The STEM Behind BitCoin

At UHCL Math Center

Kwok-Bun Yue
Professor of Computer Science
February 8, 2018

University of Houston Clear Lake

UHCL

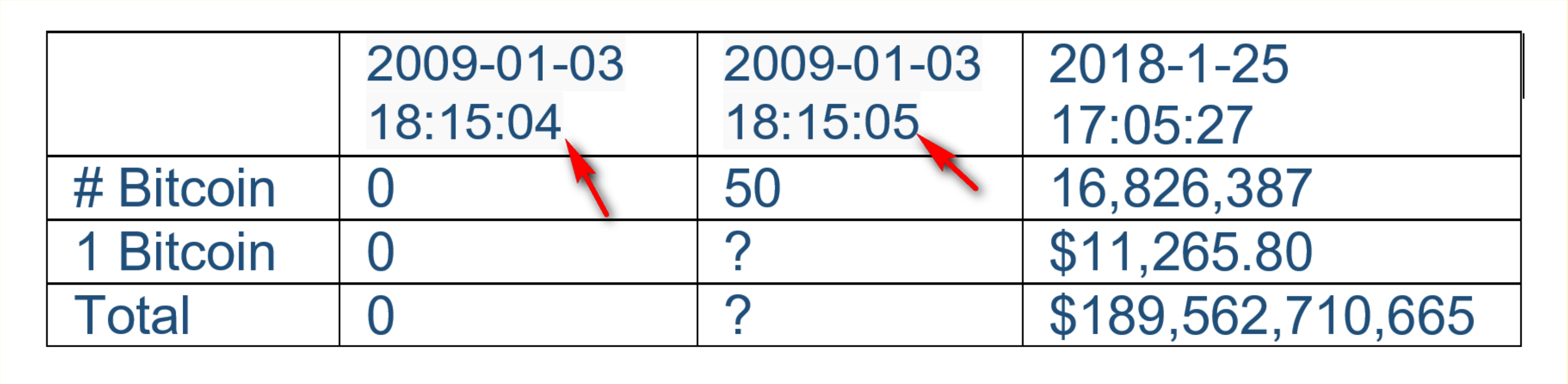
The choice is clear.

Contents

1. Bitcoin – Buzz, Bubble, and/or Beauty?
2. Bitcoin basics
3. A technical peek into Bitcoin
4. Conclusions

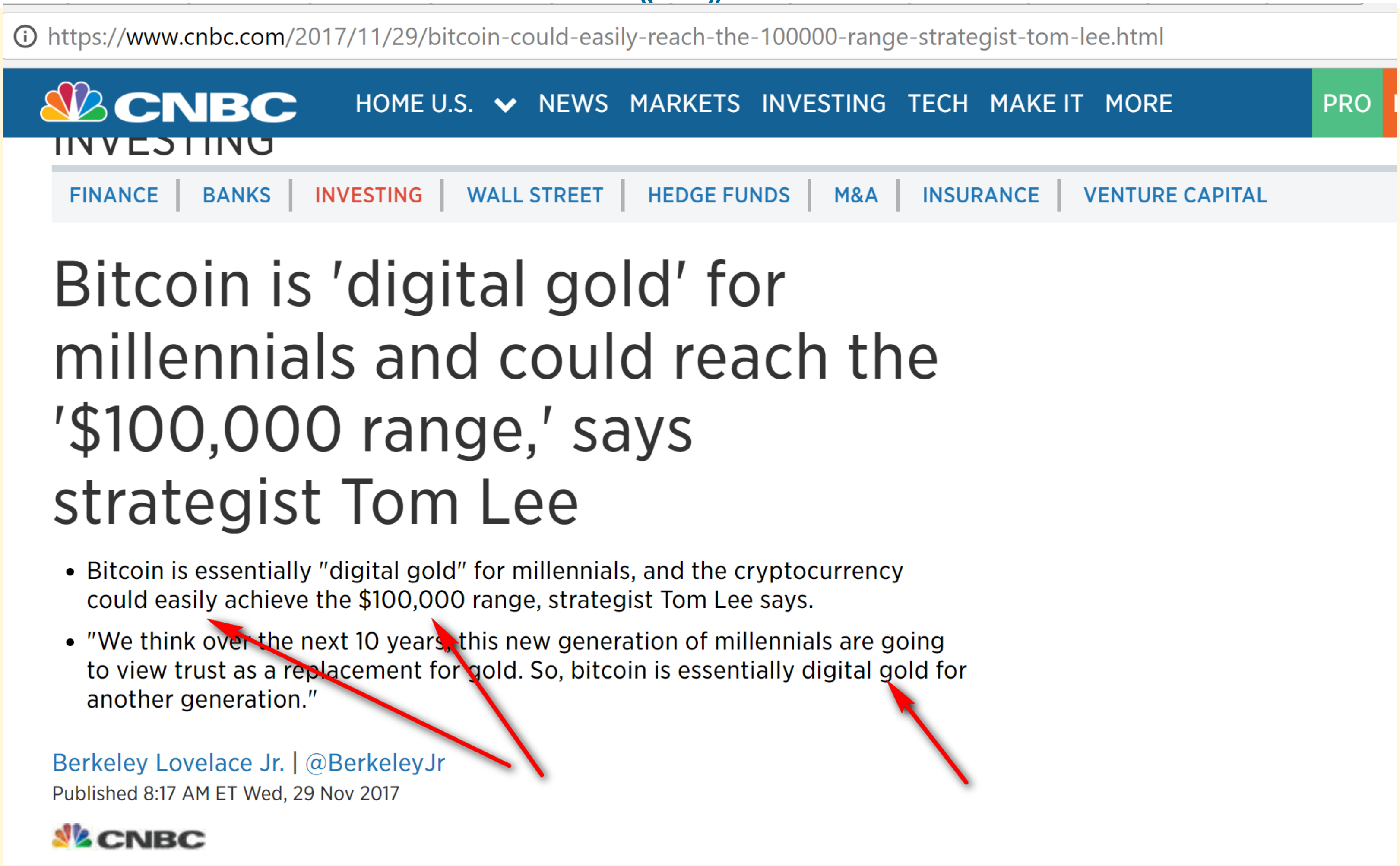
Bitcoin – Buzz, Bubble, and/or Beauty?

1. Pulling money out of thin air!
2. *Genesis block* created on 1/3/2009
3. First real world transaction: 10,000 BTC for 2 pizzas on 5/22/2010



	2009-01-03 18:15:04	2009-01-03 18:15:05	2018-1-25 17:05:27
# Bitcoin	0	50	16,826,387
1 Bitcoin	0	?	$11,265.80
Total	0	?	$189,562,710,665

Buzz/Hype



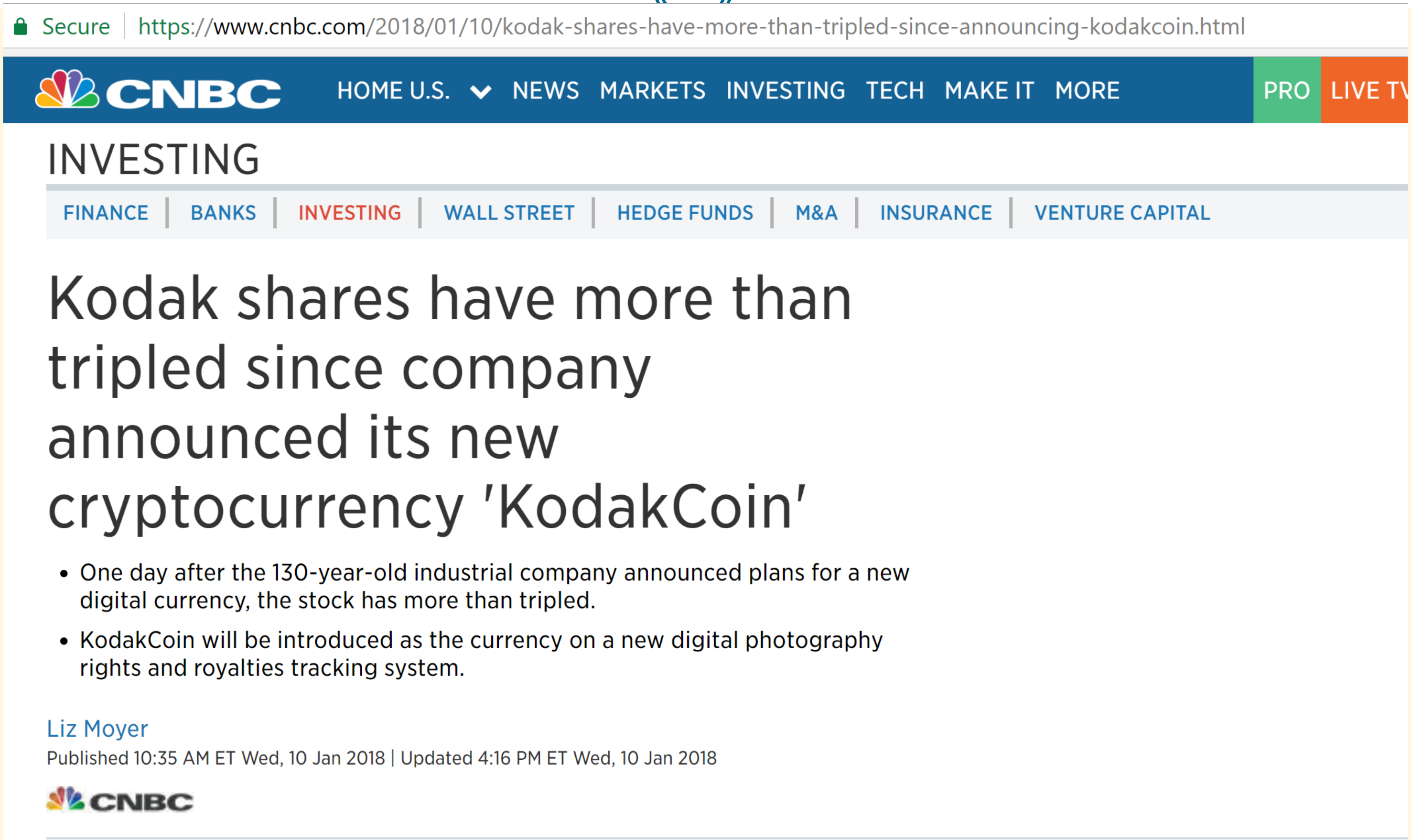
Bitcoin is 'digital gold' for millennials and could reach the '$100,000 range,' says strategist Tom Lee

- Bitcoin is essentially "digital gold" for millennials, and the cryptocurrency could easily achieve the $100,000 range, strategist Tom Lee says.
- "We think over the next 10 years, this new generation of millennials are going to view trust as a replacement for gold. So, bitcoin is essentially digital gold for another generation."

Berkeley Lovelace Jr. | @BerkeleyJr

Published 8:17 AM ET Wed, 29 Nov 2017

Buzz/Bubble



Kodak shares have more than tripled since company announced its new cryptocurrency 'KodakCoin'

- One day after the 130-year-old industrial company announced plans for a new digital currency, the stock has more than tripled.
- KodakCoin will be introduced as the currency on a new digital photography rights and royalties tracking system.

Liz Moyer

Published 10:35 AM ET Wed, 10 Jan 2018 | Updated 4:16 PM ET Wed, 10 Jan 2018

Beauty

- Bitcoin is beautifully designed with major innovations solving difficult problems in cryptocurrencies.
- Major advancements in:
    1. Cryptocurrencies
    2. Blockchain: Internet of Value (IoV), as compared to Internet of Information, and Internet of Things.
    3. Distributed systems
- Technological speaking: work in progress.

Bitcoin Misconceptions

1. Bitcoin is a coin.
2. Bitcoin is a digital token.

Bitcoin basics

- Bitcoin is the first popular crypto-currency.
- Created by Satoshi Nakamoto in 2009:

  1. White paper : Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org.
  2. A Bitcoin node's implementation storing *all* bitcoin transactions in a distributive way.

Bitcoin’s Technical

- Bitcoin now has:
  1. Bitcoin Network: a network of nodes running Bitcoin Core
  2. Open Source Bitcoin software: Bitcoin Core
  3. Bitcoin Protocol

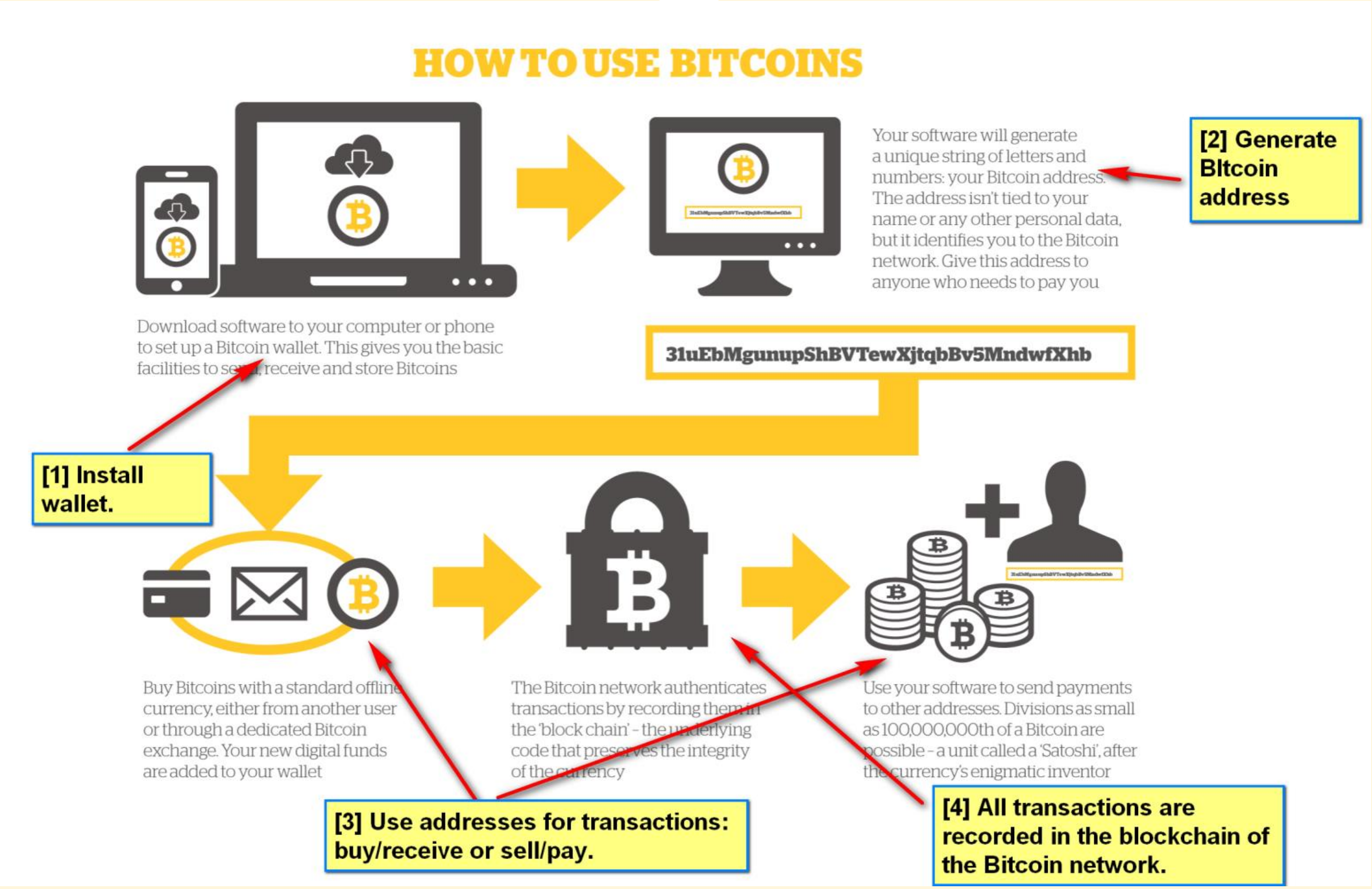
Some Bitcoin’s Characteristics

1. Distributed
2. Decentralized: no central control
3. Digital: thus cryptocurrency
4. Very secure blockchain to store ‘valueables’: Bitcoin.
5. Micropayment: trade in Satoshi; 1 BTC = 100,000,000 Satoshis.
6. Frictionless: low cost (highly debatable now).
7. Pseudonymous: a bitcoin address is anonymous but may be linked to owner outside of the bitcoin network.

Bitcoin’s Innovation

1. Cryptocurrencies: solving the value and usage system
2. Blockchain: public and secure general ledger
3. Distributed system
4. Proof of Work systems: for providing incentives and coin generation

How to use Bitcoin



HOW TO USE BITCOINS

Download software to your computer or phone to set up a Bitcoin wallet. This gives you the basic facilities to send, receive and store Bitcoins

Your software will generate a unique string of letters and numbers: your Bitcoin address. The address isn't tied to your name or any other personal data, but it identifies you to the Bitcoin network. Give this address to anyone who needs to pay you

31uEbMgunupShBVTewXjtqbBv5MndwfXhb

Buy Bitcoins with a standard offline currency, either from another user or through a dedicated Bitcoin exchange. Your new digital funds are added to your wallet

The Bitcoin network authenticates transactions by recording them in the 'block chain' - the underlying code that preserves the integrity of the currency

Use your software to send payments to other addresses. Divisions as small as 100,000,000th of a Bitcoin are possible - a unit called a 'Satoshi', after the currency's enigmatic inventor

[1] Install wallet.

[2] Generate BItcoin address

[3] Use addresses for transactions: buy/receive or sell/pay.

[4] All transactions are recorded in the blockchain of the Bitcoin network.

Bitcoin Wallet

- Software that ‘stores’ and manages Bitcoin.
  - Manages one or more private keys.
  - One private key is usually used to create one Bitcoin address.
  - Transactions are between Bitcoin addresses.
  - One may use a Master private key to create multiple private keys.

Bitcoin Exchanges

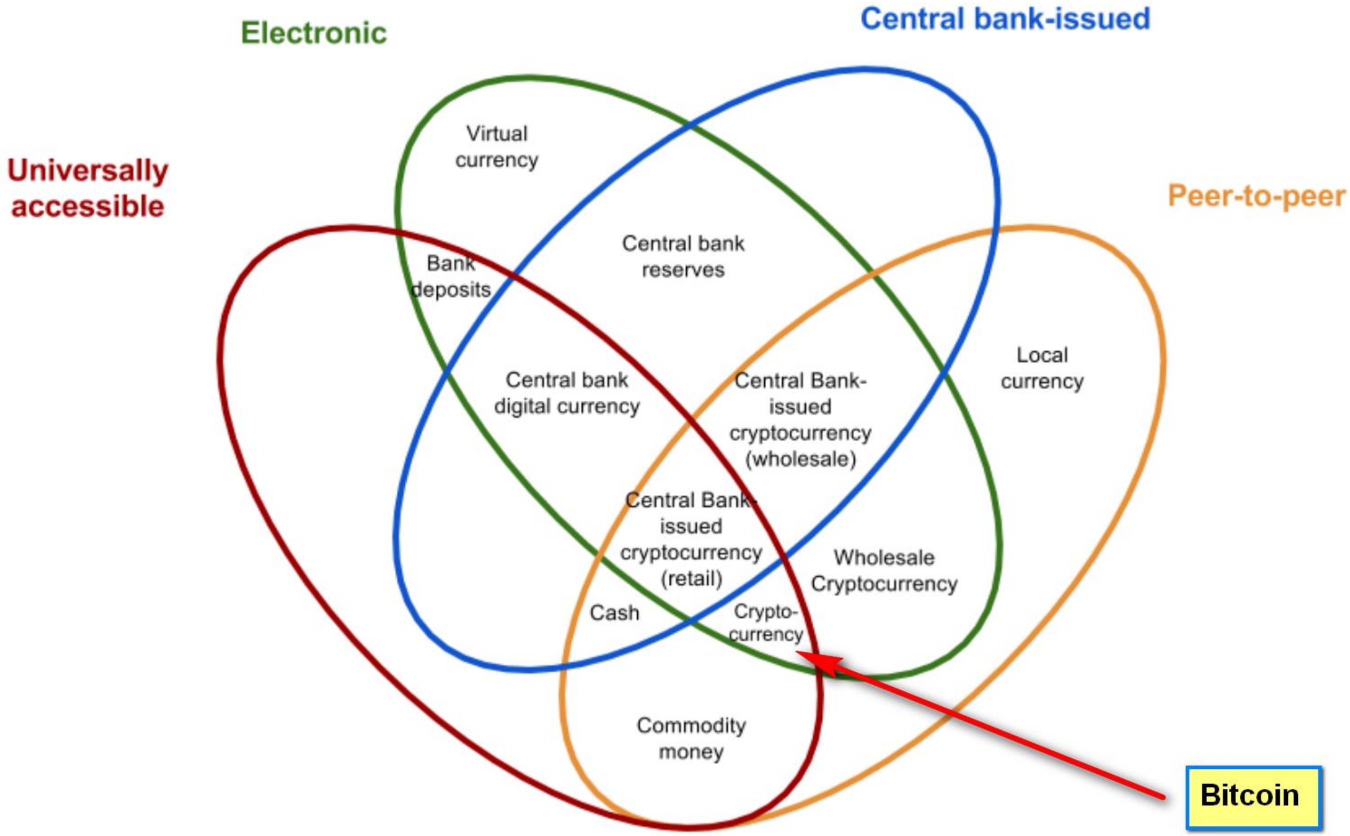
- Marketplaces for trading Bitcoins: matching sellers and buyers.
- Like stock exchange: e.g. $2,256.40 in exchanges for 2 GOOG stocks. (Replace GOOG by BTC)
- Most provide Bitcoin wallet services.

What is a Bitcoin

1. In Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”
   - An electronic coin as a *chain* of *digital signatures*.

Cryptocurrencies

The money flower: a taxonomy of money



Bitcoin

Adaptation from Bank for International Settlements (2017)

Four ‘Money Problems’

1. Value problem: why it has values.
2. Usage: Authenticity: Counterfeiting problem.
3. Usage: Double spending problem.
4. Usage: Claiming problem: can only be claimed by the transaction target.

Note that physical money mostly need to deal with the counterfeiting problem.

Some Previous Digital Money as Token

- Establishment of a *central authority* to solve the four problems, one on value, three on usage
  1. Ensure value: backed by …, which is eventually trust.
  2. Check authenticity
  3. Ensure correct delivery
  4. Ensure no double spending

Solving the double spending problem

- Before Bitcoin: using a trusted central authority (CA).
- Alice to send token coins to Bob. Basically:
  - Alice sends the coin token to the CA.
  - Token verified by the CA.
  - CA sends a new coin or exchange to other currency to Bob.

How do CA (mint) work?

1. CA keep the records of all transactions: a ledger.
    1. Why does Alice have coin token initially?
        1. She exchanges for coins using the CA.
        2. She received coins from others.
2. Transaction may look like:
    - ○ Alice’s account: 4 coin tokens -> Bob’s account.

Problems of Centralized Solution

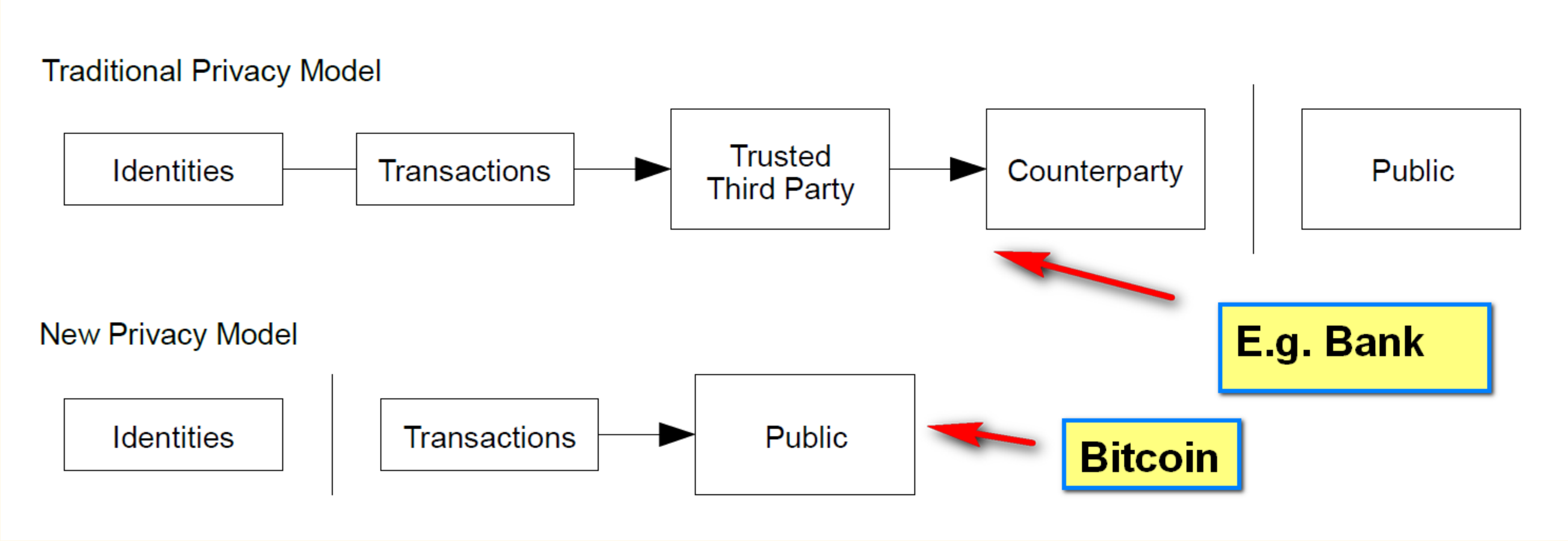
- Single point of failure/hacking/performance bottleneck/control
- Friction
  - High cost
  - Difficulty of micropayment
- Loss of anonymity/privacy

Bitcoin's solution to the usage problems

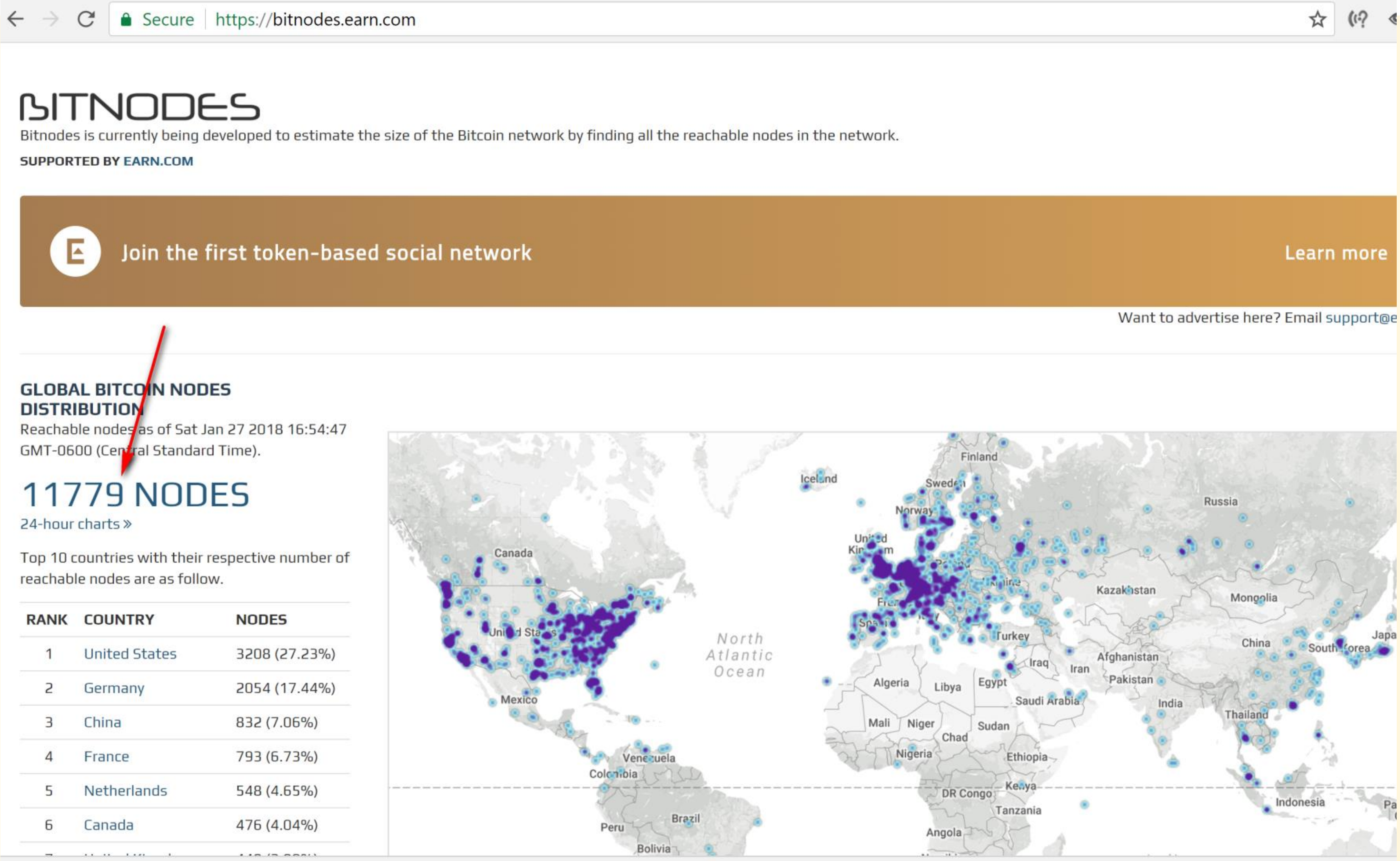
- Keeping *all* transactions in a *public* ledger in a distributed network: blockchain.
- Transaction may look like:
- Account 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY: 0.00748764 BTC to Account 1CKFAhPt4Nnk3h43EynHNFdxWgGsidXLGn

Privacy Model

- The Bitcoin model is vastly different to the model we are accustomed to.



Bitcoin Node Distributions



Secure https://bitnodes.earn.com

BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

SUPPORTED BY EARN.COM

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Jan 27 2018 16:54:47 GMT-0600 (Central Standard Time).

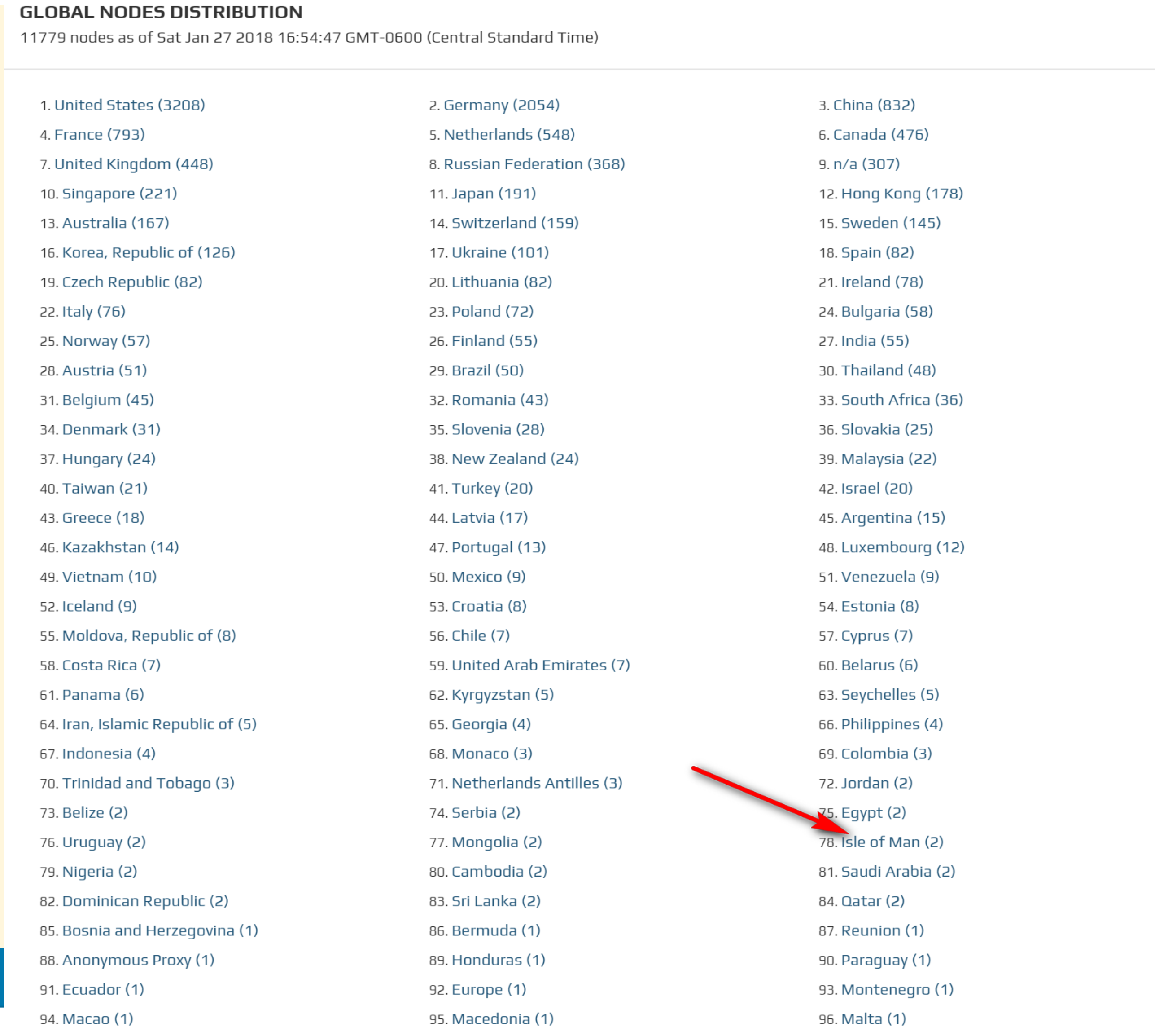
11779 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	3208 (27.23%)
2	Germany	2054 (17.44%)
3	China	832 (7.06%)
4	France	793 (6.73%)
5	Netherlands	548 (4.65%)
6	Canada	476 (4.04%)

Bitnodes' Countries



GLOBAL NODES DISTRIBUTION

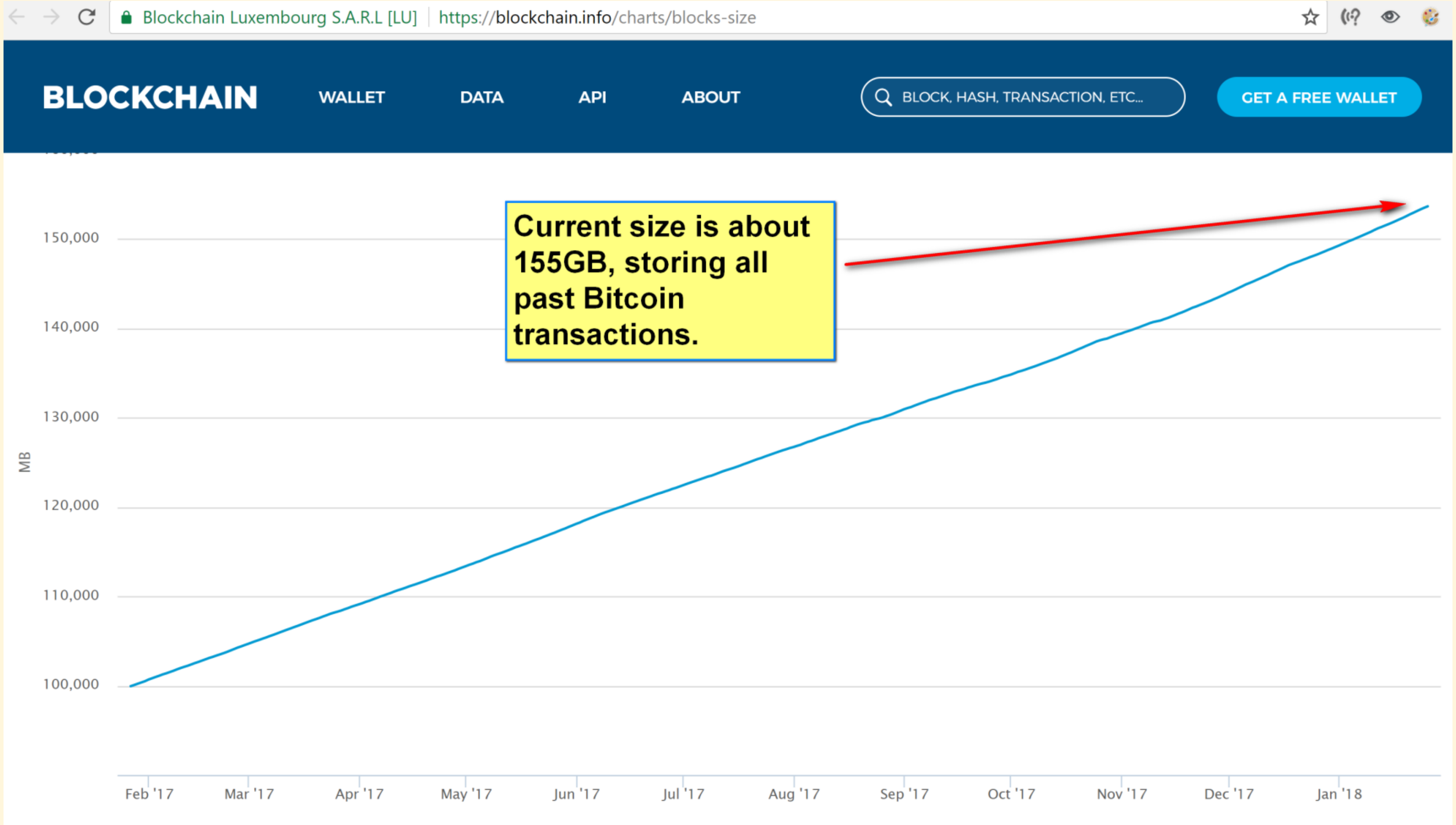
11779 nodes as of Sat Jan 27 2018 16:54:47 GMT-0600 (Central Standard Time)

1. United States (3208)	2. Germany (2054)	3. China (832)
4. France (793)	5. Netherlands (548)	6. Canada (476)
7. United Kingdom (448)	8. Russian Federation (368)	9. n/a (307)
10. Singapore (221)	11. Japan (191)	12. Hong Kong (178)
13. Australia (167)	14. Switzerland (159)	15. Sweden (145)
16. Korea, Republic of (126)	17. Ukraine (101)	18. Spain (82)
19. Czech Republic (82)	20. Lithuania (82)	21. Ireland (78)
22. Italy (76)	23. Poland (72)	24. Bulgaria (58)
25. Norway (57)	26. Finland (55)	27. India (55)
28. Austria (51)	29. Brazil (50)	30. Thailand (48)
31. Belgium (45)	32. Romania (43)	33. South Africa (36)
34. Denmark (31)	35. Slovenia (28)	36. Slovakia (25)
37. Hungary (24)	38. New Zealand (24)	39. Malaysia (22)
40. Taiwan (21)	41. Turkey (20)	42. Israel (20)
43. Greece (18)	44. Latvia (17)	45. Argentina (15)
46. Kazakhstan (14)	47. Portugal (13)	48. Luxembourg (12)
49. Vietnam (10)	50. Mexico (9)	51. Venezuela (9)
52. Iceland (9)	53. Croatia (8)	54. Estonia (8)
55. Moldova, Republic of (8)	56. Chile (7)	57. Cyprus (7)
58. Costa Rica (7)	59. United Arab Emirates (7)	60. Belarus (6)
61. Panama (6)	62. Kyrgyzstan (5)	63. Seychelles (5)
64. Iran, Islamic Republic of (5)	65. Georgia (4)	66. Philippines (4)
67. Indonesia (4)	68. Monaco (3)	69. Colombia (3)
70. Trinidad and Tobago (3)	71. Netherlands Antilles (3)	72. Jordan (2)
73. Belize (2)	74. Serbia (2)	75. Egypt (2)
76. Uruguay (2)	77. Mongolia (2)	78. Isle of Man (2)
79. Nigeria (2)	80. Cambodia (2)	81. Saudi Arabia (2)
82. Dominican Republic (2)	83. Sri Lanka (2)	84. Qatar (2)
85. Bosnia and Herzegovina (1)	86. Bermuda (1)	87. Reunion (1)
88. Anonymous Proxy (1)	89. Honduras (1)	90. Paraguay (1)
91. Ecuador (1)	92. Europe (1)	93. Montenegro (1)
94. Macao (1)	95. Macedonia (1)	96. Malta (1)

Bitcoin Core

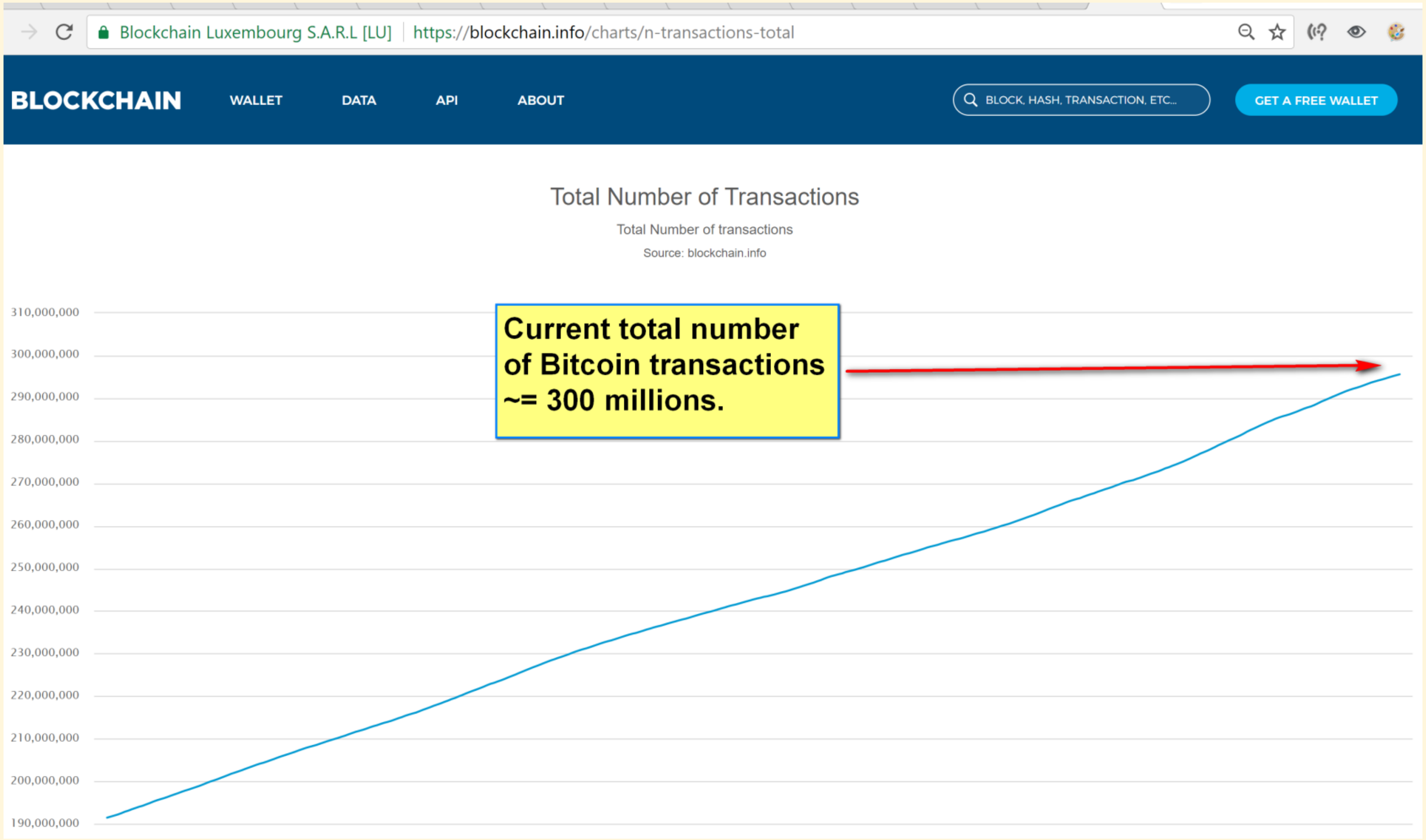
1. Contain Bitcoin node, a Bitcoin wallet, etc.
2. A full Bitcoin node contains all Bitcoin transactions in its blockchain.

Bitcoin’s Blockchain Size



Current size is about 155GB, storing all past Bitcoin transactions.

Bitcoins' Transaction History



Total Number of Transactions

Total Number of transactions

Source: blockchain.info

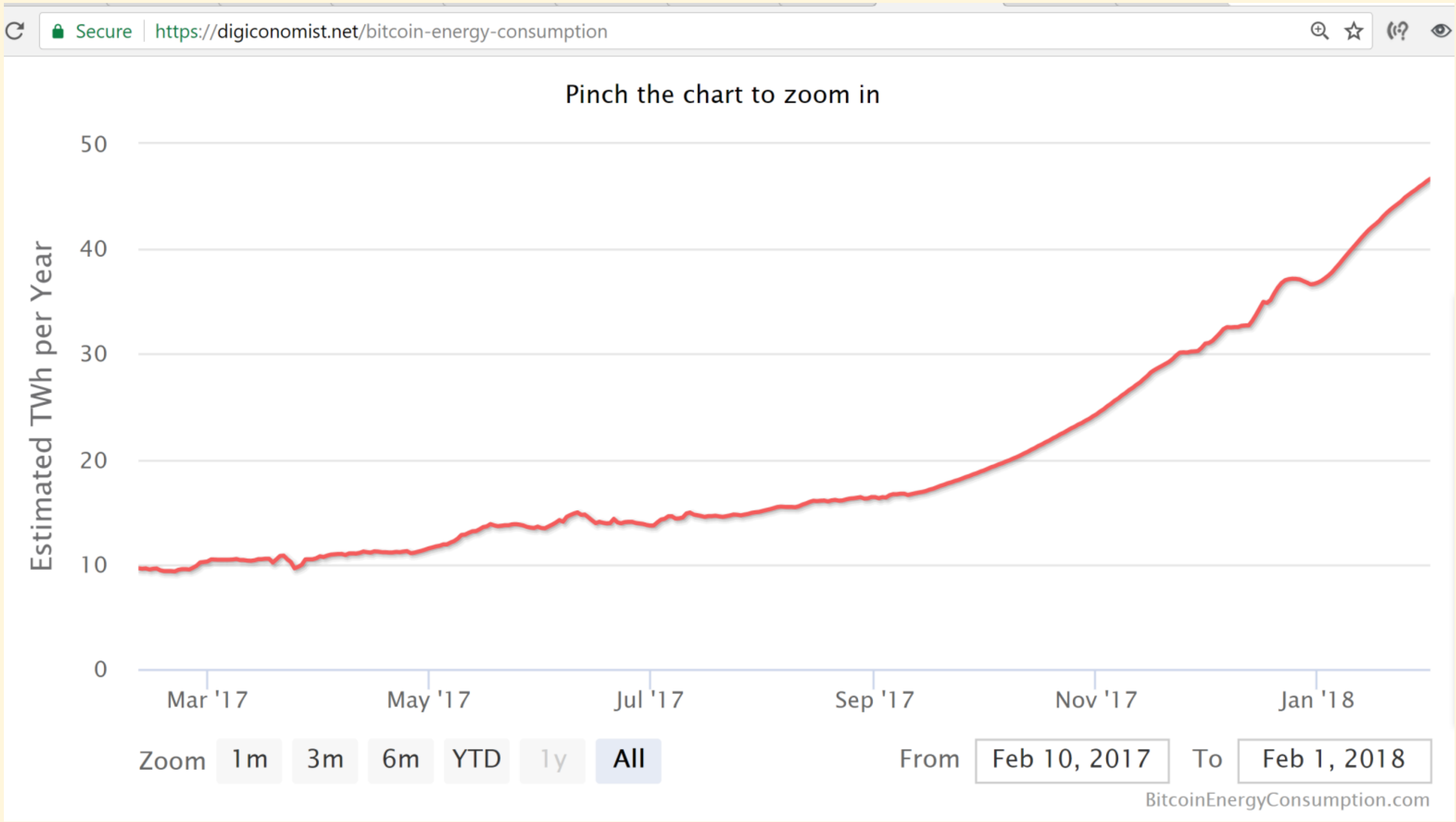
Current total number of Bitcoin transactions ~= 300 millions.

Energy Bitcoin Mining Electricity Usage

- http://www.wired.co.uk/article/how-much-energy-does-bitcoin-mining-really-use:
- All are *estimates*: from between 100MW to 3.4GW.
- That is 880,000,000 to 29,800.000.000 KWh/Year.
- About 60 countries > 29,800.000.000 KWh/Year.
- About 60 countries < 880,000,000 KWh/Year.
- About 97 countries in this range.
- Take the middle 15,000.000.000 KWh/Year: Tunisia, Cuba and North Korea.

One Estimate

Current Bitcoin Difficulty Level: 1,590,896,927,258



Looking Under the Hood

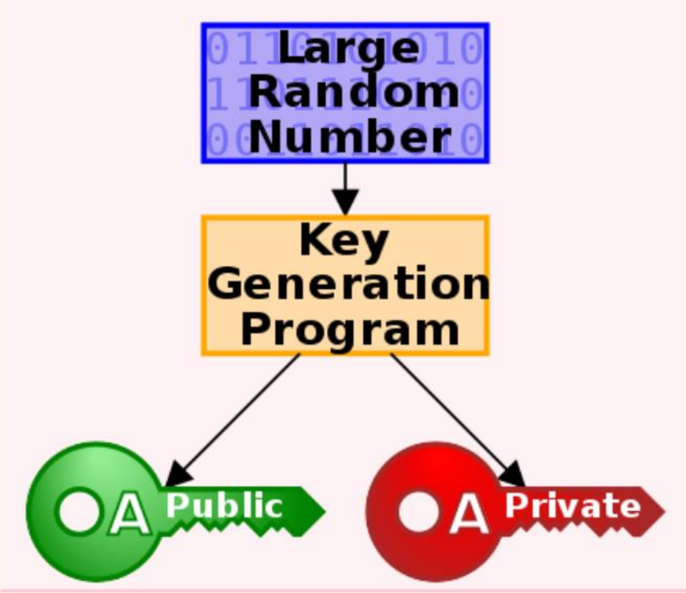
1. How does the Bitcoin address work?
2. How does transaction work?
3. How are blocks created?
4. How are coins generated/mined?

Bitcoin Address

- Use Public/Private key.
- 25 Bytes:
  1. 1 Byte: version
  2. 20 Bytes: 160-Hash is “a 160-bit hash of the public portion of a public/private ECDSA key pair.”
  3. 4 Bytes: SHA 256 checksum of the first 21 Bytes, to ensure no error in the address.
- Thus, the essential part of a Bitcoin address is the Public Key Hash (PKH).

Public and Private Key

- Public key cryptography: generate two keys:
  - Public Key: distributed to others
  - Private key: keep secret
- Applications:
  - Public key encryption
  - Digital Signature



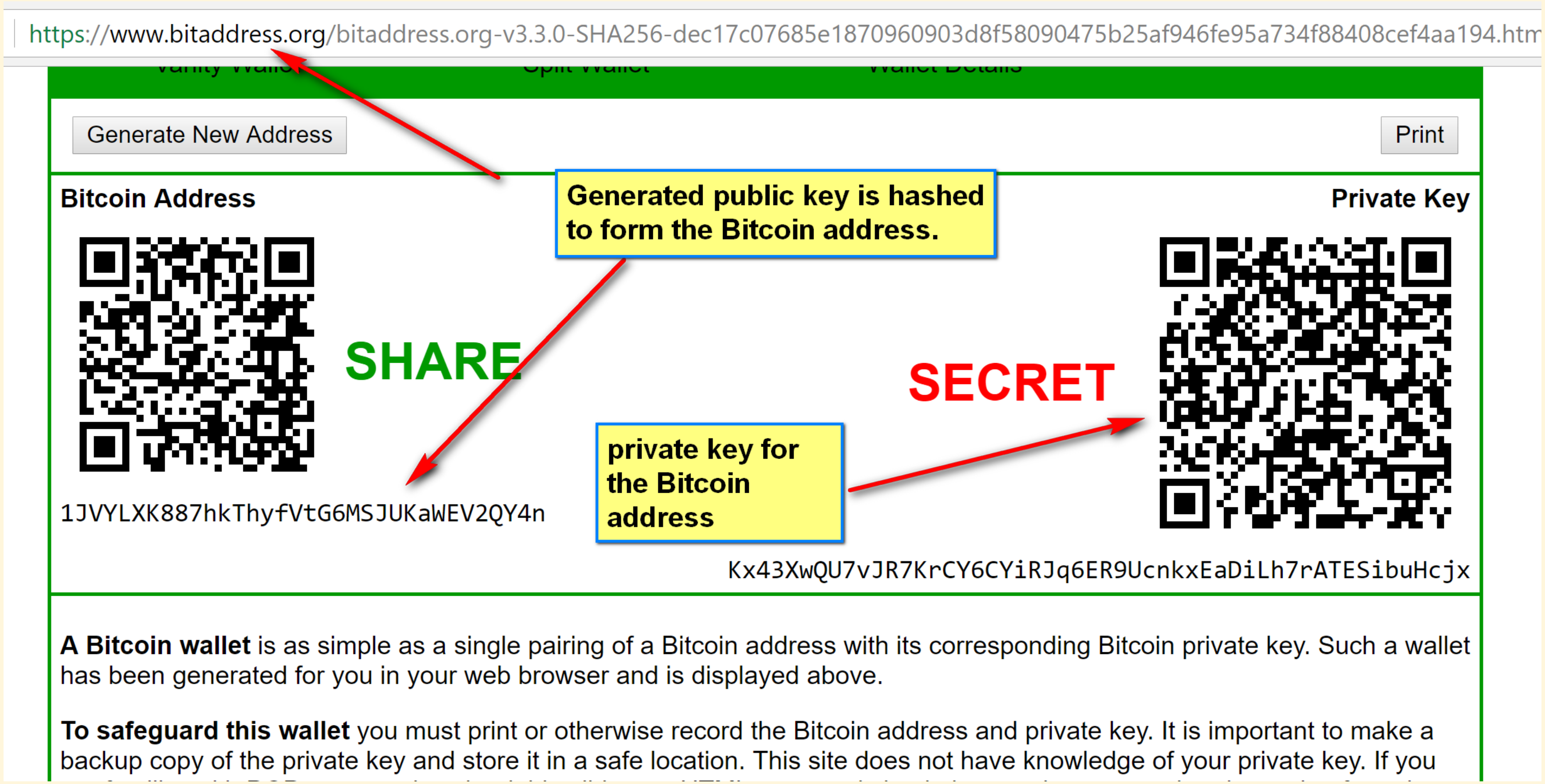
Public Key Encryption

- Alice wants to send a message to Bob that only he can read.
  1. Alice obtains [a] Bob's public key.
  2. Alice uses [a] to encrypt [b] the message.
  3. Alice sends [c] the encrypted message, to Bob.
  4. [c] can only be decrypted with [d] Bob's private key.
- Hacker intercepting [c] in the communications process cannot decrypt [c].

Digital Signature

- Alice wants others to know that she has signed (authorized) a message she is sending.
  1. Alice publicizes her [a] public key that *is known to be hers*.
  2. Alice distributes:
     1. [b] the message
     2. [c] the encrypted message, using [d] her private key.
     3. [e] the method of decryption.
  3. Signature validators can use the information in [e] to generate the [f] decrypted message from [c] and [a].
  4. Signature is validated basically if [b] = [f].

Bitcoin Address



https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a734f88408cef4aa194.htm

Bitcoin Address

SHARE

1JVYLXK887hkThyfVtG6MSJUKaWEV2QY4n

Private Key

SECRET

Kx43XwQU7vJR7KrCY6CYiRJq6ER9UcnkxEaDiLh7rATESibuHcjx

Generated public key is hashed to form the Bitcoin address.

private key for the Bitcoin address

A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

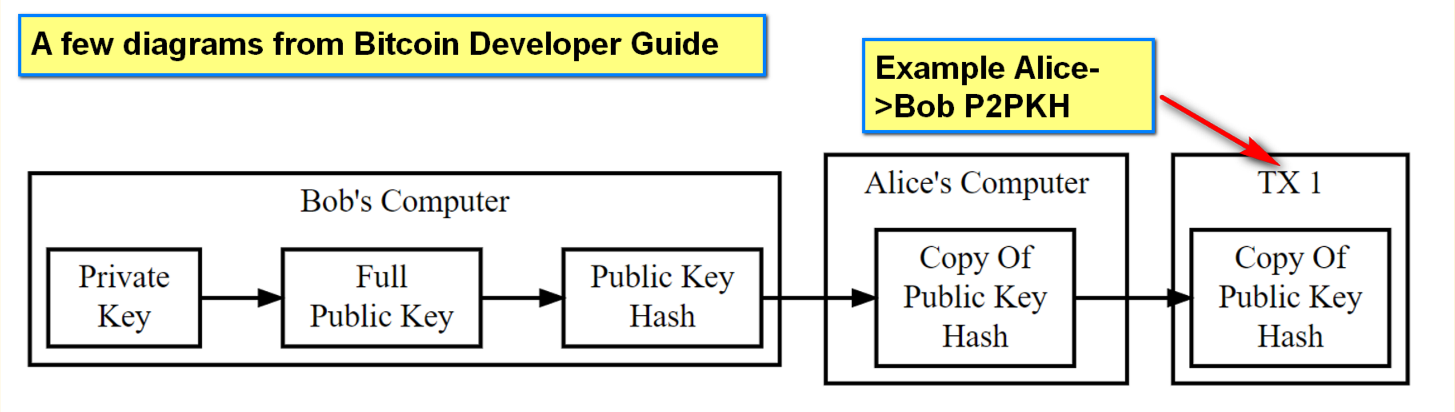
To safeguard this wallet you must print or otherwise record the Bitcoin address and private key. It is important to make a backup copy of the private key and store it in a safe location. This site does not have knowledge of your private key. If you

Bitcoin's Transactions

- The most simple (and common) type of Bitcoin transaction (P2PKH: Payment to Public Key Hash): E.g. TX1: Alice sends 0.3 BTC to Bob.
  - Bob provided a Bitcoin address to Alice (basically the PKH), which is included in TX1.
  - The 0.3 BTC sits as Unspent Transaction Outputs (UTXOs)

A few diagrams from Bitcoin Developer Guide

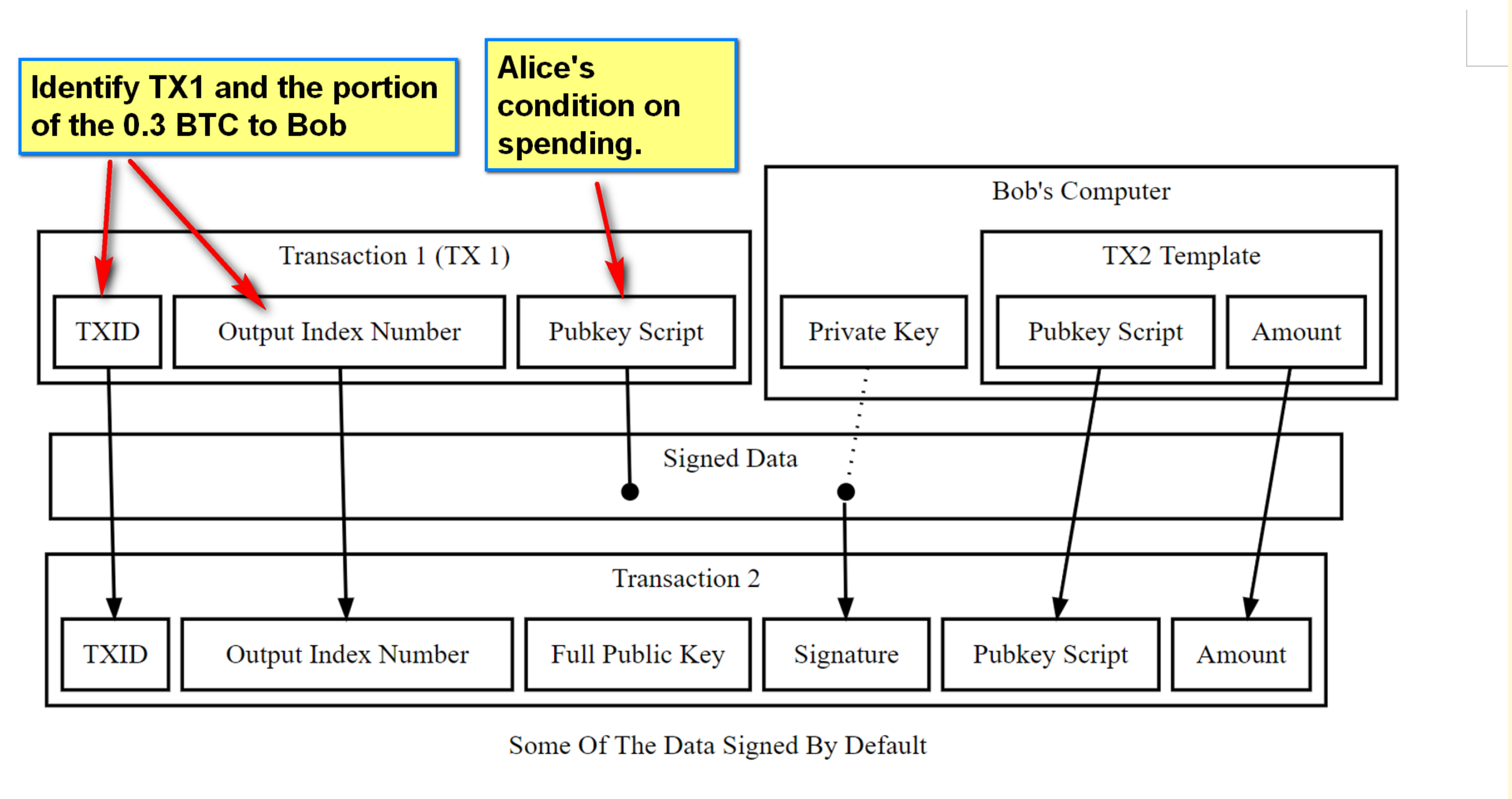
Example Alice->Bob P2PKH



Creating A P2PKH Public Key Hash To Receive Payment

Bitcoin's Transaction

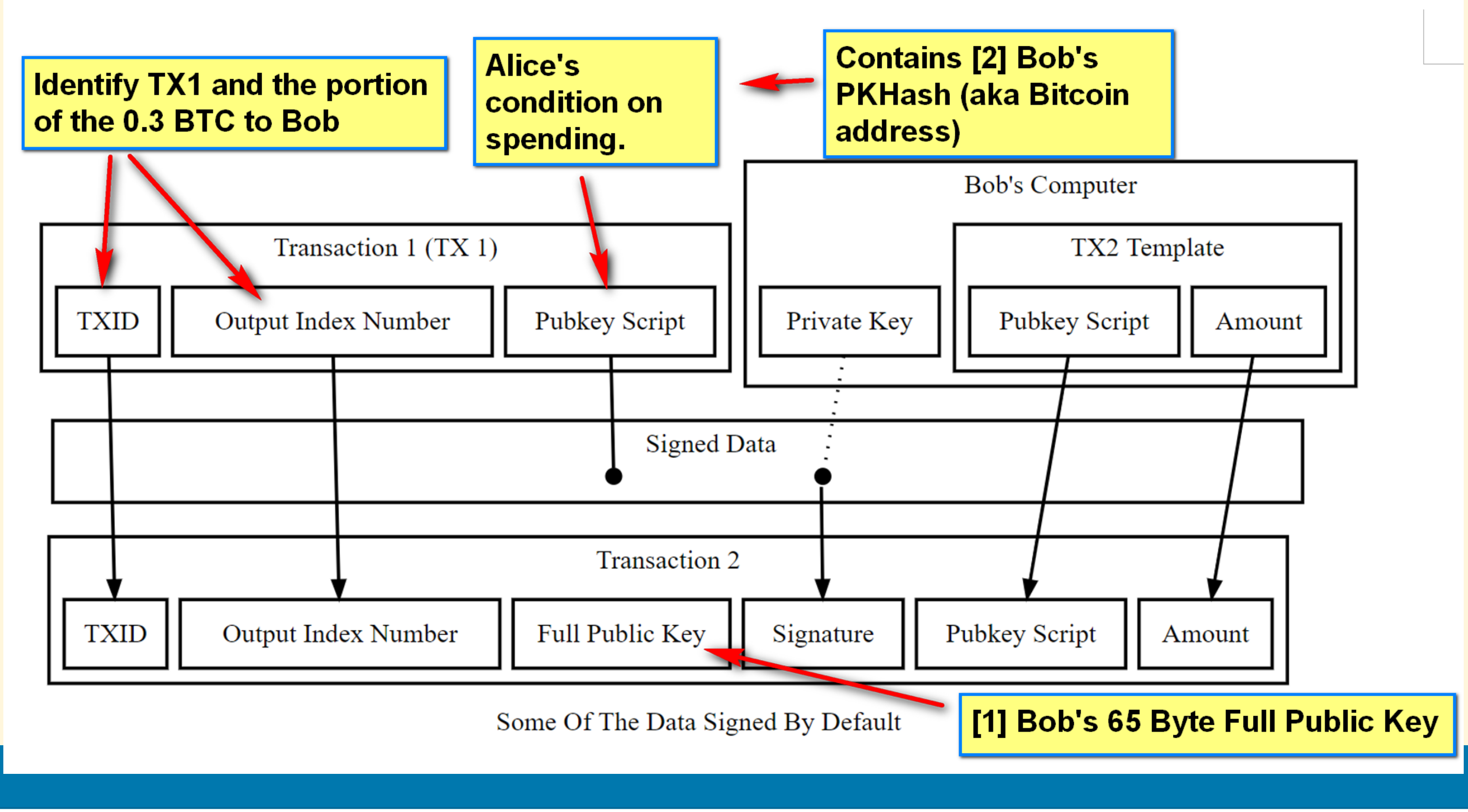
- TX2: Bob sends the 0.3 BTC sent by Alice in a P2PKH to Paul.



Some Of The Data Signed By Default

Validating Bob’s Ownership

- [A] Checking Bob’s Public Key as the output address of TX1, Alice’s 0.3 BTC: [1] hashes into [2].



Identify TX1 and the portion of the 0.3 BTC to Bob

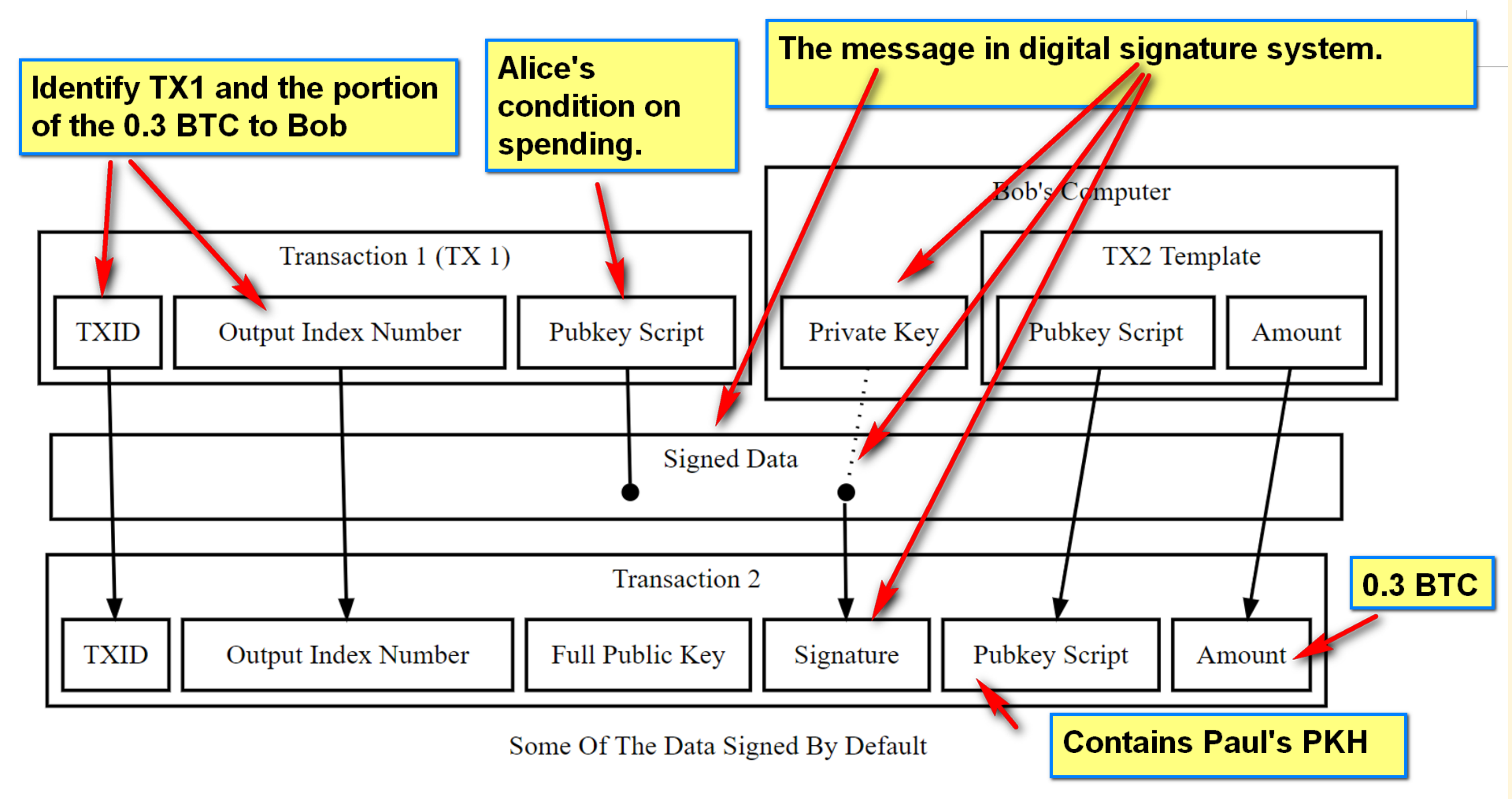
Alice's condition on spending.

Contains [2] Bob's PKHash (aka Bitcoin address)

[1] Bob's 65 Byte Full Public Key

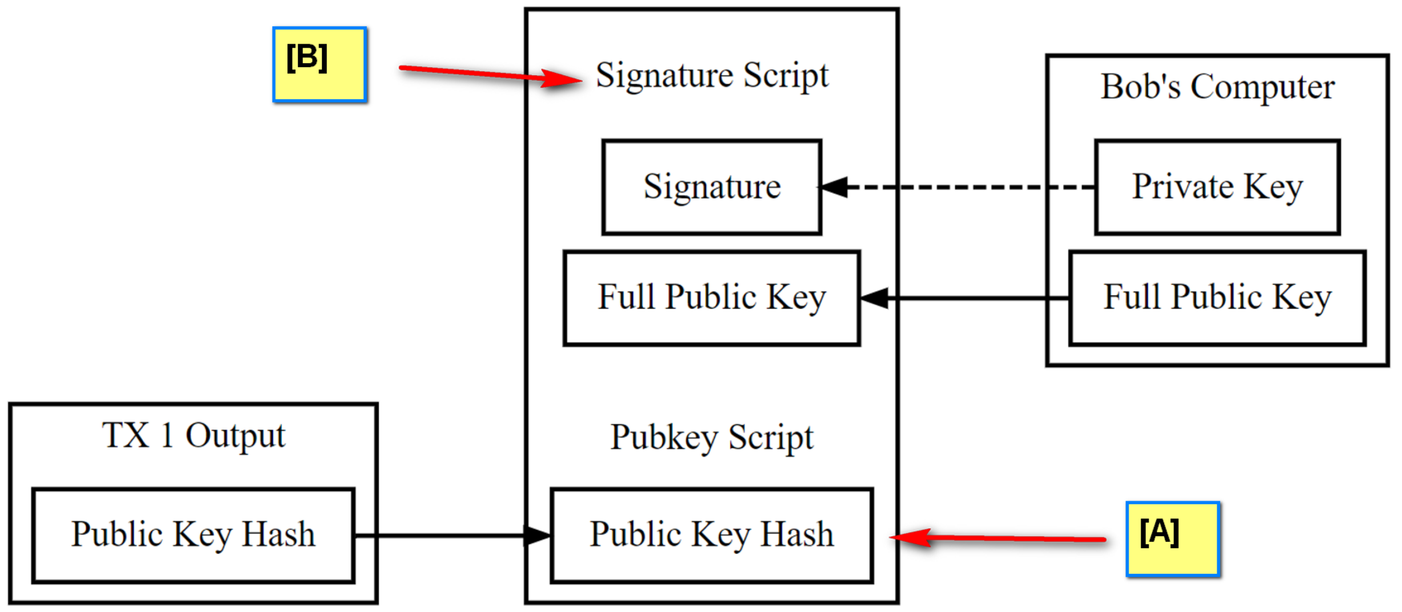
Validating Bob’s Ownership

- [B] Use Public Key-based Digital Signature System.



Putting it together

- Bitcoin has transaction scripts for proper output.



[B]

Signature Script

Signature

Full Public Key

Bob's Computer

Private Key

Full Public Key

TX 1 Output

Public Key Hash

Pubkey Script

Public Key Hash

[A]

Spending A P2PKH Output

Bitcoin transactions

- There are variety in Bitcoin transactions.
- A transaction has
  - 0 or more input addresses.
  - 1 or more output addresses.
- A transaction without an input address represents a successful mining reward to the miner’s address.

Bitcoin’s Mining

- How do you encourage participation in the Bitcoin network?
- Bitcoin nodes receive bitcoin transactions through the Bitcoin network.
- Miners attempt to create a block to contain selected transactions.
- If successful, the miner receives:
  - 12.5 newly minted BTC (currently).
  - Transactions fees in BTC (Satoshis).

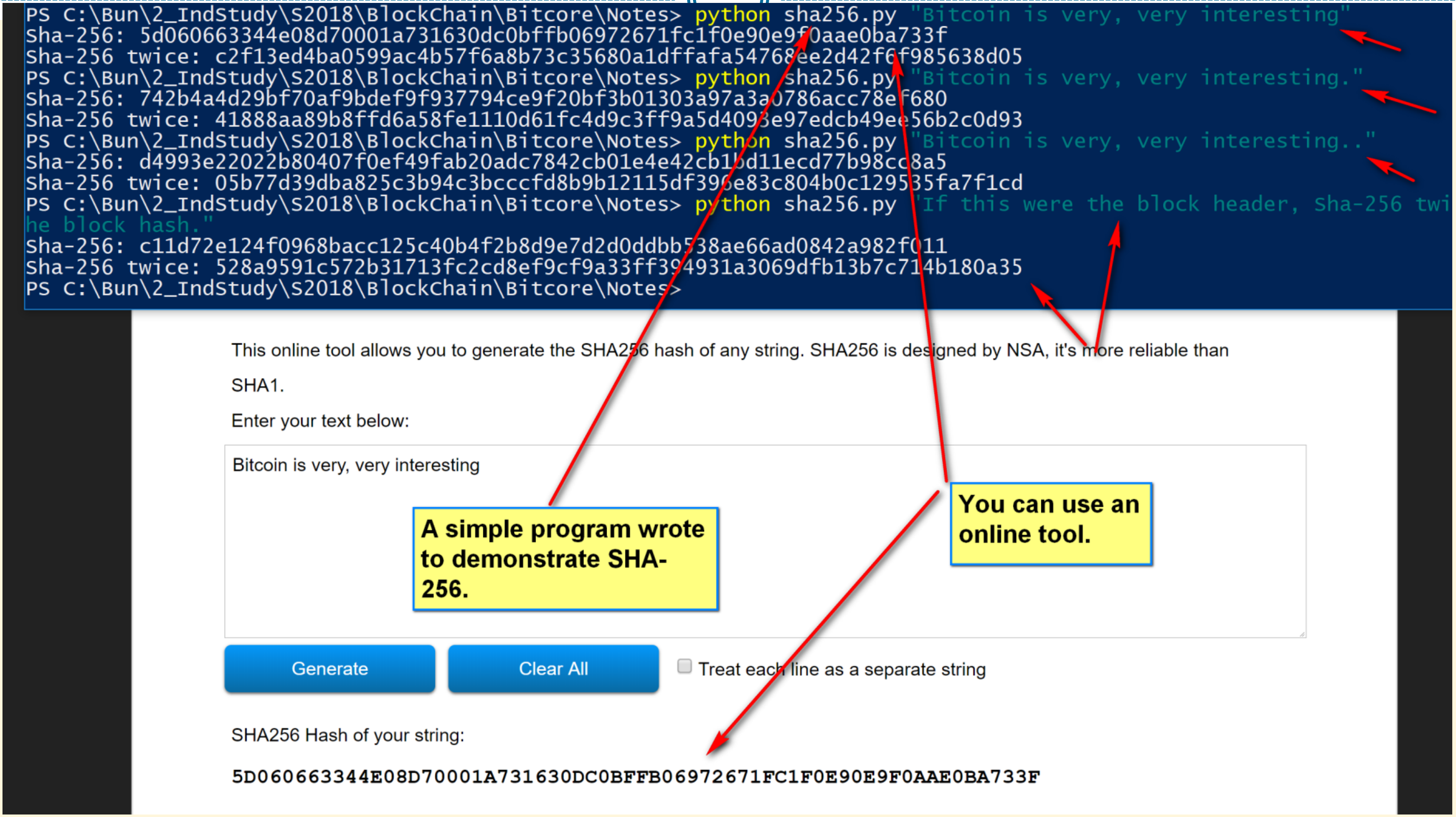
Bitcoin Mining

1. Block created averaged once every 10 minutes. Goal: 2,016 blocks per two weeks.
2. Total BTC eventually: 21 million, around 2,140.
3. About 80% of BTC mined.
4. Block creation reward halved every 210,000 blocks.
5. Based on the ‘Proof of Work’ concept in computer science

How to create a new block?

1. Hash-based.
2. A hash function: a = hash(x)
   1. Produce a nearly unique result a, known as result.
   2. One way: no reverse function to find x from a.
   3. Small change in X can result in large change in a, sometimes called the hash address.
3. Bitcoin uses SHA-256 Hash.

SHA-256



```
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> python sha256.py "Bitcoin is very, very interesting"
Sha-256: 5d060663344e08d70001a731630dc0bffb06972671fc1f0e90e9f0aae0ba733f
Sha-256 twice: c2f13ed4ba0599ac4b57f6a8b73c35680a1dffafa54768ee2d42f6f985638d05
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> python sha256.py "Bitcoin is very, very interesting."
Sha-256: 742b4a4d29bf70af9bdef9f937794ce9f20bf3b01303a97a3a0786acc78ef680
Sha-256 twice: 41888aa89b8ffd6a58fe1110d61fc4d9c3ff9a5d4093e97edcb49ee56b2c0d93
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> python sha256.py "Bitcoin is very, very interesting.."
Sha-256: d4993e22022b80407f0ef49fab20adc7842cb01e4e42cb1bd11ecd77b98cc8a5
Sha-256 twice: 05b77d39dba825c3b94c3bcccfd8b9b12115df396e83c804b0c129535fa7f1cd
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> python sha256.py "If this were the block header, Sha-256 twi
he block hash."
Sha-256: c11d72e124f0968bacc125c40b4f2b8d9e7d2d0ddbb538ae66ad0842a982f011
Sha-256 twice: 528a9591c572b31713fc2cd8ef9cf9a33ff394931a3069dfb13b7c714b180a35
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes>
```

This online tool allows you to generate the SHA256 hash of any string. SHA256 is designed by NSA, it's more reliable than SHA1.

Enter your text below:

Bitcoin is very, very interesting

SHA256 Hash of your string:

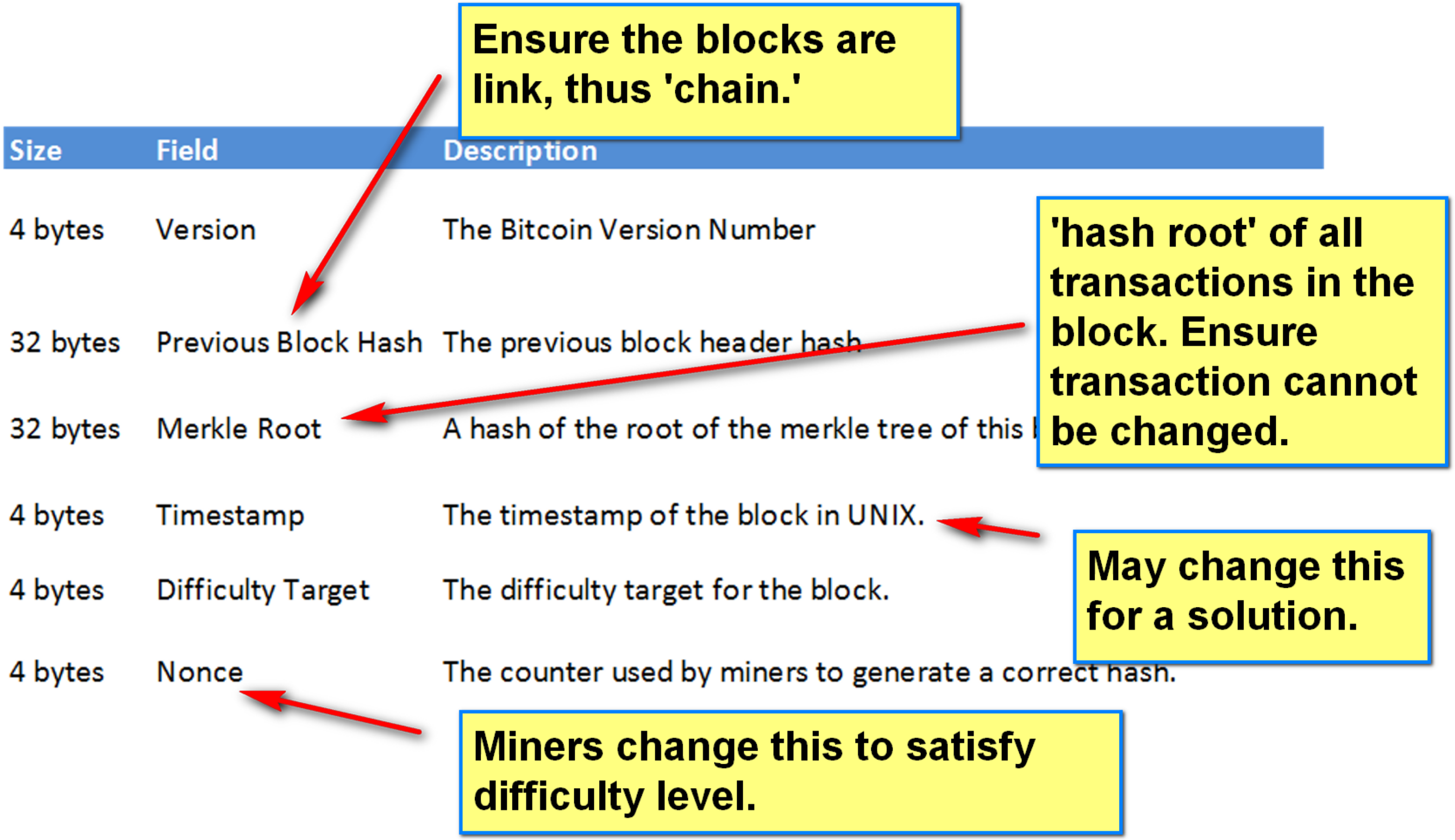
5D060663344E08D70001A731630DC0BFFB06972671FC1F0E90E9F0AAE0BA733F

A simple program wrote to demonstrate SHA-256.

You can use an online tool.

http://passwordsgenerator.net/sha256-hash-generator/

Bitcoin’s Block Header (80 Bytes)



Size	Field	Description
4 bytes	Version	The Bitcoin Version Number
32 bytes	Previous Block Hash	The previous block header hash
32 bytes	Merkle Root	A hash of the root of the merkle tree of this
4 bytes	Timestamp	The timestamp of the block in UNIX.
4 bytes	Difficulty Target	The difficulty target for the block.
4 bytes	Nonce	The counter used by miners to generate a correct hash.

Ensure the blocks are link, thus 'chain.'

'hash root' of all transactions in the block. Ensure transaction cannot be changed.

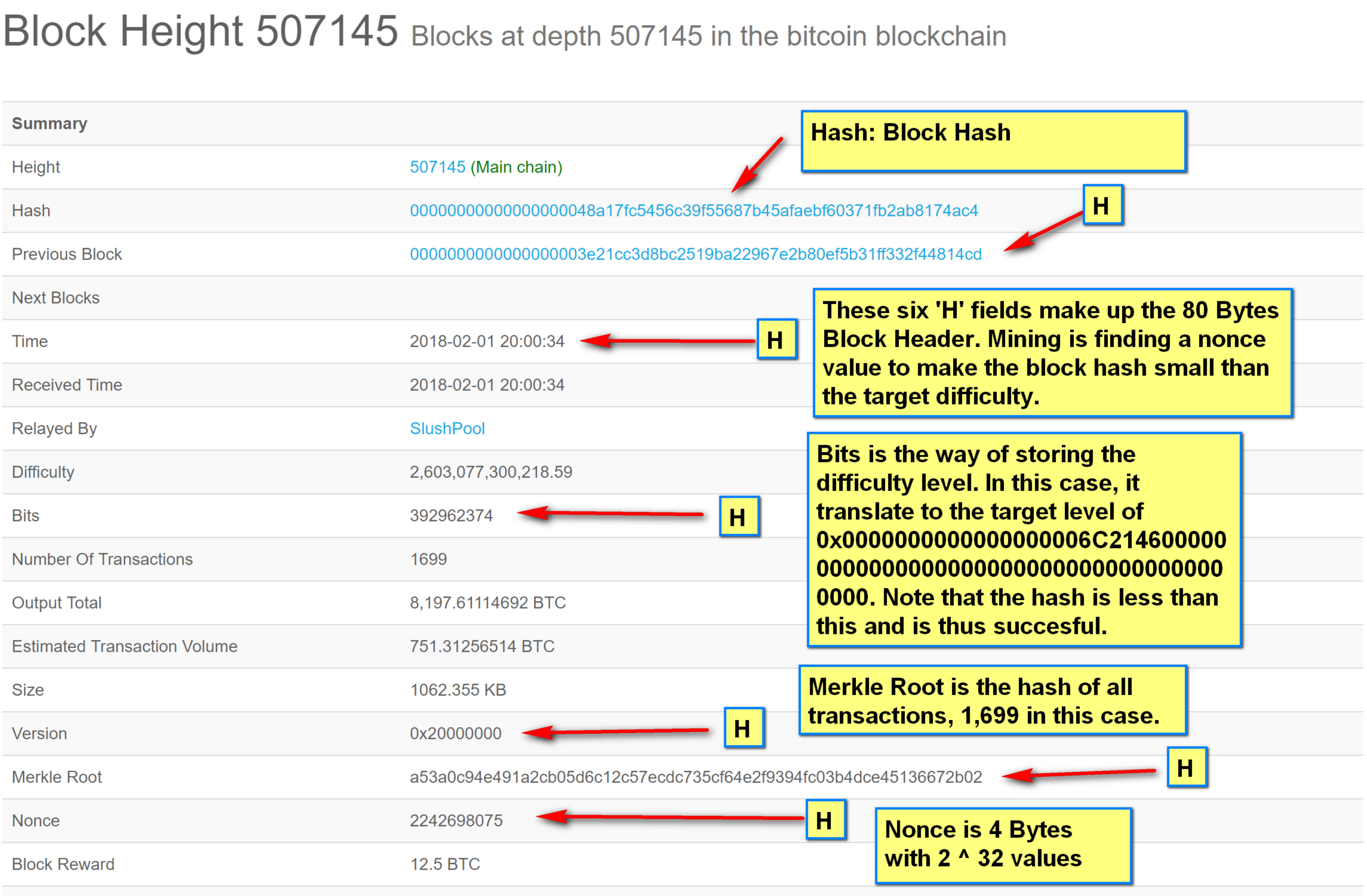
May change this for a solution.

Miners change this to satisfy difficulty level.

Proof of Work System

- Miners need to create a block with a hash those value must be smaller than a target level.
- A value of a 4 Byte nonce must be found to make the 80 Bytes block header (in which the nonce is a part) to hash to an acceptable level.
- Some desirable properties of Proof of work system:
  - The solution (nonce for bitcoin) is very difficult to find (work).
  - The solution is easy to verify.
  - Level of difficulty can be controlled easily.

Block 507,145



Block Height 507145 Blocks at depth 507145 in the bitcoin blockchain

Summary	
Height	507145 (Main chain)
Hash	000000000000000000048a17fc5456c39f55687b45afaebf60371fb2ab8174ac4
Previous Block	0000000000000000003e21cc3d8bc2519ba22967e2b80ef5b31ff332f44814cd
Next Blocks	
Time	2018-02-01 20:00:34
Received Time	2018-02-01 20:00:34
Relayed By	SlushPool
Difficulty	2,603,077,300,218.59
Bits	392962374
Number Of Transactions	1699
Output Total	8,197.61114692 BTC
Estimated Transaction Volume	751.31256514 BTC
Size	1062.355 KB
Version	0x20000000
Merkle Root	a53a0c94e491a2cb05d6c12c57ecdc735cf64e2f9394fc03b4dce45136672b02
Nonce	2242698075
Block Reward	12.5 BTC

Hash: Block Hash

H

These six 'H' fields make up the 80 Bytes Block Header. Mining is finding a nonce value to make the block hash small than the target difficulty.

H

Bits is the way of storing the difficulty level. In this case, it translate to the target level of 0x000000000000000006C214600000 0000000000000000000000000000000 0000. Note that the hash is less than this and is thus succesful.

H

Merkle Root is the hash of all transactions, 1,699 in this case.

H

H

H

Nonce is 4 Bytes with 2 ^ 32 values

Mining Block 507,145

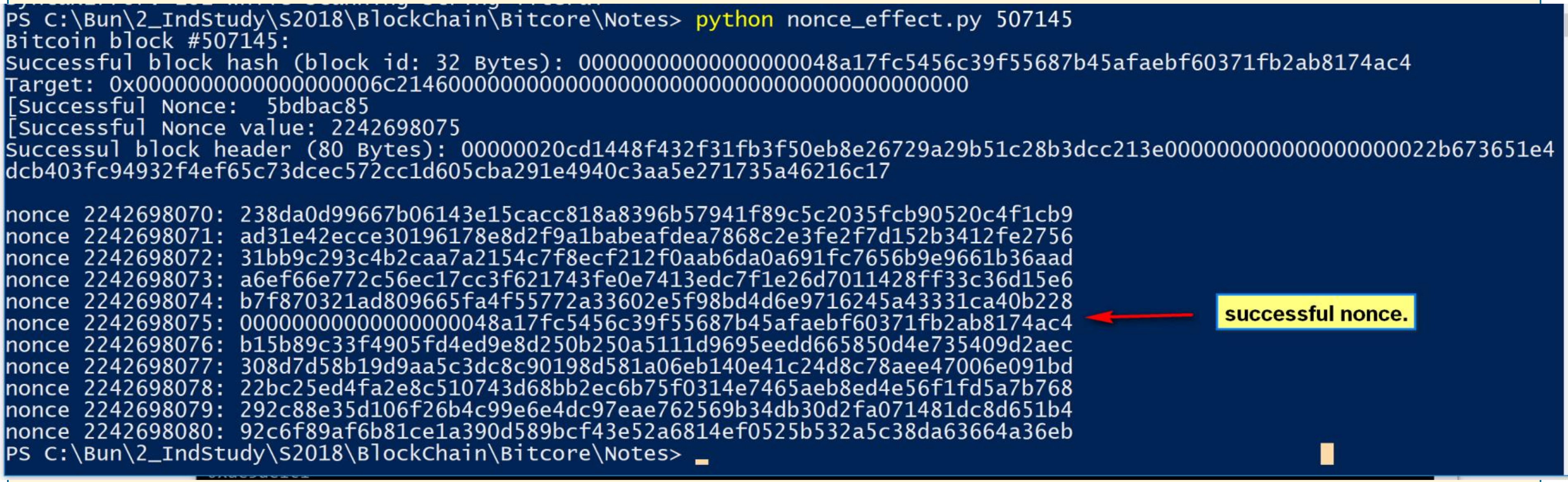
1. Target level: 0x0000000000000000006C21460000000000000000000000000000000000000000
2. Hash produced: 0x0000000000000000000048a17fc5456c39f55687b45afaebf60371fb2ab8174ac4
3. Mining successful since hash < target level.

Block 507,145 Verification

1. Hash received from the miner:
   0x000000000000000000048a17fc5456c39f55687b45afaebf60371
   fb2ab8174ac4
2. Header from the block sent by the minor:
   00000020cd1448f432f31fb3f50eb8e26729a29b51c28b3dcc213e0
   00000000000000000022b673651e4dcb403fc94932f4ef65c73dce
   c572cc1d605cba291e4940c3aa5e271735a46216c175bdbac85
3. Checking:
   1. Sha256(Sha256(header)) = hash
   2. Hash < target level
   3. Transactions input are unspent output from other transactions.

Hard to find a working nonce

- nonce_effect.py: check hash results for close nonce values.



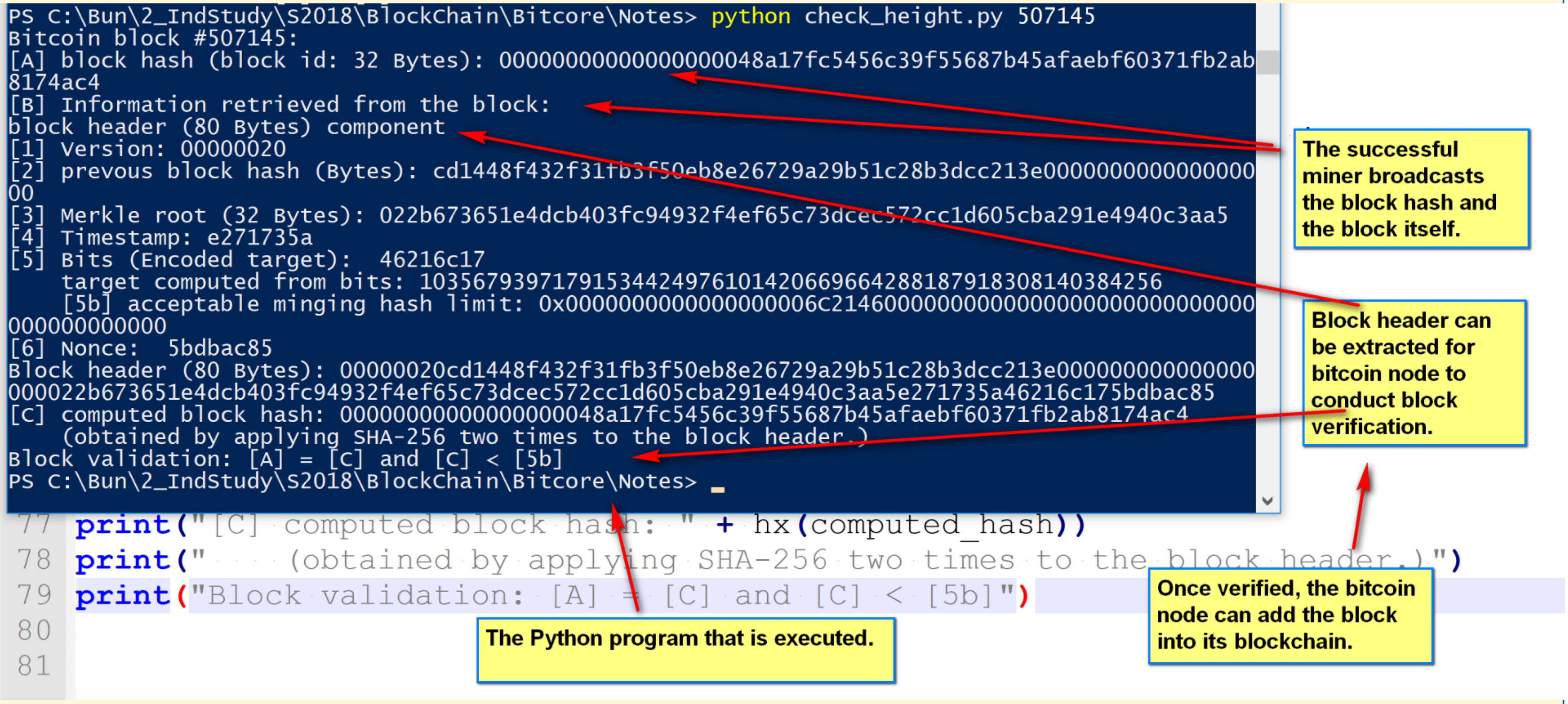
```
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> python nonce_effect.py 507145
Bitcoin block #507145:
Successful block hash (block id: 32 Bytes): 00000000000000000048a17fc5456c39f55687b45afaebf60371fb2ab8174ac4
Target: 0x0000000000000000006C2146000000000000000000000000000000000000000000
[Successful Nonce:  5bdbac85
[Successful Nonce value: 2242698075
Successul block header (80 Bytes): 00000020cd1448f432f31fb3f50eb8e26729a29b51c28b3dcc213e00000000000000000022b673651e4
dcb403fc94932f4ef65c73dcec572cc1d605cba291e4940c3aa5e271735a46216c17

nonce 2242698070: 238da0d99667b06143e15cacc818a8396b57941f89c5c2035fcb90520c4f1cb9
nonce 2242698071: ad31e42ecce30196178e8d2f9a1babeafdea7868c2e3fe2f7d152b3412fe2756
nonce 2242698072: 31bb9c293c4b2caa7a2154c7f8ecf212f0aab6da0a691fc7656b9e9661b36aad
nonce 2242698073: a6ef66e772c56ec17cc3f621743fe0e7413edc7f1e26d7011428ff33c36d15e6
nonce 2242698074: b7f870321ad809665fa4f55772a33602e5f98bd4d6e9716245a43331ca40b228
nonce 2242698075: 00000000000000000048a17fc5456c39f55687b45afaebf60371fb2ab8174ac4
nonce 2242698076: b15b89c33f4905fd4ed9e8d250b250a5111d9695eedd665850d4e735409d2aec
nonce 2242698077: 308d7d58b19d9aa5c3dc8c90198d581a06eb140e41c24d8c78aee47006e091bd
nonce 2242698078: 22bc25ed4fa2e8c510743d68bb2ec6b75f0314e7465aeb8ed4e56f1fd5a7b768
nonce 2242698079: 292c88e35d106f26b4c99e6e4dc97eae762569b34db30d2fa071481dc8d651b4
nonce 2242698080: 92c6f89af6b81ce1a390d589bcf43e52a6814ef0525b532a5c38da63664a36eb
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> _
```

Tampering Transactions

- If a hacker changes a transaction in Block 507,145:
  1. The Merkle root (hash of all transactions) changes
  2. The block header changes
  3. The block header does not hash into old, existing block hash.
  4. The block cannot be verified.
  5. The hacker needs to mine a new acceptable block hash and overpower the Bitcoin network to accept it.
  6. However, Block 507,146 uses the old block hash of block 507,145.
  7. The hacker will need to change block 507,146 too.
  8. Thus, the hacker will need to change all subsequent blocks.

A Demonstration Program: block 507,145



```
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> python check_height.py 507145
Bitcoin block #507145:
[A] block hash (block id: 32 Bytes): 00000000000000000048a17fc5456c39f55687b45afaebf60371fb2ab
8174ac4
[B] Information retrieved from the block:
block header (80 Bytes) component
[1] Version: 00000020
[2] prevous block hash (Bytes): cd1448f432f31fb3f50eb8e26729a29b51c28b3dcc213e0000000000000000
00
[3] Merkle root (32 Bytes): 022b673651e4dcb403fc94932f4ef65c73dcec572cc1d605cba291e4940c3aa5
[4] Timestamp: e271735a
[5] Bits (Encoded target):  46216c17
    target computed from bits: 10356793971791534424976101420669664288187918308140384256
    [5b] acceptable minging hash limit: 0x0000000000000000006C214600000000000000000000000000000
000000000000
[6] Nonce:  5bdbac85
Block header (80 Bytes): 00000020cd1448f432f31fb3f50eb8e26729a29b51c28b3dcc213e000000000000000
000022b673651e4dcb403fc94932f4ef65c73dcec572cc1d605cba291e4940c3aa5e271735a46216c175bdbac85
[C] computed block hash: 00000000000000000048a17fc5456c39f55687b45afaebf60371fb2ab8174ac4
    (obtained by applying SHA-256 two times to the block header.)
Block validation: [A] = [C] and [C] < [5b]
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> _
```

```
print("[C] computed block hash: " + hx(computed_hash))
print("    (obtained by applying SHA-256 two times to the block header.)")
print("Block validation: [A] = [C] and [C] < [5b]")
```

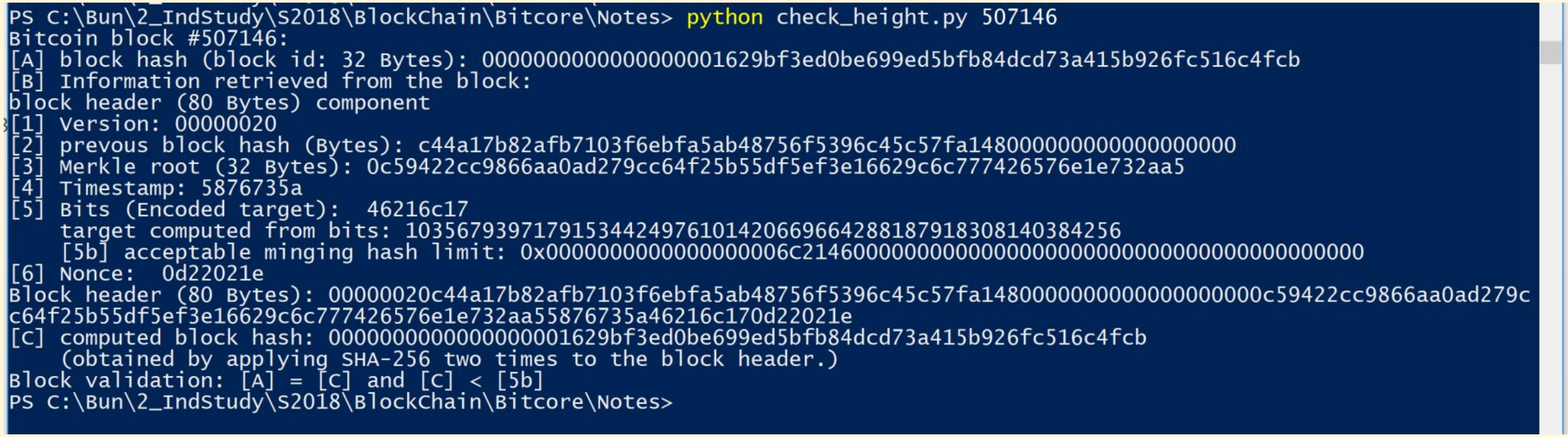
The successful miner broadcasts the block hash and the block itself.

Block header can be extracted for bitcoin node to conduct block verification.

The Python program that is executed.

Once verified, the bitcoin node can add the block into its blockchain.

Block 507,146



```
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes> python check_height.py 507146
Bitcoin block #507146:
[A] block hash (block id: 32 Bytes): 000000000000000000001629bf3ed0be699ed5bfb84dcd73a415b926fc516c4fcb
[B] Information retrieved from the block:
block header (80 Bytes) component
[1] Version: 00000020
[2] prevous block hash (Bytes): c44a17b82afb7103f6ebfa5ab48756f5396c45c57fa148000000000000000000
[3] Merkle root (32 Bytes): 0c59422cc9866aa0ad279cc64f25b55df5ef3e16629c6c777426576e1e732aa5
[4] Timestamp: 5876735a
[5] Bits (Encoded target):  46216c17
    target computed from bits: 10356793971791534424976101420669664288187918308140384256
    [5b] acceptable minging hash limit: 0x0000000000000000006c21460000000000000000000000000000000000000000
[6] Nonce:  0d22021e
Block header (80 Bytes): 00000020c44a17b82afb7103f6ebfa5ab48756f5396c45c57fa1480000000000000000000c59422cc9866aa0ad279c
c64f25b55df5ef3e16629c6c777426576e1e732aa55876735a46216c170d22021e
[C] computed block hash: 000000000000000000001629bf3ed0be699ed5bfb84dcd73a415b926fc516c4fcb
    (obtained by applying SHA-256 two times to the block header.)
Block validation: [A] = [C] and [C] < [5b]
PS C:\Bun\2_IndStudy\S2018\BlockChain\Bitcore\Notes>
```

Difficulty Level

- It is adjusted every 2 weeks to ensure that the estimated average block creation time is 10 minutes.
- Miners are racing to mine block faster, which will them make mining more difficult.

Bitcoin as a cryptocurrency

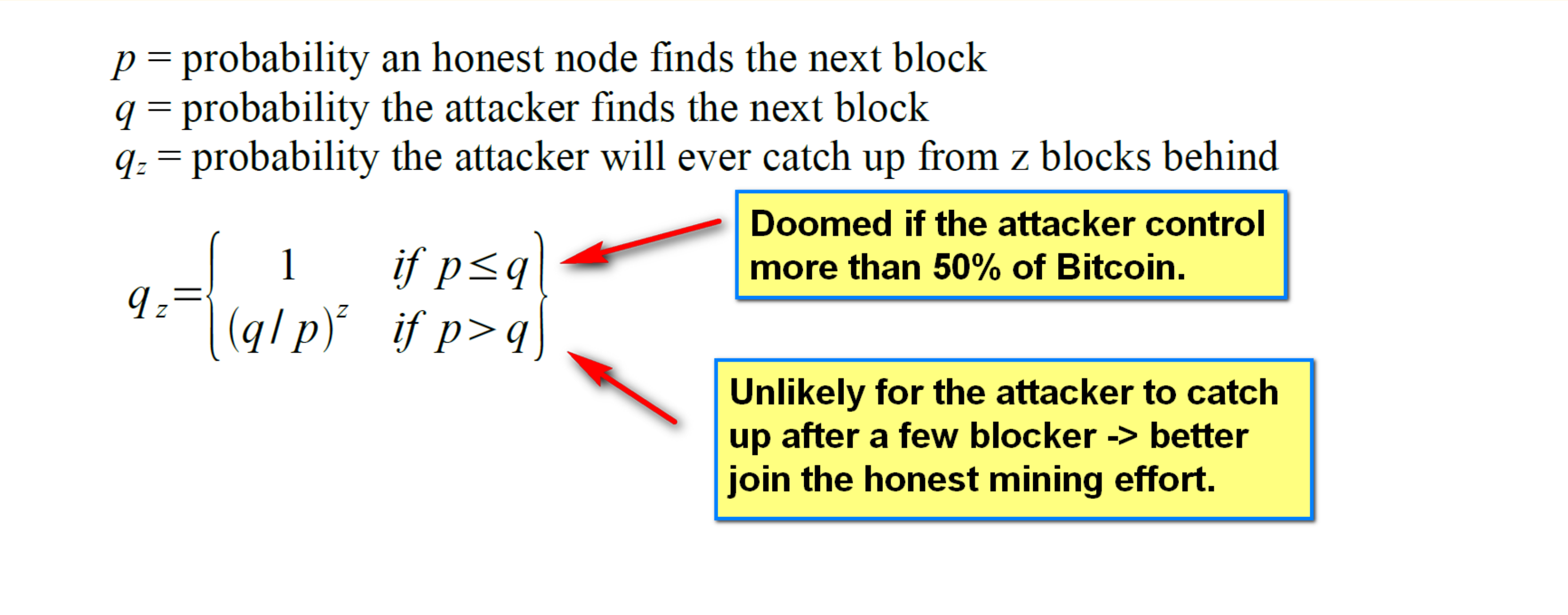
1. Solving the ‘usage’ problem:
    1. Authenticity: hashing, bitcoin address, signature.
    2. Delivery to the right party: checking and updating the blockchain.
    3. No double spending: check the blockchain whether an output transaction has been spent.
2. Solving the value problem:
    1. No intrinsic value such as ‘back up by…”
    2. Network trust.

Bitcore's Security

- No known case of successful hacking of the Bitcoin network.
- The Bitcoin network is rather tamper-proof.

Avoiding attacker controlling the network.

- From Satoshi:



p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \left\{ \begin{array}{ll} 1 & \mathit{if}\ p \le q \\ (q/p)^z & \mathit{if}\ p > q \end{array} \right\}$$

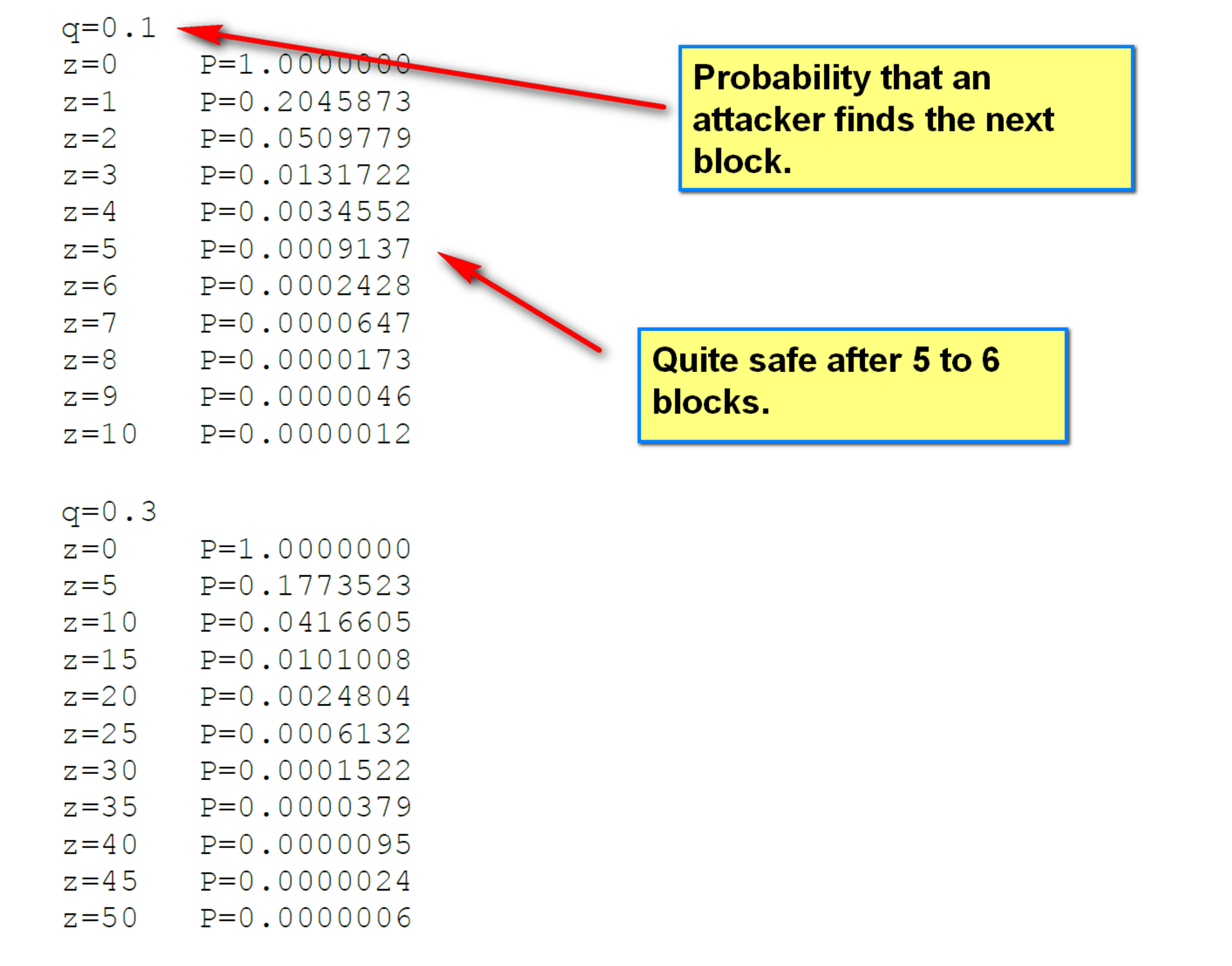
Doomed if the attacker control more than 50% of Bitcoin.

Unlikely for the attacker to catch up after a few blocker -> better join the honest mining effort.

Ensuring sender's attack to be minimal

- Scenario (from Satoshi):
  1. A sender send some BTC to someone in a transaction.
  2. After a while (z block), the sender (attacker) changes the transaction to pay to himself (may be another of his account).
  3. The recipient is alerted, but it may be too late.
- The attacker's potential progress can be modeled by a Possion distribution with an expected value of zq/p.

Result



```
q=0.1
z=0      P=1.0000000
z=1      P=0.2045873
z=2      P=0.0509779
z=3      P=0.0131722
z=4      P=0.0034552
z=5      P=0.0009137
z=6      P=0.0002428
z=7      P=0.0000647
z=8      P=0.0000173
z=9      P=0.0000046
z=10     P=0.0000012

q=0.3
z=0      P=1.0000000
z=5      P=0.1773523
z=10     P=0.0416605
z=15     P=0.0101008
z=20     P=0.0024804
z=25     P=0.0006132
z=30     P=0.0001522
z=35     P=0.0000379
z=40     P=0.0000095
z=45     P=0.0000024
z=50     P=0.0000006
```

Probability that an attacker finds the next block.

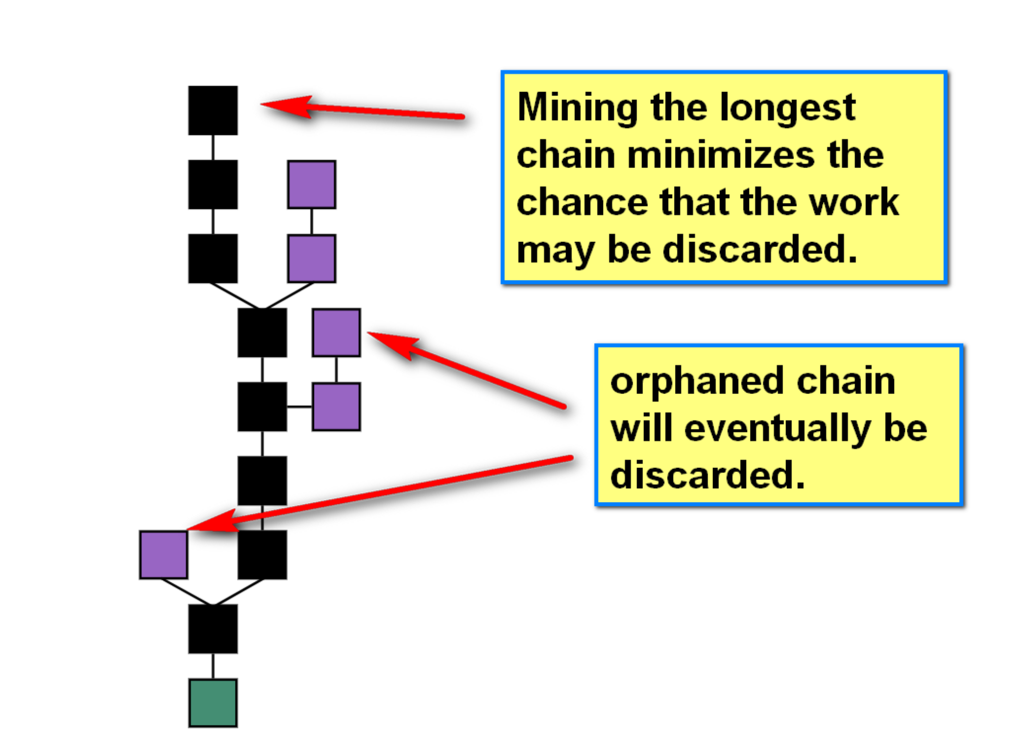
Quite safe after 5 to 6 blocks.

Consensus Problem in Distributed Systems

- Summary of the Bitcoin's process.
  1. Transactions are broadcast to nodes.
  2. Miners collect transactions into a block.
  3. When the proof of work of a block is found, miners broadcast the block and receive the mining rewards.
  4. A receiving node validate the block. Once validated, the node works on the next block.
- What should a receiving node do when *multiple* blocks have been mined and broadcasted to it?

Which block?

- Solution: Use the block in the longest chain.
  - The longest chain provides more chance for mining rewards.



Mining the longest chain minimizes the chance that the work may be discarded.

orphaned chain will eventually be discarded.

Chain’s Evolution

- This means that a block can be discarded.
- Thus, most Bitcoin clients consider confirmation of
  - Transaction: after 6 blocks.
  - Bitcoin mining award: after 100 blocks.

Summary

- Bitcoin: future unknown.
- Many technical innovations.
- Many interesting research and practical problems.
- Good to be in STEM majors.
- Send me some Satoshi. Just kidding, I don't have a Bitcoin address.

Burning Questions and Thank You