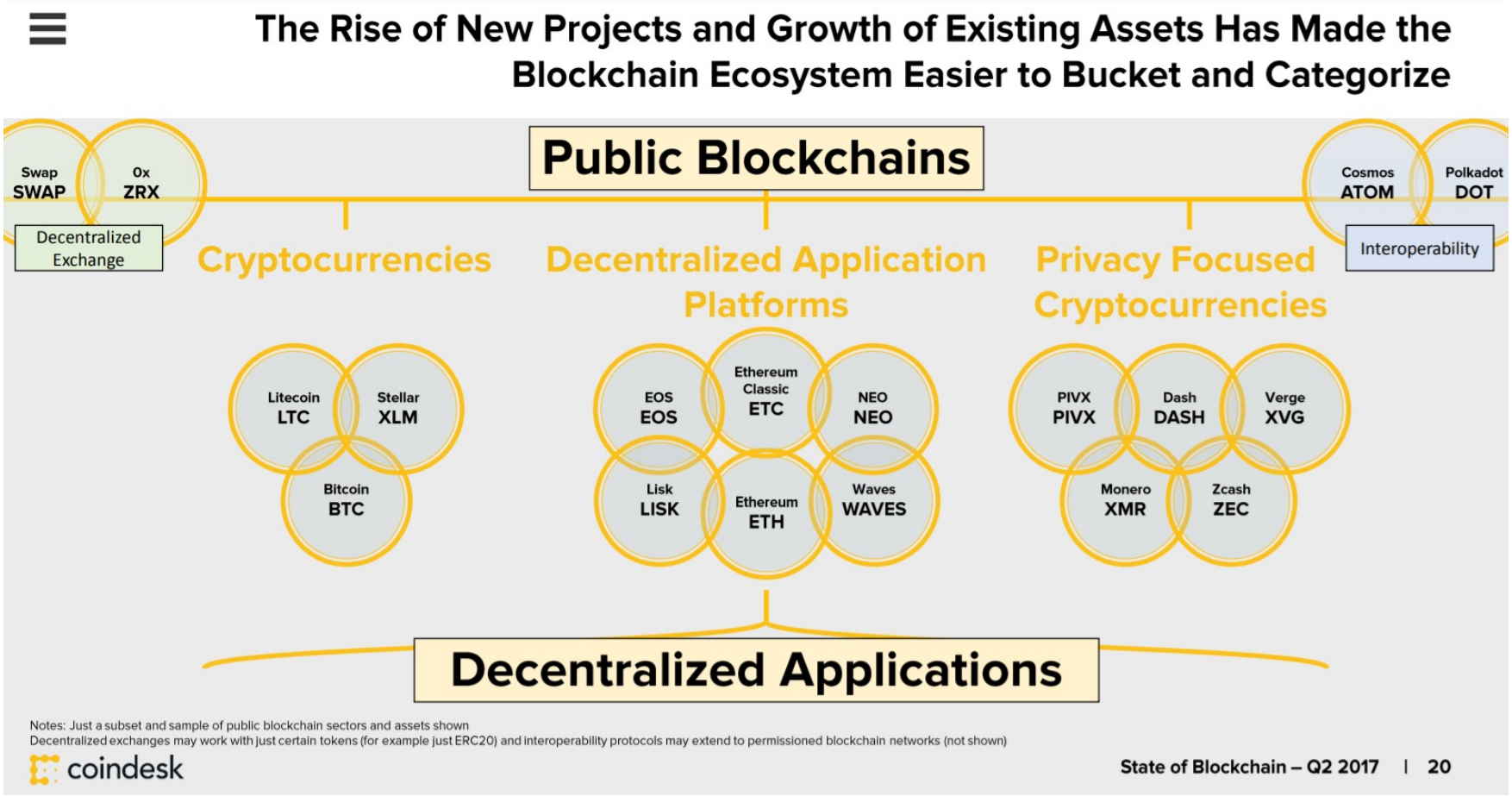
Private blockchains. Conversely

The participants are known and trusted: for example, an industry group, or a group of companies owned by an umbrella company.

Many of the mechanisms aren’t needed

or rather they are replaced with legal contracts – “You’ll behave because you’ve signed this piece of paper.”.

What is Blockchain Technology?



Blockchain Durability and Robustness

- **Blockchain technology is like the internet in that it has a built-in robustness.**

- By storing blocks of information that are identical across its network, **the blockchain cannot:**
    1. **Be controlled by any single entity.**
    2. **Has no single point of failure.**

- Bitcoin was invented in 2008. Since that time, **the Bitcoin blockchain has operated without significant disruption.** (To date, any of problems associated with Bitcoin have been due to hacking or mismanagement. In other words, these problems come from bad intention and human error, not flaws in the underlying concepts.)

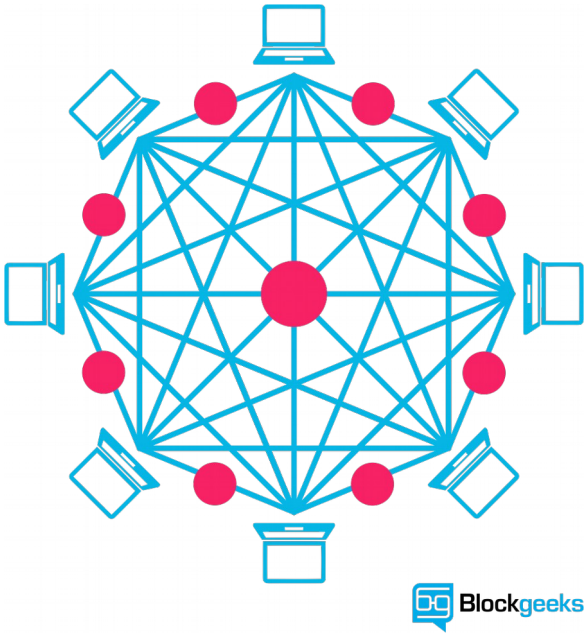
- **The internet itself has proven to be durable for almost 30 years.** It’s a track record that bodes well for blockchain technology as it continues to be developed.

Transparent and Incorruptible

- The blockchain network lives in a state of consensus, one that automatically checks in with **itself every ten minutes.**
- A kind of self-auditing ecosystem of a digital value, the network **reconciles** every transaction that happens in ten-minute intervals.
- **Each group of these transactions is referred to as a "block".** Two important properties result from this:
    - **Transparency**
      data is embedded within the network as a whole, by definition it is public.
    - **It cannot be corrupted**
      altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.

- **In theory,** this could be possible. **In practice,** it's unlikely to happen. Taking control of the system to capture Bitcoins, for instance, would also have the effect of destroying their value.

A network of nodes

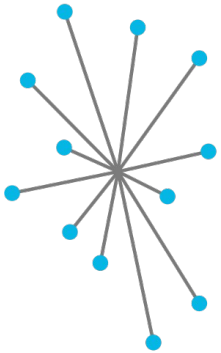


A network of so-called computing “nodes” make up the blockchain.

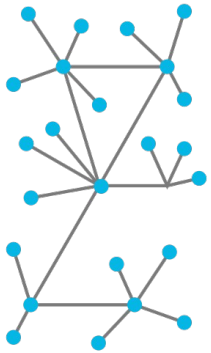
Node
(computer connected to the blockchain network using a client that performs the task of validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the blockchain network.

The Blockchain Network

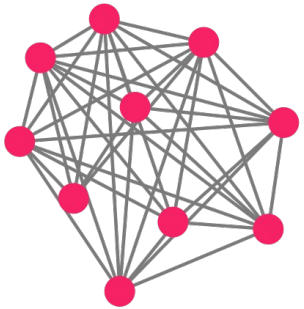
Centralized

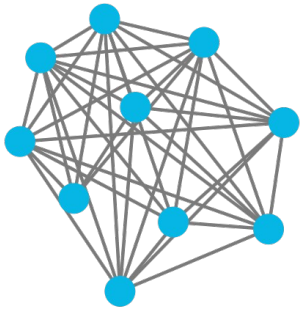


Decentralized



Distributed Ledgers





The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

Blockgeeks

A second-level network

- With blockchain technology, **the web gains a new layer of functionality.**

- Already, users can transact directly with one another — **Bitcoin transactions in 2017 averaged over $ 1,902,258,076 US per day.**

- **With the added security brought by the blockchain new internet business** are on track to unbundle the traditional institutions of finance.

- Goldman Sachs believes that blockchain technology holds great potential especially to optimize clearing and settlements, and could represent global savings of up to $6bn per year.

The Blockchain a New Web 3.0?

- Smart contracts
- The sharing economy
- Crowdfunding
- Governance
- Supply chain auditing
- File storage
- Prediction markets
- Protection of intellectual property
- Internet of Things (IoT)
- Neighbourhood Microgrids
- Identity management
- AML and KYC
- Data management
- Land title registration
- Stock trading

MORE DEPTH, PLEASE

DATA STORAGE: What is a blockchain?

A blockchain is just a file.

Blocks in a chain = pages in a book

For analogy, a book is a chain of pages. Each page in a book contains:

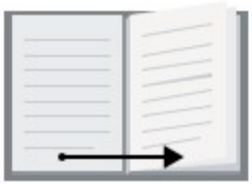
the text: for example the story

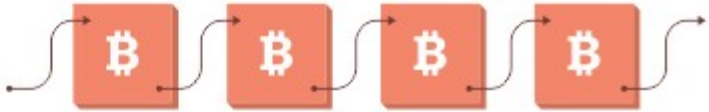
information about itself: at the top of the page there is usually the title of the book and sometimes the chapter number or title; at the bottom is usually the page number which tells you where you are in the book. This ‘data about data’ is called meta-data.

Similarly in a blockchain block, each block has:

the contents of the block, for example in bitcoin is it the bitcoin transactions, and the miner incentive reward (currently 25 BTC).

a ‘header’ which contains the data about the block. In bitcoin, the header includes some technical information about the block, a reference to the previous block, and a fingerprint (hash) of the data contained in this block, among other things. This hash is important for ordering





Block ordering in a blockchain

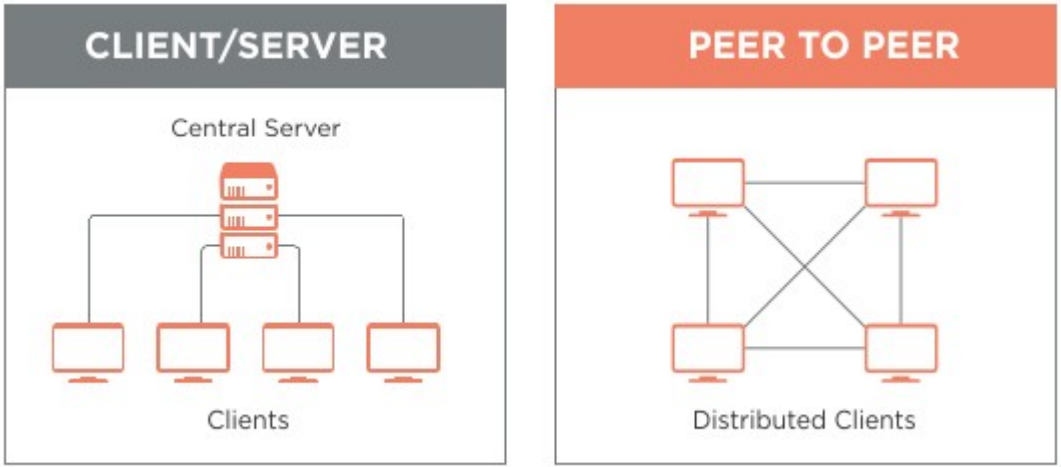
Page by page. With books, predictable page numbers make it easy to know the order of the pages. If you ripped out all the pages and shuffled them, it would be easy to put them back into the correct order where the story makes sense.

Block by block. With blockchains, 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.

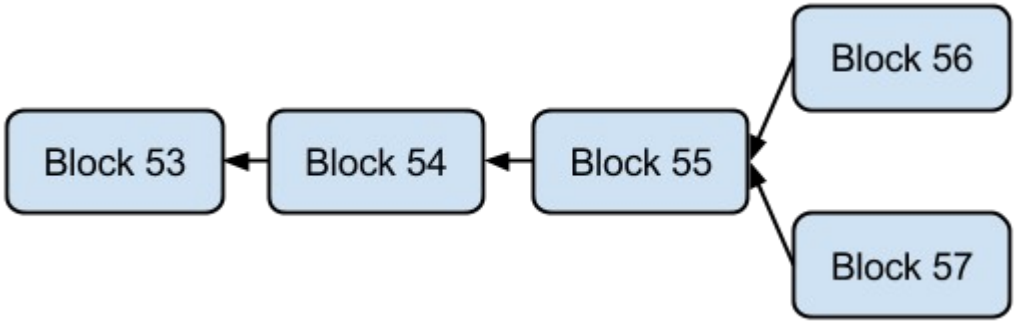
BOOK ORDERING	BLOCK ORDERING
Page 1, 2, 3, 4, 5	Block n58uf0 built on 84n855, Block 90fk5n built on n58uf0, Block 8n6d7j built on 90fk5n.
Implicit that the page builds on the page whose number is one less. eg Page 5 builds on page 4 (5 minus 1).	84n855, n58uf0, 90fk5n, 8n6d7j represent fingerprints or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

Internal consistency

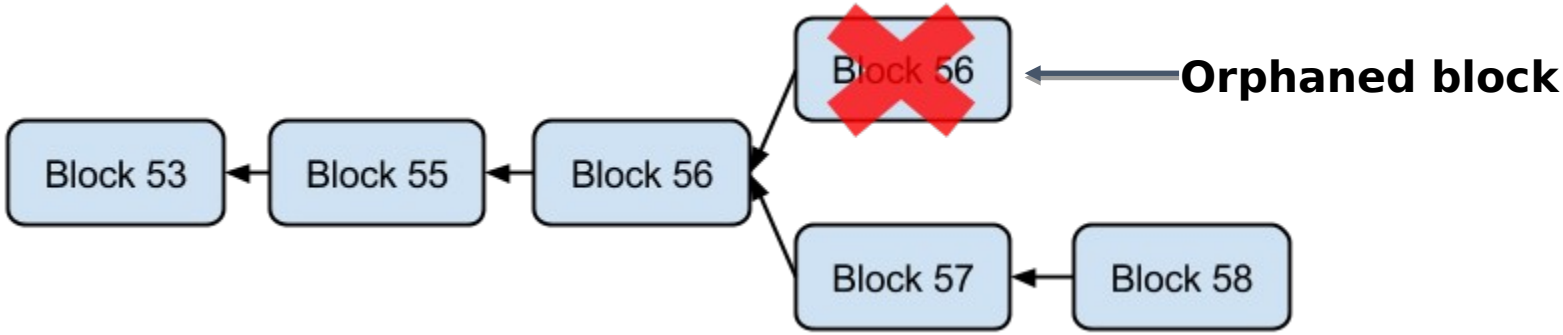
DATA DISTRIBUTION: How is new data communicated?

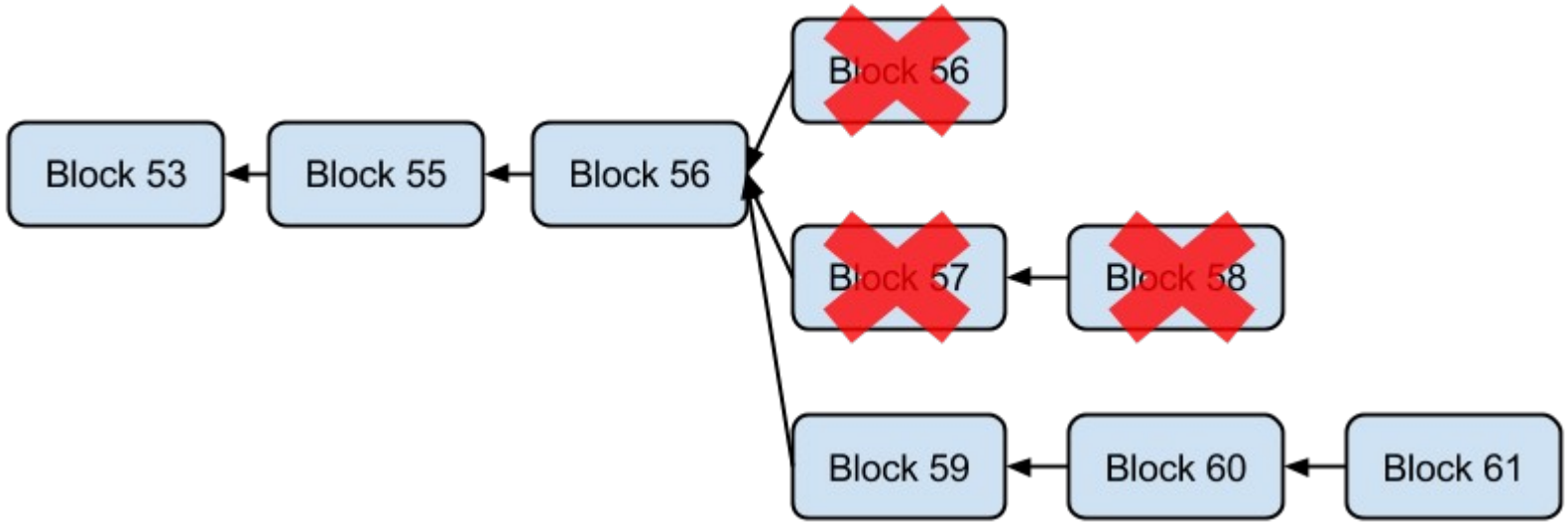


CONSENSUS: How do you resolve conflicts?

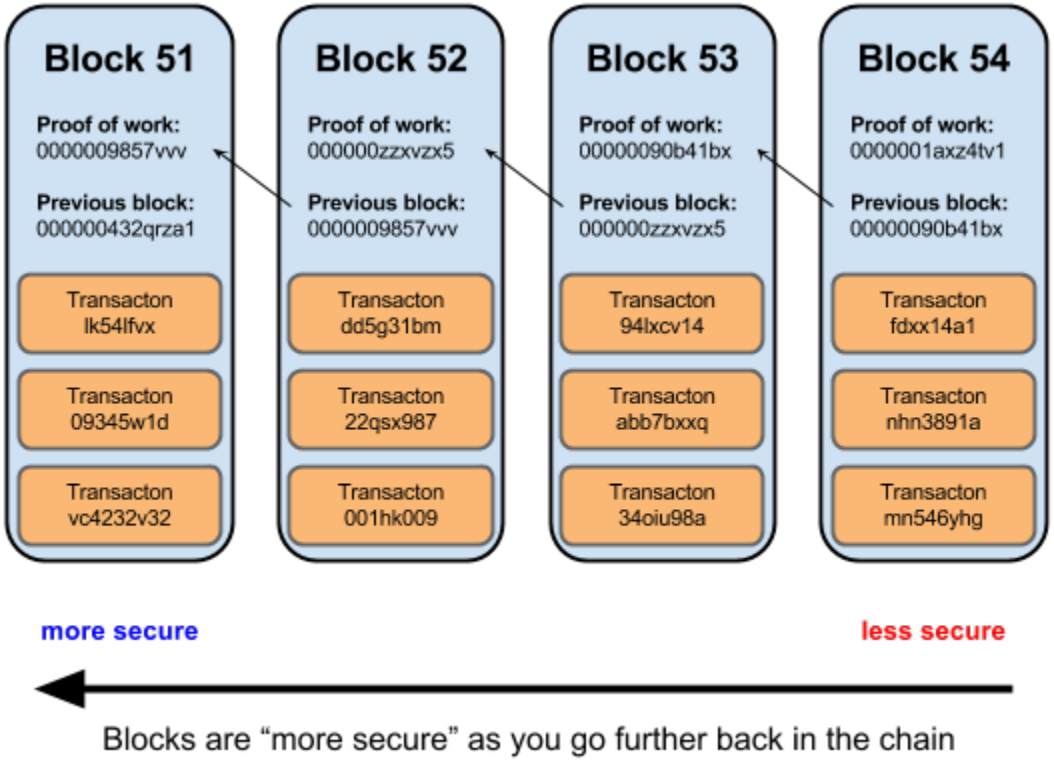


Longest chain rule.





Which block is more secure?



Blocks are “more secure” as you go further back in the chain

UPGRADES: How do you change the rules?

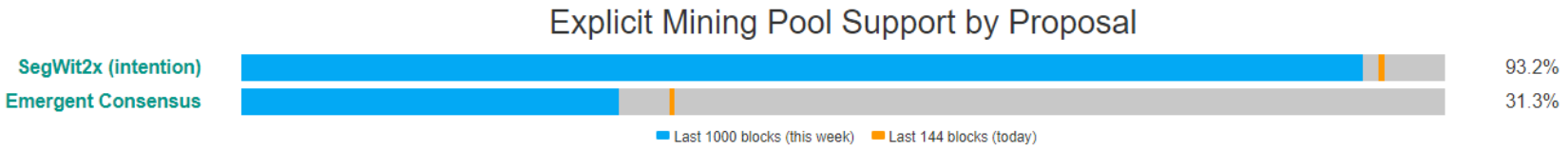
In a private, controlled network where someone has control over upgrades, this is an easy problem to solve: “Everyone must upgrade to the new logic by 31 July”.

However **in a public**, uncontrolled network, it’s a more challenging problem.

With bitcoin, there are two parts to upgrades.

1. **Suggest the change (BIPs).** First, there is the proposal stage where improvements are proposed, discussed, and written up. A proposal is referred to as a **“BIP” – a “Bitcoin Improvement Proposal”.** If it gets written into the Bitcoin core software on Github, it can then form part of an upgrade – the next version of “Bitcoin core” which is the most common “reference implementation” of the protocol.
2. **Adopt the change (miners).** The upgrade can be downloaded by nodes and block makers (miners) and run, but only if they want to (you could imagine a change which reduces the mining reward from 25 BTC per block to 0 BTC. We’ll see just how many

Who controls the Bitcoin network?



bitcoin

2017-07-23

$62B

$7B

1 BTC = $3768.96

1 BCC = $426.80

bitcoin cash

ethereum

2016-07-23

$26B

$1B

1 ETH = $277.50

1 ETC = $10.67

ethereum classic

WRITE ACCESS: How do you control who can write data?

In the bitcoin network, theoretically anyone can download or write some software and start validating transactions and creating blocks

Your computer will act as a full node which means:

- Connecting to the bitcoin network
- Downloading the blockchain
- Storing the blockchain
- Listening for transactions
- Validating transactions
- Passing on valid transactions
- Listening for blocks
- Validating blocks
- Passing on valid blocks
- Creating blocks
- ‘Mining’ the blocks

DEFENCE: How do you make it hard for baddies?

A problem with a permissionless, or open networks is that they can be attacked by anyone. So there needs to be a way of making the network-as-a-whole trustworthy, even if specific actors aren't.

What can and can't miscreants do?

A dishonest miner can:

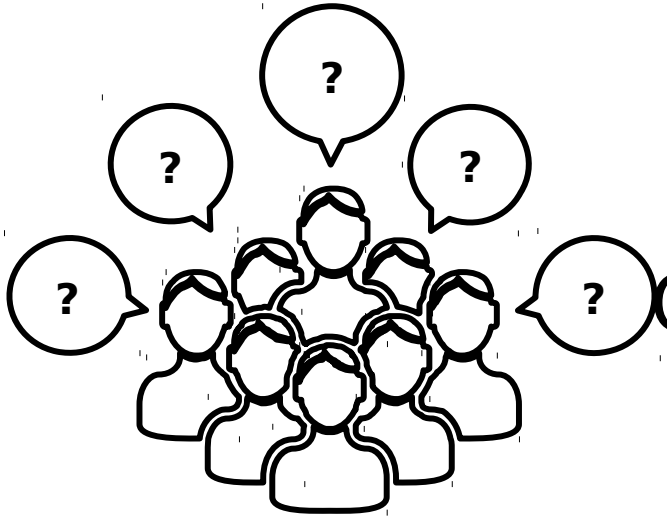
1. Refuse to relay valid transactions to other nodes
2. Attempt to create blocks that include or exclude specific transactions of his choosing
3. Attempt to create a 'longer chain' of blocks that make previously accepted blocks become 'orphans' and not part of the main chain

He can't:

4. Create bitcoins out of thin air*
5. Steal bitcoins from your account
6. Make payments on your behalf or pretend to be you

That's a relief.

Thanks for paying attention



Questions And Answers