

Blockchain 101



Rohas Nagpal

Concept

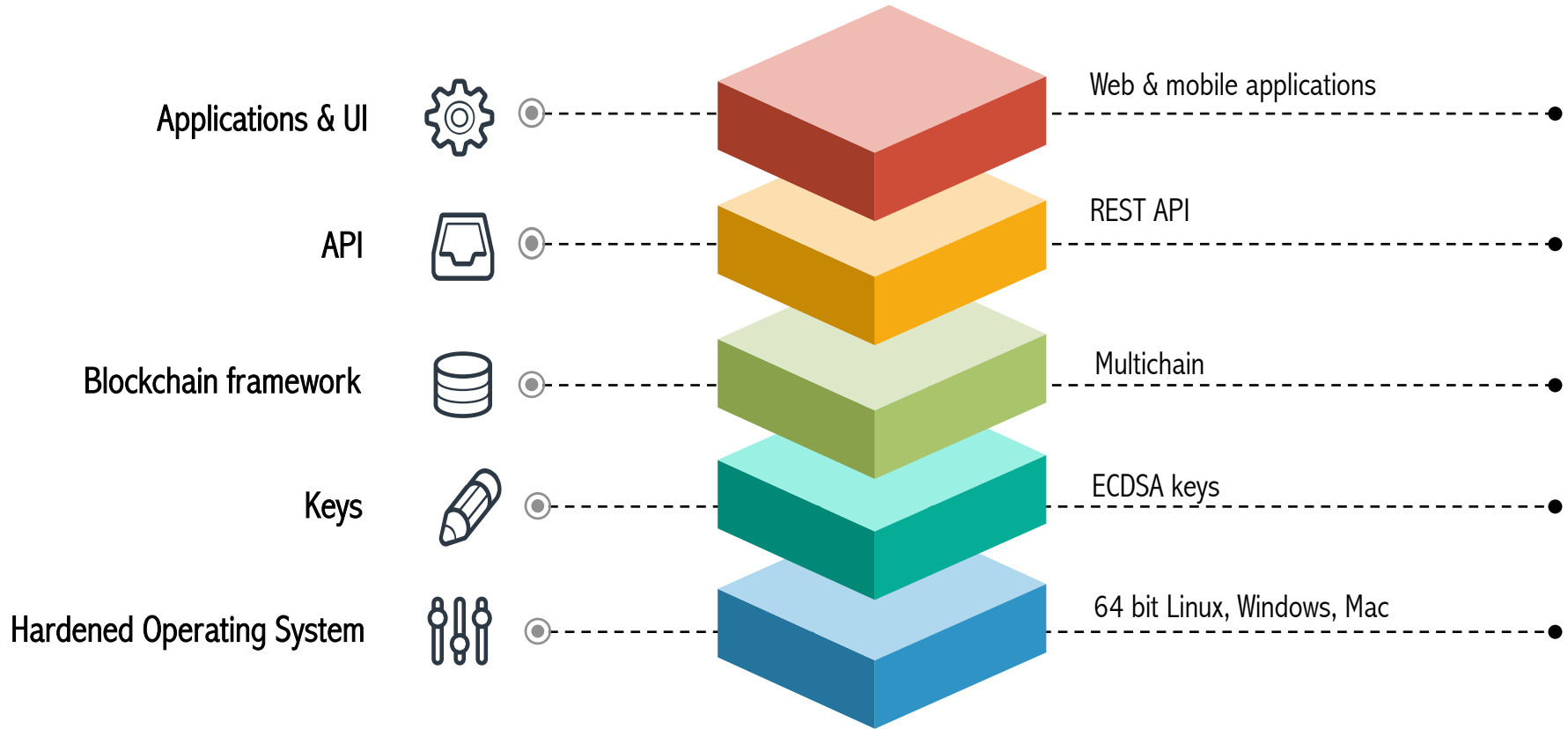
Tech Terms

Public Blockchains

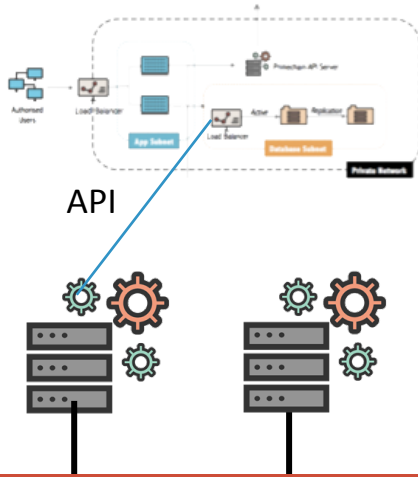
Practical
Blockchain

Security

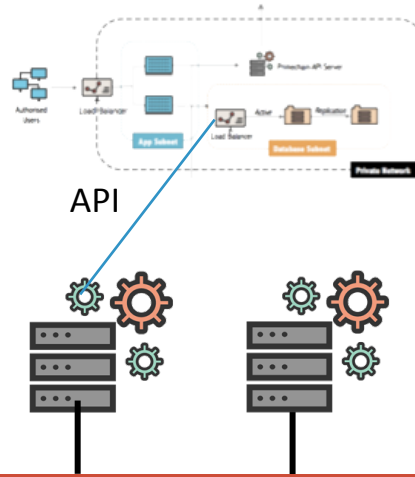
A typical HyFi node



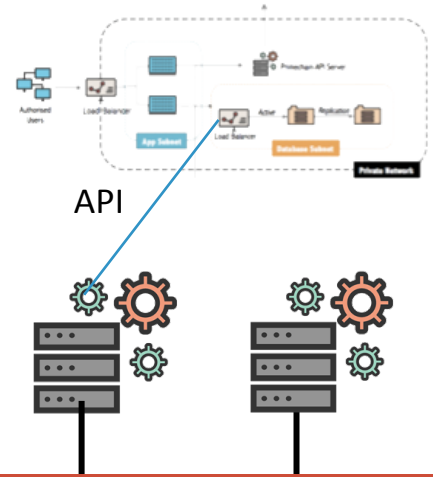
Bank A's internal network



Bank B's internal network



Company C's internal network



Addresses, Ledger, Data Streams

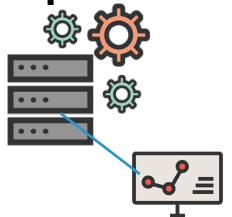
Admin nodes



Validator nodes



Blockchain Explorer





Tech terms

☑ Hash functions

- Proof of work
- Merkle Tree
- Blockchain
- Miners
- Key issues

sha256 (64) One-way Hash Function

Input	Hash
sanya	834ac48d8e6d1d7f0b8d21a5b3e81446f5a4caa63765cc23836f61844b67fb83
SANYA	4247bff9d41c0f2da68ef43c5624531da9ca5bc31b39760a67e32265082e1ba8
Sanya	513a15ed036e62c14b41b2608a5bb18aa7af2a3502c90b892f9dddabaf136bc2

Input	Hash
	b48928ef0131d6fb61b5cee25163ae104a25f0edbd4230f2e7b3daa4a9b057d3
	043a718774c572bd8a25adbeb1bfcd5c0256ae11cecf9f9c3f925d0e52beaf89

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

Tech terms

☑ Hash functions

- Proof of work
- Merkle Tree
- Blockchain
- Miners
- Key issues

- 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.

Proof of work

- 1. $\text{Sender}^{\wedge}\text{Receiver}^{\wedge}\text{Timestamp}^{\wedge}\text{Nonce}$
- 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

Computing hash 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

Original Message

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 89804 Learn more
POW:	'PASS' with domain wraptokens.com 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?

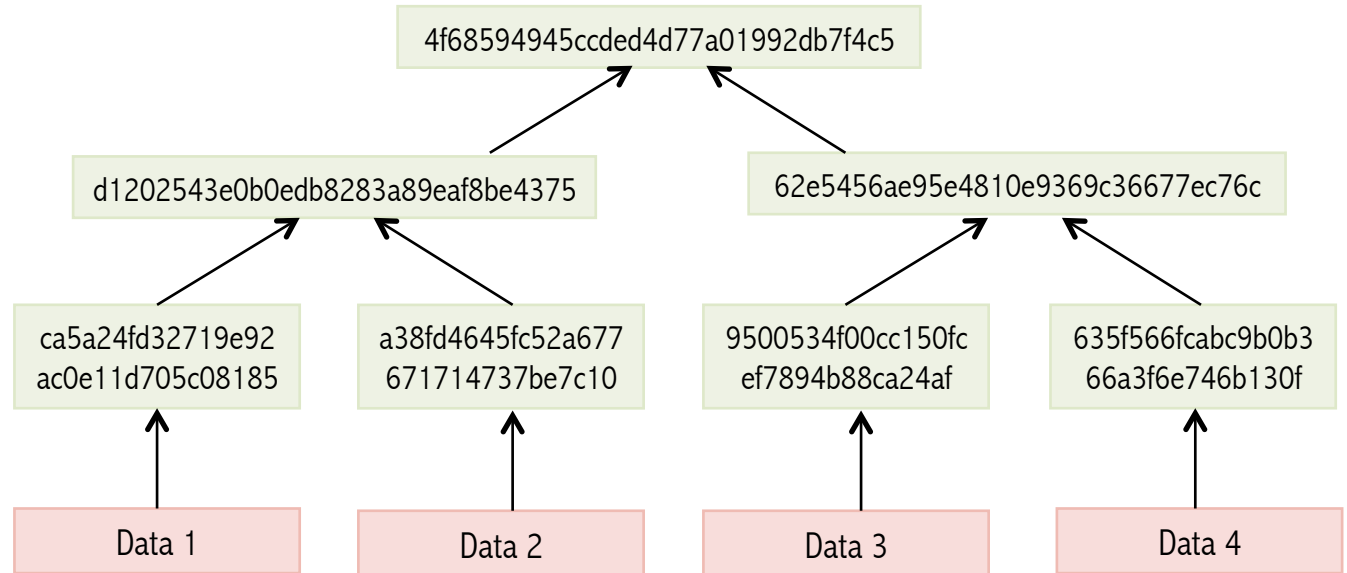
Since electronic records are easily duplicated, a “digital coin” can be spent multiple times.

Now imagine a digital coin that cannot be spent multiple times...

... that is the innovation of Bitcoin

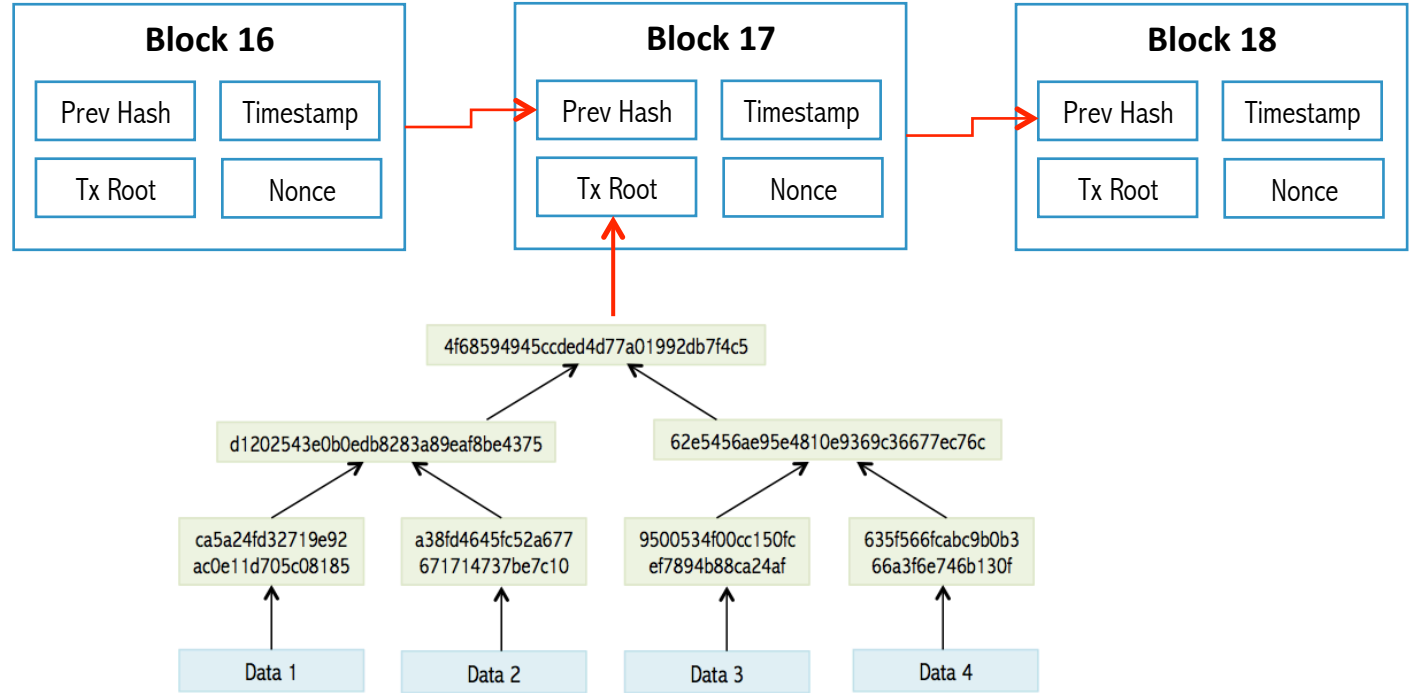
Tech terms

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



Tech terms

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



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

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

★★★★☆ 19 ratings

| 28 answered questions

Available from these
sellers.

- Designed for reliability, stability, and longevity.
- Hash Rate: 10.5TH/s $\pm 7\%$.
- Power Consumption: 1450W $\pm 7\%$ (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



Tech terms

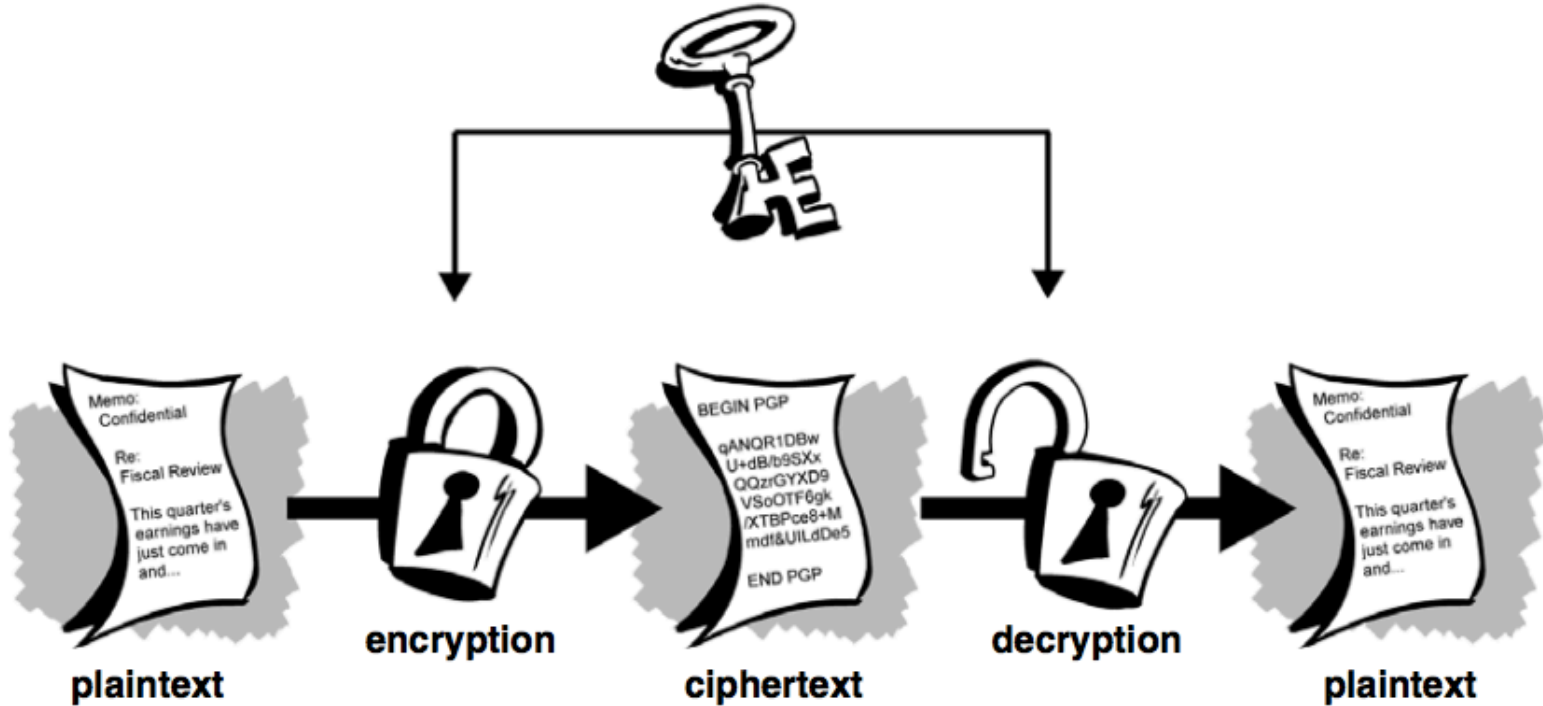
- Hash functions
- Proof of work
- Merkle Tree
- Blockchain
- ☑ Miners
- Key issues

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.



Symmetric encryption





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: o9tgRCETIHLZdNhlKKgdDshgiwvujn84

AES initialization vector: LdjZLovqlkL3

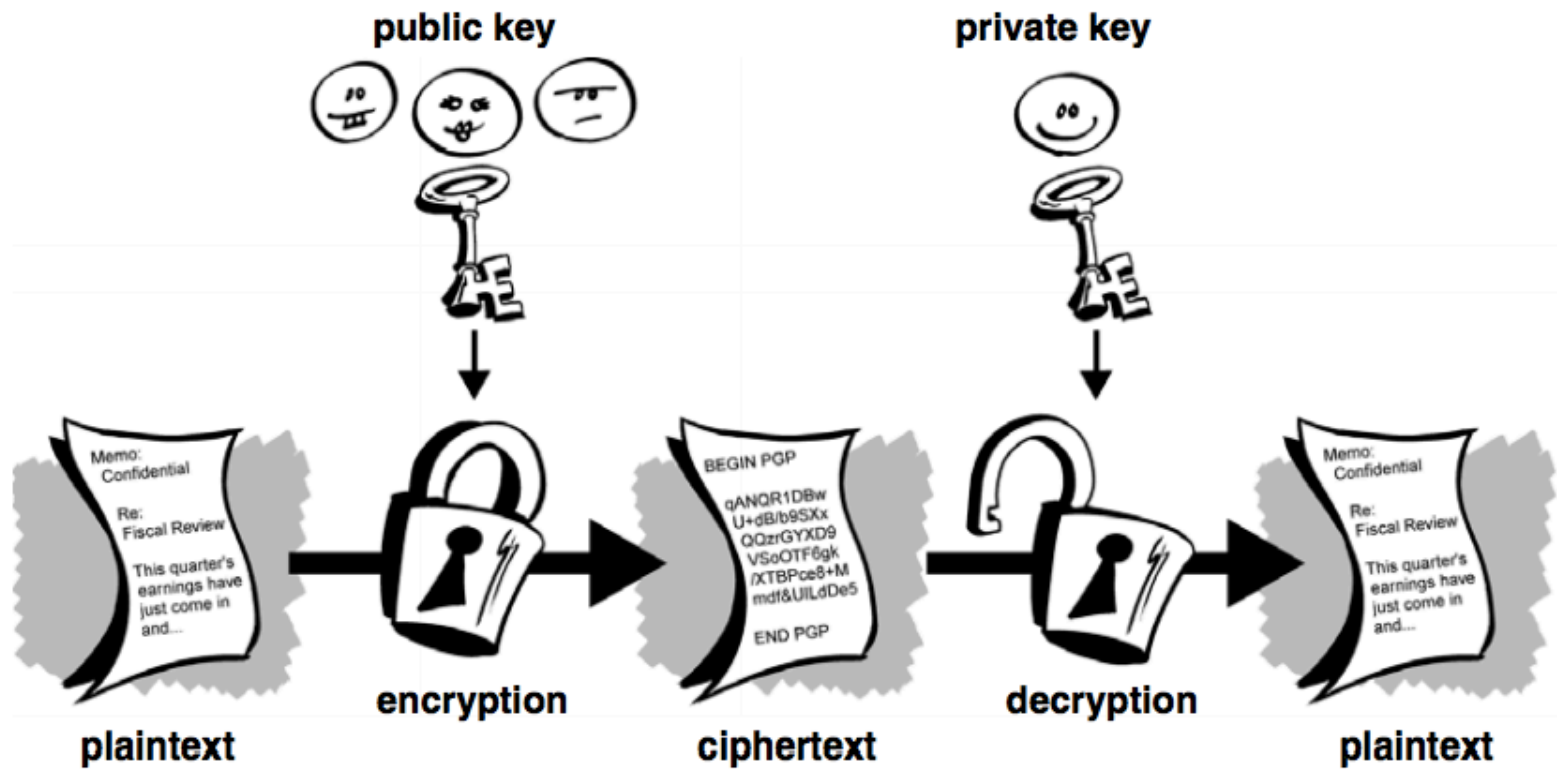
AES authentication tag: 210, 255, 136, 213, 61, 82, 117, 102, 222, 62, 93, 134, 245, 113, 100, 82

Encrypted version of the plain text data:

4896275f060be692d50406292602e6cb53a6d30426c11b0658a8dc31ed196ef4841ffa8b9c8d63
15f8798387f93157aa35bb5d280bf208d2bc645e2e184f0ea551a372b924b329b391b6ecf75f3fe
c3a1760ae306de25d3bc36cc30bf93cc9e3988c743c6925f109b6760bca77826bfd7673563b99



Asymmetric encryption





Asymmetric encryption

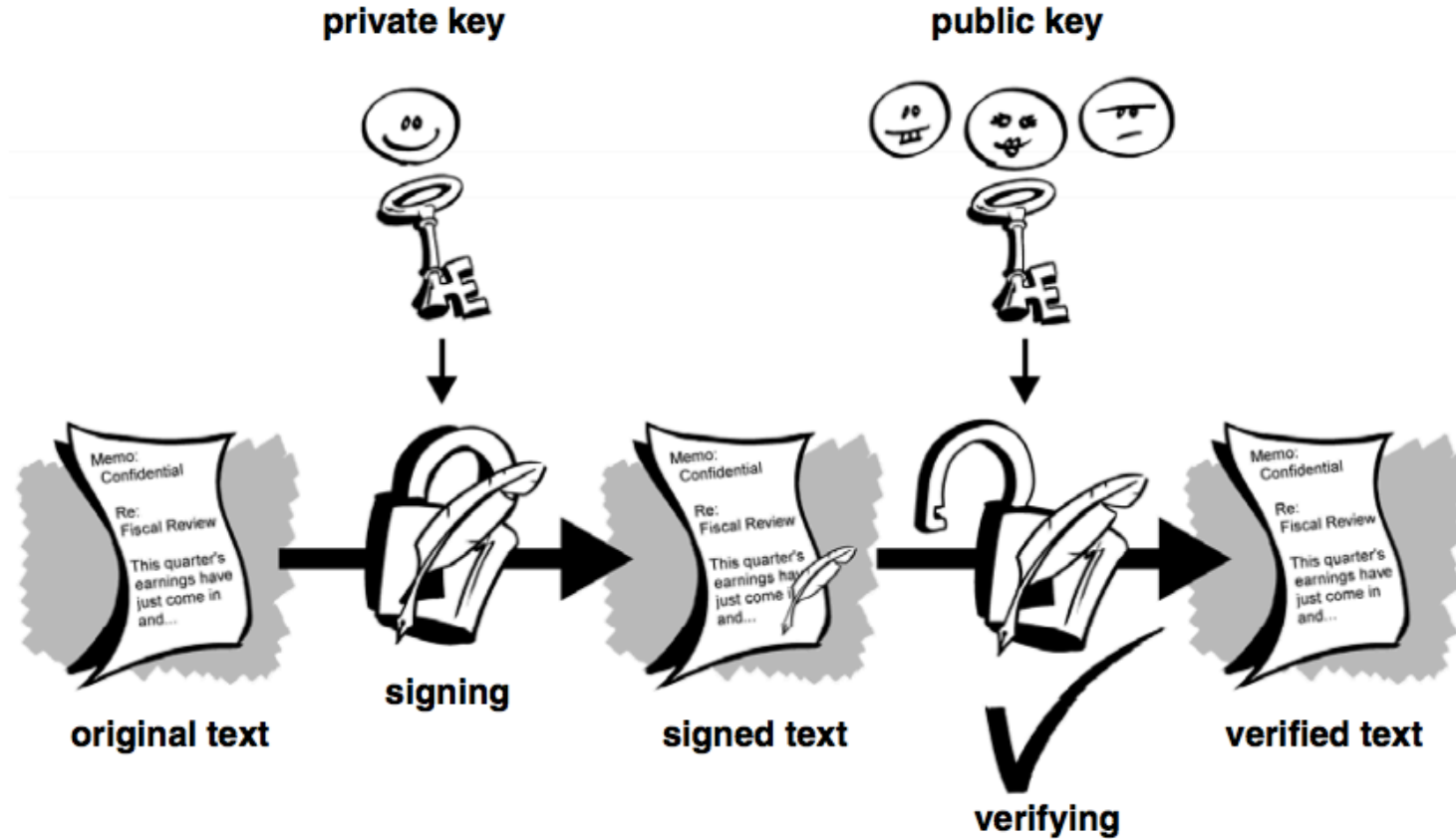
RSA encrypted version of the word “Hello”

acN4z1AbYKHbuK5Tixi+AgYwg/
3XMqVxU3UJmZrXcRuSXYSPyDLrB7+BQeiazfcFk9Wxpn
vT8nXHkQ6Hz2rTUF1K1Lv5XM33iQMqdRUa9WzQGJS9I
akS5TSw+OpxhCR0Kwa1kJ4XIa6QHwCGqUQRUo7WXTV
9k/
Lb55eLZh9bINy6LAAeYQfQX7LZMVCuC7ImJcUAKDTYuc
cgZdtAc1BCHl00Dq7rcMSLpr/
M0h+tjKE6fuGP9AuB7NznoAy+7yf9toy67DNIWAeQXptT
q8ukBJ6AzBTerUbTrbwOWlBW0yVcnsyPkXRtPUNryu5J
vqlw6//w0Fc9FG3dM+lmuzWQ5A==





Digital signature





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/

Awu70UEK43Fq1dtBcBxnrzmwOdytpsr0Grw+IPxWgbgh3Dcr4lhwgVOBb7vAoChjU
vqxlqnpDAI=



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] => 02bc47b5fdbcddec4b9dc3231344753b1c9796487c747526f01a448ba8e8dc0
    [address] => 1LEJJ7JRWnLfN6R9XqZAmejBm9qRv6mYY
    [wif] => L1WyTrwYi7tTVsWAMW2estwvJu7yHC61jfyK5EbYJLN6hQu3sGwN
)
```




Search for things like address, transaction, block

All Blockchains ▾

Search

**There are 2 blockchains with result(s) to your search
1LEJJ7JRWnLfN6R9XqZAmejjBm9qRv6mYY :**



BTC Address



BCH Address

<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

[Price →](#)

168.099 EH/s

[Estimated Hash Rate →](#)

230,200

[Transactions \(24hrs\) →](#)

3.150m BTC

[Transaction Volume →](#)

39,801 BTC

[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
2b0134e8dddd76ce253...	12:57	1.99991733 BTC	\$95,812.02
3ed1216a5cbbd60d65618...	12:57	0.00091483 BTC	\$43.83

[View All Transactions →](#)


USD

USD BTC

Poolin

address.

how blocks work.

Hash	0000000000000000000000007a5d52bf48ad43772b0564087de0ddbbc34ef240f2156 
Confirmations	5
Timestamp	2021-10-03 12:26
Height	703326
Miner	Poolin
Number of Transactions	1,113

Block Data	
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 i

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

Consensus Algorithms

```
graph LR; CA[Consensus Algorithms] --- PoET[Proof of elapsed time (PoET)]; CA --- PoW[Proof-of-Work (PoW)]; CA --- PoS[Proof-of-Stake (PoS)]; CA --- DPoS[Delegated Proof-of-Stake (DPoS)]; CA --- Hybrid[Hybrid PoW / PoS]; CA --- PoA[Proof-of-Authority (PoA)]; CA --- PoB[Proof-of-burn (PoB)]; CA --- PoSt[Proof-of-spacetime (PoSt)];
```

Proof of elapsed time (PoET)

Generates a random "wait time" for which each node goes to sleep. The node with the shortest wait time wakes up first and commits a new block e.g. Hyperledger Sawtooth.

Proof-of-Work (PoW)

Miners "solve" mathematical puzzles by investing in electricity and computational power e.g. Bitcoin, Ethereum.

Proof-of-Stake (PoS)

Users "lock" a number of coins as a "stake" and are randomly assigned validation rights for a new block e.g. Algorand.

Delegated Proof-of-Stake (DPoS)

Users "lock" a number of coins as a "stake" but outsource validation to "delegates" selected based on reputation and trustworthiness e.g. Bitshares.

Hybrid PoW / PoS

This brings together the security of Proof-of-work and the governance and energy efficiency of Proof-of-Stake e.g. Decred.

Proof-of-Authority (PoA)

Identified, known, and credible validators produce blocks in this system meant for private & enterprise blockchains.

Proof-of-burn (PoB)

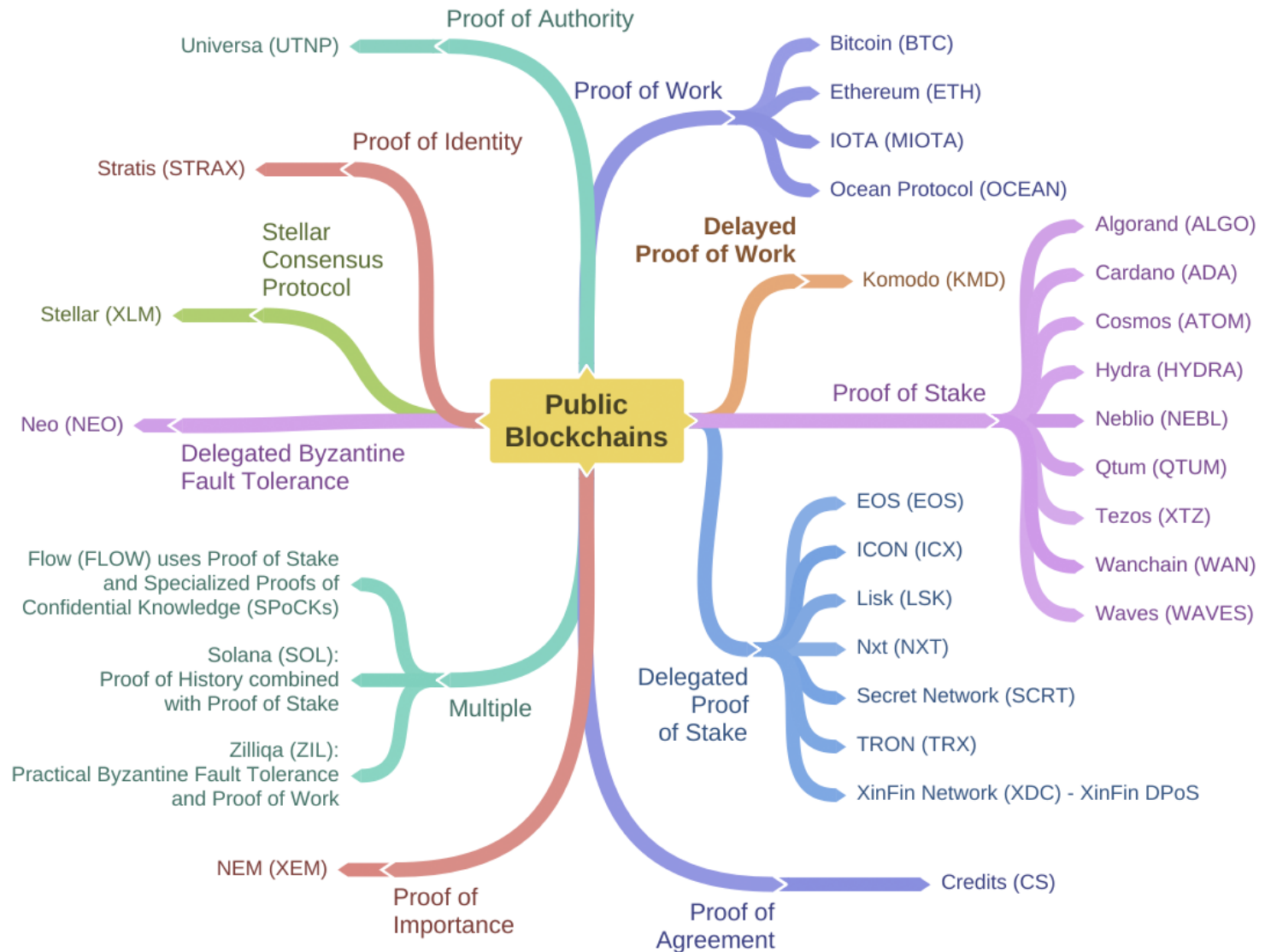
Miners reach a consensus by sending coins to an "eater" or "burn" address. This permanently eliminates coins from circulation, reduces inflation, and validates transactions e.g. Slimcoin.

Proof-of-replication (PoRep)

Storage miners prove 2 things - that they are using space to store replicas of data and that the data can easily be accessed. They get rewards in exchange for their storage space e.g. Filecoin.

Proof-of-spacetime (PoSt)

Randomly selected miners prove that they have been physically storing data for a certain period of time e.g. Filecoin.



Generate paper wallets

Bitcoin

Dash

Dogecoin

Ethereum

Litecoin

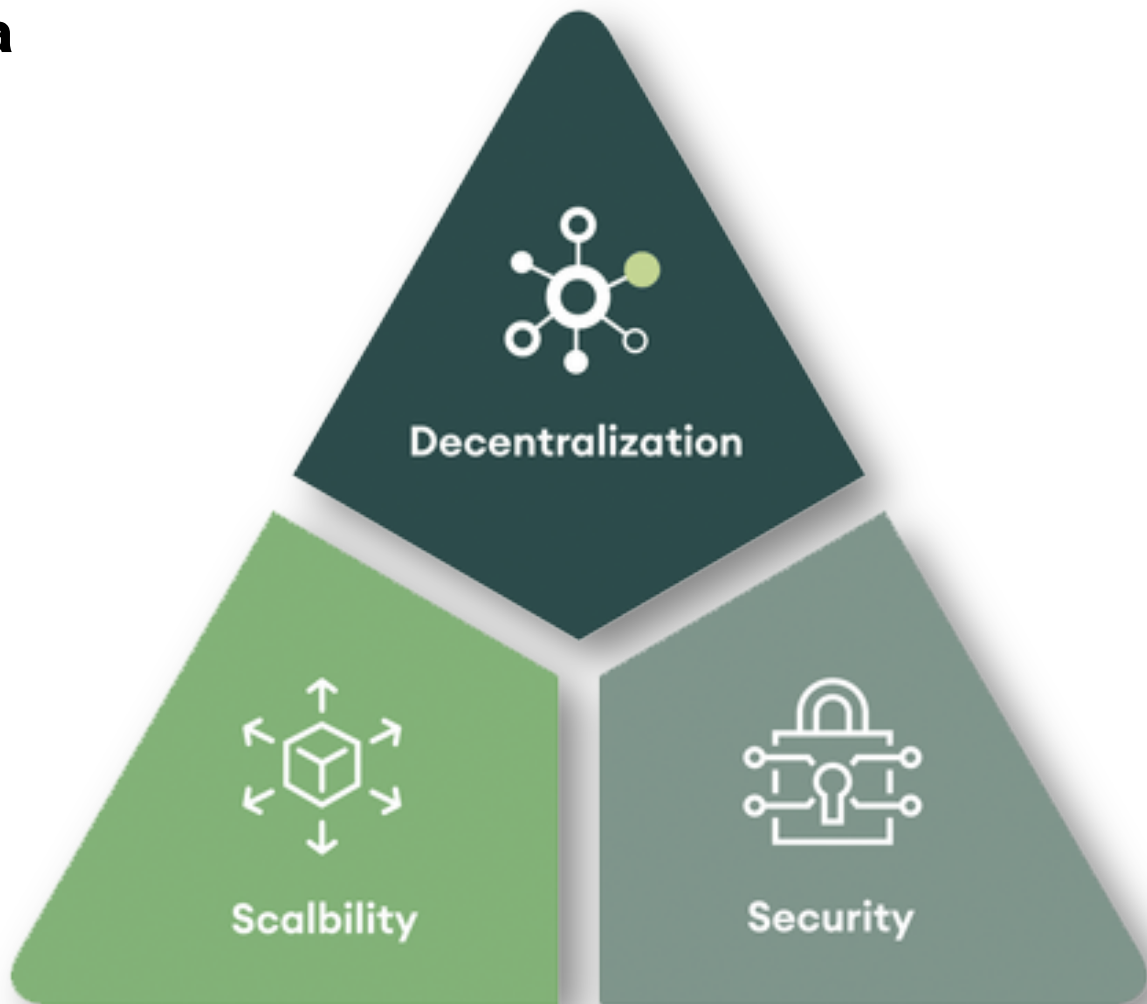
A paper wallet is an offline mechanism for storing crypto keys. A "Wallet Import Format" (wif) is a shorter version of a private key. It is **STRONGLY** advised that these keys should not be used for any high-value, or long-term storage, addresses.

```
stdClass Object
(
    [private] => 803b057c062d6b5443ce5fc84647af0d339d87f3dc8da89d7d00ee32dfce0
    [public] => 02bc47b5fdbcddec4b9dc3231344753b1c9796487c747526f01a448ba8e8dc0
    [address] => 1LEJJ7JRwNLfN6R9XqZamejjBm9qRv6mYY
    [wif] => L1WyTrwYi7tTVsWAMW2estwvJu7yHC61jfyK5EbYJLN6hQu3sGwN
)
```

Blockchain API

```
1 <?php
2 $ch = curl_init('https://api.blockcypher.com/v1/btc/main/addr');
3 curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
4 curl_setopt($ch, CURLOPT_POSTFIELDS, $post);
5
6 // execute!
7 $response = curl_exec($ch);
8
9 // close the connection, release resources used
10 curl_close($ch);
11
12 echo "<div class='table-responsive'><div class='element-box'><pre>";
13 print_r(json_decode($response)); // print json decoded response
14 echo "</div><div></pre>";
15 ?>
```


The Blockchain Trilemma



Setting up a blockchain

1. Set up and harden 2 servers
2. Install multichain
3. Create the blockchain (on the seed node)
4. Connect to the blockchain (from the secondary node)
5. Some basic commands
6. Asset Management

System requirements

System requirements:

- **Linux:** 64-bit, supports Ubuntu 12.04+, CentOS 6.2+, Debian 7+, Fedora 15+, RHEL 6.2+.
- **Windows:** 64-bit, supports Windows 7, 8, 10, Server 2008 or later.
- **Mac:** 64-bit, supports OS X 10.11 or later.
- 512 MB of RAM
- 1 GB of disk space

Installing multichain on the seed node

```
cd /tmp
```

```
wget https://www.multichain.com/download/multichain-2.1.2.tar.gz
```

```
tar -xvzf multichain-2.1.2.tar.gz
```

```
cd multichain-2.1.2
```

```
mv multichaind multichain-cli multichain-util /usr/local/bin
```

```
multichain-util create sanyachain
```

Note:

Seed node (Blue) : 206.189.141.20

Node (Green): 143.110.252.79

Installing multichain on the seed node

```
sanya — root@sanyachain: /tmp/multichain-2.1.2 — ssh root@206.189.141.20 — 90x28
root@sanyachain:~# cd /tmp
root@sanyachain:/tmp# wget https://www.multichain.com/download/multichain-2.1.2.tar.gz
--2021-03-05 11:26:56-- https://www.multichain.com/download/multichain-2.1.2.tar.gz
Resolving www.multichain.com (www.multichain.com)... 162.243.214.85
Connecting to www.multichain.com (www.multichain.com)|162.243.214.85|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 24525922 (23M) [application/x-gzip]
Saving to: 'multichain-2.1.2.tar.gz'

multichain-2.1.2.ta 100%[=====>] 23.39M 5.55MB/s in 6.0s

2021-03-05 11:27:03 (3.92 MB/s) - 'multichain-2.1.2.tar.gz' saved [24525922/24525922]

root@sanyachain:/tmp# tar -xvzf multichain-2.1.2.tar.gz
multichain-2.1.2/
multichain-2.1.2/multichain-util
multichain-2.1.2/multichain-cli
multichain-2.1.2/README.txt
multichain-2.1.2/multichaind
multichain-2.1.2/multichaind-cold
root@sanyachain:/tmp# cd multichain-2.1.2
root@sanyachain:/tmp/multichain-2.1.2# mv multichaind multichain-cli multichain-util /usr/
local/bin
root@sanyachain:/tmp/multichain-2.1.2#
```


Creating the blockchain on the seed node

```
sanya — root@sanyachain: /tmp/multichain-2.1.2 — ssh root@206.189.141.20 — 90x28
MultiChain 2.1.2 Utilities (latest protocol 20012)

Blockchain parameter set was successfully generated.
You can edit it in /root/.multichain/sanyachain/params.dat before running multichaind for
the first time.

To generate blockchain please run "multichaind sanyachain -daemon".
root@sanyachain:/tmp/multichain-2.1.2# multichaind sanyachain -daemon

MultiChain 2.1.2 Daemon (Community Edition, latest protocol 20012)

Starting up node...

Looking for genesis block...
Genesis block found

Other nodes can connect to this node using:
multichaind sanyachain@206.189.141.20:5793

This host has multiple IP addresses, so from some networks:
multichaind sanyachain@10.47.0.5:5793
multichaind sanyachain@10.122.0.2:5793

Listening for API requests on port 5792 (local only - see rpcallowip setting)

Node ready.
```


Installing multichain on other nodes

```
cd /tmp
```

```
wget https://www.multichain.com/download/multichain-2.1.2.tar.gz
```

```
tar -xvzf multichain-2.1.2.tar.gz
```

```
cd multichain-2.1.2
```

```
mv multichaind multichain-cli multichain-util /usr/local/bin
```


Installing multichain on the second node

```
sanya — root@sanyachain-node: /tmp/multichain-2.1.2 — ssh root@143.110.252.79 — 90x28
root@sanyachain-node:~# cd /tmp
root@sanyachain-node:/tmp# wget https://www.multichain.com/download/multichain-2.1.2.tar.g
z
--2021-03-05 11:29:49-- https://www.multichain.com/download/multichain-2.1.2.tar.gz
Resolving www.multichain.com (www.multichain.com)... 162.243.214.85
Connecting to www.multichain.com (www.multichain.com)|162.243.214.85|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 24525922 (23M) [application/x-gzip]
Saving to: 'multichain-2.1.2.tar.gz'

multichain-2.1.2.tar.gz 100%[=====>] 23.39M 4.70MB/s in 10s

2021-03-05 11:30:01 (2.26 MB/s) - 'multichain-2.1.2.tar.gz' saved [24525922/24525922]

root@sanyachain-node:/tmp# tar -xvzf multichain-2.1.2.tar.gz
multichain-2.1.2/
multichain-2.1.2/multichain-util
multichain-2.1.2/multichain-cli
multichain-2.1.2/README.txt
multichain-2.1.2/multichaind
multichain-2.1.2/multichaind-cold
root@sanyachain-node:/tmp# cd multichain-2.1.2
root@sanyachain-node:/tmp/multichain-2.1.2# mv multichaind multichain-cli multichain-util
/usr/local/bin
root@sanyachain-node:/tmp/multichain-2.1.2#
```


Connecting to the blockchain

```
sanya — root@sanyachain-node: /tmp/multichain-2.1.2 — ssh root@143.110.252.79 — 102x23  
root@sanyachain-node:/tmp/multichain-2.1.2# multichaind sanyachain@206.189.141.20:5793
```

```
MultiChain 2.1.2 Daemon (Community Edition, latest protocol 20012)
```

```
Retrieving blockchain parameters from the seed node 206.189.141.20:5793 ...  
Blockchain successfully initialized.
```

```
Please ask blockchain admin or user having activate permission to let you connect and/or transact:
```

```
multichain-cli sanyachain grant 15DV5d65uNfRYVJhWu8uqpd2JZHB42dtA9EXg4 connect
```

```
multichain-cli sanyachain grant 15DV5d65uNfRYVJhWu8uqpd2JZHB42dtA9EXg4 connect,send,receive
```

```
root@sanyachain-node:/tmp/multichain-2.1.2#
```


Granting permission to the node

```
sanya — root@sanyachain: ~ — ssh root@206.189.141.20 — 90x28
root@sanyachain:~# multichain-cli sanyachain grant 15DV5d65uNfRYVJhwu8uqpd2JZHB42dtA9EXg4
connect,send,receive
{"method":"grant","params":["15DV5d65uNfRYVJhwu8uqpd2JZHB42dtA9EXg4","connect,send,receive
"],"id":"49722926-1614944523","chain_name":"sanyachain"}

c1ac7781320f4b860f440b8e978d80e3e8fe208ac18c2bb1360119c1bcb9915d
root@sanyachain:~#
```


Retrieving blockchain parameters from the seed node

```
root@sanyachain-node:~# multichaind sanyachain -daemon

MultiChain 2.1.2 Daemon (Community Edition, latest protocol 20012)

Retrieving blockchain parameters from the seed node 206.189.141.20:5793 ...
Other nodes can connect to this node using:
multichaind sanyachain@143.110.252.79:5793

This host has multiple IP addresses, so from some networks:
multichaind sanyachain@10.47.0.6:5793
multichaind sanyachain@10.122.0.3:5793

Listening for API requests on port 5792 (local only - see rpcallowip setting)

Node ready.
```


Entering interactive mode on both nodes

sanya — root@sanyachain: ~ — ssh root@206.189.141.20 — 90x28

```
root@sanyachain:~# multichain-cli sanyachain
```

MultiChain 2.1.2 RPC client

Interactive mode

sanyachain: █

sanya — root@sanyachain-node: ~ — ssh root@143.110.252.79 — 102x23

```
root@sanyachain-node:~# multichain-cli sanyachain
```

MultiChain 2.1.2 RPC client

Interactive mode

sanyachain: █

getinfo

returns general
information about this
node and blockchain

The *burnaddress* is
an address with no
known private key.

```
sanya — root@sanyachain: ~ — ssh root@206.189.141.20 — 77x34
{"method": "getinfo", "params": [], "id": "68240971-1614947567", "chain_name": "sanyachain"}

{
  "version" : "2.1.2",
  "nodeversion" : 20102901,
  "edition" : "Community",
  "protocolversion" : 20012,
  "chainname" : "sanyachain",
  "description" : "MultiChain sanyachain",
  "protocol" : "multichain",
  "port" : 5793,
  "setupblocks" : 60,
  "nodeaddress" : "sanyachain@206.189.141.20:5793",
  "burnaddress" : "1XXXXXXXXWkXXXXXXXXXXXXXXXXWHXXXXXXXXb8JpzE",
  "incomingpaused" : false,
  "miningpaused" : false,
  "offchainpaused" : false,
  "walletversion" : 60000,
  "balance" : 0,
  "walletdbversion" : 3,
  "reindex" : false,
  "blocks" : 59,
  "timeoffset" : 0,
  "connections" : 0,
  "proxy" : "",
  "difficulty" : 5.96046447753906e-8,
  "testnet" : false,
  "keypoololdest" : 1614943941,
  "keypoolsize" : 2,
  "paytxfee" : 0,
  "relayfee" : 0,
  "errors" : ""
}
```


getblockchainparams

returns a list of values of
this blockchain's
parameters

Most of these would
be *true* in a public
blockchain

```
sanya — root@sanyachain: ~ — ssh root@206.189.141.20 — 77x34
sanyachain: getblockchainparams
{"method":"getblockchainparams","params":[],"id":"78798788-1614947885","chain_name":"sanyachain"}

{
  "chain-protocol" : "multichain",
  "chain-description" : "MultiChain sanyachain",
  "root-stream-name" : "root",
  "root-stream-open" : true,
  "chain-is-testnet" : false,
  "target-block-time" : 15,
  "maximum-block-size" : 8388608,
  "maximum-chunk-size" : 1048576,
  "maximum-chunk-count" : 1024,
  "default-network-port" : 5793,
  "default-rpc-port" : 5792,
  "anyone-can-connect" : false,
  "anyone-can-send" : false,
  "anyone-can-receive" : false,
  "anyone-can-receive-empty" : true,
  "anyone-can-create" : false,
  "anyone-can-issue" : false,
  "anyone-can-mine" : false,
  "anyone-can-activate" : false,
  "anyone-can-admin" : false,
  "support-miner-precheck" : true,
  "allow-arbitrary-outputs" : false,
  "allow-p2sh-outputs" : true,
  "allow-multisig-outputs" : true,
  "setup-first-blocks" : 60,
  "mining-diversity" : 0.3,
  "admin-consensus-upgrade" : 0.5,
  "admin-consensus-txfilter" : 0.5,
  "admin-consensus-admin" : 0.5,
```



```
"admin-consensus-activate" : 0.5,  
"admin-consensus-mine" : 0.5,  
"admin-consensus-create" : 0,  
"admin-consensus-issue" : 0,  
"lock-admin-mine-rounds" : 10,  
"mining-requires-peers" : true,  
"mine-empty-rounds" : 10,  
"mining-turnover" : 0.5,  
"first-block-reward" : -1,  
"initial-block-reward" : 0,  
"reward-halving-interval" : 52560000,  
"reward-spendable-delay" : 1,  
"minimum-per-output" : 0,  
"maximum-per-output" : 1000000000000000,  
"minimum-offchain-fee" : 0,  
"minimum-relay-fee" : 0,  
"native-currency-multiple" : 100000000,  
"skip-pow-check" : false,  
"pow-minimum-bits" : 8,  
"target-adjust-freq" : -1,  
"allow-min-difficulty-blocks" : false,  
"only-accept-std-txs" : true,  
"max-std-tx-size" : 4194304,  
"max-std-op-returns-count" : 32,  
"max-std-op-return-size" : 2097152,  
"max-std-op-drops-count" : 5,  
"max-std-element-size" : 40000,  
"chain-name" : "sanyachain",  
"protocol-version" : 20012,  
"network-message-start" : "f1f0c2e7",  
"address-pubkeyhash-version" : "00442387",  
"address-scripthash-version" : "05492207",  
"private-key-version" : "8026c204",  
"address-checksum-value" : "c5c93ee9",
```



```
  "address-checksum-value" : "c5c93ee9",
  "genesis-pubkey" : "0289d2b2628b1f3ae258a375ec0d5f50649530118c0077da516ce
6181aa096dbf4",
  "genesis-version" : 1,
  "genesis-timestamp" : 1614943941,
  "genesis-nbits" : 536936447,
  "genesis-nonce" : 31,
  "genesis-pubkey-hash" : "1f3dd933970080976d92f5658ecd9d1ab2188e75",
  "genesis-hash" : "00d7ad2af1a15f2b979388d563103d00ac7b3d5a6cd98e49ba9cbc0
a1664b76a",
  "chain-params-hash" : "2003f2d0d193b0f0b29d94e481ec691ed7754ac7b7ba28da27
93429978c6425c"
}
```


listaddresses

returns information about the addresses

getnewaddress

returns a new address whose private key is added to the wallet

listaddresses

returns information about the addresses


```
sanya — root@sanyachain: ~ — ssh root@206.189.141.20 — 82x30
sanyachain: listaddresses
{"method":"listaddresses","params":[],"id":"83093890-1614948300","chain_name":"sanyachain"}

[
  {
    "address" : "15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb",
    "ismine" : true
  }
]
sanyachain: getnewaddress
{"method":"getnewaddress","params":[],"id":"27927198-1614948312","chain_name":"sanyachain"}

12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7
sanyachain: listaddresses
{"method":"listaddresses","params":[],"id":"27423664-1614948322","chain_name":"sanyachain"}

[
  {
    "address" : "15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb",
    "ismine" : true
  },
  {
    "address" : "12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7",
    "ismine" : true
  }
]
sanyachain: 
```


Issuing an open asset

```
issuefrom 15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb  
15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb  
'{"name":"SanyaCoin","open":true}' 50000 0.01 0  
'{"Type":"Cryptocurrency Token", "Issue date":"8-March-2021"}
```


Issuing an open asset

```
sanyachain: issuefrom 15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb 15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb '{"name":"SanyaCoin","open":true}' 50000 0.01 0 '{"Type":"Cryptocurrency Token", "Issue date":"8-March-2021"}'
```

```
{"method":"issuefrom","params":["15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb","15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb",{"name":"SanyaCoin","open":true},50000,0.01,0,{"Type":"Cryptocurrency Token","Issue date":"8-March-2021"}],"id":"94478489-1614949408","chain_name":"sanyachain"}
```

```
81bdb493ae8124efbac1057a528af4e009b39618e61f16b99fd20f27df85d1f1
```



```
sanyachain: listassets
{"method":"listassets","params":[],"id":"76159034-1614949440","chain_name":"sanyachain"}

[
  {
    "name" : "SanyaCoin",
    "issuetxid" : "81bdb493ae8124efbac1057a528af4e009b39618e61f16b99fd20f27df85d1f1",
    "assetref" : "60-266-48513",
    "multiple" : 100,
    "units" : 0.01,
    "open" : true,
    "restrict" : {
      "send" : false,
      "receive" : false,
      "issue" : true
    },
    "details" : {
      "Type" : "Cryptocurrency Token",
      "Issue date" : "8-March-2021"
    },
    "issueqty" : 50000,
    "issueraw" : 5000000,
    "subscribed" : false
  }
]
sanyachain: █
```


sendassetfrom

15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb

12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7

SanyaCoin

25

```
rohasnagpal — root@sanyachain: ~ — ssh root@206.189.141.20 — 65x7
sanyachain: sendassetfrom 15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb
12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7 SanyaCoin 25
{"method":"sendassetfrom","params":["15DuKhdp485dArupQDyG6RFz594M
5RJaBftVpb","12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7","SanyaCoin",
25],"id":"37218936-1614950239","chain_name":"sanyachain"}
ecbcb48efa839fbb969c0b11c378aa23c7980173e1cd01620e29777d981e6f9b
```



```
rohasnagpal — root@sanyachain: ~ — ssh root@206.189.141.20 — 78x24
sanyachain: getaddressbalances 15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb
{"method":"getaddressbalances","params":["15DuKhdp485dArupQDyG6RFz594M5RJaBftVpb"],"id":"30153090-1614950580","chain_name":"sanyachain"}

[
  {
    "name" : "SanyaCoin",
    "assetref" : "60-266-48513",
    "qty" : 49975
  }
]
sanyachain:
sanyachain: getaddressbalances 12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7
{"method":"getaddressbalances","params":["12Q24F1vSNP5efpGbD5FqkqsoLoREFJrui1uG7"],"id":"15257492-1614950612","chain_name":"sanyachain"}

[
  {
    "name" : "SanyaCoin",
    "assetref" : "60-266-48513",
    "qty" : 25
  }
]
sanyachain: █
```


HyFi Technical Documentation

Everything you need to build with HyFi.



Introduction

HyFi Blockchain uses the Multichain framework with distributed consensus between identified block validators.



Setting up a node

There are 3 HyFi Networks: mainNet, Haddock (testNet) and Calculus (testNet)



Addresses

Addresses can be of 2 types (custodial and non-custodial) and can have various permissions.



Assets

HyFi assets can be stablecoins, wrapped tokens, NFTs and Open Blockchain Tokens.



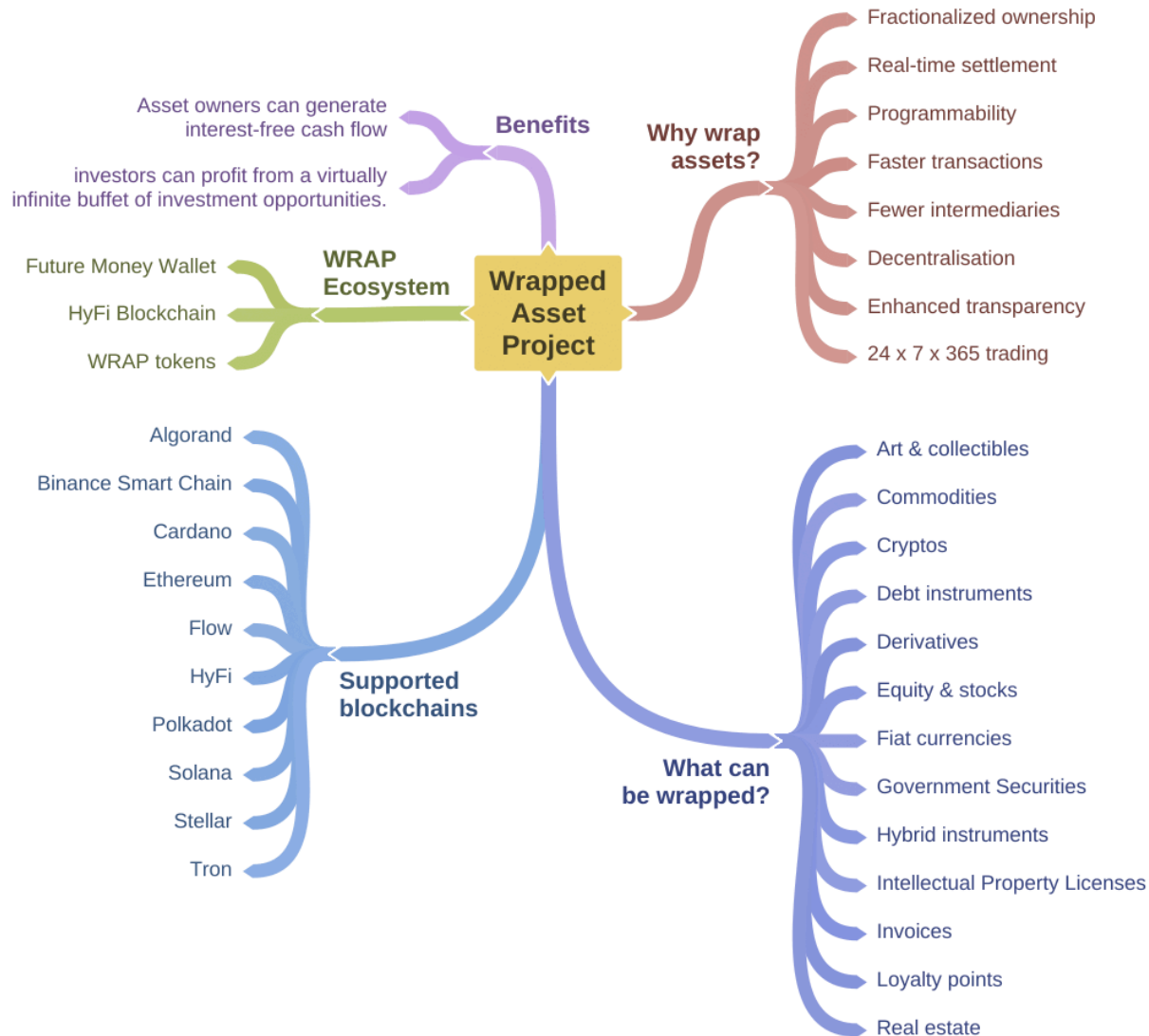
Transactions

Transactions can be one-way payments or atomic exchange transactions.



Electronic Signatures

Electronic Signatures can be generated using custodial and non-custodial addresses.



Careers in Blockchain

- Design
- Development
- Architecture
- Security
- Product management