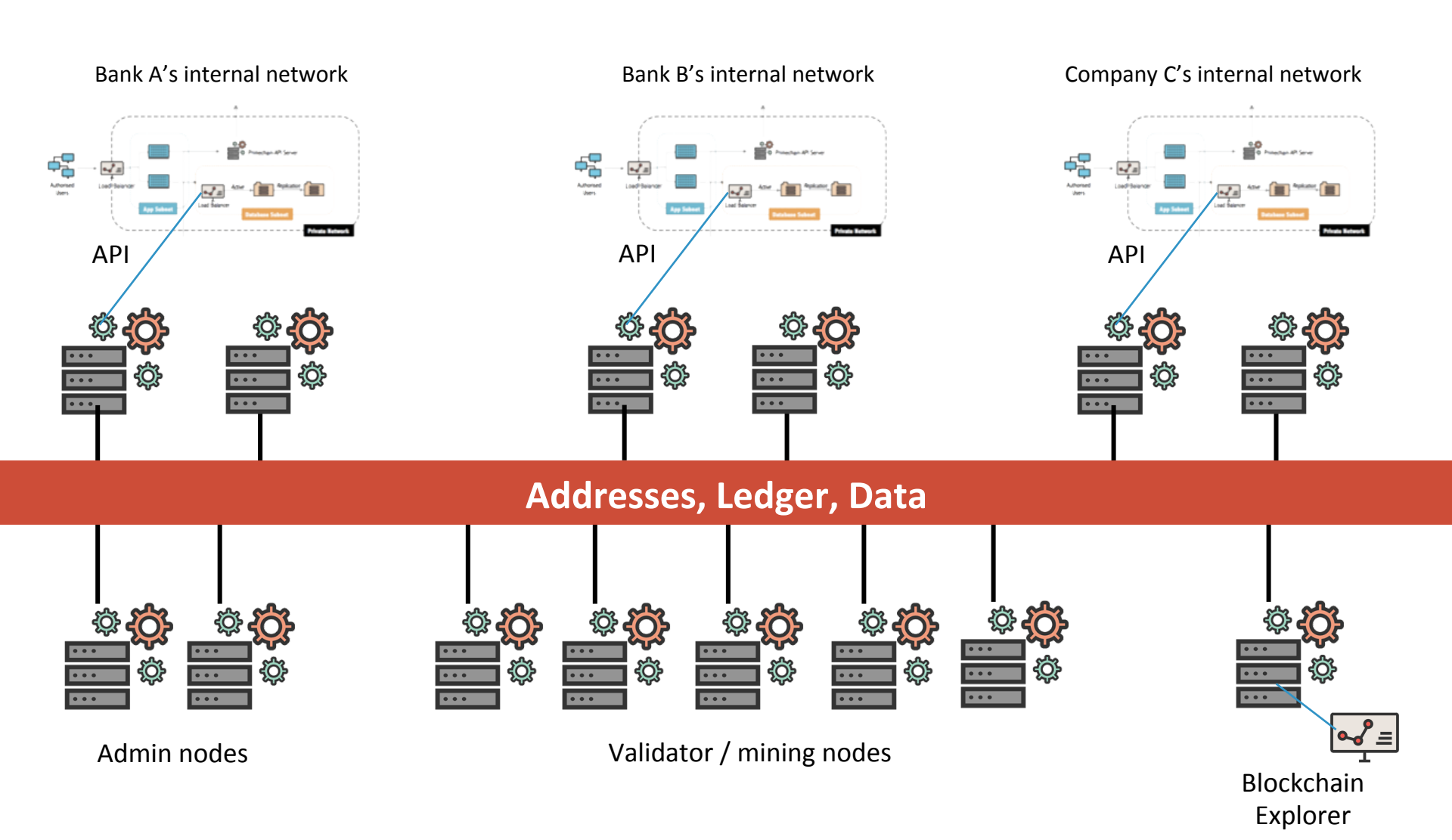
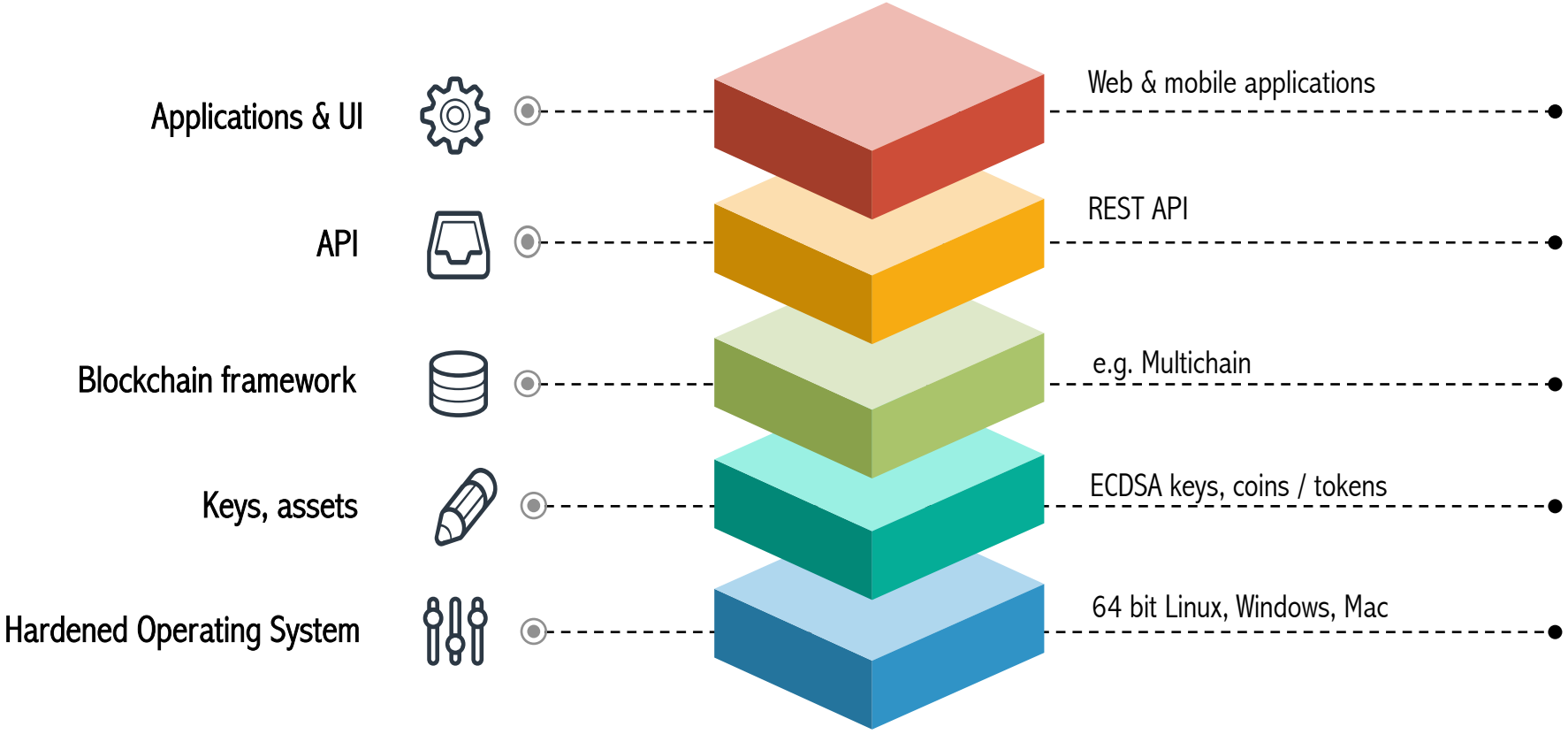
Blockchain Basics

Rohas Nagpal

Concept	Tech Terms	Public Blockchains	Practical Blockchain	Security


Bank A’s internal network
Bank B’s internal network
Company C’s internal network
API
API
API
Addresses, Ledger, Data
Admin nodes
Validator / mining nodes
Blockchain Explorer

Conceptual


Applications & UI
API
Blockchain framework
Keys, assets
Hardened Operating System
Web & mobile applications
REST API
e.g. Multichain
ECDSA keys, coins / tokens
64 bit Linux, Windows, Mac

Hash functions

sha256 (64) One-way Hash Function
Returns a hexadecimal number of 64 digits

Input	Hash
sanya	834ac48d8e6d1d7f0b8d21a5b3e81446f5a4caa63765cc23836f61844b67fb83
SANYA	4247bff9d41c0f2da68ef43c5624531da9ca5bc31b39760a67e32265082e1ba8
Sanya	513a15ed036e62c14b41b2608a5bb18aa7af2a3502c90b892f9dddabaf136bc2

Input	Hash
	b48928ef0131d6fb61b5cee25163ae104a25f0edbd4230f2e7b3daa4a9b057d3
	043a718774c572bd8a25adbeb1bfcd5c0256ae11cecf9f9c3f925d0e52beaf89

https://emn178.github.io/online-tools/sha256.html

Hexadecimal

Hexadecimal	Decimal
0 - 9	0 - 9
a	10
b	11
c	12
d	13
e	14
f	15

Hexadecimal	Decimal
0123456789abcdef	81985529216486895
0023456789abcdef	9927935178558959
0003456789abcdef	920735923817967
0000456789abcdef	76310993685999

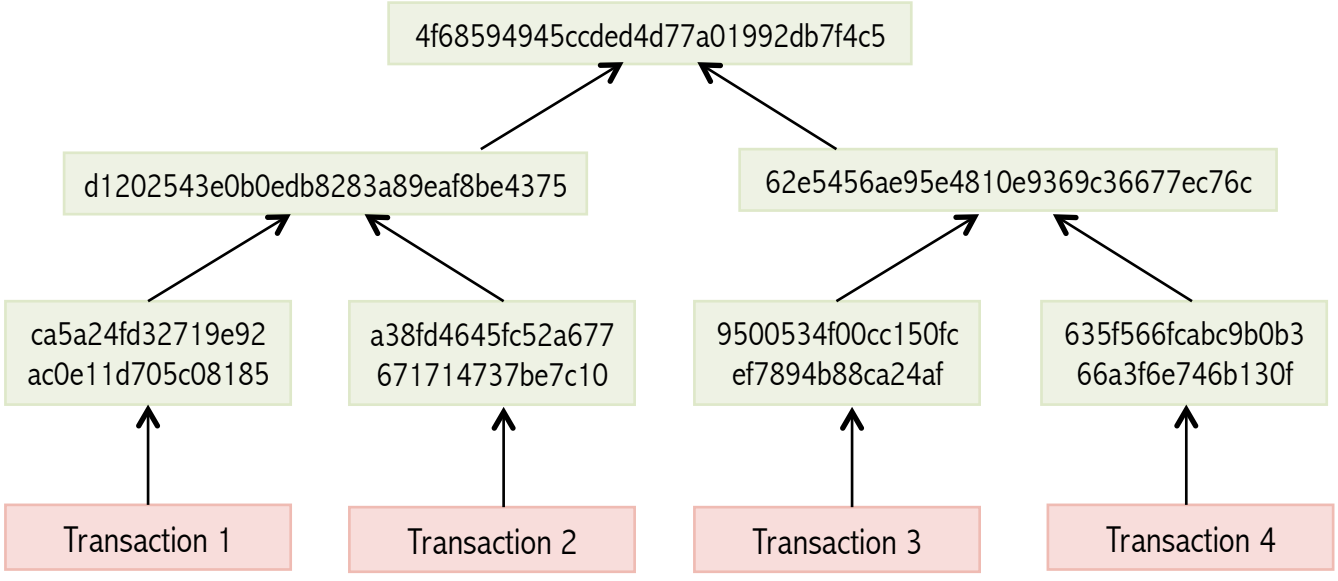
You can try the hexadecimal to decimal converter here:
https://www.rapidtables.com/convert/number/decimal-to-hex.html

Tech terms

- ☑ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ○ Miners
- ○ Keys

- **Hash functions** take an electronic record (such as a PDF file, a video, an email etc.) and produce a fixed-length output e.g. 64 characters.
- If the information is changed in any way – even a comma is changed in a 3000 page document – a different output value is produced.
- There's no way to calculate the original record from the hash.

Merkle Tree



Each transaction is digitally signed by the sender's private key

- Sender's address
- Receiver's address
- Asset
- Quantity

15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb
12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7
SanyaCoin
25

Proof of work

1. Sender^Receiver^Timestamp^Nonce
2. Hash begins with 4 zeros

input	sanya@example.com^samairah@example.com^1633083025593^0
hash	6d64ea2efd1aa3b21909e64f605a4f875b3985e86b218943e7489f521dc565e4

input	sanya@example.com^samairah@example.com^1633083025593^1
hash	6479a7f3b15e5cfa4c199e5dc55255ba1931a77ec6dbddb1f050e303e22bc785

... increase nonce till ....

input	sanya@example.com^samairah@example.com^1633083025593^161000
hash	0000f8f6092ab3e99b64498c5c076a05d0fa11e2d2dc8cd4fb9922366cce34a9

- Infinite nonces exists for any given string.
- Computing nonce is not trivial, verification is.

Successful nonces below 500000 for sanya@example.com^samairah@example.com^1633083025593^

161000: 0000f8f6092ab3e99b64498c5c076a05d0fa11e2d2dc8cd4fb9922366cce34a9

202312: 00001f4ef566329793537e0a80d383dfe2b22094e9190f9cb164f85331cdbe10

290121: 00003d69dde677f9a075bbfb99711791bcf0769e87d5472c4c4c83f48e73cd53

321204: 0000e5568c58683f350911ce4220526f789c55c72041d51e332bc667e005aa2b

371484: 0000e2ad4784e07506d84392af36f96604eed4b2c18784162f8280da7b3ba0a4

375962: 00000d10f84056ea3f6511c89f77a68d9fc78645f65a8f81da3e9ecebe75e77b

384144: 0000123625b4c8fa92e0c1b92e12ae7dcf292e80eec9587b3acfff4841b0a938

388971: 00005cb9e30b73df8fc7519b534a7b29d130775bc8d97183a7d27e941321dc28

Message ID	<CAOskhaDiE6x+2kN28gsj24HfmZcmmQb2Nt0zqDFFpL77UZ6mVA@mail.wraptokens.com>
Created at:	Fri, Oct 1, 2021 at 3:40 PM (Delivered after 15 seconds)
From:	Shinam Arora <shinam@wraptokens.com>
To:	Rohas Nagpal <rohas@wraptokens.com>
Subject:	Crypto with Rohas
SPF:	PASS with IP 23.83.209.24 Learn more
DKIM:	'PASS' with domain wraptokens.com Learn more
POW:	'PASS' with 89804 Learn more

CAOskhaDiE6x+2kN28gsj24HfmZcmmQb2Nt0zqDFFpL77UZ6mVA@mail.wraptokens.com
^shinam@wraptokens.com^rohas@wraptokens.com^1633026600^89804

000050cb0c7f59a6e0e1e9cb27937a8a43d23152e811e51b4d8a643c73e3997c

Tech terms

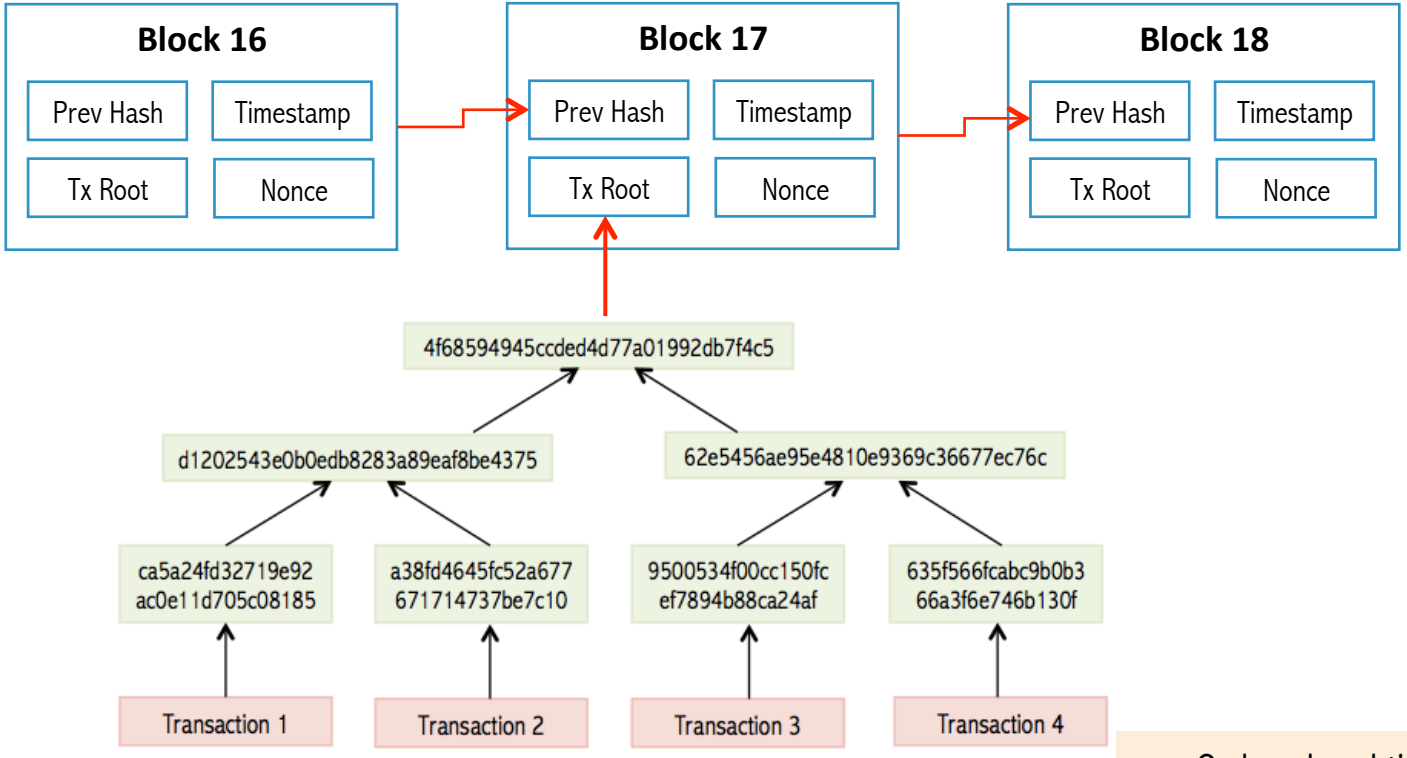
- ○ Hash functions
- ☑ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ○ Miners
- ○ Key issues

Can you double-spend physical currency?
In case of physical currency notes, you cannot double-spend a note because once you hand the note over to someone, you don't have the note anymore to spend again.

Can you double-spend virtual currency?
Since electronic records are easily duplicated, a "digital coin" can be spent multiple times.

Now imagine a digital coin that cannot be spent multiple times...
... that is the innovation of Bitcoin

Blockchain



- Ordered and time-stamped record.
- Prevents double-spending.
- Prevents modification of previous records.

Bitcoin

- Bitcoin's first block, block 0, was mined on January 03, 2009 at 11:45 PM GMT.
- The Bitcoin block reward halves every 210,000 blocks.
- The current block reward is 6.25 and will become 3.125 BTC after the halving at block 840,000 (approx 06-May-2024 12:39 UTC).
- Difficulty changes every 2016 blocks - approx 14 days.
- Blockchain events (halving, forking, ICOs etc.) are measured in blocks and not conventional dates / times.

Bitcoin

- After six confirmations/blocks, a transaction is confirmed beyond reasonable doubt.

See:

- https://en.bitcoin.it/wiki/Bitcoin
- https://en.bitcoin.it/wiki/Difficulty

The raw hex version of the Genesis block looks like:

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

See: https://en.bitcoin.it/wiki/Genesis_block

Block 703326

USD BTC

This block was mined on October 03, 2021 at 12:26 PM GMT+5:30 by Poolin. It currently has 5 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC ($299,424.94). The reward consisted of a base reward of 6.25000000 BTC ($299,424.94) with an additional 0.05706740 BTC ($2,733.98) reward paid as fees of the 1113 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 2,622.38402955 BTC ($125,633,147.86) were sent in the block with the average transaction being 2.35614019 BTC ($112,877.94). Learn more about how blocks work.

Hash	00000000000000000007a5d52bf48ad43772b0564087de0ddbbc34ef240f2156
Confirmations	5
Timestamp	2021-10-03 12:26
Height	703326
Miner	Poolin
Number of Transactions	1,113

Tech terms

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

- While a gold miner digs into the earth to discover gold, a bitcoin miner uses computational power to calculate hashes.
- To add an entire block to the block chain, a Bitcoin miner must successfully hash a block header to a value below the target threshold.
- Miners spend on **computational power** and **electricity** and are compensated by way of a **reward** for each block they mine and **transaction fees**.
- Miners usually operate as part of a large pool instead of as individuals.

Tech terms

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

Hashrate = speed of mining (hash / second)

The number of times hash values are calculated for PoW every second.

Measured in units of:

- k (kilo, 1,000)
- M (mega, 1 million)
- G (giga, 1 billion)
- T (tera, 1 trillion)

Tech terms

- Hash functions
- Proof of work
- Merkle Tree
- Blockchain
- ☑ Miners
- Key issues

Roll over image to zoom in

AntMiner T9+ 10.5TH/s @ 0.136W/GH 16nm ASIC Bitcoin & Bitcoin Cash Miner

Brand: Bitmain

4.2 out of 5 stars 19 ratings | 28 answered questions

Available from these sellers.

- Designed for reliability, stability, and longevity.
- Hash Rate: 10.5TH/s ±7%.
- Power Consumption: 1450W ±7% (Power supply sold separately).
- Easy to use web interface. No host computer required.
- Power supply sold separately. APW3++ on a 220v outlet recommended OR EVGA SuperNova 1600 G2.

Tech terms

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

Tech terms

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

Transaction Fees

- When a new bitcoin block is generated, the information for all of the transactions is included with the block.
- All transaction fees are collected by that miner.
- Transaction fees are voluntary for the person making the bitcoin transaction.
- No miner necessarily needs to accept the transactions and include them in the new block being created.

Transaction Details

Overview | State | Comments

Transaction Hash:	0x4c102e972301b999318df70e3d3a067994dcc83951f07f7f37c45ff7e922beec
Status:	Success
Block:	12998572 347285 Block Confirmations
Timestamp:	53 days 18 hrs ago (Aug-10-2021 04:39:03 PM +UTC) | Confirmed within 30 secs
From:	0xc8a65fadf0e0ddaf421f28feab69bf6e2e589963 (PolyNetwork Exploiter 1)
To:	0xc8a65fadf0e0ddaf421f28feab69bf6e2e589963 (PolyNetwork Exploiter 1)
Value:	0 Ether ($0.00)

Overview State Comments

Gas Limit:	2,000,000
Gas Used by Transaction:	22,104 (1.11%)
Base Fee Per Gas:	0.000000049687887027 Ether (49.687887027 Gwei)
Burnt Fees:	0.001098301054844808 Ether
Nonce Position	22 11
Input Data:	WHAT IF I MAKE A NEW TOKEN AND LET THE DAO DECIDE WHERE THE TOKENS GO

View Input As

EOS Staking

Estimated Yearly Reward **1% - 2%**

Minimum Requirement **0.25 EOS**

Deposit | Buy

NEO Staking

Estimated Yearly Reward **1% - 2%**

Minimum Requirement **0.001 NEO**

Buy

ONE Staking

Estimated Yearly Reward **1% - 2%**

Minimum Requirement **100 ONE**

Deposit | Buy

QTUM Staking

Estimated Yearly Reward **1% - 1.5%**

Minimum Requirement **1 QTUM**

Deposit | Buy

TRX Staking

Estimated Yearly Reward **1% - 3%**

Minimum Requirement **5 TRX**

Deposit | Buy

XTZ Staking

Estimated Yearly Reward **1.5% - 3%**

Minimum Requirement **1 XTZ**

Buy

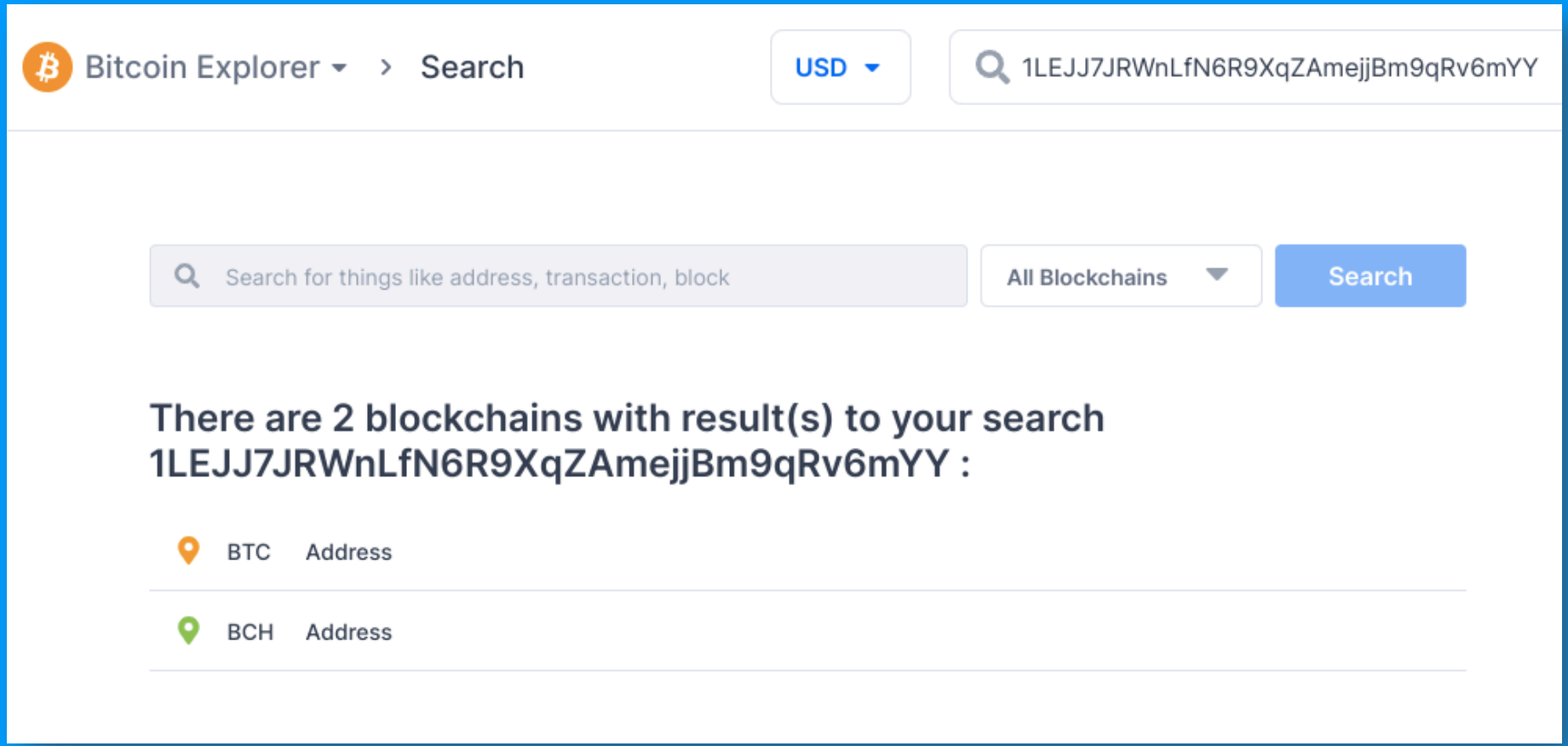
Generate paper wallets

Bitcoin | Dash | Dogecoin | Ethereum | Litecoin

A paper wallet is an offline mechanism for storing crypto keys. A "Wallet Import Format" (wif) is a shorter version of a private key. It is STRONGLY advised that these keys should not be used for any high-value, or long-term storage, addresses.

```
stdClass Object
(
    [private] => 803b057c062d6b5443ce5fc84647af0d339d87f3dc8da89d7d00ee32dfce0
    [public] => 02bc47b5fdbcdec4b9dc3231344753b1c9796487c747526f01a448ba8e8dc0
    [address] => 1LEJJ7JRWnLfN6R9XqZAmejjBm9qRv6mYY
    [wif] => L1WyTrwYi7tTVsWAMW2estwvJu7yHC61jfyK5EbYJLN6hQu3sGwN
)
```

For more on Keys, Addresses, Wallets, see:
https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch04.html



https://www.blockchain.com/search?search=1LEJJ7JRWnLfN6R9XqZAmejjBm9qRv6mYY

Bitcoin

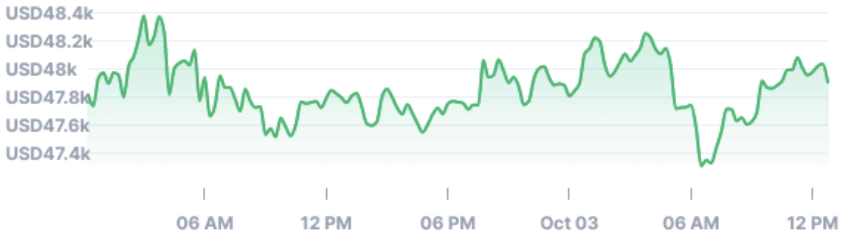
Blockchain information for Bitcoin (BTC) including historical prices, the most recently mined blocks, the mempool size of unconfirmed transactions, and data for the latest transactions.

$47,907.99	168.099 EH/s	230,200	3.150m BTC	39,801 BTC
Price →	Estimated Hash Rate →	Transactions (24hrs) →	Transaction Volume →	Transaction Volume (Est) →

Price

The price of Bitcoin over the last day

1 Day



View All Prices →

Mempool Size (Bytes)

The aggregate size of unconfirmed transactions in bytes

1 Day

View All Charts →

Latest Blocks

The most recently mined blocks

Height	Mined	Miner	Size
703330	5 minutes	Unknown	450,082 bytes
703329	7 minutes	F2Pool	1,452,738 bytes
703328	9 minutes	AntPool	1,358,422 bytes
703327	13 minutes	Unknown	1,323,995 bytes
703326	30 minutes	Poolin	1,139,093 bytes
703325	31 minutes	ViaBTC	1,432,363 bytes

View All Blocks →

Latest Transactions

The most recently published unconfirmed transactions

Hash	Time	Amount (BTC)	Amount (USD)
a465dcf0a4a9e94fe2e18...	12:57	0.02996321 BTC	$1,435.48
0edcb71673b3e5386580...	12:57	0.01034288 BTC	$495.51
edceba0cfee1d9c4ac1bf8...	12:57	0.00958346 BTC	$459.12
dbf8f84474e0e9a47c93b...	12:57	0.00447512 BTC	$214.39
2b0134e8ddddd76ce253...	12:57	1.99991733 BTC	$95,812.02
3ed1216a5cbbd60d65618...	12:57	0.00091483 BTC	$43.83

View All Transactions →

Block 703326

USD BTC

This block was mined on October 03, 2021 at 12:26 PM GMT+5:30 by Poolin. It currently has 5 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC ($299,424.94). The reward consisted of a base reward of 6.25000000 BTC ($299,424.94) with an additional 0.05706740 BTC ($2,733.98) reward paid as fees of the 1113 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 2,622.38402955 BTC ($125,633,147.86) were sent in the block with the average transaction being 2.35614019 BTC ($112,877.94). Learn more about how blocks work.

Hash	00000000000000000007a5d52bf48ad43772b0564087de0ddbbc34ef240f2156
Confirmations	5
Timestamp	2021-10-03 12:26
Height	703326
Miner	Poolin
Number of Transactions	1,113

Difficulty	18,997,641,161,758.95
Merkle root	02e46b72d9d4d9c408a98e169ef1c1e6dcb0ba496d819a73712532ac1397c842
Version	0x3fffe004
Bits	386,846,955
Weight	3,999,605 WU
Size	1,139,093 bytes
Nonce	769,993,502
Transaction Volume	2622.38402955 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.05706740 BTC

Block Transactions

Fee 0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 362 bytes)
(0.000 sat/vByte - 335 virtual bytes)

6.30706740 BTC

5 Confirmations

Hash cfbef44fff531b05d51f59936169ba0f863ba5096...

2021-10-03 12:26

COINBASE (Newly Generated Coins)

1PQwtwajfHWyAkedss5utw... 6.30706740 BTC
OP_RETURN 0.00000000 BTC
OP_RETURN 0.00000000 BTC
OP_RETURN 0.00000000 BTC

Fee 0.00050000 BTC
(131.579 sat/B - 65.963 sat/WU - 380 bytes)
(263.158 sat/vByte - 190 virtual bytes)

0.16338598 BTC

5 Confirmations

Hash 0fef11e026f2eded64604deb30f4f6a46e060ce0...

2021-10-03 12:26

bc1qwqdg6squsna38e4679... 0.16388598 BTC

3DpCVv9NDD2Zhtz1DsVH2... 0.03000000 BTC
bc1qwqdg6squsna38e4679... 0.13338598 BTC

Address

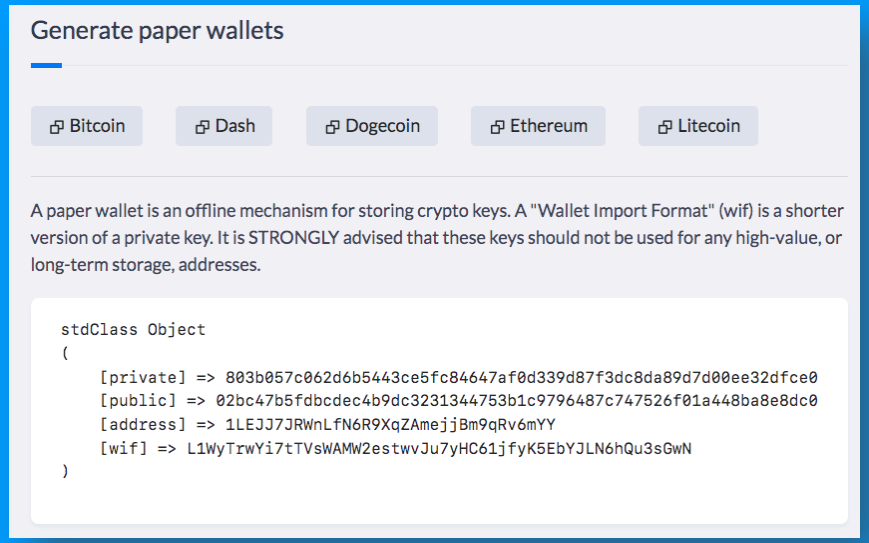
USD BTC

This address has transacted 2,202 times on the Bitcoin blockchain. It has received a total of 7,724.32374103 BTC ($370,056,824.54) and has sent a total of 7,622.88129432 BTC ($365,196,920.82). The current value of this address is 101.44244671 BTC ($4,859,903.72).

Address	1PQwtwajfHWyAkedss5utwBvULqbGocRpu
Format	BASE58 (P2PKH)
Transactions	2,202
Total Received	7724.32374103 BTC
Total Sent	7622.88129432 BTC
Final Balance	101.44244671 BTC

Transactions

Fee	0.00002812 BTC (12.442 sat/B - 3.111 sat/WU - 226 bytes)	-6.34876803 BTC 3 Confirmations
Hash	b4baf044230485fcc54f87b4b88e0e29f3c72de...	2021-10-03 12:31
	1PQwtwajfHWyAkedss5utw... 6.34876803 BTC	1DAWZskS3hW1zbw1NbJX... 0.23874048 BTC 1zgmvYi5x1wy3hUh7AjKgpc... 6.10999943 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 362 bytes) (0.000 sat/vByte - 335 virtual bytes)	+6.30706740 BTC 4 Confirmations



Blockchain API

```php
<?php
$ch = curl_init('https://api.blockcypher.com/v1/btc/main/addrs');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_POSTFIELDS, $post);

// execute!
$response = curl_exec($ch);

// close the connection, release resources used
curl_close($ch);

echo "<div class='table-responsive'><div class='element-box'><pre>";
print_r(json_decode($response)); // print json decoded response
echo "</div><div></pre>";
?>
```

Symmetric encryption

I fear not the man who has practiced 10,000 kicks once, but I fear the man who has practiced one kick 10,000 times.

AES Password: o9tgRCETlHLZdNhlKKgdDshgiwvujn84
AES initialization vector: LdjZLovqIkL3
AES authentication tag: 210, 255, 136, 213, 61, 82, 117, 102, 222, 62, 93, 134, 245, 113, 100, 82

Encrypted version of the plain text data:
4896275f060be692d50406292602e6cb53a6d30426c11b0658a8dc31ed196ef4841ffa8b9c8d63
15f8798387f93157aa35bb5d280bf208d2bc645e2e184f0ea551a372b924b329b391b6ecf75f3fe
c3a1760ae306de25d3bc36cc30bf93cc9e3988c743c6925f109b6760bca77826bfd7673563b99

Digital signature

A sample ECDSA private key

VFGxBp56YTFwAkwtLn3rxKh4ah8JYRtKf2Kb3YkKyTqFnD1XdyWXmPX6

A sample ECDSA public key

03b085ad524868aa32ba05109bf0448b188bfd3627fde1c91c127d938c07815879

Sample data

I fear not the man who has practiced 10,000 kicks once, but I fear the man who has practiced one kick 10,000 times.

Sample digital signature for the above data

H/zH4VWkOv9/
Awu7OUEK43Fq1dtBcBxnrzmwOdytpsr0Grw+lPxWgbgh3Dcr4lhwgVOBb7vAoChjU
vqxlqnpDAI=

Reading material

Chapter C9. Technical Crypto Concepts of the Future Money Playbook
http://rohasnagpal.com/future-money.php

How to send an email to an Ethereum address
https://rohas.substack.com/p/how-to-send-an-email-to-an-ethereum

Blockchain Consensus Encyclopedia
https://tokens-economy.gitbook.io/consensus

Elliptic Curve Digital Signature Algorithm
https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

How SHA-256 Works Step-By-Step
https://qvault.io/cryptography/how-sha-2-works-step-by-step-sha-256

Bitcoin whitepaper
https://bitcoin.org/bitcoin.pdf

Activities

Create a free **Future Money Wallet** account
https://www.futuremoneywallet.com

- Generate paper wallets: https://www.futuremoneywallet.com/dashboard.php
- Explore the Developer Dashboard: https://www.futuremoneywallet.com/dashboard_dev.php

Explore Bitaddress: https://www.bitaddress.org