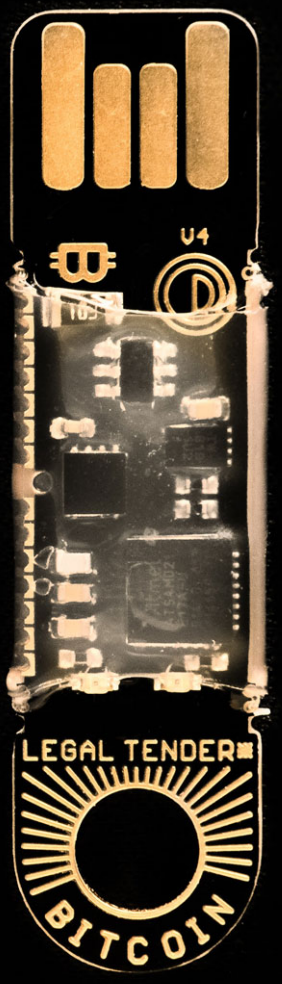
Future Money Playbook 2021



Compiled by Rohas Nagpal

Money is the most universal and
most efficient system of mutual trust
ever devised.

Even people who do not believe in the
same god or obey the same king
are more than willing to use
the same money.

Yuval Harari

Legal stuff

I have to tell you this. My scary lawyers insist….

Some of the links in this document are affiliate links, meaning, at no additional cost to you, I will earn a commission if you click through and make a purchase.

The information in my documents, social media networks, websites, and videos is for general information only and should not be taken as constituting professional advice from me.

I am not a financial adviser. You should consider seeking independent legal, financial, taxation, or other advice to check how the information relates to your unique circumstances.

I am not liable for any loss caused, whether due to negligence or otherwise arising from the use of, or reliance on, the information provided directly or indirectly.

I link to external resources for your convenience. I am selective about them but I don't endorse them.

No investigation has been made of common-law trademark rights in any word. Words that are known to have current trademark registrations are shown with an initial capital and are also identified as trademarks.

The inclusion or exclusion of any word, or its capitalization, in this book is not, however, an expression of the author's opinion as to whether or not it is subject to proprietary rights, nor is it to be regarded as affecting the validity of any trademark.

This book is provided "as is" and the author makes no representations or warranties, express or implied either in respect of this book or the software, websites and other information referred to in this book.

By way of example, but not limitation, the author makes no representations or warranties of merchantability or fitness for any particular purpose or that the use of licensed software, database or documentation will not infringe any third party patents, copyrights, trademarks or other rights.

The chosen case scenarios are for instructional purposes only and any association to an actual case and litigation is purely coincidental. Names and locations presented in the case scenarios are fictitious and are not intended to reflect actual people or places.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favouring by the author, and the information and statements shall not be used for the purposes of advertising.

Images courtesy:
Unsplash
Pixabay.com
Freepik.com

Contents

How do crypto investors make money?

- ❑ Buy low, HODL (Hold on for Dear Life) and sell high. This sounds simple. But its not. Accurately predicting prices for crypto assets is really tough.
- ❑ Cryptocurrency dividends. Some crypto assets pay dividends similar to how companies pay dividends to shareholders.
- ❑ Cryptocurrency staking. Some crypto currencies pay you for staking – holding the currency and securing the network.
- ❑ Operating cryptocurrency master nodes.
- ❑ Cryptocurrency mining.
- ❑ Crypto day trading. Really tough and risky way to make money.
- ❑ Betting on prediction markets. Yes, its like gambling.
- ❑ Operating exchanges, lending platforms, blockchains. This is one of the smartest ways to profit from the crypto world.
- ❑ Starting new cryptocurrencies. Enough said.

1. History of money

Our ancestors started off with the barter system - something like "I will give you 2 buffaloes in return for 5 shiny new super-sharp axes".

Soon they realised that the barter system had too many limitations:

- ⌘ everyone didn't want buffaloes,
- ⌘ buffaloes were not divisible (not too many people would want 0.35 buffaloes)
- ⌘ buffaloes were not portable (imagine having to carry a buffalo on your shoulders while going shopping).

So they moved on to more acceptable, divisible, homogeneous and portable forms of money - cowry shells, salt, gold, silver and lots more.

The Chinese invention of paper eventually led to the birth of **paper currency**, which was initially backed by gold or other precious metals.

Then the world moved on to **fiat money** - currency that's declared as legal tender by a government but not backed by a physical commodity.

Have a look at an Indian note (anything except a 1-rupee note). It carries a promise signed by the Governor of the Reserve Bank of India (RBI) :

“I promise to pay the bearer the sum of one hundred rupees”.

If you were to take this note to the Governor of the RBI, he would (probably) give you coins or one-rupee notes totalling 100 rupees. (Disclaimer: I haven't tried it)

Only the RBI can issue such notes because section 31 of the *Reserve Bank of India Act, 1934* states that:

> *"No person in India other than the Bank or, as expressly authorized by this Act, the Central Government shall draw, accept, make or issue any bill of exchange, hundi, promissory note or engagement for the payment of money payable to bearer on demand, or borrow, owe or take up any sum or sums of money on the bills, hundis or notes payable to bearer on demand of any such person…"*

Remember the demonetization of some notes in India a few years ago? Well, legally speaking, this is what happened:

> The legal tender character of the bank notes in denominations of ₹ 500 and ₹ 1000 issued by the Reserve Bank of India was withdrawn with the promulgation of the *Specified Bank Notes (Cessation of Liabilities) Ordinance 2016 (GoI Ordinance No. 10 of 2016* dated December 30, 2016).

As a result, with effect from December 31, 2016, the above Bank Notes ceased to be the liabilities of the Reserve Bank of India and ceased to have the guarantee of the Central Government.

What is Money?

This brings us to an essential question – what is money?

Money's a matter of functions four,
a Medium, a Measure, a Standard, a Store.

So goes the couplet based on William Stanley Jevons analysis of money in 1875.

This meant that for something to be called money, it must function as:

- ❑ a medium of exchange,
- ❑ a measure of value,
- ❑ a standard of deferred payment and
- ❑ a store of value.

The birth of computers and the Internet brought in many electronic payment systems including:

- debit cards,
- stored value cards,
- giro transfers,
- credit cards,
- net-banking,
- electronic bill payments,
- electronic cheques,
- mobile wallets,
- digital gold currencies,
- digital wallets,
- electronic funds transfer at point of sale,
- mobile banking,
- online banking,
- payment cards,
- real-time gross settlement systems,
- SWIFT,
- wire transfers and more.

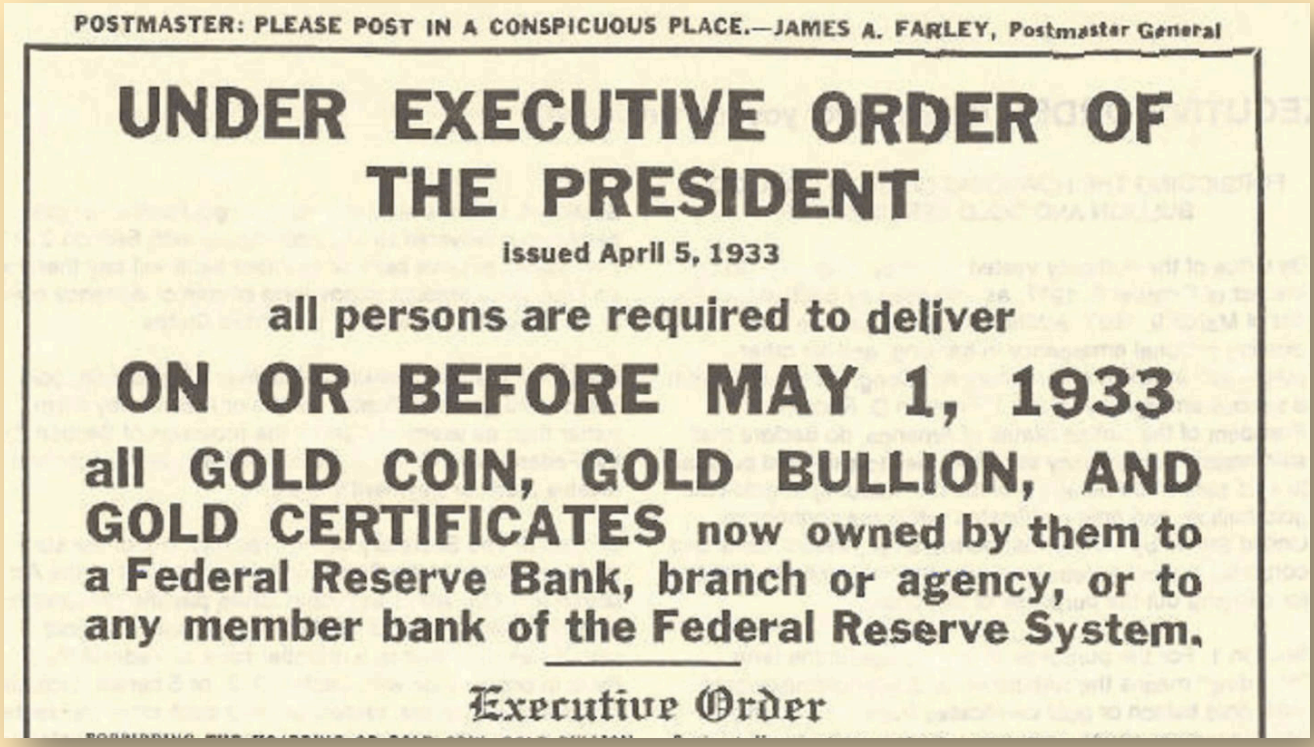
And then came Satoshi Nakamoto's path breaking whitepaper - *Bitcoin: A Peer-to-Peer Electronic Cash System* in October 2008. This brought the world **Bitcoin**, the first truly peer-to-peer electronic currency.

According to the *FATF report on Virtual Currencies - Key Definitions and Potential AML/CFT Risks*, **Virtual currency** is a digital representation of value that can be digitally traded and functions as:

- a medium of exchange; and/or
- a unit of account; and/or
- a store of value,

but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction.

It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

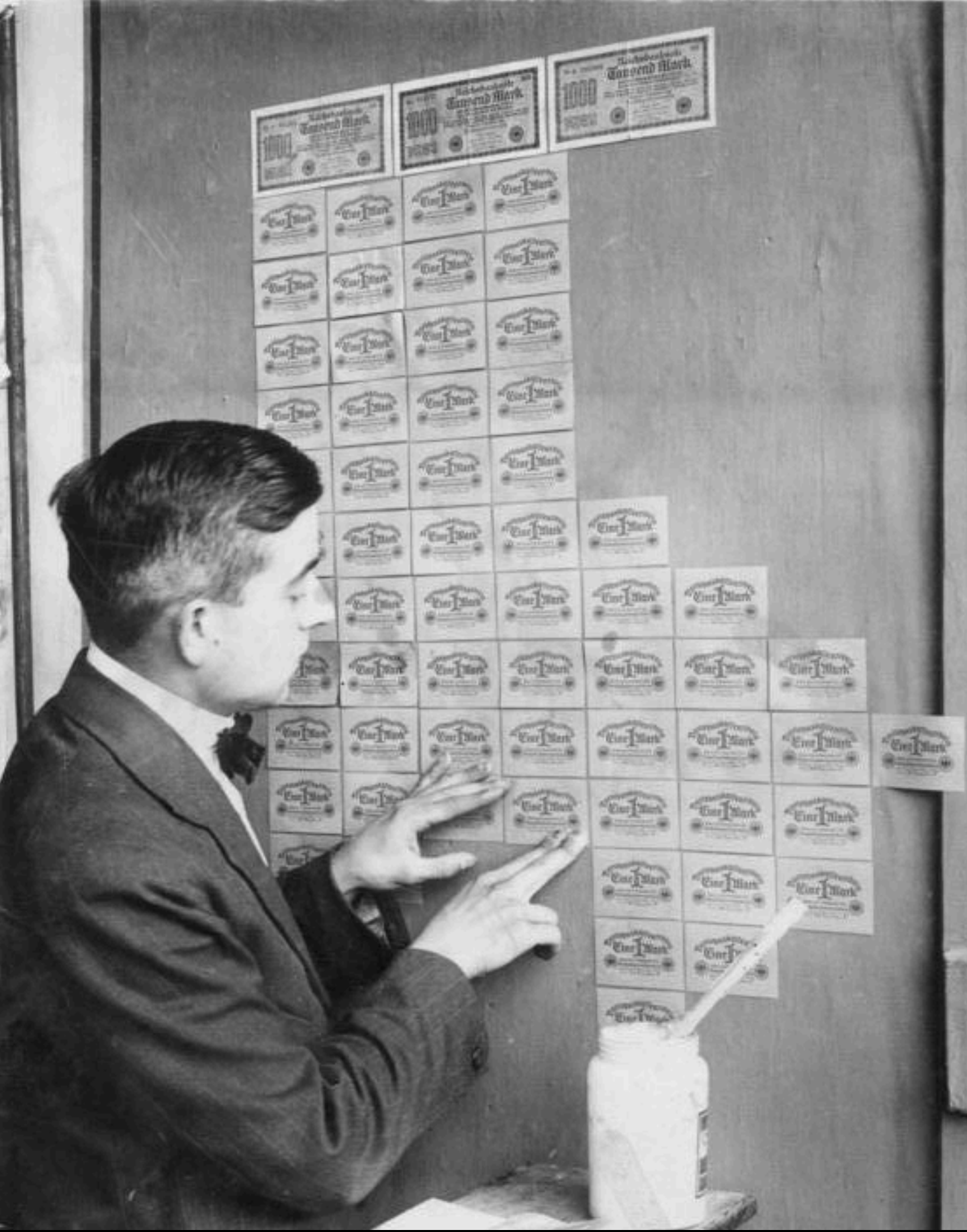
Executive Order

On June 5, 1933, the US went off the gold standard, when its Congress enacted a joint resolution nullifying the right of creditors to demand payment in gold.

On August 15, 1971, President Richard Nixon announced that the United States would no longer convert dollars to gold at a fixed value, thus completely abandoning the gold standard.

Source: https://www.history.com

In 2008, the Zimbabwe Dollar was replaced by a new dollar that was equal to 10 billion of the old dollars. And people think Bitcoin is volatile!



Using banknotes as wallpaper during German hyperinflation, 1923
Source: https://rarehistoricalphotos.com

Virtual currency is differentfrom **fiat currency** (a.k.a. “real currency,” “real money,” or “national currency”). Fiat money is the coin and paper money of a country that is:

- ❑ designated as its legal tender;
- ❑ circulates; and
- ❑ is customarily used and accepted as a medium of exchange in the issuing country.

It is distinct from **e-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

According to the World Bank, E-Money can be held on cards, devices, or on a server. Examples include pre-paid cards, electronic purses, such as M-PESA in Kenya, or web-based services, such as PayPal.

A lot of crypto-currencies have piggybacked on Bitcoin’s underlying innovation – the **blockchain**. In fact we now have thousands of virtual currencies being used around the world.

We have become a world where bankers wake up each morning wondering – "has the meaning of money and banking changed while I slept?".

This rapid change in the global money ecosystem has implications for all of us...
... Governments looking to clamp down on money laundering, tax evasion and terrorist funding
... banks looking to understand the implications of the virtual currencies
... law enforcement looking to clamp down on the Mafia using Bitcoin
... businesses looking for faster and cheaper ways to receive and transfer money globally.

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

9 pages that disrupted money forever

The original whitepaper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” can be downloaded from: https://bitcoin.org/bitcoin.pdf

Bitcoin earned a lot of notoriety primarily because of its use by members of the now shut-down Silk Road - an illegal online marketplace that facilitated the sale of hundreds of millions of dollars worth of drugs, guns, stolen financial information, counterfeit documents and more.

All Silk Road transactions were conducted exclusively in bitcoin.

Silk Road creator Ross Ulbricht is currently serving two life sentences in prison after being found guilty of money laundering, computer hacking, and conspiracy to traffic narcotics.

The first Bitcoin real-world transaction took place on 22nd May, 2010 and involved 10,000 bitcoins being exchanged for $25 worth of pizza.

laszlo
Full Member

Activity: 199
Merit: 487

Re: Pizza for bitcoins?
May 22, 2010, 07:17:26 PM
Merited by vizique (10), vapourminer (1), Searing (1), BitcoinFX (1), 600watt (1), Aricoin (1), dektox (1)

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:08 -0400

Download: IMG_0984.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:22 -0400

Download: IMG_0985.jpg

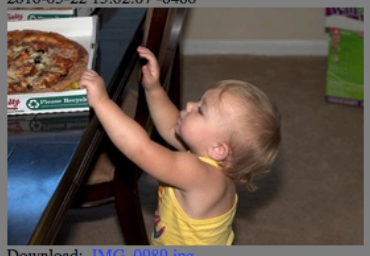
5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:29 -0400

Download: IMG_0986.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:56 -0400

Download: IMG_0988.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:02:07 -0400

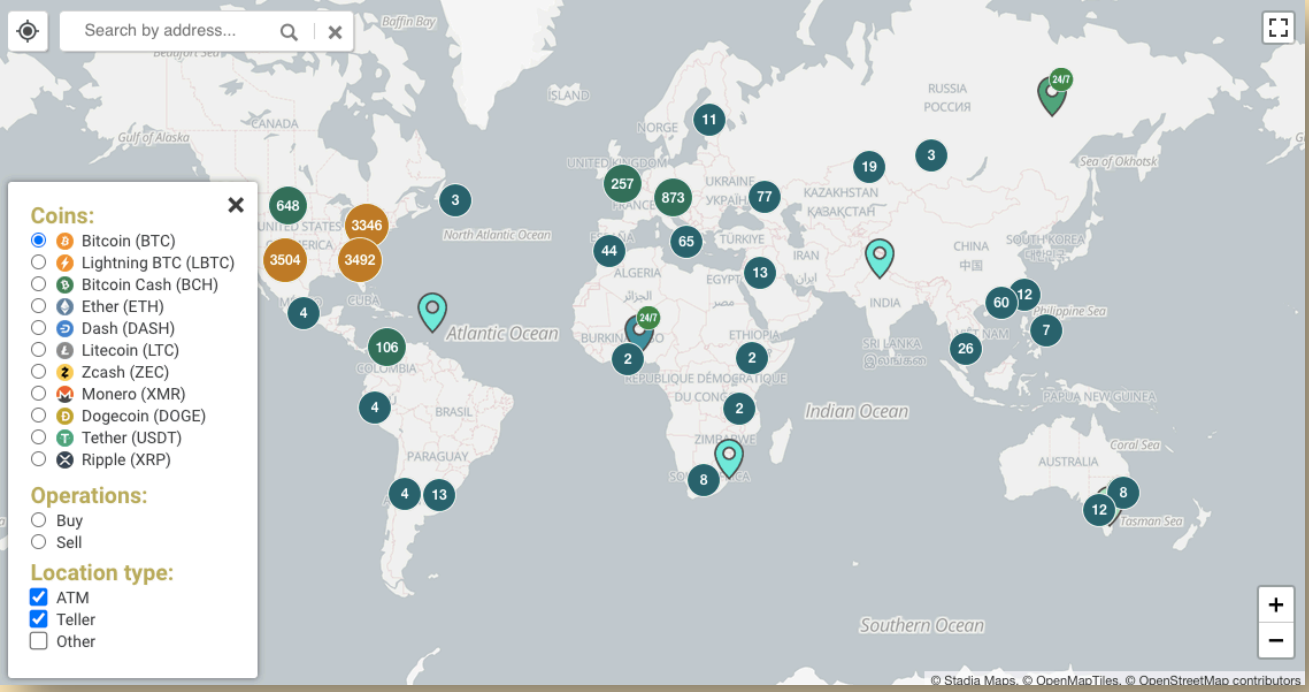


Download: IMG_0989.jpg

NewLibertyStandard
Sr. Member

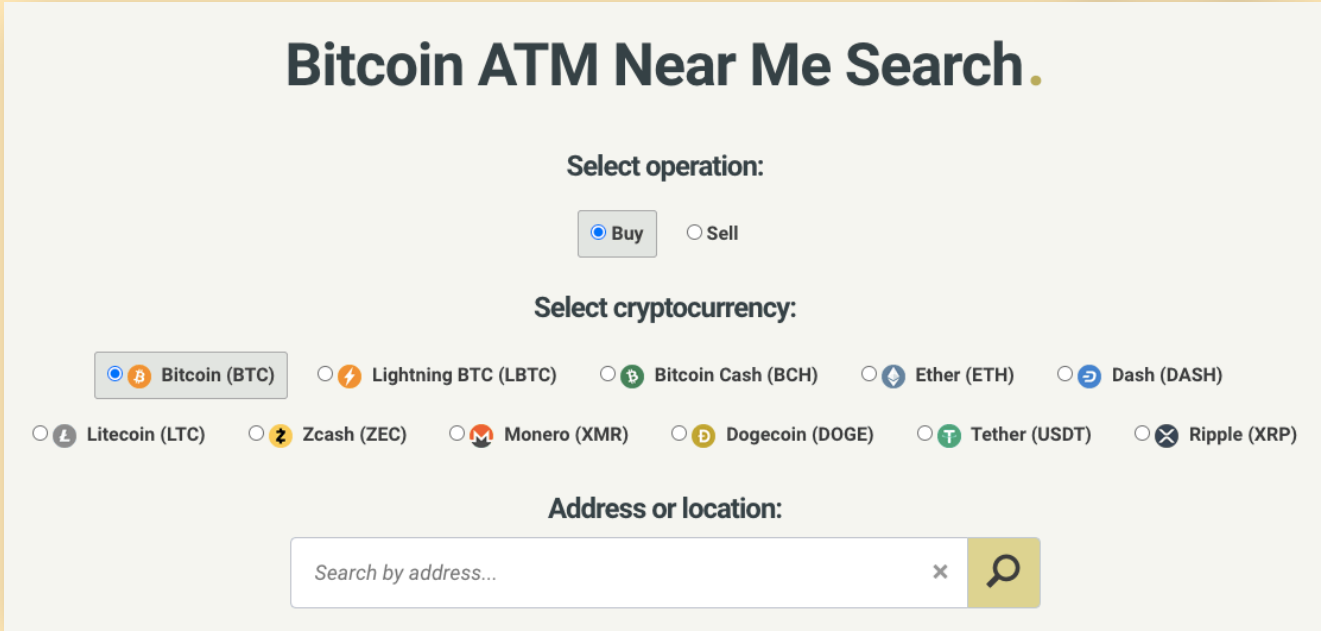
Re: Pizza for bitcoins?
May 23, 2010, 12:59:26 AM

That pizza looks delicious! Adorable kid.

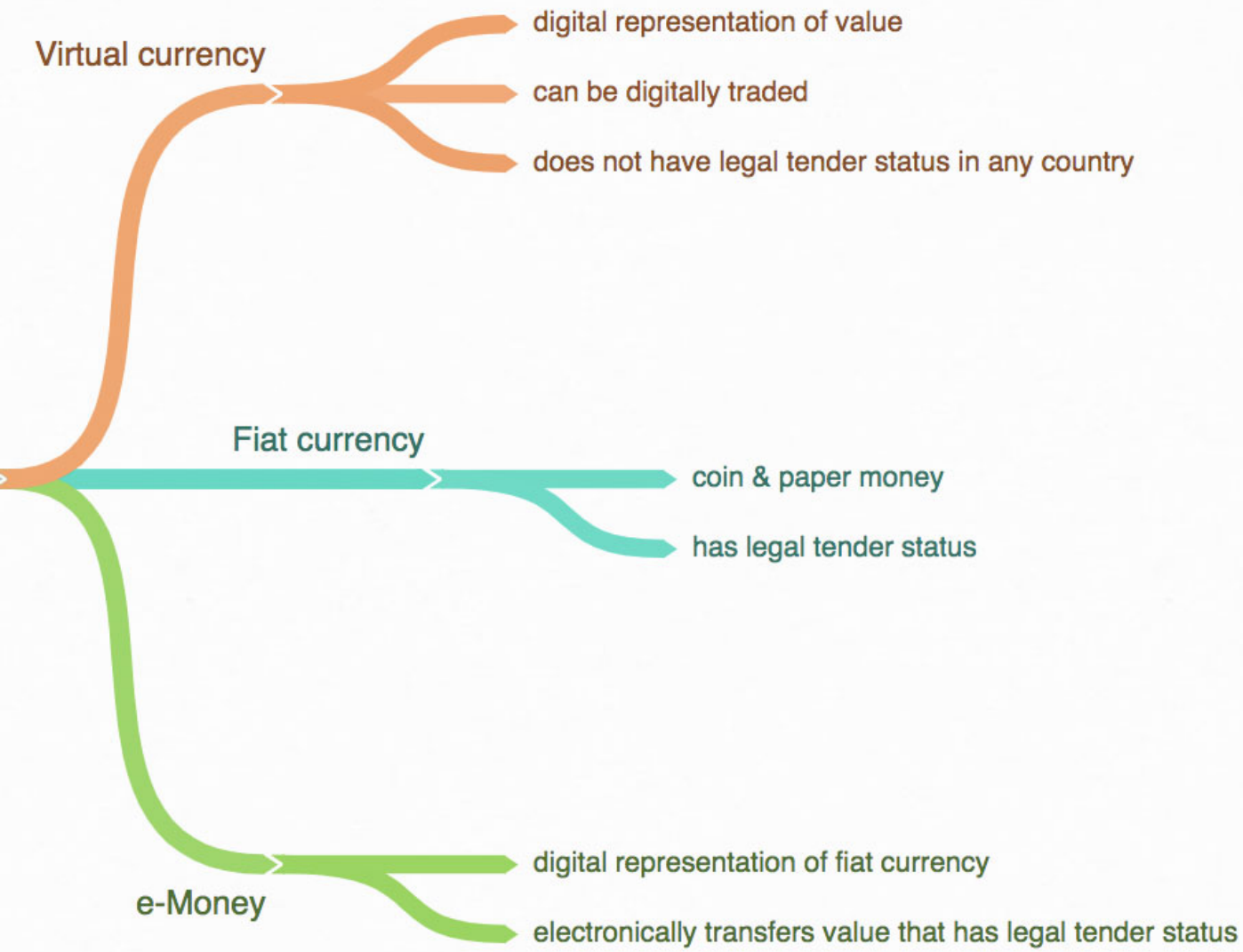


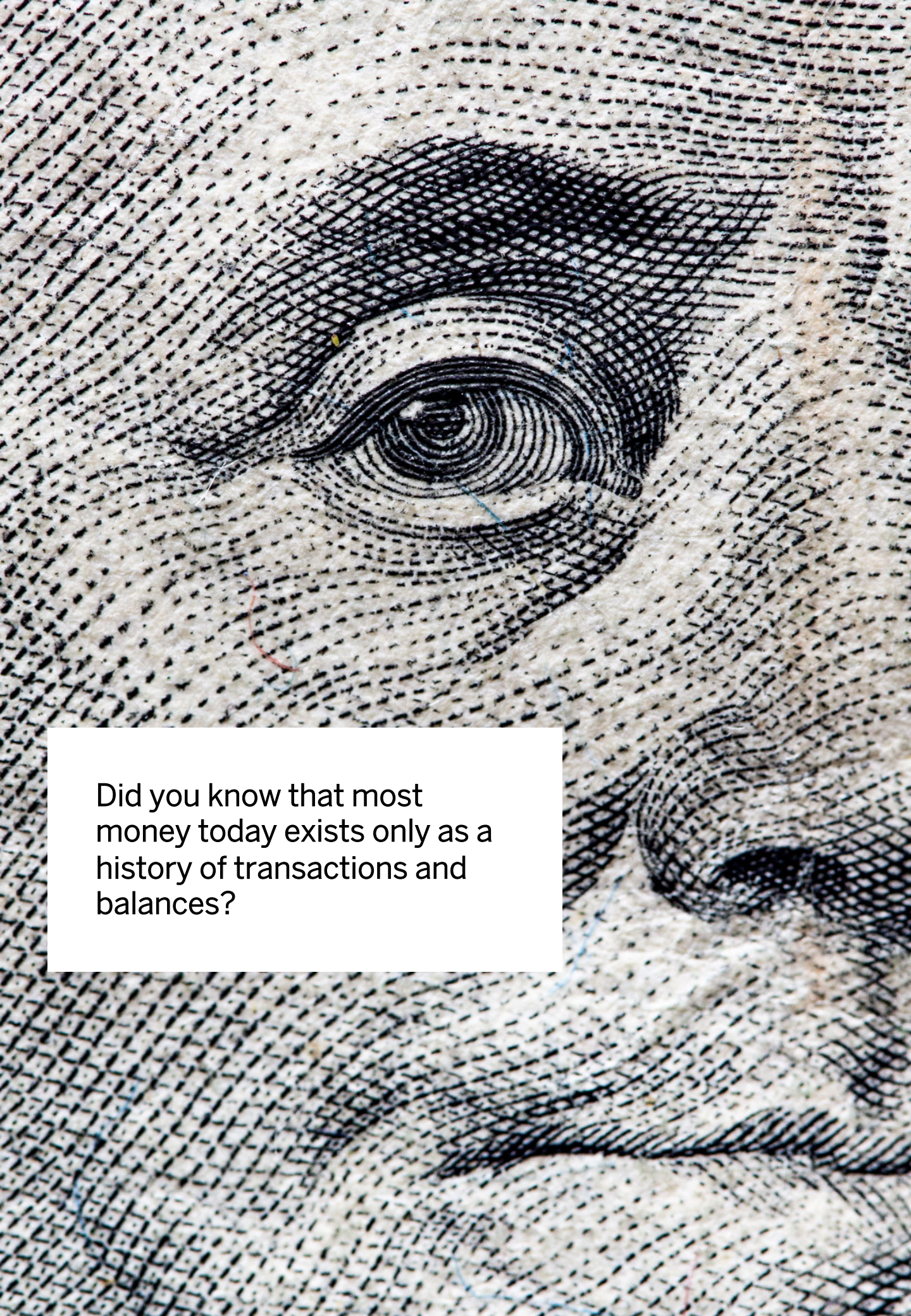
If you are looking for a crypto ATM near you, try:
https://coinatmradar.com

For revenue & costs of running a crypto ATM, see:
https://coinatmradar.com/blog/revenue-and-costs-of-running-a-bitcoin-atm



Types of Money




Did you know that most
money today exists only as a
history of transactions and
balances?

Did you know?

There is more than one type of Bitcoin...

The first "original" bitcoins were mined on 3 January 2009.

A new cryptocurrency called "Bitcoin Cash" was the result of a 2017 hard fork by miners who were unhappy with "segregated witness technology" being incorporated into Bitcoin.

The Bitcoin Cash network was hard forked in 2018 to create Bitcoin Satoshi Vision (BSV) in an effort to stay true to the original vision for bitcoin.

2. Tech terms

Sanya's a naughty young girl who's been grounded for a week. She wants to sneak out for coffee with her friends but obviously can't let her dad know about it. She's not allowed to use her cellphone, so the only way for her to call her friends is using the good old landline in her dad's room.

Since she regularly gets grounded, she and her friends have worked out a simple system for sharing secrets. When she says, "*have you read the book I told you about*" she actually means "*let's sneak out tonight*".

When she says something about "*page 10*" of the book, she means "*pick me up at 10 pm*". Continuing the logic, page 11 would mean 11 pm and so on.

So on the phone she asks her friend "*Have you read the book I told you about? Page 12 is really funny*", she means, "*Let's sneak out tonight, pick me up at midnight*".

What we have just seen is **cryptography** (and a rebellious teenager) in action in the real world.

The sentence "Let's sneak out tonight, pick me up at midnight" is **plain text** – what Sanya actually wants to convey.

The sentence "Have you read the book I told you about? Page 12 is really funny" is the **cipher text** – something that an adversary (her dad in this case) should not be able to understand.

Encryption is the process of converting plain text to cipher text. The reverse process is **decryption**. This science of encrypting and decrypting messages (*cryptography*) has been used for thousands of years.

It is believed that when Julius Caesar sent messages to his generals, he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

For example, if we want to encode the word “SECRET” using Caesar’s key value of 3, we offset the alphabet so that the 3rd letter down, (D), begins the alphabet.

So starting with
ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get
DEFGHIJKLMNOPQRSTUVWXYZABC
where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, “SECRET” encrypts as “VHFUHW”.

To allow someone else to read the cipher text, you tell him or her that the **key** is 3.

This method is called **symmetric cryptography** and involves using the same key for encrypting as well as decrypting a message. This naturally poses a serious problem – what if an adversary gets hold of this key? At some point of time the sender and receiver need to exchange the key. That’s when an adversary could get hold of the key.

In modern cryptography, **keys** are really really large numbers.

The *secure-key-exchange* problem was solved with the birth of **asymmetric key cryptography** – in which two different but related keys are used - the public key to encrypt data and the corresponding private key to decrypt the data.

If Sanya were to send an encrypted message to Sameer, she would encrypt the message using his **public key** (which is available to the world).

Once encrypted, the message can only be decrypted using Sameer’s **private key** (which would only be available to Sameer).

A 1024-bit RSA key pair generated using PGP

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
lQHgBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/
AERegEtzoFiveSzbeFQtNhxDIOSPJc60Y8v2nTecI0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPApi
OFXhUrkHF0DmrmEpa5UpHjpO3sD+Hlvg84N6jHjAIRMlNMAyrg/
e4i6ABGzAuxYbJCs6ax9mxdrFAQARAQABAwvtDcK53Fr7j9Ss3v83ZR7g1DgFfY3oo97XWb
mJ02BdRGy/
C+aIuu3wMRNqmPo5w1I8VVCjjM02eqSr0+8mbLLX0Dwqbn33QitGW34Upt6EI+fv0ObKbJRi2
Hc628l3mi+jjsskxvQ8oavtSJL2j/
xTEtL+wvqObcFxllsyjpH5N1wY7xQ5BPSNjYLFZr99MXycFhee14V2YdQv0iPZFrJnvCQFWXL
AiX1L9AH5DgwmXLtNCPbIQnRwyLPyWSOT4yH8e6ibqIBvMhpGe4WOAzuccHL6jjZrokVrBB
u50Z6EqGFkzS8X6iygvSATOjr3L/
X9EW7Fw098CcVK3lDB93rpeXR+tU370nV+0FgXQqUzQ3SJ6vZwdlwy6cmjZOWmd/
YrbGLOyyW+zFFSZFdiG480ELozMfMsqp3OJvElvhRgS/tbA/
94jpOtzhWV9Du0pd7otCBBYmhpbmF2IEJoYXR0IDxhYkBhc2lhbmxhd3Mub3JnPp0B4AQ+b
wwyAQQAmkqdApHtWspZdNfqeEROxctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLRnW+N4QUAgm
+eNNsTrqZZjJUP526dOTK8RmxV4QJeh2Q0bsLPs6SXTlPwfBWPpt+U/
kfrSt8ZJF5lWR0jaiJG2hE3dBiuszPa+6cJUDuQnYCVCHZARCKLcAEQEAAQPT8PBQW4y8b
4C7BvhjnGAATQliwRajv6uWmfUFcI+DPdtAZh3yb9EKWmS8vSkSnz+pWG1dEkuURyvBGJM
Dxs/
FB+CMouTQejhA11Ho5tblas8HnoNPeQv1x9Xas+lrs1j2AmfrLWwKEQAuH9di+d9DRU6YHxy1
ocIHZELXR9ECsSP0C1iSeuJn+u4HLP3y4uBHcGRdihLRIUSCJ0tXd2meRAxw4dsZllDAeb21i
2Tj+l0SngTEzFj8fSuvAxoXRv30gq5VLbH5WDbJah5n688THMAUIUC5dlG8MMXMgmUe887l
wKEqSvLqCk5ymHmCdZiJQQEpAxVbXb9bkKs2UhxN1zRnug4OcR411XOqlvlBwsk121yY760
6mZ7r+icnXvLLEVezmegXsN8mlhAnb+p629HPZSMFOSHgX3CwhIwTKDaMxZBft94Fk8w3l/
NBuwQJYg===Emf5
-----END PGP PRIVATE KEY BLOCK-----
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQCNBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/
AERegEtzoFiveSzbeFQtNhxDIOSPJc60Y8v2nTecI0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPApi
OFXhUrkHF0DmrmEpa5UpHjpO3sD+Hlvg84N6jHjAIRMlNMAyrg/
e4i6ABGzAuxYbJCs6ax9mxdrFAQARAQABtCBBYmhpbmF2IEJoYXR0IDxhYkBhc2lhbmxhd3
Mub3JnPokAtAQQAQIAHgUCPm8MMQUJAeKFAAgLAwkIBwIBCgIZAQUbAwAAAAKCRDR
PtuuStKFCIJwA/9t1Cjpi+hjVaWjJx1BZpoGv4b+t/
Qb03J9ABFUatbypUX5jmMmCUT7h3TgiCgT5F4imvijm4+uCDeoHz0Uj+nPfvW8guMd805s/
+3oU+FT4R2qYvEX6MAQVex67TJ0pHvmiV55Mn/
apNvTdvgSXJbQfHuza9u1QPEUm+LlVdOZx7kAjQQ+bwwyAQQAmkqdApHtWspZdNfqeERO
xctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLRnW+N4QUAgm+eNNsTrqZZjJUP526dOTK8RmxV4Q
Jeh2Q0bsLPs6SXTlPwfBWPpt+U/
kfrSt8ZJF5lWR0jaiJG2hE3dBiuszPa+6cJUDuQnYCVCHZARCKLcAEQEAAYkAqAQYAQIAEg
UCPm8MMgUJAeKFAAUbDAAAAAAKCRDRPtuuStKFCADiA/
0csZOSY9Ztyvw2iVSJqf9g4u3z+ePmEcwy2RK5tuOXU2p7HvEBMKeLlG9Dxg0xwy7cVvHejjA
n4LxMPG9j26TinLCAfqHs7C1og8an1tHstrM4Icw7pWx5fIRLiqQLqEc/
RVFLBKU3nMAjgu0E9wjHicWFwsxUfeF5qD9kAsI0Og===klTT
-----END PGP PUBLIC KEY BLOCK-----
```

To understand how this works, let's look at the RSA algorithm (named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman).

The RSA public-key encryption algorithm works in the following manner:

1. Generation of a public-private key pair.

2. Encryption of a message (plain text) with the public key generated in step (1) to get the cipher-text.

3. Decryption of the cipher-text by using the corresponding private key generated in step (1).

Step 1: Generation of a key pair

1. Select two large integer primes p and q.

2. Multiply p and q to get a number n, that means, $pq = n$.

3. Obtain φ which is the product of $(p-1)$ and $(q-1)$, that means $\varphi = (p-1)(q-1)$.

4. Select e such that $1<e<\varphi$ and the greatest common divisor of e and φ is 1. That means e and φ are coprime.

5. Compute d such that $1<d<\varphi$ and $ed \equiv 1 \bmod \varphi$. This means that the value of d must be such that $ed-1$ should be completely divisible by φ or
   $(ed-1) / \varphi$ should be an integer.

6. The public-key is (e, n) and the corresponding private key is (d, n).

Step 2: Encryption process

Suppose the message to be encrypted is m. The cipher-text c is obtained by raising the message to the value of e and finding out its modulo n.

That means
$c = m^e \bmod n$.

Step 3: Decryption process

Decryption is achieved by raising the cipher-text *c* obtained in step 2 to the value of *d* and finding out its modulo *n*.

That means $m=c^d \bmod n$.

Let's try the algorithm with really small prime numbers: 3 and 11. (In reality the primes chosen would be really really large).

1. Choose $p = 3$ and $q = 11$

2. Compute $n = p * q = 3 * 11 = 33$

3. Compute $\varphi = (p - 1) * (q - 1) = 2 * 10 = 20$

4. Choose e such that $1 < e < \varphi$ and e and φ are coprime. Let $e = 7$

5. Compute a value for d such that $1<d<\varphi$ and $ed \equiv 1 \bmod \varphi$.
   One solution is $d = 3$.

6. Public key is $(e, n) \Rightarrow (7, 33)$
   Private key is $(d, n) \Rightarrow (3, 33)$

7. Suppose the plain text is 2.
   The cipher text will be $c = m^e \bmod n$.
   That's $2^7 \bmod 33 = 128 \bmod 33 = 29$

8. The decryption will be
   $c^d \bmod n$
   $= 29^3 \bmod 33$
   $= 24389 \bmod 33$
   $= 2$

See: https://www.cs.utexas.edu/~mitra/honors/soln.html

The security of the RSA cryptosystem is based on the *integer factorization* problem. Any adversary who wishes to decipher the cipher-text *c* must do so by using the publicly available information *(n, e).* One possible method is to first factor *n*, and then compute φ and *d* just as was done in the above mentioned steps.

The factoring of *n* is currently computationally infeasible (provided sufficiently large prime numbers are chosen as *p* and *q*) and therein lies the strength of the RSA cryptosystem.

Before we get into the nuts and bolts of how crypto-currencies work, we need to understand some more concepts including **hash functions**. A one-way *hash function* takes an input (e.g. a PDF file, a video, an email, a string etc.) and produces a fixed-length output e.g. 160-bits.

The hash function ensures that if the information is changed in any way – even by just one bit – an entirely different output value is produced. The table below shows some sample output values using the sha1 (40) hash function.

Computing hash of an electronic record is a very simple process e.g. in php it can be done with:
hash_file('sha256', $filename).]

Input	Hash
sanya	c75491c89395de9fa4ed29affda0e4d29cbad290
SANYA	33fef490220a0e6dee2f16c5a8f78ce491741adc
Sanya	4c391643f247937bee14c0bcca9ffb985fc0d0ba

It can be seen from the table above that by changing the input from **sanya** to **SANYA**, an entirely different hash value is generated.

What must be kept in mind is that irrespective of the size of the input, the hash output will always be of the same size.

Two things must be borne in mind with regard to one-way hash functions:

1. It is computationally infeasible to find two different input messages that will yield the same hash output.

2. It is computationally infeasible to reconstruct the original message from its hash output.

Having understood hash functions, let's have a look at another interesting concept called **proof-of-work**.

This is invented to reduce spam and denial of service attacks by requiring a computer to spend some time and processing power to solve something.

One such proof-of-work system that is used in crypto-currencies is **hashcash**.

The basic premise of *hashcash* is that if the sender of an email can prove that she has spent reasonable time and computational power to solve some puzzle, it can be believed that the sender is not a spammer.

The logic is that spamming would be economically infeasible if a spammer had to spend non-trivial time and computational power for every single email being sent.

Let's develop an elementary proof-of-work system, based on hashcash, which can be used to control spam.

Let's presume that rohasnagpal@gmail.com is sending an email to info@primechain.in

The sender must include something similar to the following in the header of the email:

rohasnagpal@gmail.com:info@primechain.in:06112016:xxxx

That's 4 pieces of information separated by colons:

1. the sender's email address
2. the receiver's email address
3. the current date in DDMMYYYY format
4. something that needs to be calculated by the sender's computer. Let's call it a ***nonce*** (abbreviation for "number only used once").

The objective is to find an input that would result in a sha256 hash which begins with 4 zeros.

So we start the nonce at a value of 0 and then keep incrementing it (1, 2, 3 …) and calculating the hash.

Something like this:

Input	rohasnagpal@gmail.com:info@primechain.in:06112016:0
sha256 Hash	2d87bf06373f4e91b43ab6180e30da0bf3f98efb44c5d5e2f7151b3179413bf6

Input	rohasnagpal@gmail.com:info@primechain.in:06112016:1
sha256 Hash	cb3616e4ab0cee86badf0a598d1a151e06289c2c7e35f91554dc1ad7d128a99d

Input	rohasnagpal@gmail.com:info@primechain.in:06112016:2
sha256 Hash	8d04a9e7ccd2c84549744c7fdbd48e3784ea3ab10020499a89349875726e3536

And so on till .. 76063

Input	rohasnagpal@gmail.com:info@primechain.in:06112016:76063
sha256 Hash	0000b3c73f0cd6a92158b713fbade5f898dffeefc0a615d050b1ea391bd39906

Calculating this may not take a genuine sender a lot of time and computational power but if a spammer were to make these calculations for millions of emails, it will take a non-trivial amount of time and computational power.

At the receiver's end, the computer will simply take the following line from the header of the email and calculate the hash.

rohasnagpal@gmail.com:info@primechain.in:06112016:76063

If the hash begins with a pre-defined number of zeros (4 in this example), the email would not be considered spam.

This will take the receiver a trivial amount of time and computational power since it just has to calculate the hash of one input. The date can be used as an additional validation parameter – e.g. if the date is within 24 hours of the time of receipt, the email will be approved for download.

A very important application of public key cryptography is a **digital signature**. In this, the signer first calculates the hash of the message she wants to digitally sign. Then using her private key and the hash, she creates a digital signature, using the relevant algorithm.

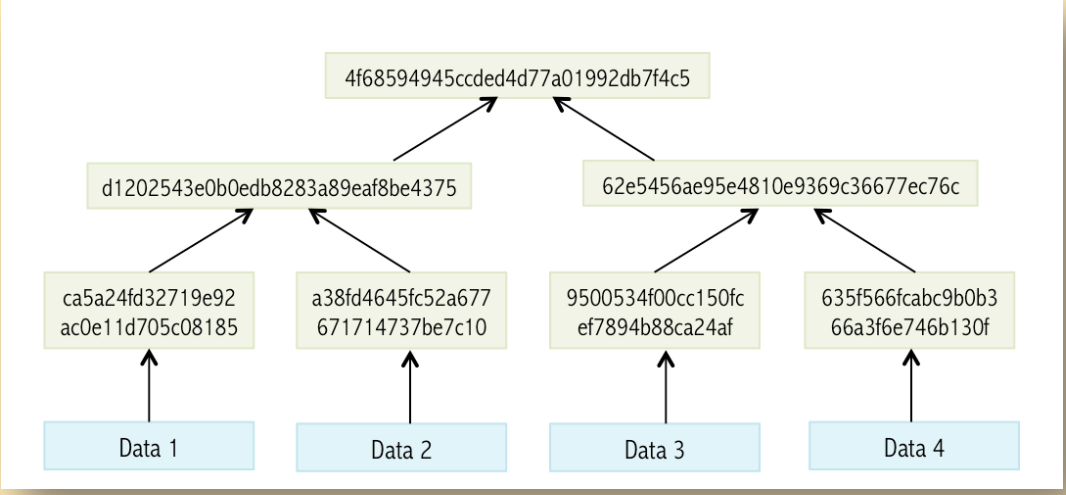
This **digital signature** is unique to the message. The signer then sends the message and the digital signature to the receiver. The receiver re-computes the hash from the message. The receiver also computes another string using the digital signature and the signer's public key (using the relevant algorithm). If this string and the hash match, the digital signature is verified.

Blind digital signatures were subsequently developed for use in digital cash and cryptographic voting systems. In this system, the content of the message is disguised before it is signed. The resulting blind signature can be verified against the original, un-blinded message in the manner of a regular digital signature.

However, blind digital signatures do not solve the **double-spending** problem. 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. Since electronic records are easily duplicated, a "digital coin" can be spent multiple times.

Bitcoin solves the double-spending problem through the **blockchain** - a public ledger containing an ordered and time-stamped record of transactions. In addition to preventing double-spending, the blockchain prevents the modification of previous transaction records.

A block of one or more new transactions is collected into the transaction data part of a block. Copies of each transaction are hashed, and the hashes are then paired, hashed, paired again, and hashed again until a single hash remains, the **merkle root** of a **merkle tree**.

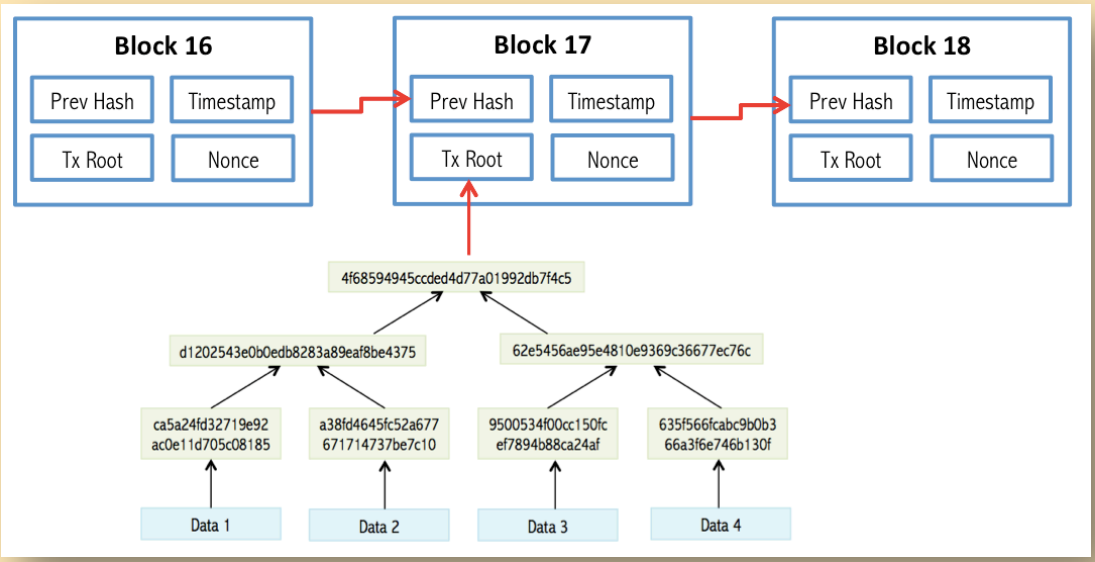


4f68594945ccded4d77a01992db7f4c5 is the merkle root of the 4 transactions (or pieces of data) in the illustration above.

This is stored in the block header. Additionally, each block also stores the hash of the header of the previous block.

This chains the blocks together and ensures that a transaction cannot be modified without modifying the block that records it and all following blocks. Transactions are also chained together.

This is illustrated below:



Lets consider a simple illustration of how the blockchain works. Consider a block that has 6 transactions a, b, c, d, e and f.

The *merkle tree* is:
d1 = double-hash (a)
d2 = double-hash (b)
d3 = double-hash (c)
d4 = double-hash (d)
d5 = double-hash (e)
d6 = double-hash (f)

d7 = double-hash (d1 concatenated with d2)
d8 = double-hash (d3 concatenated with d4)
d9 = double-hash (d5 concatenated with d6)

d10 = double-hash (d7 concatenated with d8)
d11 = double-hash (d9 concatenated with d9)
Since there are an odd number of hashes, we take d9 twice

d12 = double-hash (d10 concatenated with d11)

d12 is the *merkle root* of the 6 transactions in this block.

This is stored in the block header. Additionally, each block also stores the hash of the header of the previous block.

This chains the blocks together and ensures that a transaction cannot be modified without modifying the block that records it and all following blocks. Transactions are also chained together.

Bitcoin uses a *proof-of-work* technique similar (but more complex) than the one discussed earlier in this document.

Since “good” cryptographic hash algorithms convert arbitrary inputs into “seemingly-random” hashes, it is not feasible to modify the input to make the hash predictable.

To prove that she did some extra work to create a block, a **miner** must create a hash of the block header, which does not exceed a certain value.

The term *miner* must not be compared with a gold or coal miner in the real world.

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.

Bitcoin miners spend a lot of money (for computational power and electricity) and are compensated by way of a reward for each block they mine – this was initially 50 bitcoins per block and is halving every 210,000 blocks. Miners also earn transaction fees. Miners usually operate as parts of large pools.

Interestingly, Bitcoins can be also be mined with a pencil and paper. See: http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html

The first-ever Bitcoin block is known as the **genesis block**. Each subsequent block is addressed by its **block height**, which represents the number of blocks between it and the genesis block.

New blocks are added to the block chain if their hash is at least as challenging as a **difficulty** value expected by the Bitcoin *consensus protocol*. According to the bitcoin protocol, it should take 2 weeks for 2016 blocks to be generated. If the time taken is more or less than 2 weeks then the difficulty value is relatively decreased or increased.

A Bitcoin **address** is an identifier of 26 to 35 alphanumeric characters, beginning with the number 1 or 3, which represents a possible destination for a bitcoin payment. Addresses can be generated at no cost by any user of Bitcoin.

There are currently two address formats in common use:

Common P2PKH which begin with the number 1 e.g.
1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Newer P2SH type starting with the number 3 e.g.
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Bitcoin **wallets** at their core are a collection of private keys.

These collections are stored digitally in a file, or can even be physically stored on pieces of paper.

The simplest Bitcoin **wallet** is a program, which performs these functions:

- ❑ generates private keys,
- ❑ derives the corresponding public keys,
- ❑ helps distribute those public keys as necessary,
- ❑ monitors for outputs sent to those public keys,
- ❑ creates and signs transactions spending those outputs, and
- ❑ broadcasts the signed transactions.

Although it's called a **wallet**, a Bitcoin wallet does not store bitcoins. The wallet is a collection of public-private key-pairs.

As discussed, the **blockchain** is a database of transaction information. It is constantly growing and is sent out to all nodes in the Bitcoin network. Every transaction is distributed to the network and all valid transactions are included in the next block, which is mined.

Imagine a real-world transaction where your salary is transferred to your bank account through an online transfer made by your employer. You then use your debit card to pay for dinner.

This transfers some of the money to the restaurant's account. In these 2 transactions, did you see a single currency note? No. So we can say that in today's world most money exists as a history of transactions and balances.

Bitcoin, or for that matter most virtual currencies, works the same way. They don't actually "exist" in the true sense of the word. They just are there!

A bitcoin can be divided down to 8 decimal places - 0.00000001 is the smallest amount, also referred to as a **satoshi**.

The last block that will generate bitcoins will be block 6,929,999. This is expected to be generated around the year 2140 AD.

After that, the total number of bitcoins will remain static at just below 21 million.

More about blockchains

Imagine a world without computer databases. There would be no e-commerce, no ATMs, no Internet banking, no Facebook, no Gmail, no WhatsApp! Almost everything that makes the Internet so powerful and useful depends upon computer databases.

The digital world relies very heavily on computer databases, even though most users are unaware of it. Now imagine a database that is provably immutable/unchangeable and almost impossible to hack. That's a blockchain. At its core, a blockchain is an ordered and time-stamped sequence of "blocks of information".

- Blockchain technology was invented by the unknown inventor of the bitcoin crypto-currency in 2008. Simply put, the bitcoin crypto-currency runs on the bitcoin blockchain — a public blockchain where anyone can become a miner and details of every single bitcoin transaction are stored on each node.

- Blockchain is an innovative mix of decades old, tried and tested technologies including Public key cryptography (1970s), Cryptographic hash functions (1970s) and proof-of-work (1990s).

- Over the last few years, many derivative projects (e.g. ethereum, multichain) and blockchain-inspired distributed ledger systems (e.g. BigchainDB, Corda, Hyperledger Burrow / Fabric / Sawtooth, Quorum) have been created.

- Blockchains are provably immutable and enable the rapid transfer and exchange of crypto-tokens (which can represent assets) without the need for separate clearing, settlement & reconciliation.

- Blockchains can create public-private key pairs and also be used for generating and verifying digital signatures.

- Blockchain solutions can be permissioned (e.g. a Government run land registry) or permission-less (e.g. Bitcoin, where anyone can become a miner). Blockchain solutions can be private (e.g. a contract management system implemented in a pharmaceutical company), public (e.g. an asset backed cryptocurrency) or hybrid (e.g. a group of banks running a shared KYC platform).

- Blockchains can handle data authentication & verification very well. This includes immutable storage (data stored on a blockchain cannot be changed or deleted), digital signatures and encryption. Data in almost any format can be stored in the blockchain.

- Blockchains can handle smart asset management very well. This includes issuance, payment, exchange, escrow, and retirement of smart assets. A smart/crypto asset is the tokenized version of a real-world asset e.g. gold, silver, oil, land.

- Blockchains do not have a single point of control or a single point of failure.

- For organizations, blockchain technology can minimize fraud; accelerate information and money flow; greatly improve auditability and streamline processes.

- The original blockchain, which powers the bitcoin crypto-currency, used proof of work as a consensus mechanism. But today there are multiple distributed ledger systems that offer a host of consensus mechanisms such as Proof of stake, Byzantine fault tolerant, Deposit based consensus, Federated Byzantine Agreement, Proof of Elapsed Time, Derived PBFT, Redundant Byzantine Fault Tolerance, Simplified Byzantine Fault Tolerance, Federated consensus, Round Robin and Delegated Proof of Stake.

- One method of providing privacy on a blockchain is the separation of concerns, in which data is sent only to the relevant parties of a transaction. Optionally, the hash of the data is broadcast to all the nodes. This method is used in Corda, Quorum, and Hyperledger Fabric. Another method of providing privacy on a blockchain involves broadcasting of encrypted data across the entire network.

Forks

Source: https://unhashed.com/bitcoin-cryptocurrency-forks-list

A “fork” is the term used to describe a single blockchain diverging into two paths. Generally this occurs as the result of a significant change in the network’s protocol that effectively splits the blockchain into an old way of doing things and a new way of doing things.

Forks can be categorized as hard forks or soft forks.

Hard forks are the result of network changes that are so extensive that every node participating in the network must upgrade their software in order to be compatible with the new processes.

A hard fork is a fundamental change in the way a blockchain operates, such that any nodes that do not upgrade their software are on a different blockchain altogether.

Soft forks, by contrast, are backwards-compatible. The rules of the network have been changed, but nodes running the old software will still be able to validate transactions.

This is less dramatic than a hard fork.

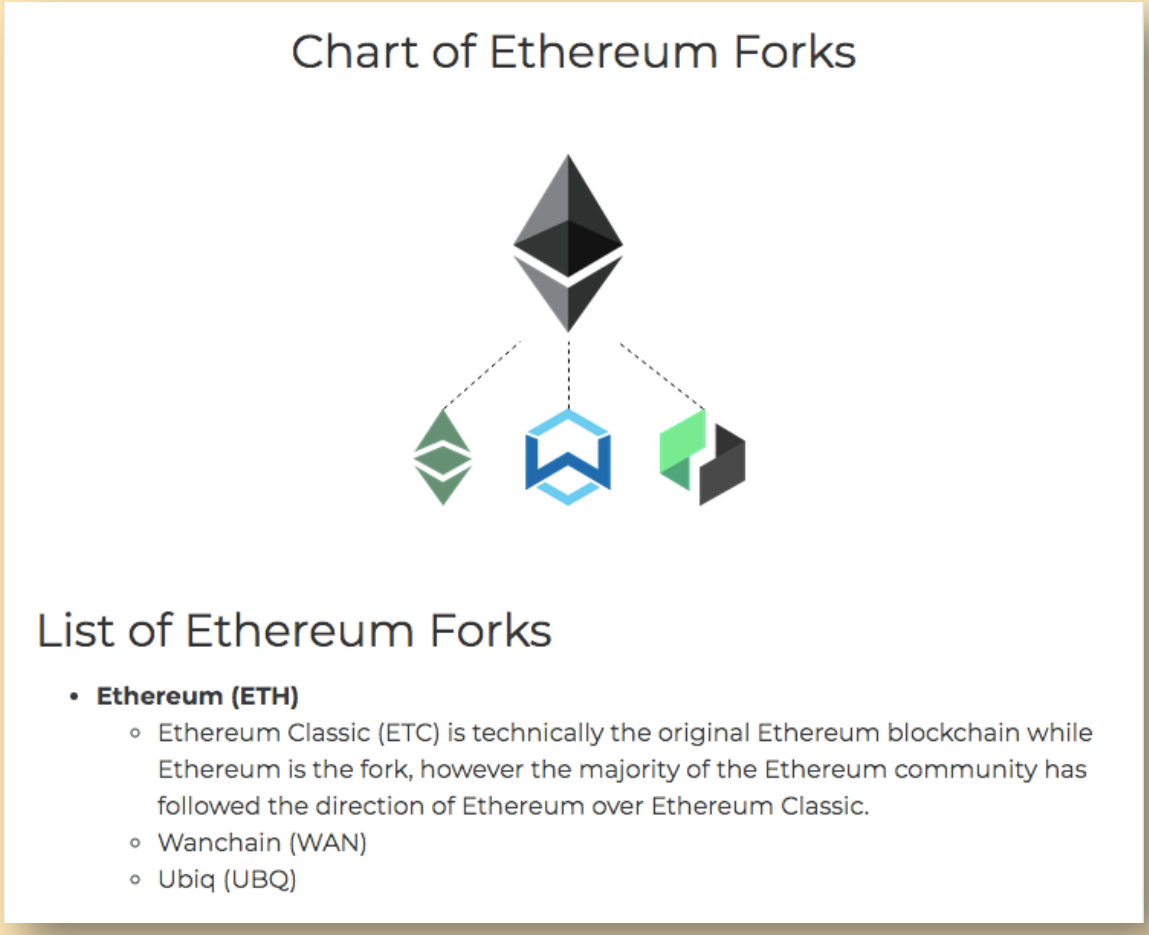


Chart of Bitcoin Blockchain and Software Forks

List of Bitcoin Blockchain and Software Forks

Each indent below represents a fork and includes forks of forks.

- **Bitcoin (BTC)**
  - Litecoin (LTC)
    - Junkcoin (JKC)
      - Lukycoin (LKY)
        - Dogecoin (DOGE)
    - Monacoin (MONA)
    - LitecoinCash (LCC)
    - CloakCoin (CLOAK)
    - Einsteinium (EMC2)
    - Feathercoin (FTC)
  - Bitcoin Cash (BCH)
  - Dash (DASH)
    - PIVX (PIVX)
      - Blocknet (BLOCK)
  - Bitcoin Gold (BTG)
  - Zcash (ZEC)
    - Zclassic (ZCL)
      - Bitcoin Private (BTCP)
      - ZenCash (ZEN)
    - Komodo (KMD)
  - Qtum (QTUM)
  - Bitcoin Diamond (BCD)
  - Peercoin (PPC)
    - Novacoin (NVC)
      - Blackcoin (BLK)
        - Stratis (STRAT)
        - Greencoin (GRE)
      - Vertcoin (VTC)
      - BitcoinDark (BTCD)
    - Hshare (HSR)
    - Nexus (NXS)
  - Decred (DCR)
  - DigiByte (DGB)
  - Syscoin (SYS)
  - Reddcoin (RDD)
  - Elastos (ELA)
  - Emercoin (EMC)
  - GroestIcoin (GRS)
  - NavCoin (NAV)
  - Viacoin (VIA)

List of Ripple Forks

- **Ripple (XRP)**
  - Stellar (XLM) started out as a fork, but is no longer considered a fork as it now uses its own codebase.

List of Monero Forks

- **Monero (XMR)** was originally a fork of Bytecoin, but no longer considered a fork as it now uses its own codebase.
  - Electroneum (ETN)
  - Monero Original (XMO)
  - Monero Classic (XMC)

List of Bytecoin Forks

- **Bytecoin (BCN)**
  - DigitalNote (XDN)

List of NXT Forks

- **NXT (NXT)**
  - NEM (NEM) started out as a fork, but is no longer considered a fork as it now uses its own codebase.
  - Ardor (ARDR)
  - Burst (BURST)

List of Lisk Forks

- **Lisk (LSK)**
  - Ark (ARK)

List of Zcoin Forks

- **Zcoin (XZC)**
  - SmartCash (SMART)

Proof-of-work requires a ton of computational power. This consumes a huge amount of electricity and generates a lot of heat.

Proof-of-stake (PoS) as a consensus mechanism, on the other hand, is much more energy efficient. In PoS, participants lock their coins (that's their “stake”). At particular intervals, the blockchain randomly assigns someone the right to validate the next block.

The chances of being chosen are directly proportional to the amount of coins. More the stake, higher the chance.

Staking rewards vary based on the blockchain and sometimes even on a per-block basis. A **staking pool** is when a group of participants come together to increase he chances of validating blocks and subsequently earning the reward.

Delegated Proof of Stake (DPoS) can be compared to a mutual fund. Participants "commit" their coin balances as votes which are then used to elect a number of delegates. These delegates manage the blockchain on behalf of their "voters".

Practically speaking, staking simply requires you to hold your coins with a relevant exchange or in a relevant wallet.

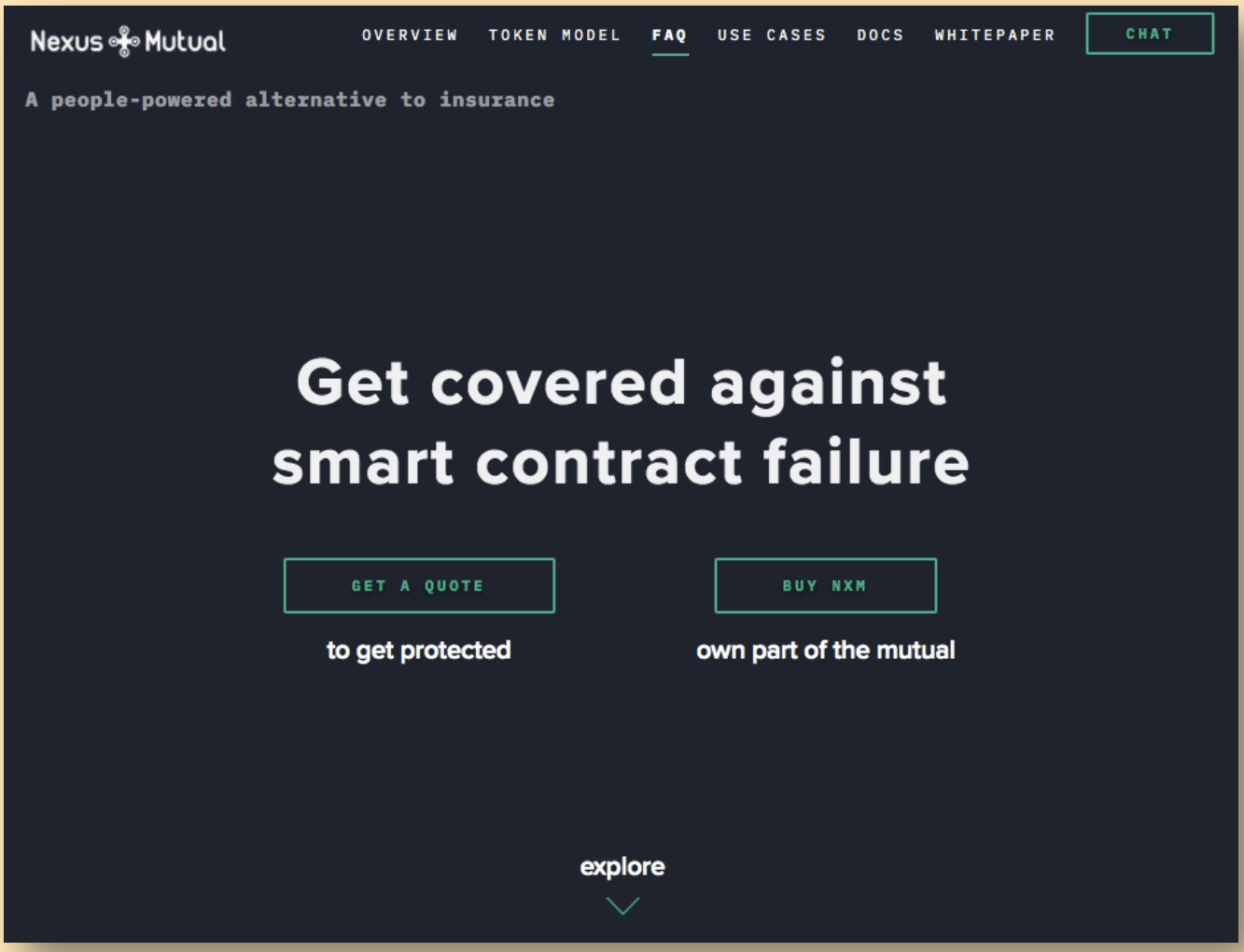
Did you know that Blockchains can be hacked...

Many people believe that blockchains cannot be hacked. Well, that's not true! Here are some examples.

Bitcoin was hacked in August 2010 when some hackers exploited a vulnerability and generated billions of bitcoins which were sent to two addresses on the network. The vulnerability was fixed, the transaction was erased from the transaction log and the Bitcoin network was forked to an updated version.

On 15th August, a "bad" transaction got into block 74638 due to a bug in Bitcoin’s code. This was fixed in block 74691 by when the "good" blockchain overtook the "bad" one.

In 2016, the "hacking" of a poorly written smart contract led to the #Ethereum blockchain being hard forked to roll back the theft of millions of dollars. This also led to the birth of the Ethereum Classic blockchain whose native asset is ETC.



Nexus Mutual replaces traditional insurance with a decentralised alternative. It provides a "Smart Contract Cover" to protect against hacks in the smart contracts.

https://nexusmutual.io

3. Smart Contracts

Smart contracts are neither "smart" nor legal "contracts". They are self-executing, business automation applications which run on blockchains.

Things to know about smart contracts:

- ❑ The rules for automating processes must be accurate.
- ❑ High quality programming is crucial.
- ❑ The data being fed into a smart contract must be accurate.
- ❑ Once a smart contract is written, it cannot be changed.

Real-time data feeds must be supplied to the blockchain. These feeds are the “middleware” between the data and the smart contract and are called "**oracles**”.

According to Shermin Voshmgir in *Token Economy*, oracles can be of the following types:

1. Software Oracles
They handle information data that originates from online sources, like temperature, prices of commodities and goods, flight or train delays, etc. The software oracle extracts the needed information and pushes it into the smart contract.

2. Hardware Oracles
Some smart contracts need information directly from the physical world, for example, a car crossing a barrier where movement sensors must detect the vehicle and send the data to a smart contract, or RFID sensors in the supply chain industry.

3. Inbound Oracles
They provide data from the external world.

4. Outbound Oracles
They provide smart contracts with the ability to send data to the outside world. An example would be a smart lock in the physical world, which receives payment on its blockchain address and needs to unlock automatically.

5. Consensus-based Oracles
They get their data from human consensus and prediction markets like Augur and Gnosis. Using only one source of information could be risky and unreliable. To avoid market manipulation, prediction markets implement a rating system for oracles. For further security, a combination of different oracles may be used, where, for example, 3 out of 5 oracles could determine the outcome of an event.

Augur is an “open, global prediction market protocol that allows anyone to create a market for anything. There is no single entity that controls the protocol; it’s community owned and operated.”

Gnosis builds new market mechanisms for decentralized finance. Their 3 interoperable product lines allow the secure creation, trading, and holding of digital assets on Ethereum.

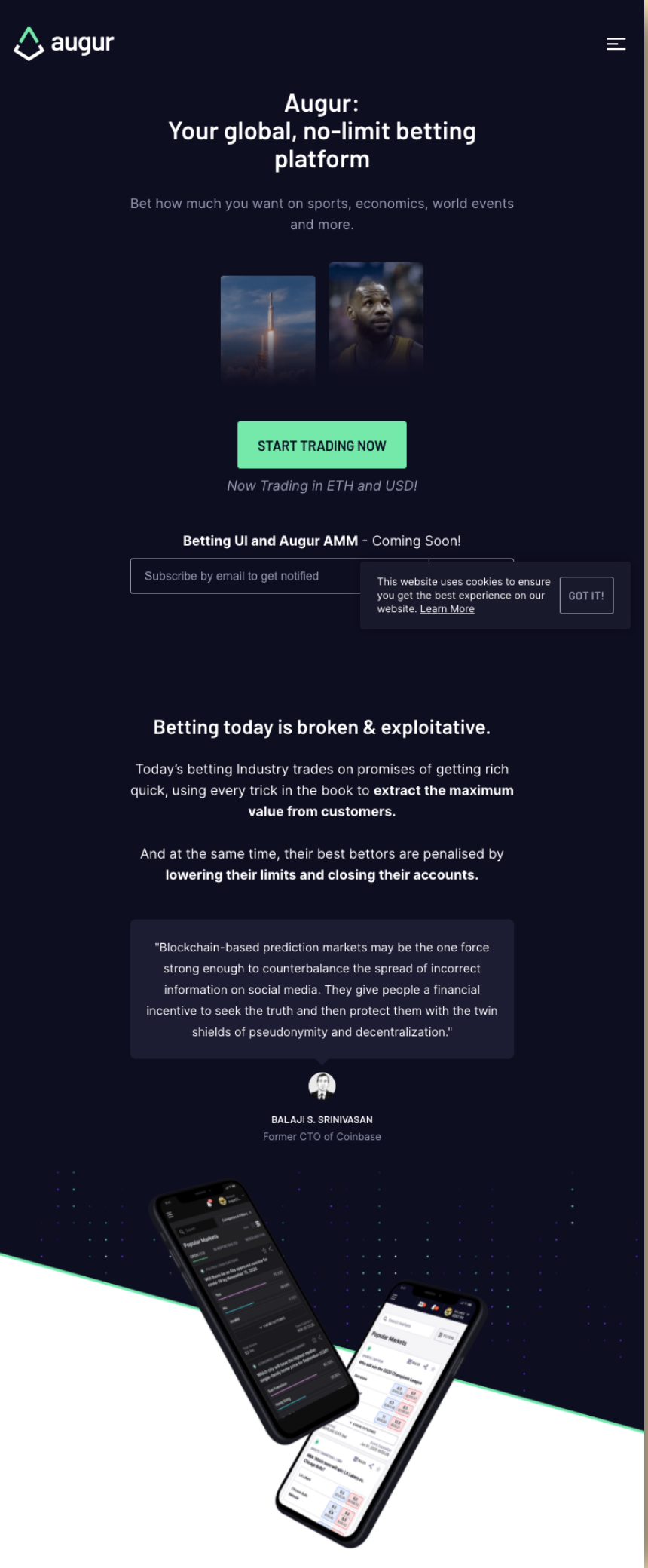
As of December 2020, the most prominent Smart Contract Coins are:

- ❑ Ethereum (ETH)
- ❑ Cardano Ada (ADA)
- ❑ Stellar (XLM)
- ❑ EOS (EOS)
- ❑ Tron (TRX)
- ❑ NEM (XEM)
- ❑ Tezos (XTZ)
- ❑ Neo (NEO)
- ❑ VeChain (VET)
- ❑ Cosmos (ATOM)

A smart contract for creating a simple cryptocurrency

```
pragma solidity ^0.4.21;

contract Coin {
    // The keyword "public" makes those variables
    // readable from outside.
    address public minter;
    mapping (address => uint) public balances;

    // Events allow light clients to react on
    // changes efficiently.
    event Sent(address from, address to, uint amount);

    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() public {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) public {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) public {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        emit Sent(msg.sender, receiver, amount);
    }
}
```

For an explanation of the smart contract, see:
https://docs.soliditylang.org/en/v0.4.24/introduction-to-smart-contracts.html



Augur is not a prediction market, it is a protocol for cryptocurrency users to create their own prediction markets.

Augur is a set of open source smart contracts that can be deployed to the Ethereum blockchain.

https://augur.net

4. DeFi

Decentralized finance (DeFi) is an "experimental" form of finance.

It does not rely on intermediaries (e.g. brokerages, exchanges, banks) and instead uses smart contracts.

DeFi platforms enable users to:
- ❑ lend or borrow funds
- ❑ speculate using derivatives
- ❑ trade cryptocurrencies
- ❑ insure against risks
- ❑ earn interest

MakerDAO, launched in 2015, is the first DeFi platform. It allows people to take out loans of the Dai stablecoin which is pegged to the U.S. dollar.

DeFi is powered by DApps (decentralized blockchain applications). Use cases include:

1. **Decentralized exchanges** (DEXs), where the transactions don't happen through centralised intermediaries like cryptocurrency exchanges. Instead, they happen directly between participants through smart contract programs.

2. **Flash loans**, which are unsecured loans that must be repaid in the same transaction (this is a duration of minutes or even seconds). They are primarily used to make money from arbitrage by taking advantage of price disparities across different trading platforms.

3. **Lending platforms**, where smart contracts replace banks.

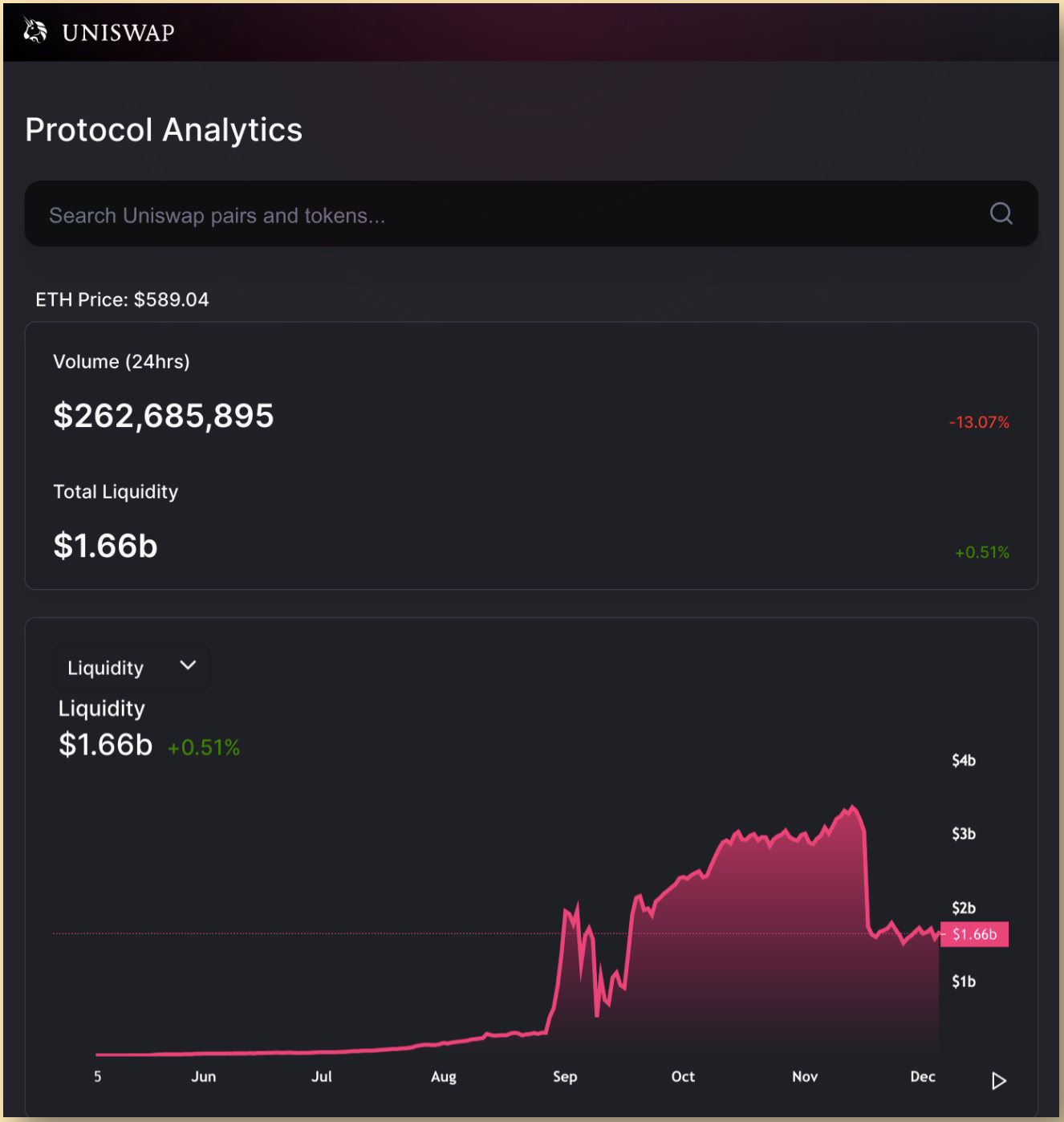
4. **"Wrapped" bitcoins** which is a way of sending bitcoin to the Ethereum blockchain. This enables earning of interest on the bitcoins lent via the decentralized lending platforms.

5. **Prediction markets**, which are markets for betting on future events e.g. elections.

6. **Yield farming**, where users scan through multiple DeFi tokens in search of opportunities for larger returns.

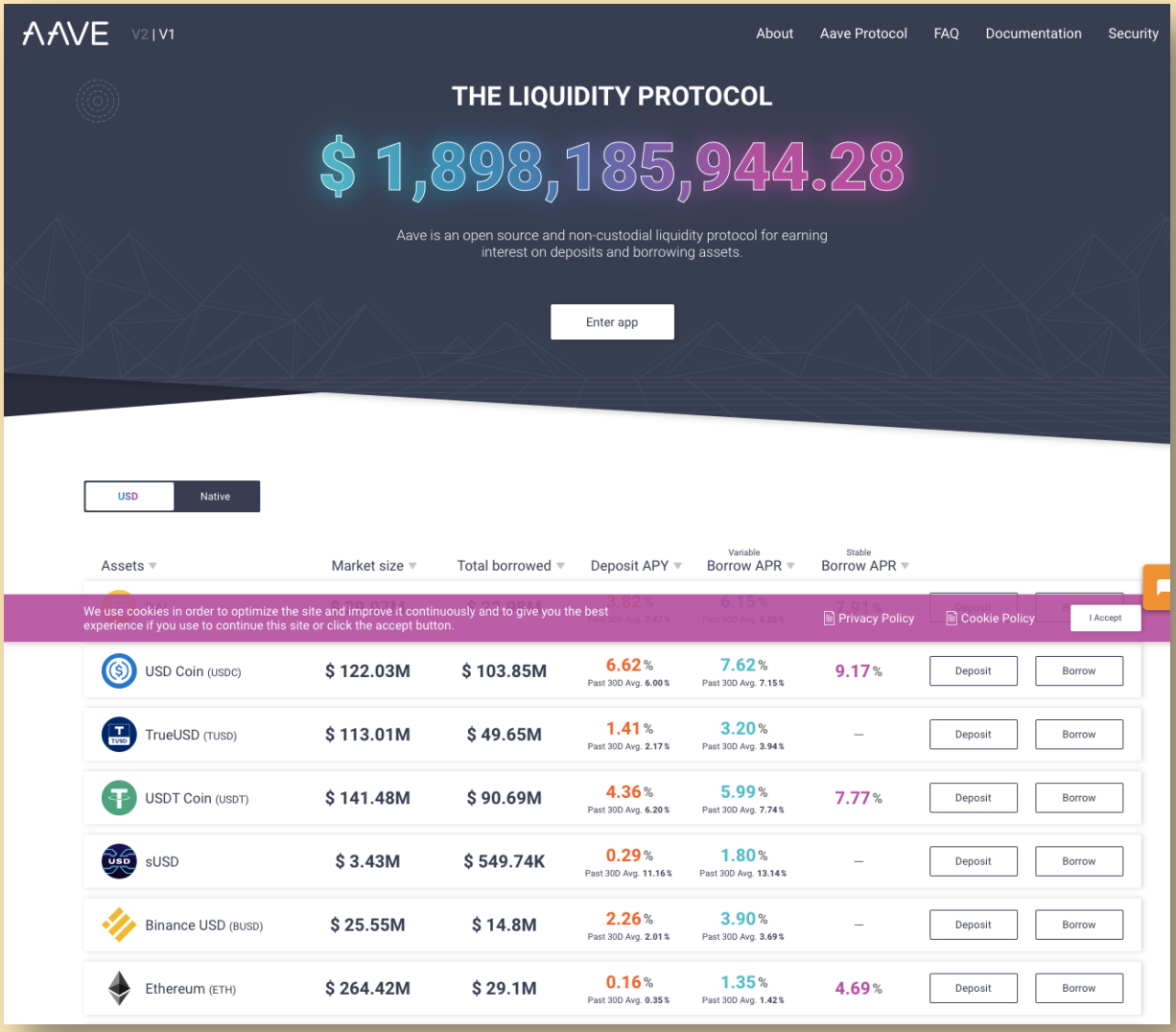
Since blockchain transactions are irreversible, it is very difficult to reverse incorrect transactions or cases where the smart contract code contains errors. An example is Yam Finance which had deposits of $750 million. It crashed in a few days post-launch because of code errors.

DeFi use cases are usually non-compliant with Know Your Customer (KYC) and anti-money laundering (AML) laws.



Uniswap is a decentralized exchange (dex) that runs on the Ethereum blockchain. It enables the trading of hundreds of Ethereum digital tokens. The Uniswap algorithm "incentivizes" users to form liquidity pools for tokens by issuing trade fees to those who provide liquidity.

https://info.uniswap.org/home



Aave is a decentralized non-custodial money market protocol where users can participate as depositors or borrowers. Depositors provide liquidity to the market to earn a passive income, while borrowers are able to borrow in an overcollateralized (perpetually) or undercollateralized (one-block liquidity) fashion.

https://aave.com

The platform has 2 type of fees:

- From borrowers, a 0.00001% of the loan amount is collected on loan origination.
- From Flash Loans, a 0.09% is collected from the loan amount.

There are also transaction fees for Ethereum Blockchain usage, which depend on the network status and transaction complexity.

5. Stablecoins

A stablecoin is a blockchain-based token that is valued by reference to an underlying fiat currency or basket of assets.

Fiat Collateralized Stablecoins are blockchain assets that are backed 1:1 with fiat currency.

Stablecoins combine the benefits of a blockchain (e.g. transparency and speed), without the inherent volatility risk of crypto-currencies.

Stablecoins can reduce counterparty and settlement risk, decrease capital requirements and enable instant value transfer.

Stablecoins are a technological innovation as well as a financial innovation.

Conventional payment systems involve the movement of E-money across multiple private databases (of banks, money transfer organizations etc.). This is why typical cross-border payments involve high cost and time.

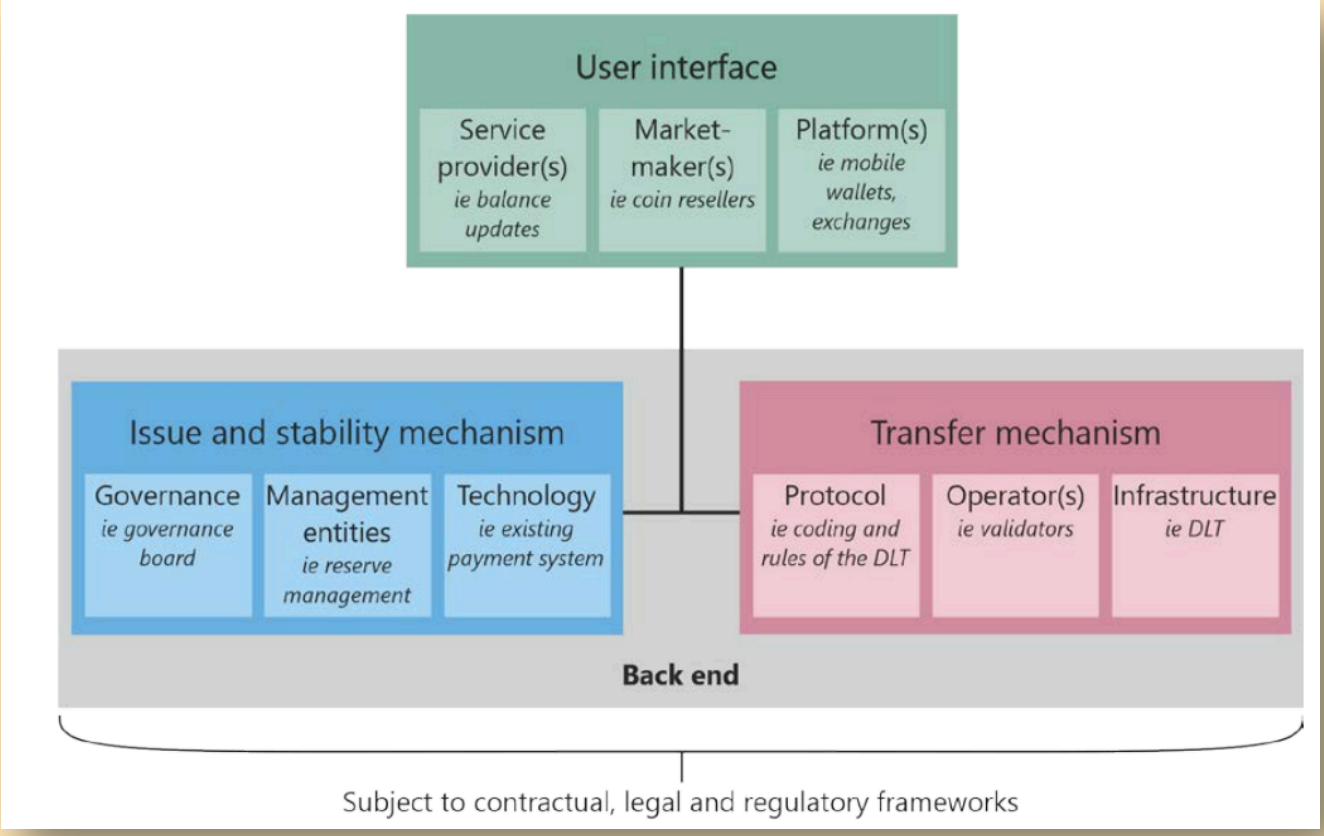
Blockchain technology removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending.

A stablecoin runs on a permissioned blockchain, and not in private databases, and that is why movement of stablecoins can happen in real-time at near zero cost.

The United Nations recognises 180 currencies across the world – Indian Rupee, US dollar, Euro Japanese Yen, etc. E-money is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency – i.e. it electronically transfers value that has legal tender status.

Stablecoins are E-money and not virtual or crypto currencies. This makes stablecoins legal in most countries.

A functional view of the stablecoin ecosystem
(Source: Investigating the impact of global stablecoins)



Further reading

The rise of digital money
https://www.rohasnagpal.com/docs/future-money/IMF-Digital-Money.pdf

Investigating the impact of global stablecoins
https://www.bis.org/cpmi/publ/d187.pdf

Stablecoins: risks, potential and regulation
https://www.bis.org/publ/work905.pdf

According to the International Monetary Fund (IMF), cash and bank deposits could soon be surpassed by e-money.

6. Central Bank Digital Currency

Fiat currency is a currency established as money by government regulation, monetary authority or law. Central bank digital currency (CBDC) is the digital form of fiat money.

China's "**digital yuan**" is the world's most advanced "central bank digital currency" initiative. 4 million transactions totalling 2 billion yuan have been completed as of December 2020.

The People's Bank of China (PBOC) has in the past issued 10 million yuan worth of digital currency to 50,000 randomly selected citizens in Shenzhen.

The second scheme will involve 200 digital yuan "red envelopes" being given to 100,000 citizens selected through a lottery.

The Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements have collaborated on a report setting out common foundational principles and core features of a CBDC.

These principles emphasize that, in order for any jurisdiction to consider proceeding with a CBDC, these criteria would have to be satisfied:

- **"Do no harm".** New forms of money supplied by the central bank should continue supporting the fulfilment of public policy objectives and should not interfere with or impede a central bank's ability to carry out its mandate for monetary and financial stability.

  For example, a CBDC should maintain and reinforce the "singleness" or uniformity of a currency, allowing the public to use different forms of money interchangeably.

- **Coexistence.** Central banks have a mandate for stability and proceed cautiously in new territory. Different types of central bank money – new (CBDC) and existing (cash, reserve or settlement accounts) – should complement one another and coexist with robust private money (eg commercial bank accounts) to support public policy objectives. Central banks should continue providing and supporting cash for as long as there is sufficient public demand for it.

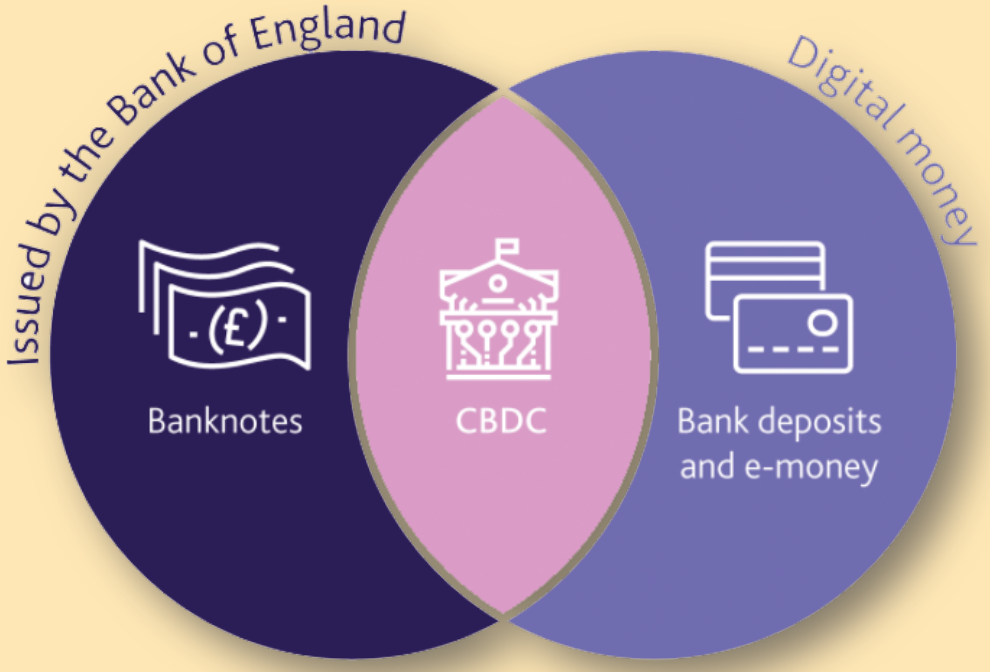
- **Innovation and efficiency.** Without continued innovation and competition to drive efficiency in a jurisdiction's payment system, users may adopt other, less safe instruments or currencies.

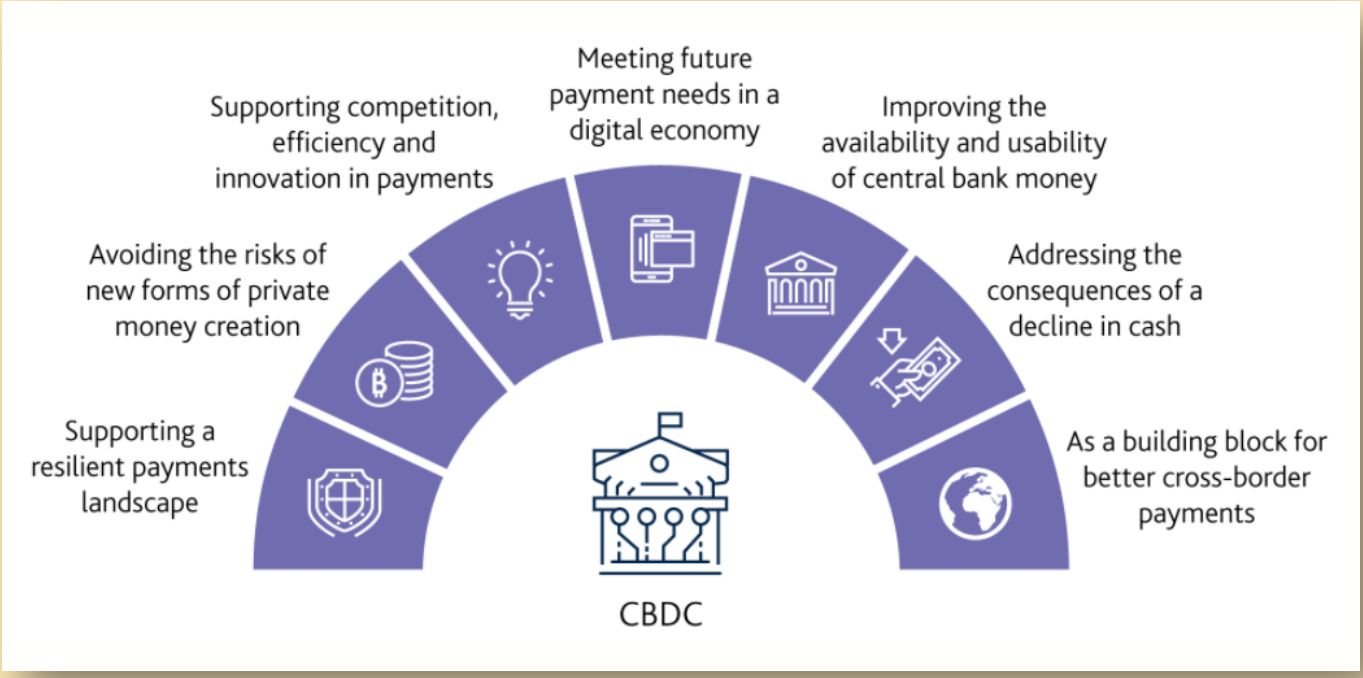
Further reading

- Central bank digital currencies: foundational principles and core features: https://www.bis.org/publ/othp33.pdf

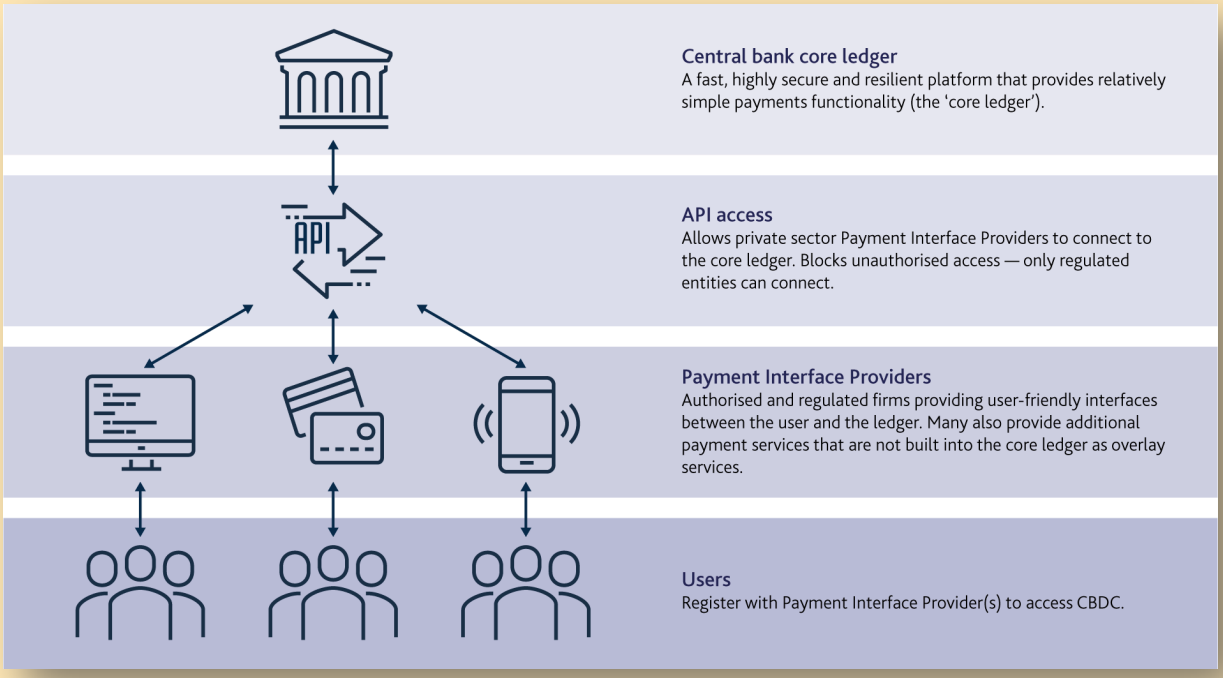
- Central bank digital currencies by Committee on Payments and Market Infrastructures: https://www.bis.org/cpmi/publ/d174.pdf

- Discussion Paper on Central Bank Digital Currency - Opportunities, challenges and design (Bank of England): https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf





Source: Bank of England



Bank of England's illustrative model of CBDC designed to store value and enable UK payments by households and businesses.

China's "digital yuan" is the world's most advanced Central Bank Digital Currency" initiative. 4 million transactions totalling 2 billion yuan had been completed as of December 2020.

7. eMoney

According to the International Monetary Fund (IMF), there are five types of money:

1. Central bank money – e.g. US dollars or Indian Rupees in notes and coins cash and its digital counterpart - central bank digital currency (CBDC).

2. Crypto-currency e.g. bitcoin

3. B-money, which comprises commercial bank deposits.

4. E-money, which is electronically stored monetary value denominated in, and pegged to, a common unit of account such as the euro, dollar, rupee or renminbi, or a basket thereof.

5. I-money (investment money), an equity-like instrument that entails a claim on assets, e.g. gold.

The two most common forms of money today (cash and bank deposits) will face tough competition and could even be surpassed by e-money (electronically stored monetary value denominated in, and pegged to, a common unit of account such as the euro, dollar, or renminbi, or a basket thereof).

According to the IMF, the adoption of e-money may also grow rapidly elsewhere for one or several of at least six reasons:

- **Convenience**: E-money is better integrated into our digital lives when compared with b-money or central bank money.

- **Ubiquity**: Cross-border transfers of e-money would be faster and cheaper than those of cash and bank deposits.

- **Complementarity**: If assets like stocks and bonds were moved to blockchains, blockchain-based forms of e-money would allow seamless payment of automated transactions (so-called delivery versus payment, assuming blockchains were designed to be interoperable), thereby potentially realizing substantial efficiency gains from avoiding manual back-office tasks.

  More generally, e-money functionality more naturally lends itself to being extended by an active developer community, which may draw on open source codes as opposed to proprietary technologies underpinning b-money.

  Developers could for instance allow users to determine the goods that e-money could purchase—a useful feature for remittances or philanthropic donations.

- **Transaction costs**: Transfers in e-money are nearly costless and immediate, and thus are often more attractive than card payments or bank-to-bank transfers especially across borders.

  As a result, people might even agree to sell their car for an e-money payment, as the funds would immediately show up in their account, without any settlement lag and corresponding risks.

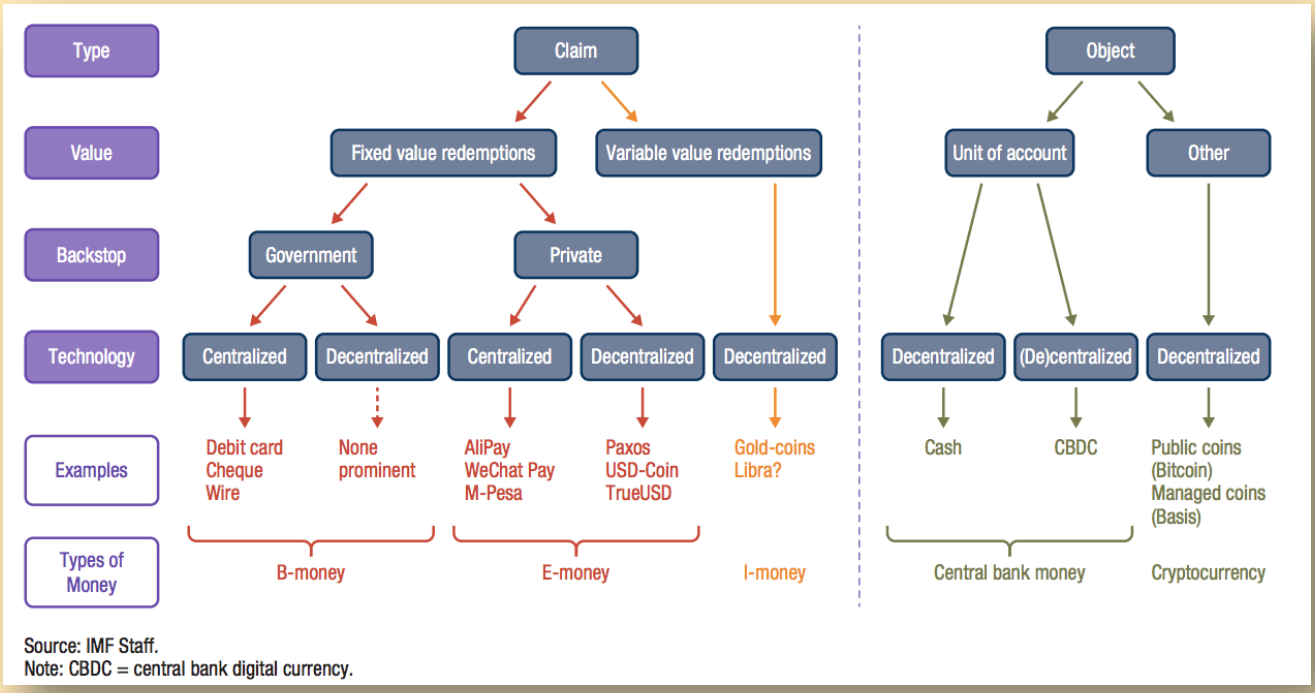
- **Trust**: In some countries where e-money is taking off, users trust telecommunications and social media companies more than banks.

- **Network effects**: If merchants and peers also use e-money, its value to prospective users is all the greater. And as new users join, the value to all participants - existing and prospective - grows.

In China and Kenya, e-money already rules.

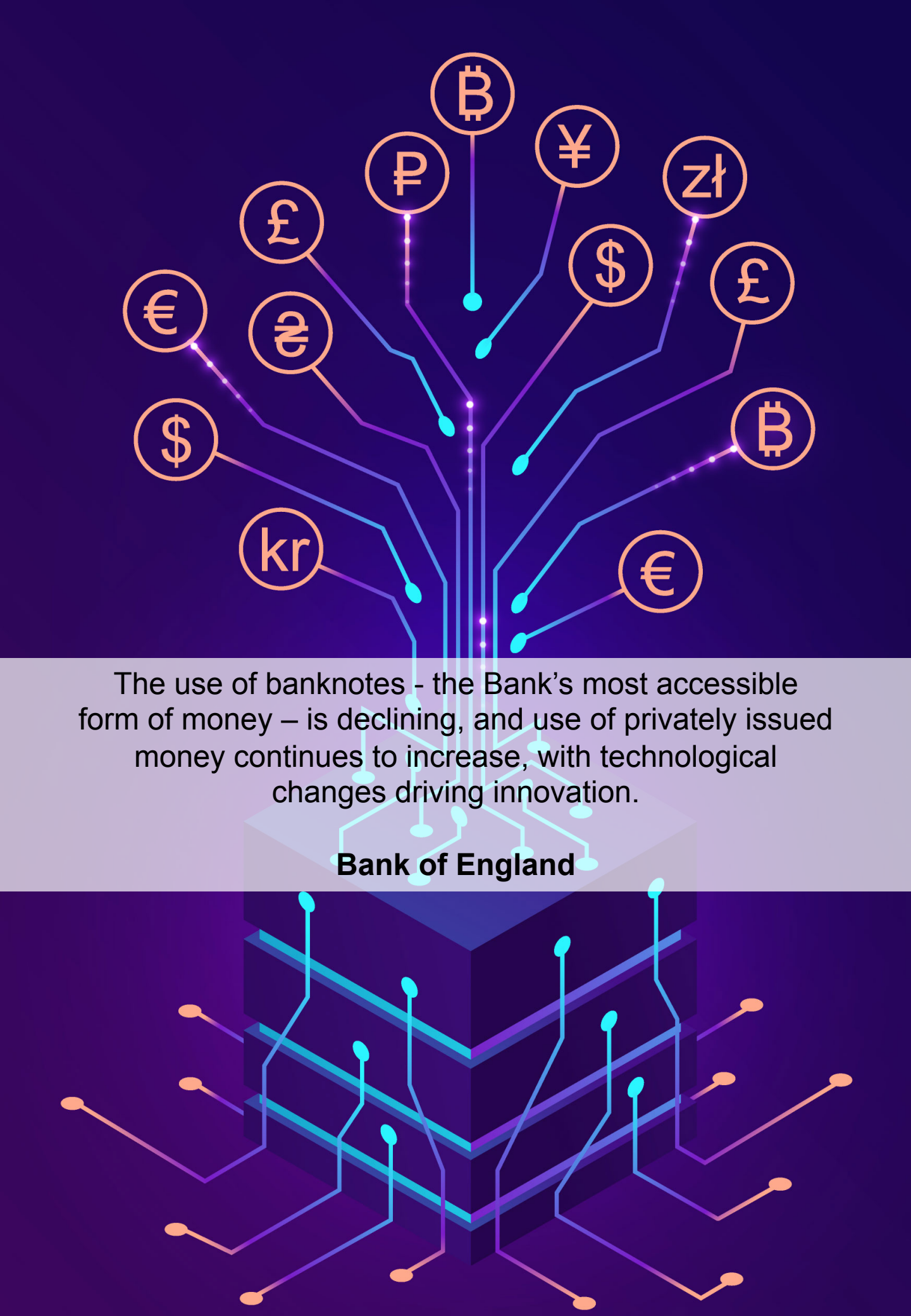
90% of Kenyans over age 14 pay with M-Pesa, and the value of e-money transactions in China, such as with WeChat Pay and Alipay, surpass those worldwide of Visa and Mastercard combined.

Money Trees



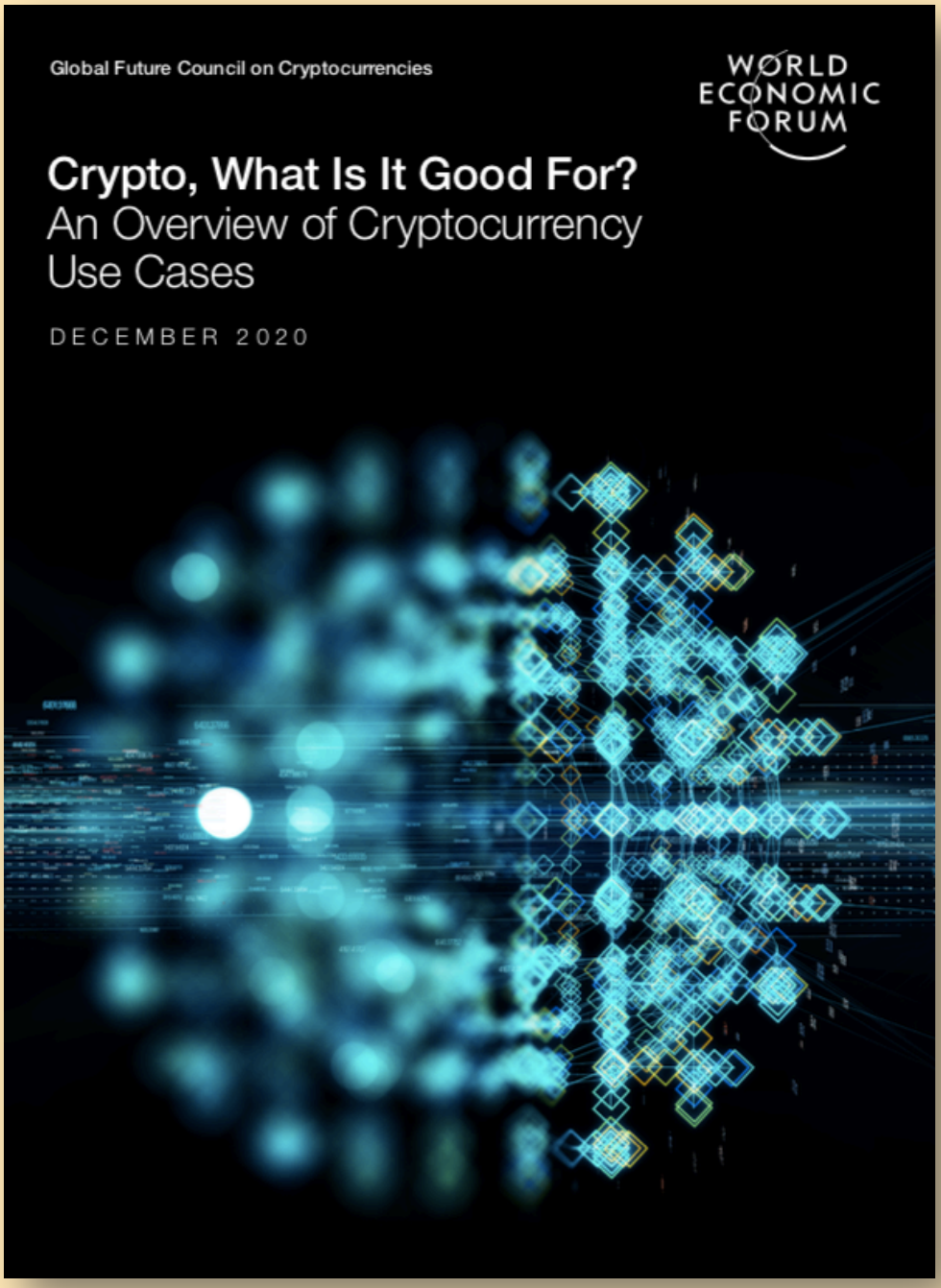
Source: IMF Staff.
Note: CBDC = central bank digital currency.

Source: IMF



The use of banknotes - the Bank's most accessible form of money – is declining, and use of privately issued money continues to increase, with technological changes driving innovation.

Bank of England



Crypto, What Is It Good For?
An Overview of Cryptocurrency Use Cases
http://www3.weforum.org/docs/WEF_Cryptocurrency_Uses_Cases_2020.pdf

8. Prime crypto currencies

According to the FATF report on Virtual Currencies - Key Definitions and Potential AML/CFT Risks, Cryptocurrency has the following characteristics:

- ❑ it is math-based,
- ❑ it is a decentralised convertible virtual currency
- ❑ it is protected by cryptography (it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy)
- ❑ it relies on public and private keys to transfer value from one person (individual or entity) to another
- ❑ it must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties who protect the network in exchange for the opportunity to obtain a randomly distributed fee.

There are thousands of cryptocurrencies out there so it is essential that we agree on a method of grading them.

At Primechain Technologies, a future money company, we are developing the **BITT method** of grading cryptocurrencies.

Under this method points are given for the following 4 criteria:

1. Business model (max 3 points)
2. Impact on society (max 3 points)
3. Team (max 2 points)
4. Tech (max 2 points)

1. Business model (max 3 points)
The business model is "how the cryptocurrency's stakeholders will make money" - creators, miners, partners, etc.

2. Impact on society (max 3 points)
Impact on society measures how this cryptocurrency can make the world a better place and focuses on the humanitarian and environmental aspects.

3. Team (max 2 points)
A crypto-currency is a long term play. So it is essential that it’s managed by a great team with relevant experience and a history of leading successful projects in the industry.

4. Tech (max 2 points)
And finally, the tech platform that the cryptocurrency runs on must be efficient, scalable, and secure.

8.1 Bitcoin (BTC)

Bitcoin is the world's first cryptocurrency. It was launched in 2009 and is the largest cryptocurrency in terms of market capitalization.

New bitcoins are generated roughly every 10 minutes by miners who help to maintain the network. A total of approximately 21 million bitcoins will be generated by the year 2140 AD.

For the latest prices, see:
https://www.coindesk.com/price/bitcoin

One of the simplest ways of buying / selling Bitcoin is by using peer-to-peer marketplace like Paxful or LocalBitcoins.

Paxful

Paxful is a peer-to-peer marketplace that provides 350 ways to buy and sell Bitcoin, including Bank Transfer, UPI transfer, IMPS transfer, Gift Cards, Debit/Credit cards and Digital currencies. You can also use it to buy / sell Tether.

Official site:
https://paxful.com/?r=X5Ywwa837YA

Paxful has a 5 step verification process:
- ❑ Confirm your email
- ❑ Confirm your phone
- ❑ Verify your Government issued ID
- ❑ Verify your address
- ❑ Video verification

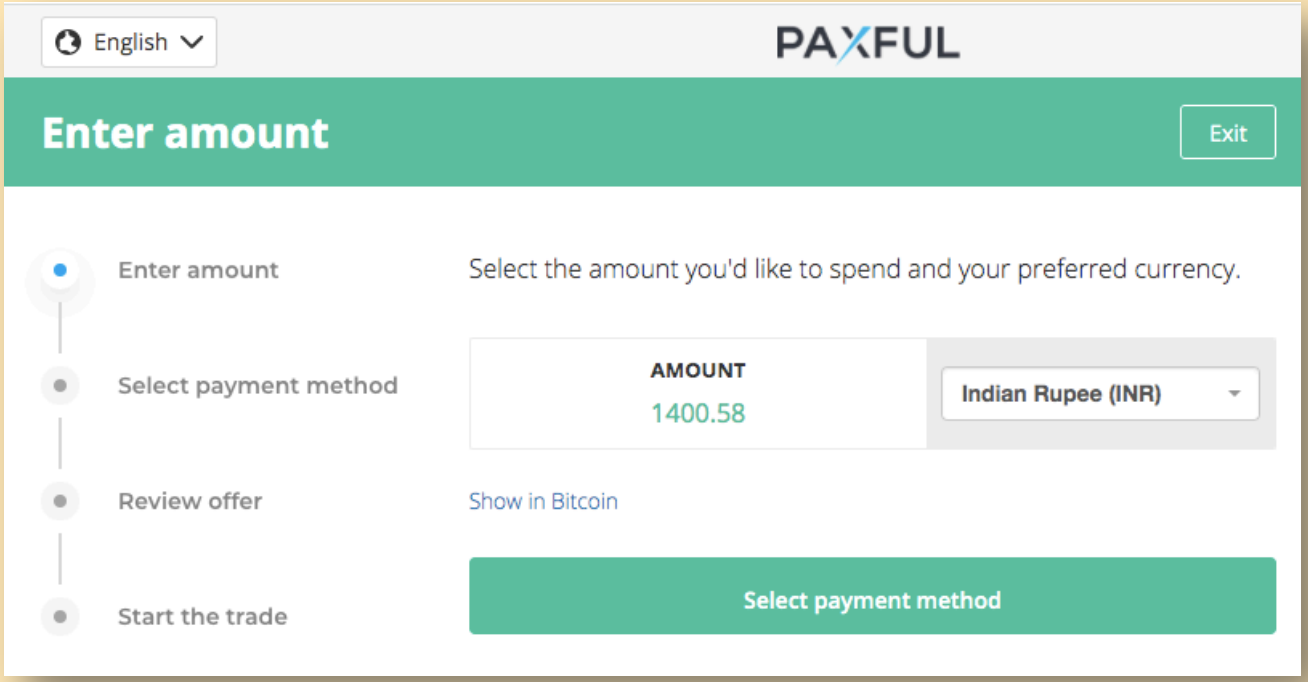
You can buy / sell / send upto $1000 without verification

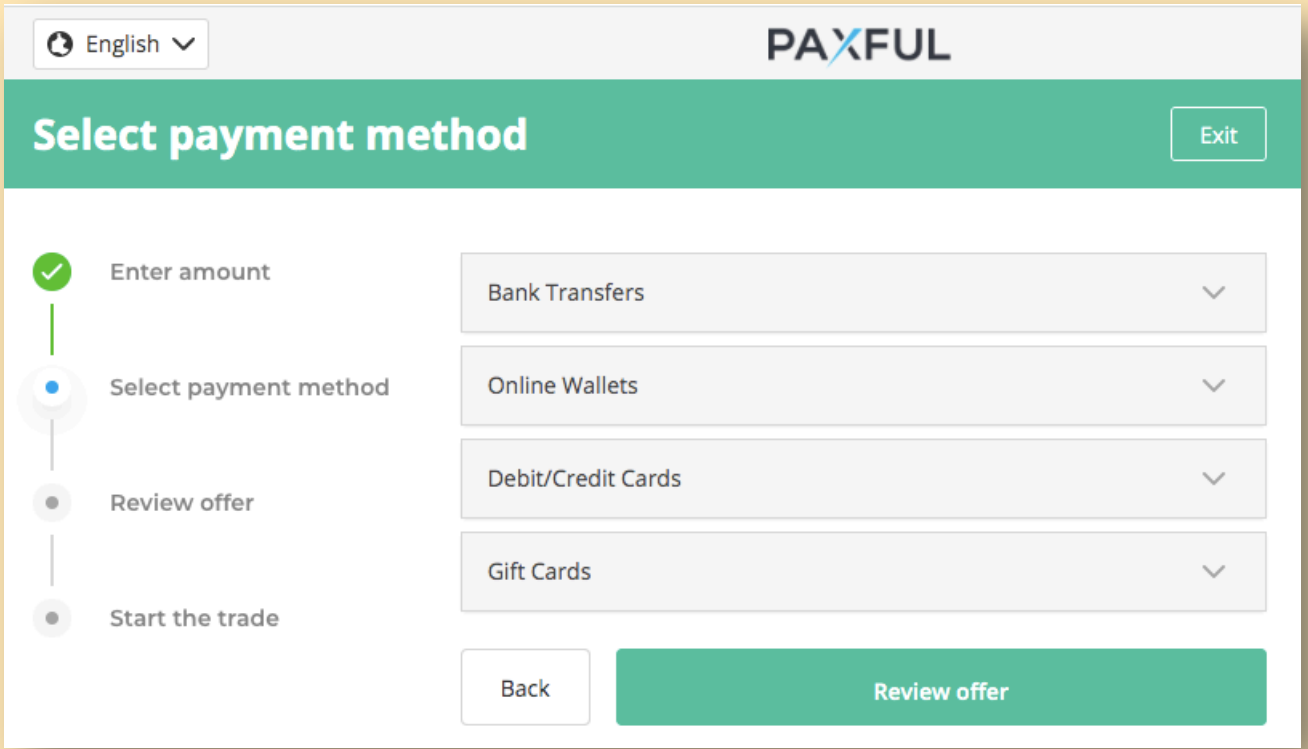
Security features:
- ❑ It is compulsory to set security questions answers.
- ❑ Two factor authentication using SMS or Google Authenticator / Authy is optional but highly recommended.

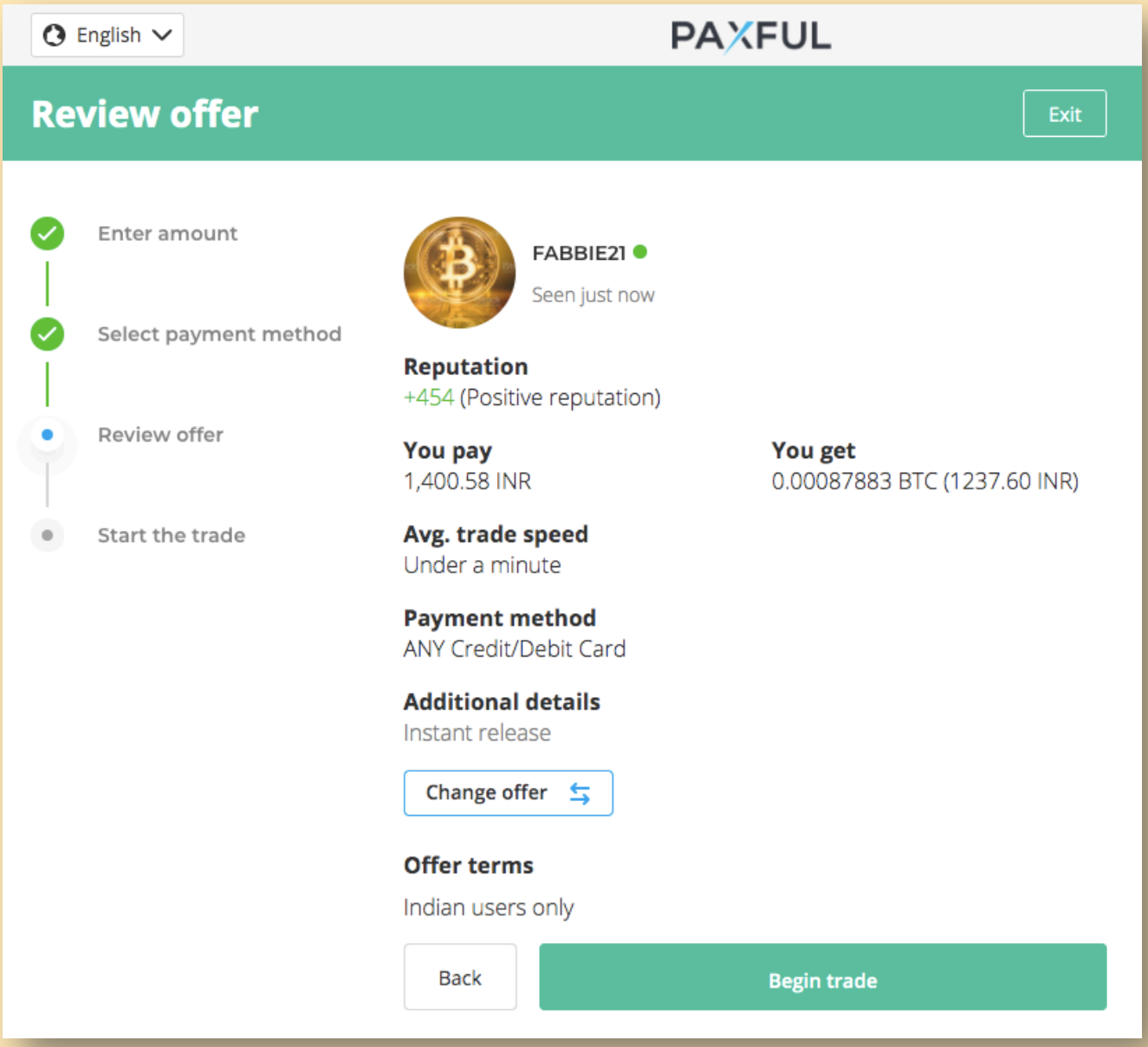
When you login, you can see details of:
- ❑ Active sessions
- ❑ Account activity

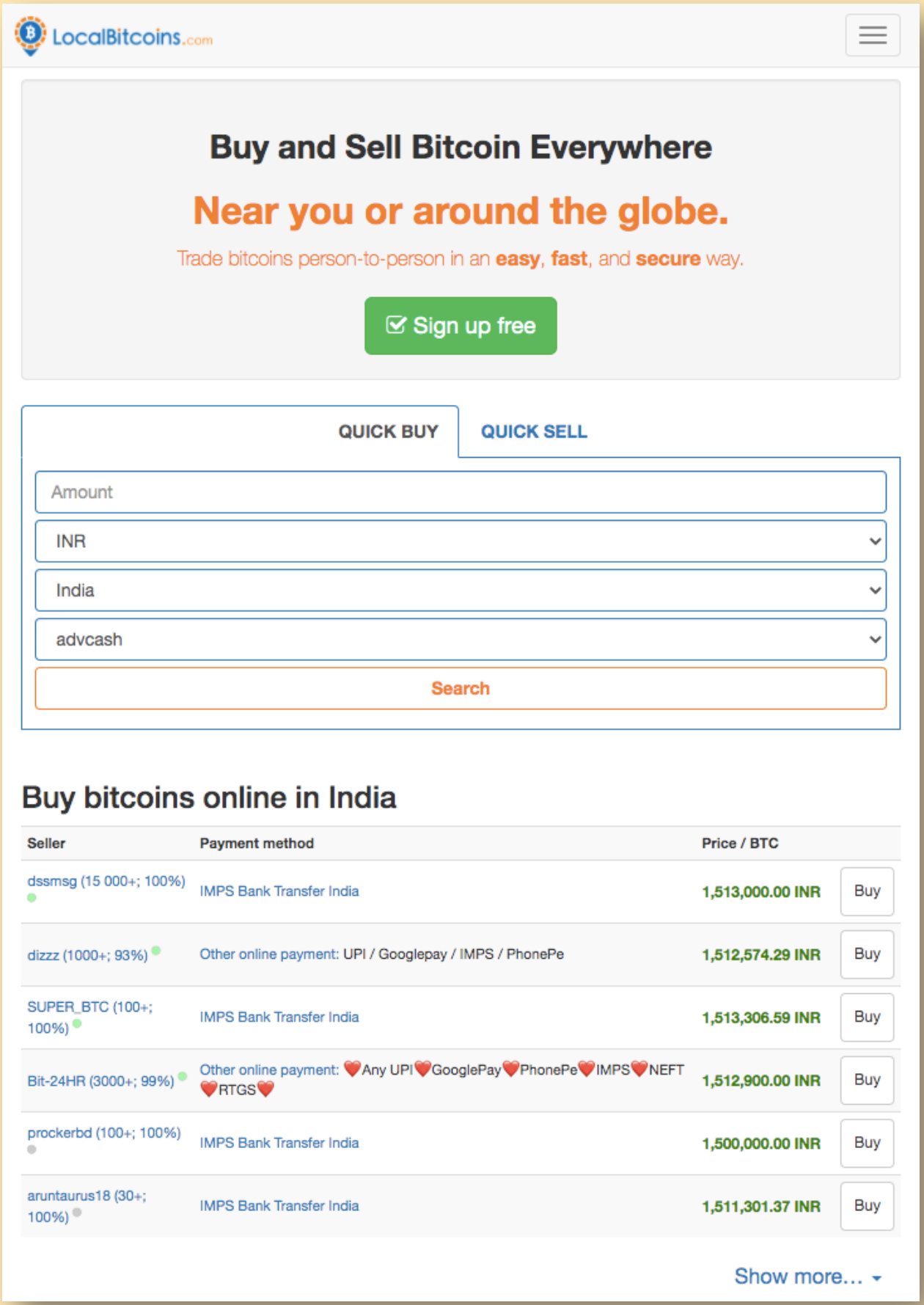
Paxful also gives users a free Bitcoin wallet maintained by BitGo.

How PAXFUL works

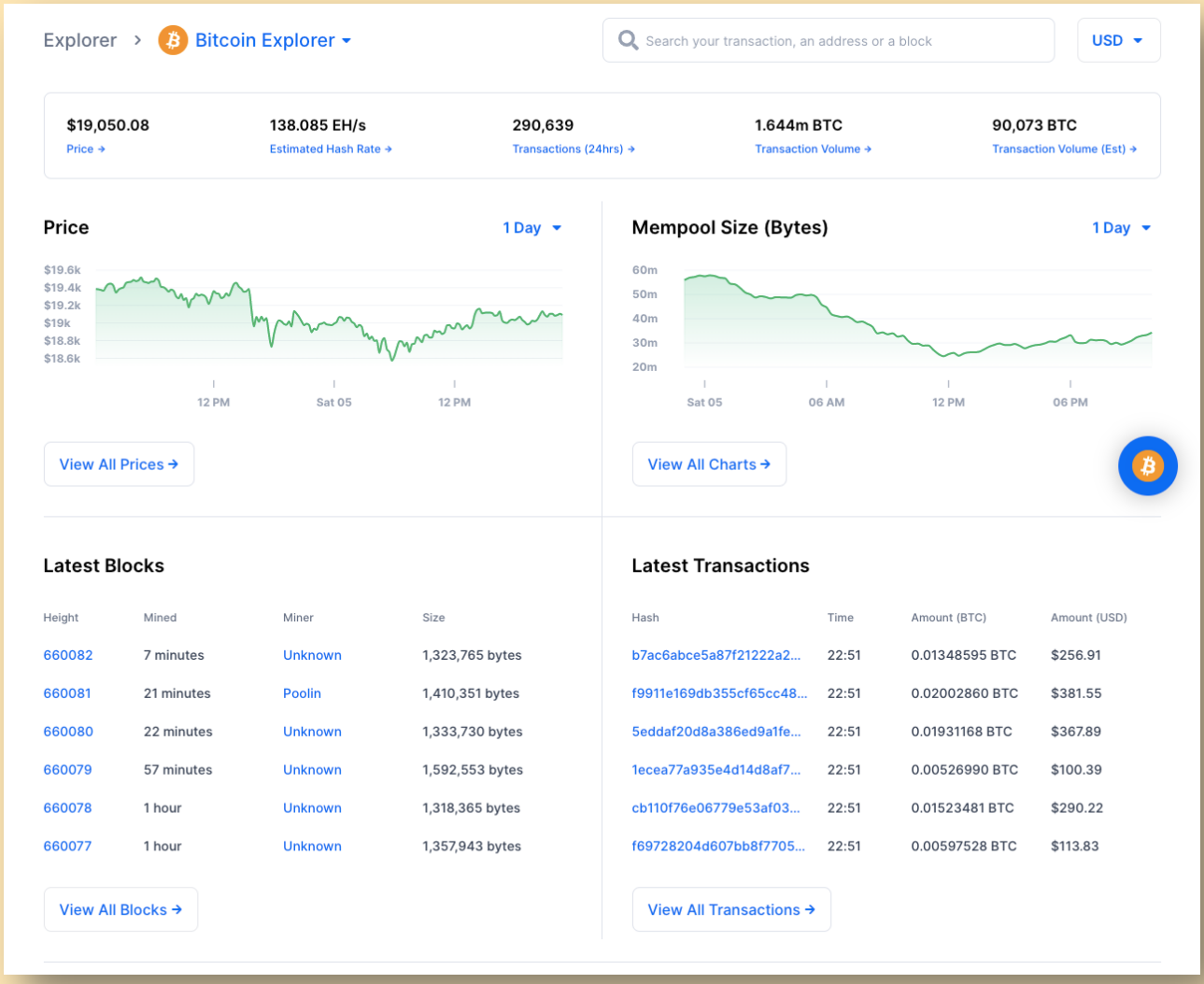





English
PAXFUL
Review offer
Exit
Enter amount
Select payment method
Review offer
Start the trade
FABBIE21
Seen just now
Reputation
+454 (Positive reputation)
You pay
1,400.58 INR
You get
0.00087883 BTC (1237.60 INR)
Avg. trade speed
Under a minute
Payment method
ANY Credit/Debit Card
Additional details
Instant release
Change offer
Offer terms
Indian users only
Back
Begin trade


LocalBitcoins.com
Buy and Sell Bitcoin Everywhere
Near you or around the globe.
Trade bitcoins person-to-person in an easy, fast, and secure way.
Sign up free
QUICK BUY
QUICK SELL
Amount
INR
India
advcash
Search
Buy bitcoins online in India
Seller
Payment method
Price / BTC
dssmsg (15 000+; 100%)
IMPS Bank Transfer India
1,513,000.00 INR
Buy
dizzz (1000+; 93%)
Other online payment: UPI / Googlepay / IMPS / PhonePe
1,512,574.29 INR
Buy
SUPER_BTC (100+; 100%)
IMPS Bank Transfer India
1,513,306.59 INR
Buy
Bit-24HR (3000+; 99%)
Other online payment: Any UPI GooglePay PhonePe IMPS NEFT RTGS
1,512,900.00 INR
Buy
prockerbd (100+; 100%)
IMPS Bank Transfer India
1,500,000.00 INR
Buy
aruntaurus18 (30+; 100%)
IMPS Bank Transfer India
1,511,301.37 INR
Buy
Show more...

All bitcoin transactions can be seen on a Bitcoin Explorer:



https://www.blockchain.com/explorer

Omni

Omni is a platform for creating and trading custom digital assets and currencies. It is a software layer built on top of Bitcoin.

https://www.omnilayer.org

Omni can be used for:

- **Creating custom currencies**
  With Omni it's simple to create tokens to represent custom currencies or assets and to transact these via the Bitcoin blockchain.

- **Blockchain based crowdfunding**
  Crowdsale participants can send bitcoins or tokens directly to an issuer address and the Omni Layer automatically delivers the crowdfunded tokens to the sender in return - all without needing to trust a third party.

- **Trading peer-to-peer**
  Participants can use the distributed exchanges provided by the Omni Layer to exchange tokens for other tokens or bitcoins directly on the blockchain without the need for a third party exchange.

Omni Wallet is a free, hosted web wallet that can be used to send and receive Bitcoin or Omni assets. It can also be used to create assets, launch crowdsales, and trade on the distributed exchange
https://www.omniwallet.org

Omni blockchain explorer can be used to view Omni transactions on the Bitcoin network, lookup Omni asset (smart property) information and view asset trading on the distributed exchange.
https://omniexplorer.info

Omni Core is a fully-validating desktop wallet. It is a superset of Bitcoin Core available for Mac OS X, Windows, and Linux. It facilitates peer-to-peer distributed exchange trading.
https://www.omnilayer.org/download.html

There is no bitcoin!

"There is no spoon," goes a mind-blowing line from "The Matrix" movie.

Similarly, there is no bitcoin.

Bitcoins don't exist like gold or silver or shares or land.

What we call "bitcoins" are not "property" in the traditional sense. They simply represent a series of transactions between "addresses" which look like this: 1AHr3RDJS7v8ruFLbVoxXsgVeGqYqALqQ8

And transactions are digitally "signed" using private keys that look like this: Kytj7WpTKxtV7XnVLzv72BPpFRTwDi82NTmjUEKc9x1o8ctVHhrT

Crypto is a word cumulatively used for cryptocurrencies and a host of other cryptographically powered financial innovations.

Do NOT invest in crypto till you actually understand how they work and how you can securely trade and hold them.

8.2 Bitcoin Cash (BCH)

In July 2017, miners representing more than 80% of bitcoin computing power voted to incorporate the SegWit2x (segregated witness) technology. This reduces the data to be verified in each block "by removing signature data from the block of data that needs to be processed in each transaction and having it attached in an extended block".

Bitcoin Cash was started by miners and developers who had reservations about the segregated witness technology. In August 2017, they initiated a hard fork and created a new currency Bitcoin Cash (BCH).

BCH has its own blockchain and due to its increased block size of 8 MB and an adjustable level of difficulty it processes transactions faster and cheaper.

For the latest prices, see:
https://www.coindesk.com/price/bitcoin-cash

8.3 Bitcoin Satoshi Vision (BSV)

In November 2018, the Bitcoin Cash network was hard forked to create Bitcoin Satoshi Vision (BSV) in an effort to stay true to the original vision for bitcoin while facilitating scalability and faster transaction.

For the latest prices, see:
https://www.coindesk.com/price/bitcoin-sv

8.4 ETH

Ethereum is "the world's programmable blockchain". It was built to overcome the various limitations of the Bitcoin blockchain.

Ethereum is programmable, can be used for multiple digital assets and is a marketplace of financial services, games and apps.

ETH is a crypto currency that fuels and secures Ethereum.

Every Ethereum transaction costs a fee. That fee is paid in ETH. Ethereum miners are similar to Bitcoin miners and are paid a fee to process and verify transactions.

For the latest prices, see:
https://www.coindesk.com/price/ethereum

ETH has value because of the following reasons:

- ❑ It is used to pay transaction fees.
- ❑ It is a digital store of value because the creation of new ETH slows down over time.
- ❑ It is used as collateral for crypto loans, or as a payment system.
- ❑ It is considered an investment, like other cryptocurrencies.

Ethereum enables the creation & trading of unlimited assets (called tokens).

The most popular Ethereum tokens are:

- ❑ **Stablecoins**, which mirror the value of fiat currencies like INR or USD.
- ❑ **Governance tokens** which represent voting power in decentralized organisations.
- ❑ **Collectible tokens / non-fungible tokens (NFTs)** that represent a collectible, piece of digital art, etc.

To learn about Ethereum ERC-20 tokens, see:
https://docs.ethhub.io/guides/a-straightforward-guide-erc20-tokens

To learn more about Ethereum non-fungible ERC-721 tokens, see:
https://docs.ethhub.io/built-on-ethereum/erc-token-standards/erc721/

Some key terms:

- An Ethereum **account** is an entity that can send transactions and has a balance.
- An Ethereum **account** has an Ethereum **address**, like an inbox has an email address. You can use this to send funds to an account.
- A **wallet** is a product that allows you to manage your Ethereum account, like view your account balance, send transactions and more. Most wallet products will let you generate an Ethereum account. So you don't need one before you download a wallet.

8.5 Ethereum Classic (ETC)

Ethereum Classic originated from a much debated hard fork of the ethereum blockchain in 2016. A decentralized autonomous organization (DAO) which had been created on the Ethereum blockchain was hacked and about $60 million of ether was stolen.

The Ethereum code was altered to return the stolen funds to investors. Many nodes objected to this fork as it meant that the blockchain is not immutable. These nodes continued to run and mine the "pre-fork" version of the ethereum blockchain which is now known as ethereum classic.

For the latest prices, see:
https://www.coindesk.com/price/ethereum-classic

8.6 LINK

Chainlink is a tokenized oracle network that provides price and events data collected from on-chain and real-world sources. It aims to offer a solution to the "oracle problem" or the ability to get the off-chain data needed to operate many blockchain-based smart contracts.

The token incentivizes participants to provide and use this data. Chainlink does not operate its own blockchain. Instead, the token protocol is blockchain agnostic and can run on many different blockchains simultaneously.

For the latest prices, see:
https://www.coindesk.com/price/chainlink

8.7 Lumen (XLM)

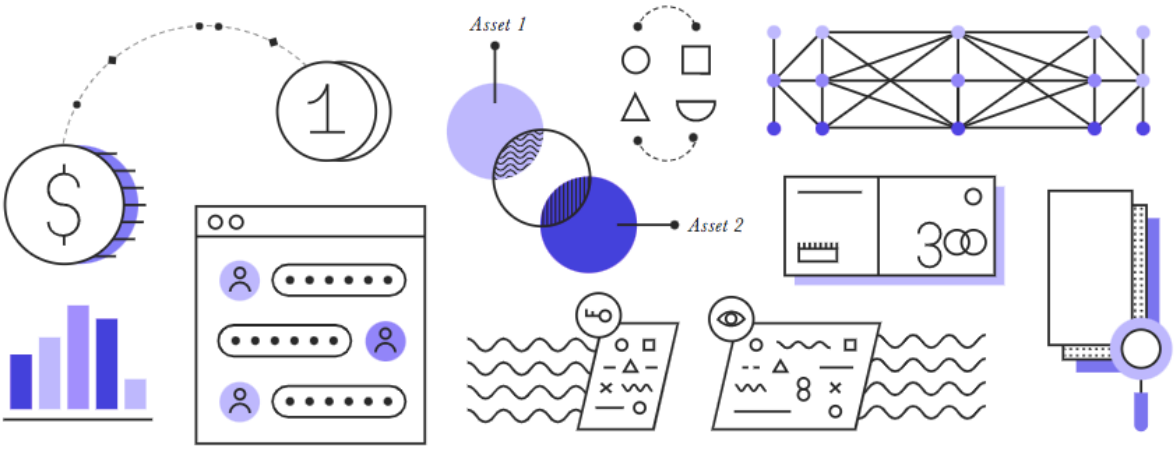
Lumen (XLM) is the native cryptocurrency for Stellar - an open source blockchain payment system.

Stellar transactions are faster because it uses a federated byzantine agreement (FBA) algorithm and not a traditional mining network to validate transactions.

For the latest prices, see:
https://www.coindesk.com/price/stellar

TOOLS

Tools to help you build the future of finance



Interact with the network

Monitor your account and create transactions

Account Viewer

Check your account and send basic lumen payments

Laboratory

Compose complex transactions and explore Stellar operations

Explore the network

Understand the shape of the network and follow ledger changes

Transaction Explorer

Explore transactions and network activity on StellarExpert

Node Explorer

View network nodes on Stellarbeat and visualize consensus

Dashboard

Live metrics about the Stellar public network and testnet.

Store and send assets

Use apps called wallets to store your private key and send payments

Ledger Nano S

The Ledger Nano S stores your private key offline and connects with many web and desktop apps

Keybase

Keybase is an encrypted communication app with a built-in Stellar wallet

Solar Wallet

Solar Wallet is a Stellar wallet with multi-signature support

Lobstr

Lobstr is a custodial Stellar wallet with 2FA key recovery

Trade on the Stellar DEX

Explore order books, make traders, and hangout in trollboxes

StellarX

Trade on the Stellar decentralized exchange using this DEX UI from Coinsquare

Stellarport

Trade on the Stellar decentralized exchange using this DEX UI

Stellarterm

Trade on the Stellar decentralized exchange using this DEX UI by Lobstr

Kelp

Make markets with our open-source trading bot

8.8 Litecoin (LTC)

Commonly called the “digital silver” to Bitcoin’s “digital gold”, Litecoin is a cryptocurrency based on the Bitcoin codebase.

Around 84 million litecoins will be created in total - 4 times the total bitcoin supply. Litecoin blocks are created every 2.5 minutes - 4 times faster than Bitcoin.

For the latest prices, see:
https://www.coindesk.com/price/litecoin

8.9 ADA

ADA is the native token of Cardano.

ADA is a digital currency. Every ADA transaction is recorded on the **Cardano** blockchain which implements the **Ouroboros** blockchain protocol.

Every ADA holder also holds a stake in the Cardano network. ADA stored in a wallet can be:

- delegated to a stake pool to earn rewards – to participate in the successful running of the network or
- pledged to a stake pool to increase the pool's likelihood of receiving rewards.

For the latest prices, see:
https://www.coindesk.com/price/cardano

Daedalus Wallet is a full-node desktop wallet that downloads a full copy of the Cardano blockchain and independently validates every transaction in its history.
https://daedaluswallet.io

Yoroi is a one-click-install, light wallet for Cardano. With Yoroi, it is not necessary to download a copy of the blockchain's history.
https://yoroi-wallet.com

Useful links

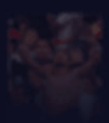
- Cardano website: https://cardano.org/
- Cardano blockchain explorer: https://explorer.cardano.org/en
- Delegate your stake: https://cardano.org/stake-pool-delegation
- Operate a stake pool: https://cardano.org/stake-pool-operation

Augur:
Your global, no-limit betting platform

Bet how much you want on sports, economics, world events and more.

START TRADING NOW

Now Trading in ETH and USD!



Betting UI and Augur AMM - Coming Soon!

Subscribe by email to get notified | NOTIFY ME

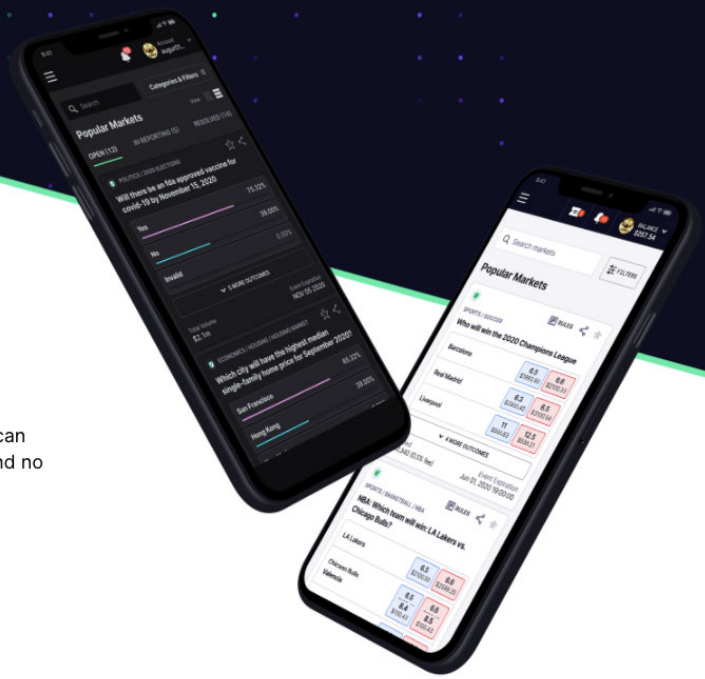
Betting today is broken & exploitative.

Today's betting Industry trades on promises of getting rich quick, using every trick in the book to **extract the maximum value from customers.**

And at the same time, their best bettors are penalised by **lowering their limits and closing their accounts.**

"Blockchain-based prediction markets may be the one force strong enough to counterbalance the spread of incorrect information on social media. They give people a financial incentive to seek the truth and then protect them with the twin shields of pseudonymity and decentralization."

BALAJI S. SRINIVASAN
Former CTO of Coinbase



Augur is building something better.

A transparent exchange with no limit on what you can bet on, no max limits on the amount you can bet and no rollover requirements.

8.10 EOS

EOS is the native cryptocurrency for the EOS.io blockchain which is similar to the Ethereum blockchain.

It can process 1 million transactions per second without any fees. Block producers are chosen through a delegated-proof-of-stake (DPoS) mechanism. In order to vote, users must stake tokens for 3 days without selling them. This puts them at risk of losing money if the price of the token drops during those days.

There is no maximum supply limit of the EOS tokens while inflation is capped at 5% annually.

For the latest prices, see:
https://www.coindesk.com/price/eos

9.1 Binance USD (BUSD)

Binance (BUSD) is a 1:1 USD-backed stablecoin approved by the New York State Department of Financial Services (NYDFS). It is issued by Binance in partnership with Paxos.

Key points:

- ❑ BUSD is a highly regulated 1:1 USD-backed crypto stablecoin.
- ❑ BUSD are digitised US Dollars and are always purchased and redeemed at 1 BUSD for 1 US dollar.
- ❑ Binance and Paxos don't charge a fee for the purchase or redemption of Binance USD (BUSD) However bank charges/wire fees may apply.
- ❑ Supported on both ERC-20 and BEP-2.

Official site:
https://www.binance.com/in/busd

Deposit your Binance USD and earn interest with lending.
https://www.binance.com/en/lending#lending-demandDeposits

For the latest prices, see:
https://www.coindesk.com/price/bitcoin-sv

9.2 Diem

Diem is the new name for Facebook "Libra" which was originally proposed in June of 2019 as a cryptocurrency. Due to backlash from governments and regulators, Facebook went back to the drawing board. It is now set to be launched in January 2021 as a stablecoin.

So, what's the difference between stable coins and cryptocurrencies? Cryptocurrencies are generated by mathematical algorithms while stable coins are the blockchain representations of fiat currencies.

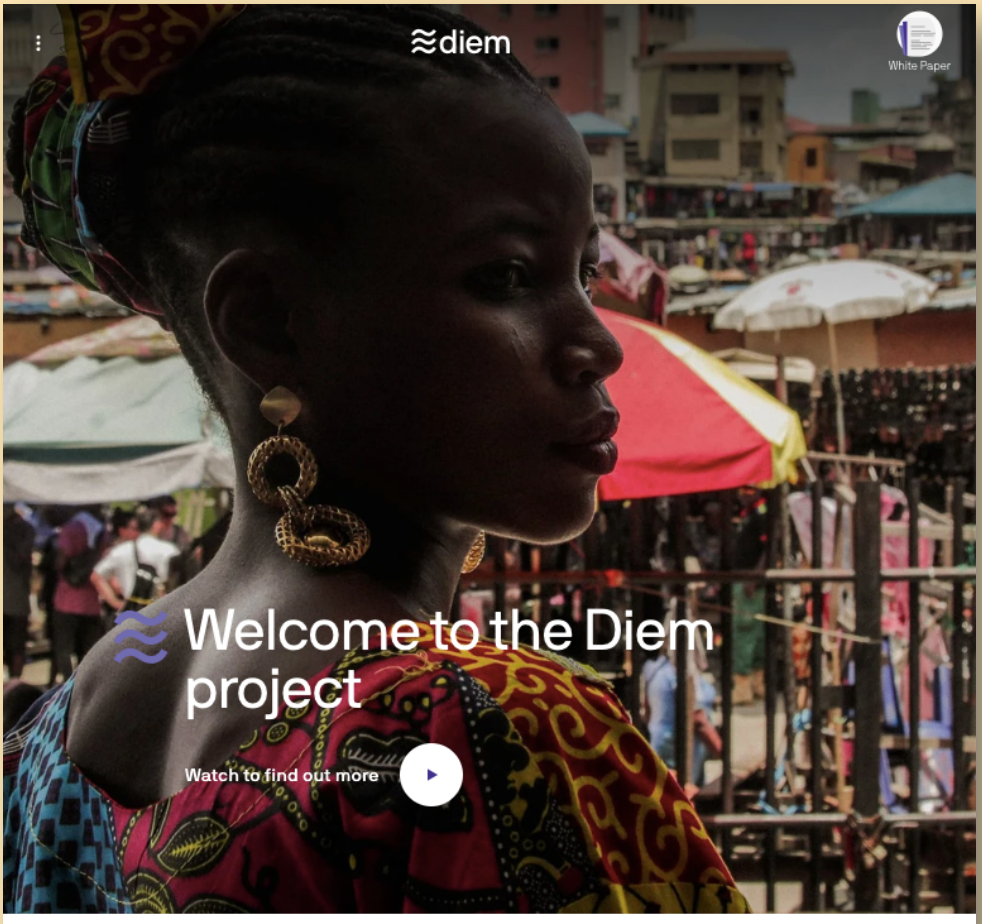
Diem will initially have 4 stablecoins - pegged to the US dollar, Pounds Sterling, Euro, and Singapore Dollar. These stable coins will be backed by cash and government securities.

Initially, Libra was planned to be a permission-less blockchain. This would have made it easy for criminals to use it for money laundering. Since there was huge opposition from Governments and regulators, Diem will now be a permissioned blockchain. Diem will also enable Know Your Customer (KYC) for all users.

Diem will compete with SWIFT, a global mechanism for money transfer used by banks.

While cross border money transfers using SWIFT take days and cost a lot, it would take a few seconds and near-zero fees using Diem. Plus SWIFT requires users to have a bank account. For using Libra you would only need a smartphone.

Official site:
https://www.diem.com/en-us/



The Diem mission

To build a trusted and innovative financial network that empowers people and businesses around the world.

Provide people everywhere access to safe and affordable financial services. So people everywhere can live better lives.

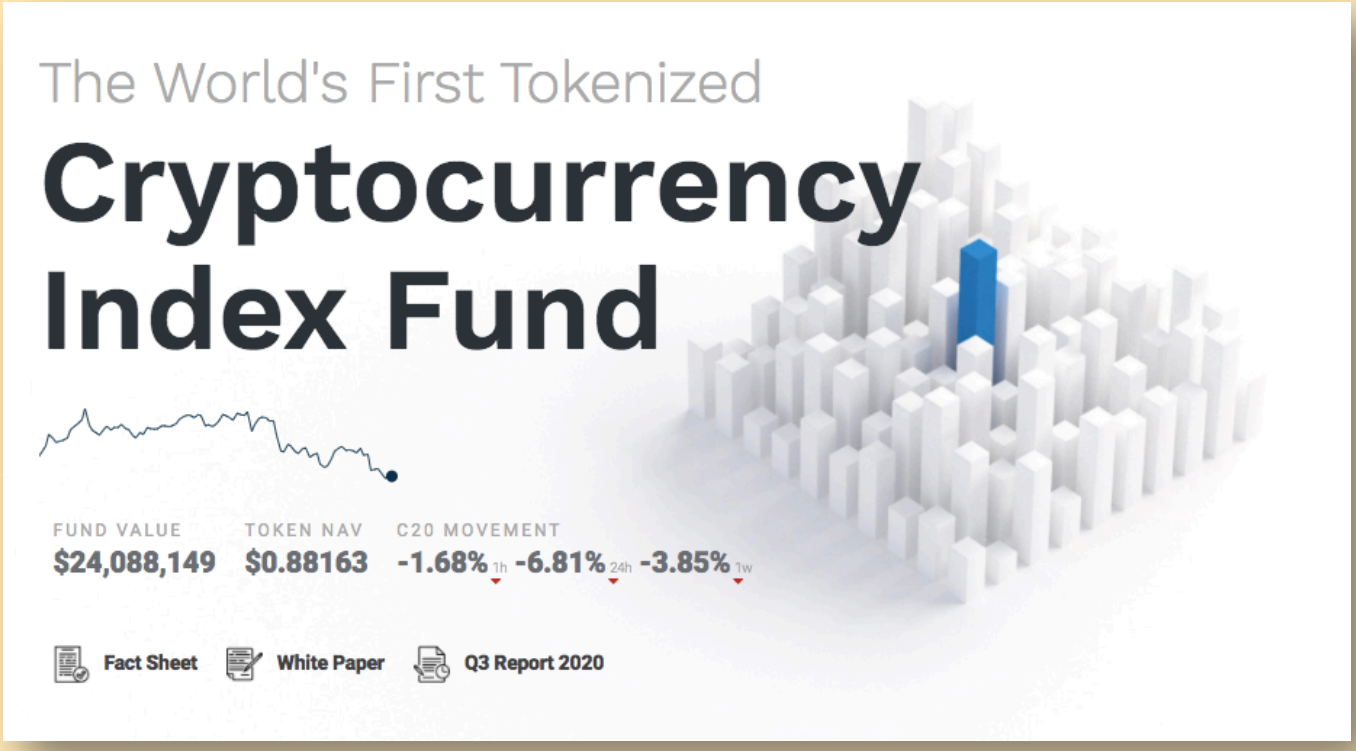
Rohas Nagpal's Top 5 Crypto predictions for 2021

https://www.youtube.com/watch?v=AKgpJ3Wn0xM

Cryptocurrency Index

Similar to a stock index like BSE-SENSEX or S&P 500, a cryptocurrency index measures and tracks the changes in cryptocurrency markets.

https://cix100.com



CRYPTO20 is an autonomous, high-performance, low-cost cryptocurrency index fund.

https://www.crypto20.com/en

10. Crypto Wallets

A crypto wallet facilitates the sending and receiving of crypto assets and gives ownership of the crypto asset balance to the user.

Mobile wallets

- ✓ Portable and convenient; ideal when making transactions face-to-face
- ✓ Designed to use QR codes to make quick and seamless transactions
- ⌘ App marketplaces can delist / remove wallet making it difficult to receive future updates
- ⌘ Damage or loss of device can potentially lead to loss of funds

Desktop wallets

- ✓ Environment enables users to have complete control over funds
- ✓ Some desktop wallets offer hardware wallet support, or can operate as full nodes
- ⌘ Difficult to utilize QR codes when making transactions
- ⌘ Susceptible to bitcoin-stealing malware/spyware/viruses

Hardware wallets

- ✓ One of the most secure methods to store funds
- ✓ Ideal for storing large amounts of bitcoin
- ⌘ Difficult to use while mobile; not designed for scanning QR codes
- ⌘ Loss of device without proper backup can make funds unrecoverable

Remember

Crypto Wallets are not a banks or exchanges.

They do NOT hold your keys, your funds, or your information.

If something goes wrong, they CANNOT access your accounts, recover your keys, reset your passwords, or reverse transactions.

Your tokens and coins are not on on the respecive blockchain. They are NOT in your wallet or on blockchain explorers.

A crypto wallet is like a doorway that allows you to interact with the blockchain in a convenient way.

bitaddress

www.bitaddress.org is a JavaScript Client-Side Bitcoin Wallet Generator. It enables Bitcoin addresses and their corresponding private keys to be conveniently generated in a web browser.

Live site: https://www.bitaddress.org

To generate a Bitcoin wallet (which is a Bitcoin address and its corresponding Bitcoin private key), simply move your mouse randomly on the bitaddress page.

A wallet will be generated in your web browser. It will look something like this:

In the example above, your **bitcoin address** is:
1AHr3RDJS7v8ruFLbVoxXsgVeGqYqALqQ8

and your **private key** is:
Kytj7WpTKxtV7XnVLzv72BPpFRTwDi82NTmjUEKc9x1o8ctVHhrT

Together they constitute your wallet.

Things to remember:

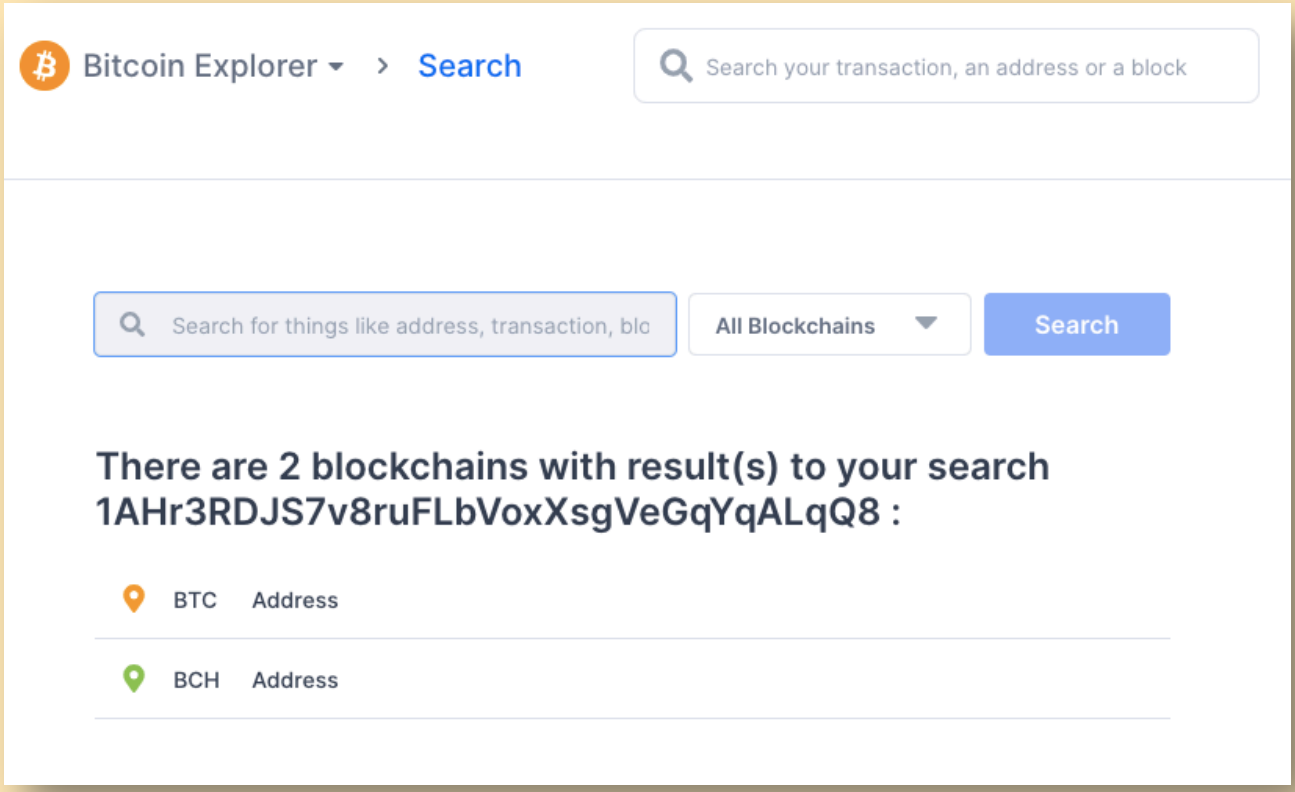
- ❑ To safeguard your wallet, you can print the Bitcoin address and private key.
- ❑ Remember to keep a backup copy of the private key in a safe location. If you print your wallet then store it in a zip lock bag to keep it safe from water. Treat a paper wallet like cash.
- ❑ If you leave/refresh the site or press the "Generate New Address" button then a new private key will be generated and the previously displayed private key will not be retrievable.
- ❑ Your Bitcoin private key should be kept a secret. Whomever you share the private key with has access to spend all the bitcoins associated with that address.
- ❑ You can add funds to this wallet by instructing others to send bitcoins to your Bitcoin address.
- ❑ You can check your balance by going to www.blockchain.info and entering your Bitcoin address.
- ❑ You can spend your bitcoins downloading and using a bitcoin p2p clients and importing your private key to the p2p client wallet.

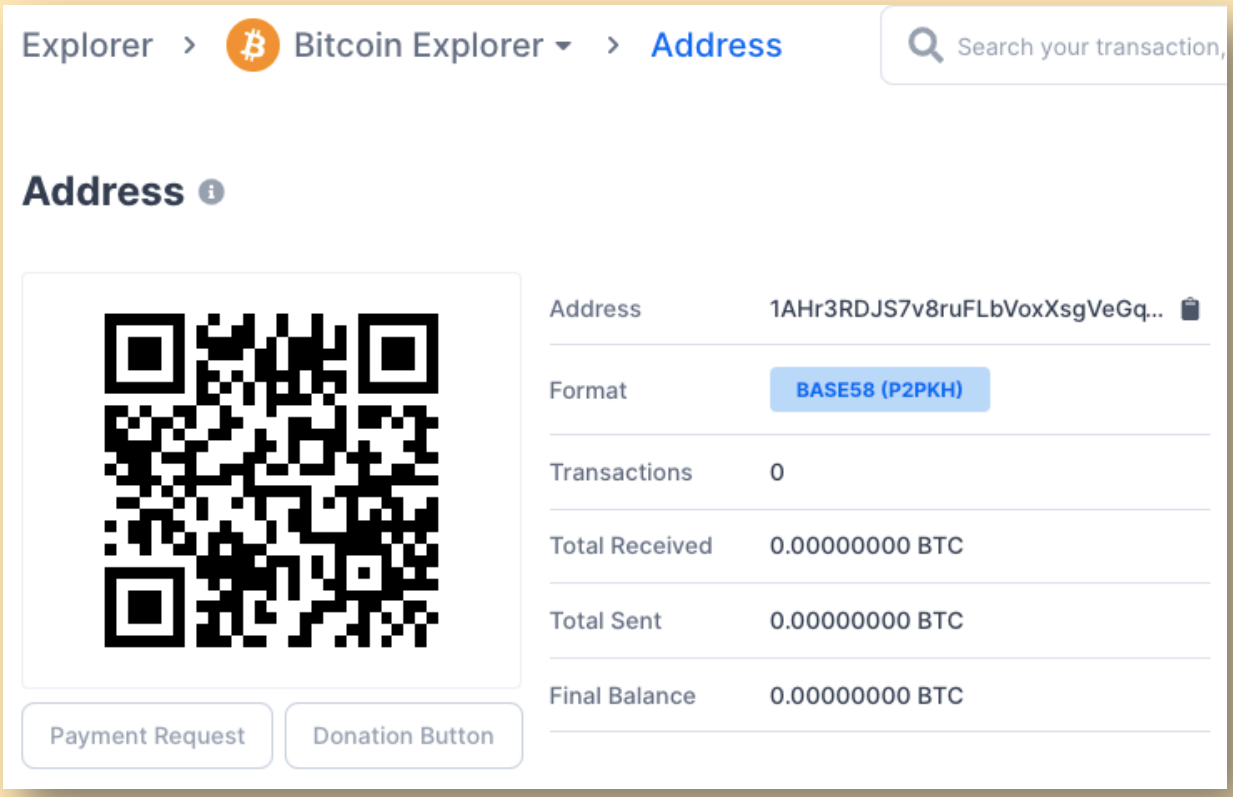
Open source project

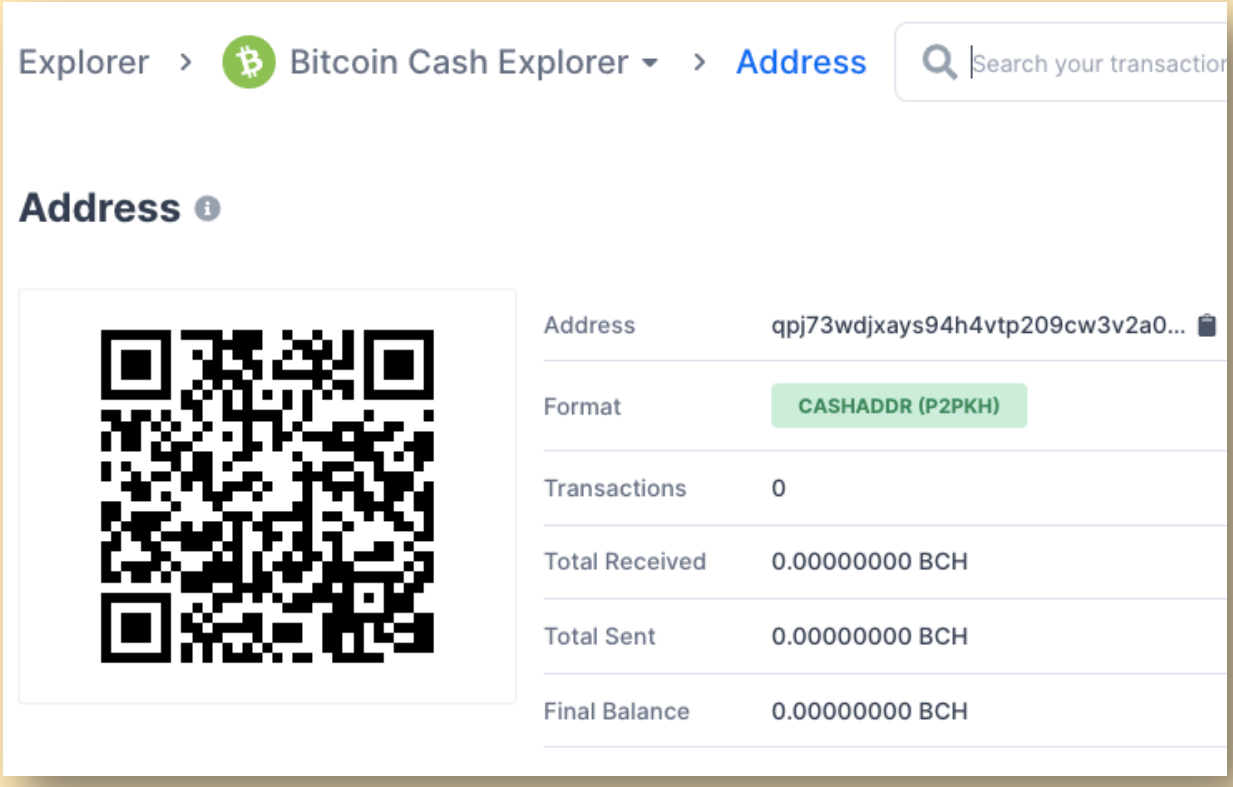
The bitaddress.org project provides an all-in-one HTML document with embedded JavaScript/Css/Images. The JavaScript is readable not minified and contains no XMLHttpRequest's (no AJAX). The benefit of this technique is you can load the JavaScript locally and trust that the JavaScript did not change after being loaded.

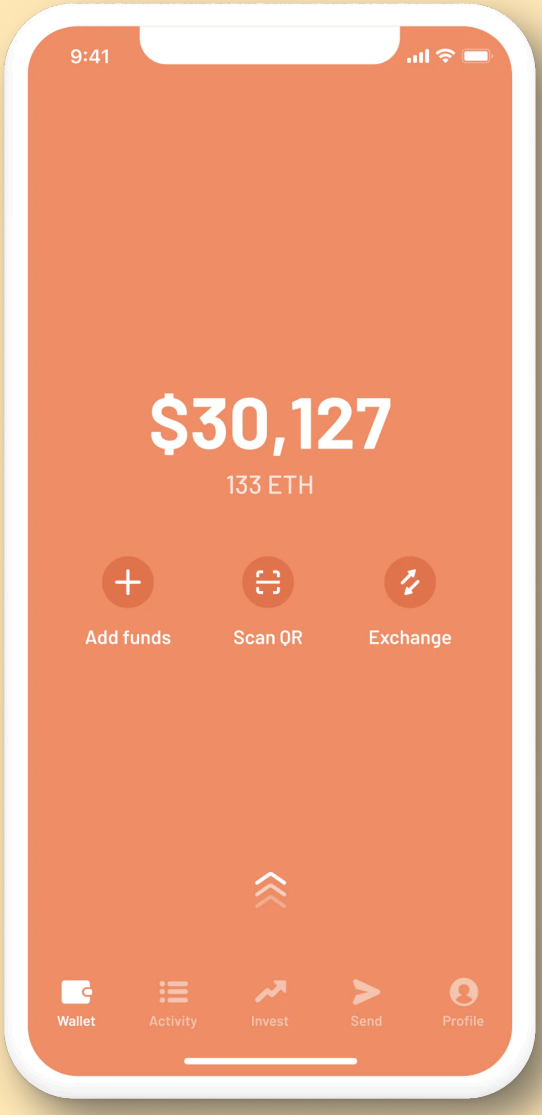
Github repo
https://github.com/pointbiz/bitaddress.org


Blockchain.com
Wallet
Exchange
Explorer
1AHr3RDJS7v8ruFLbVoxXsgVe
Log In
Sign Up
The World's Most Popular Way to Buy, Hold, and Use Crypto
Trusted by 60M Wallets - with Over $620 Billion in Transactions - Since 2013
Get Started
Bitcoin BTC $19,210.30 +1.45% Buy Trade
Ethereum ETH $600.16 +2.51% Buy Trade
XRP XRP $0.6138 +5.83% Trade


Bitcoin Explorer
Search
Search your transaction, an address or a block
Search for things like address, transaction, blo
All Blockchains
Search
There are 2 blockchains with result(s) to your search 1AHr3RDJS7v8ruFLbVoxXsgVeGqYqALqQ8 :
BTC Address
BCH Address


Explorer
Bitcoin Explorer
Address
Search your transaction,
Address
Address
1AHr3RDJS7v8ruFLbVoxXsgVeGq...
Format
BASE58 (P2PKH)
Transactions
0
Total Received
0.00000000 BTC
Total Sent
0.00000000 BTC
Final Balance
0.00000000 BTC
Payment Request
Donation Button


Explorer
Bitcoin Cash Explorer
Address
Search your transactior
Address
Address
qpj73wdjxays94h4vtp209cw3v2a0...
Format
CASHADDR (P2PKH)
Transactions
0
Total Received
0.00000000 BCH
Total Sent
0.00000000 BCH
Final Balance
0.00000000 BCH

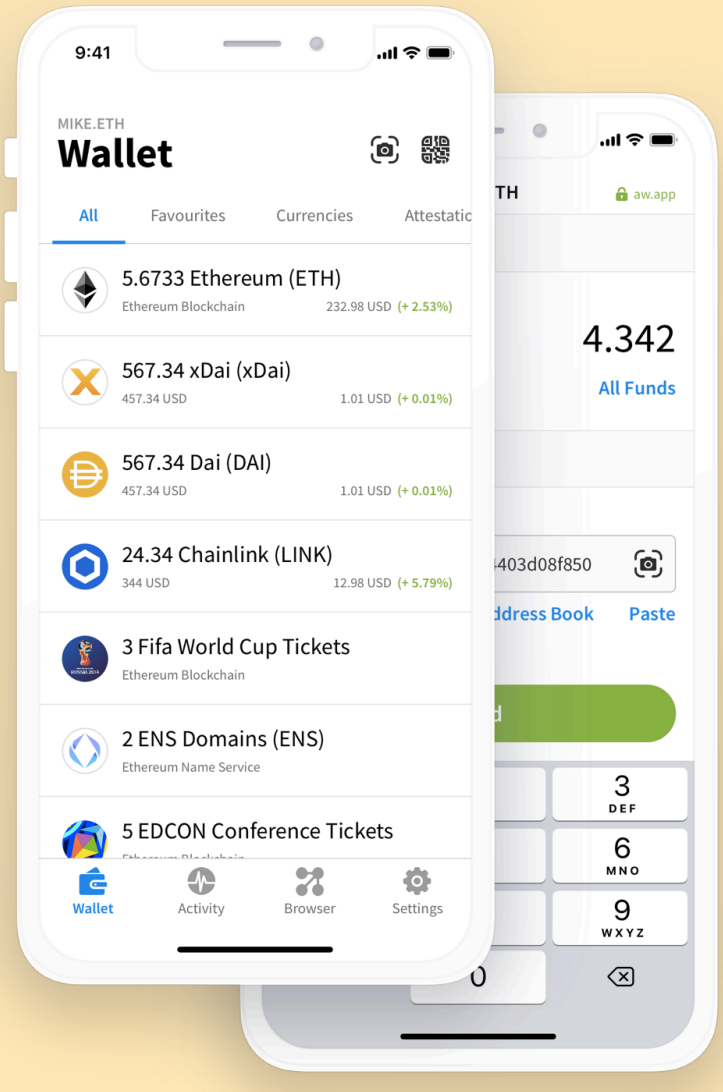


Argent

Argent is a crypto wallet that can be used to:

- store and send crypto
- borrow crypto
- earn interest and
- invest

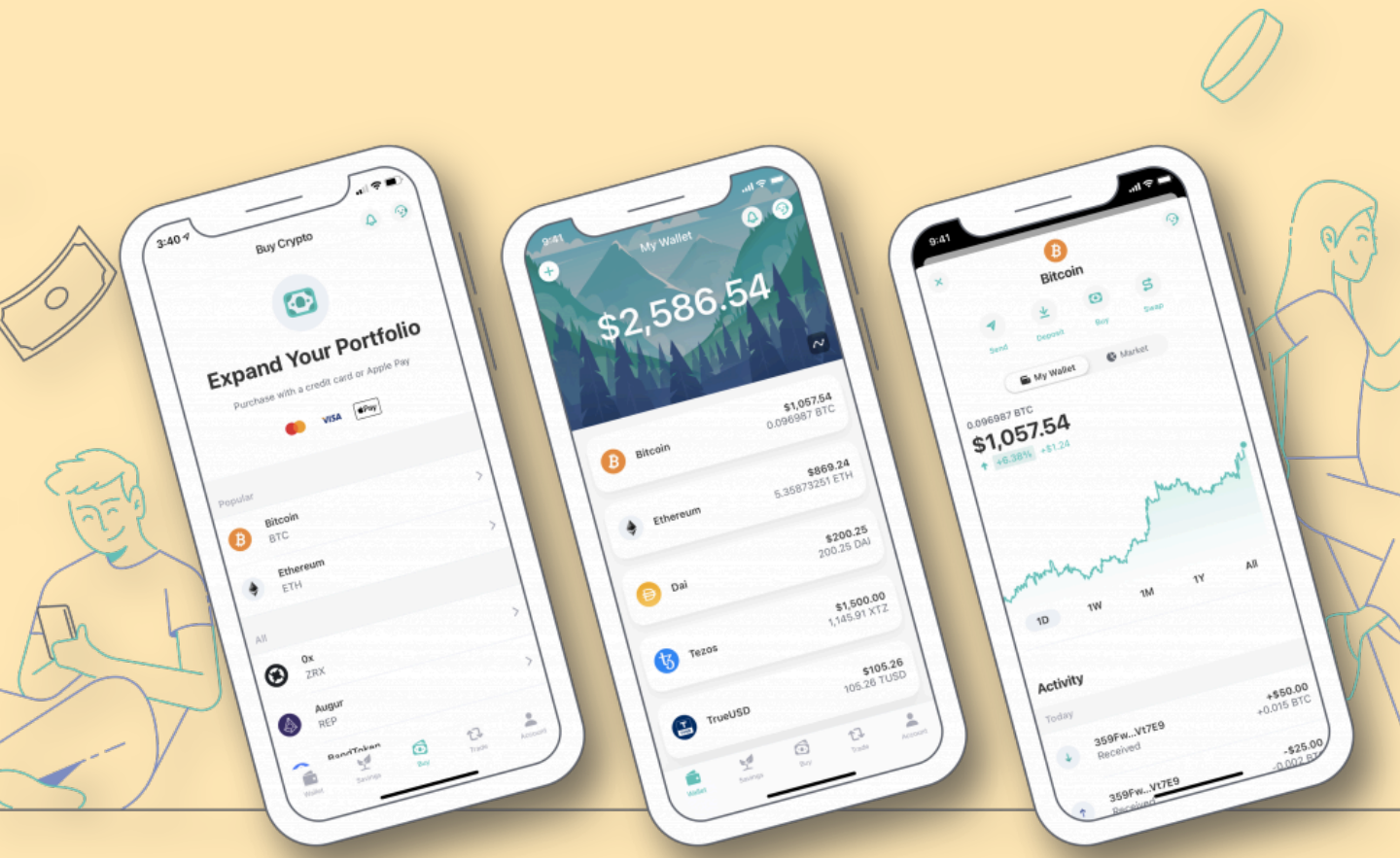
https://www.argent.xyz



AlphaWallet

AlphaWallet is an open-source production-ready and easy to customise white-label wallet.

https://alphawallet.com



ZenGo

ZenGo is the first keyless crypto wallet.

It uses facial biometrics instead of passwords, private keys and seed phrases. It also acts like a "savings account" by making it easy to earn interest on your crypto holdings.

https://zengo.com

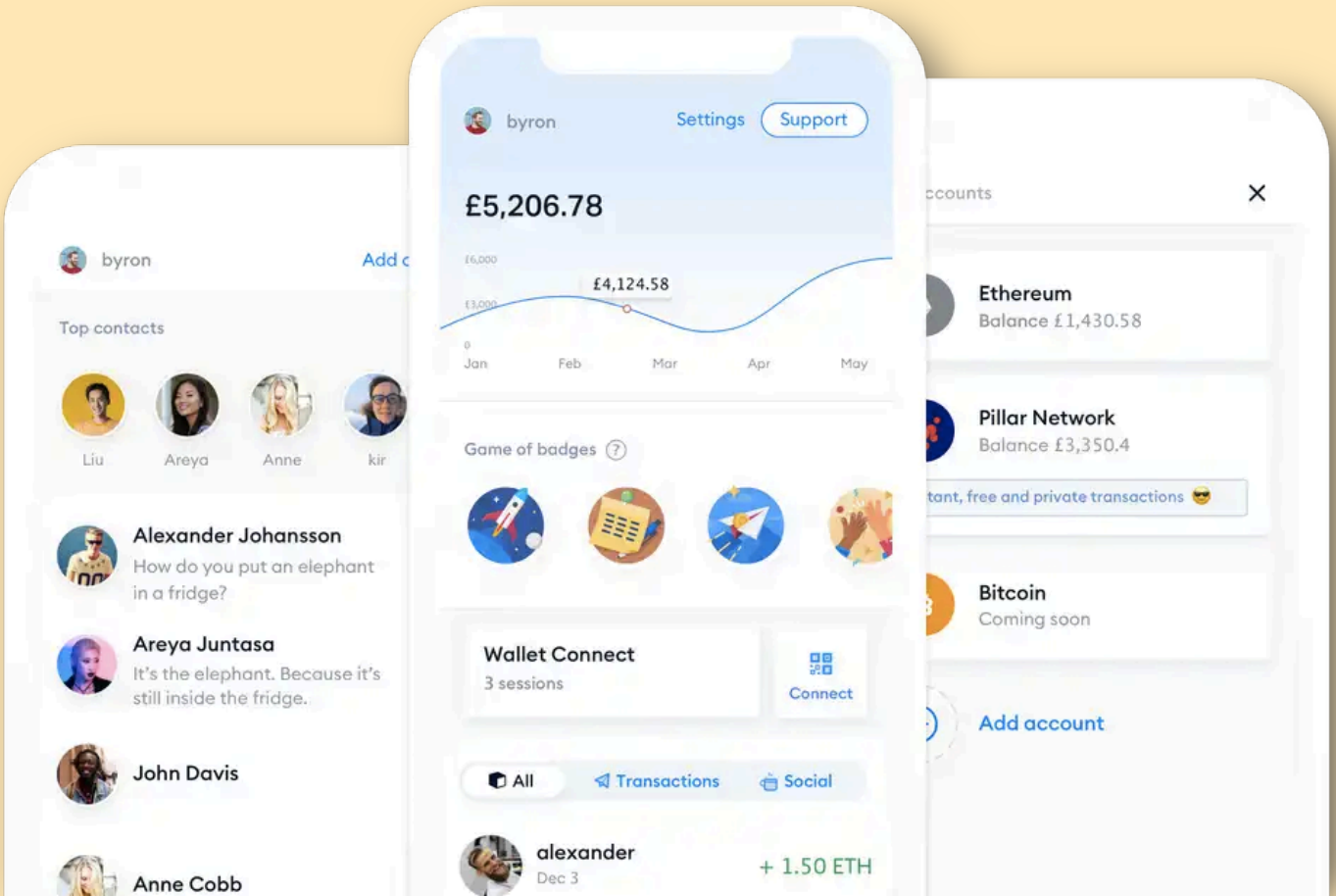
Pillar

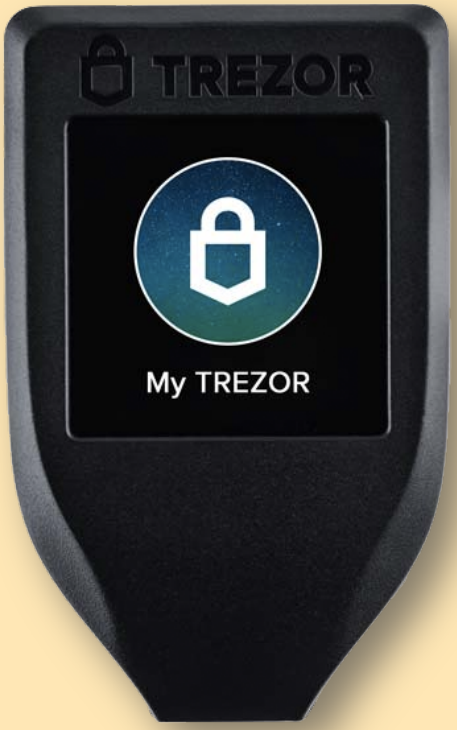
Pillar is a non-custodial, community-owned wallet with its own L2 Payment Network.

Core features include:

- ❑ 100% encrypted chats with your contacts.
- ❑ Unlimited transactions without fees in any token.
- ❑ Buy crypto directly - USD, GBP and EUR available in the app.
- ❑ Pillar replaces alpha-numeric addresses with simple usernames
- ❑ Pillar Offers Engine enables you to find the best deals to swap your Tokens, all in one place.

https://pillarproject.io



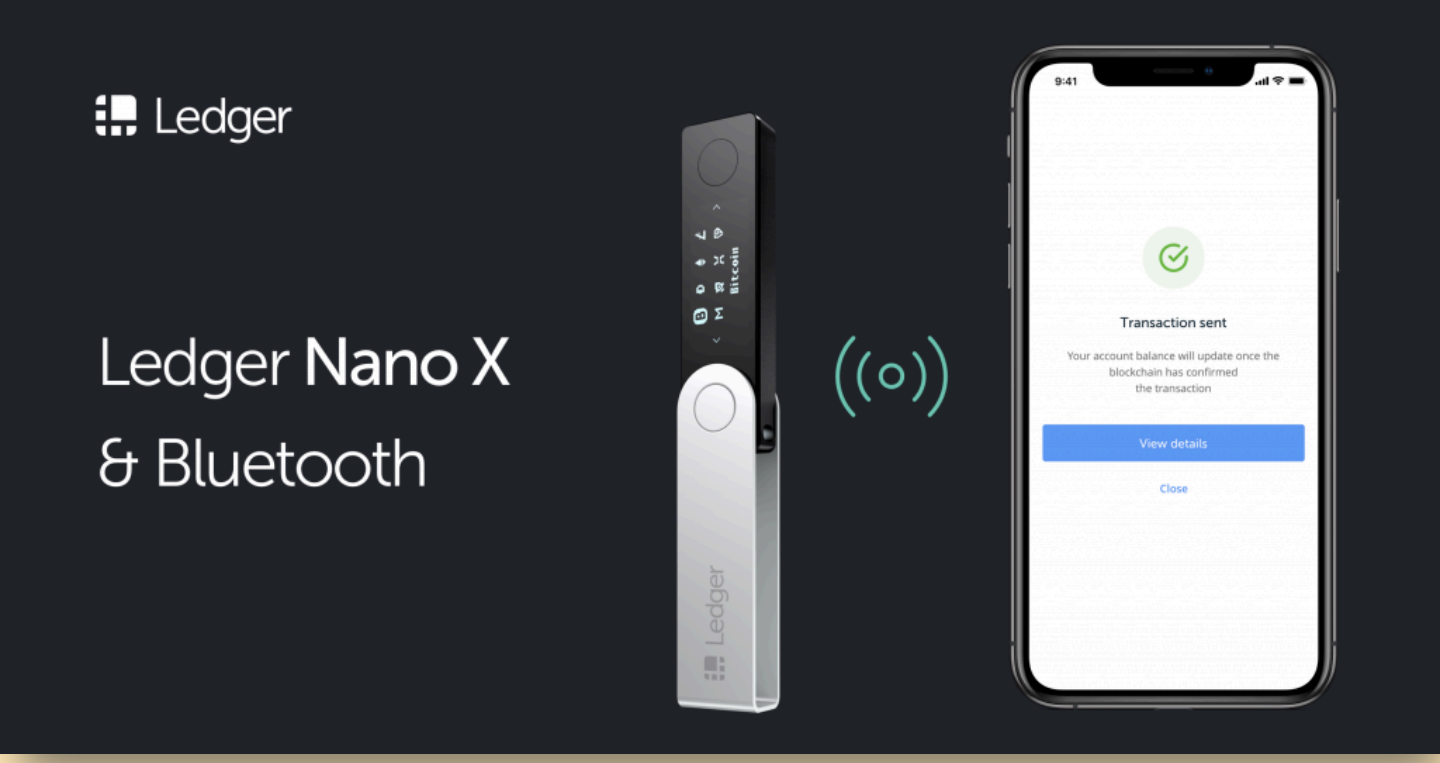


The Trezor Model T is a cryptocurrency hardware wallet for coins, passwords and other digital keys. Its features include:

- ❑ Your keys never leave the device.
- ❑ A touchscreen to verify and approve all operations.
- ❑ Easy back up option.
- ❑ Shamir Backup (SLIP39) - a method of splitting the seed into multiple unique shares. To recover the wallet, a specified number of shares has to be collected and used.
- ❑ Trezor Password Manager
- ❑ Works as a U2F hardware token* - its display informs you about the authentication request before you approve it, by displaying the service you are logging in to.
- ❑ Trezor devices currently support Windows (version 10 or newer), MacOS (version 10.11 and higher), Linux and Android. iOS, ChromeOS and Windows Phone are not yet supported.

*** Note:** The U2F standard for universal two-factor authentication tokens enables USB, NFC, or Bluetooth to provide two-factor authentication. It is supported in Chrome, Firefox, and Opera for Google, Facebook, Dropbox, and GitHub accounts.

https://shop.trezor.io/product/trezor-model-t



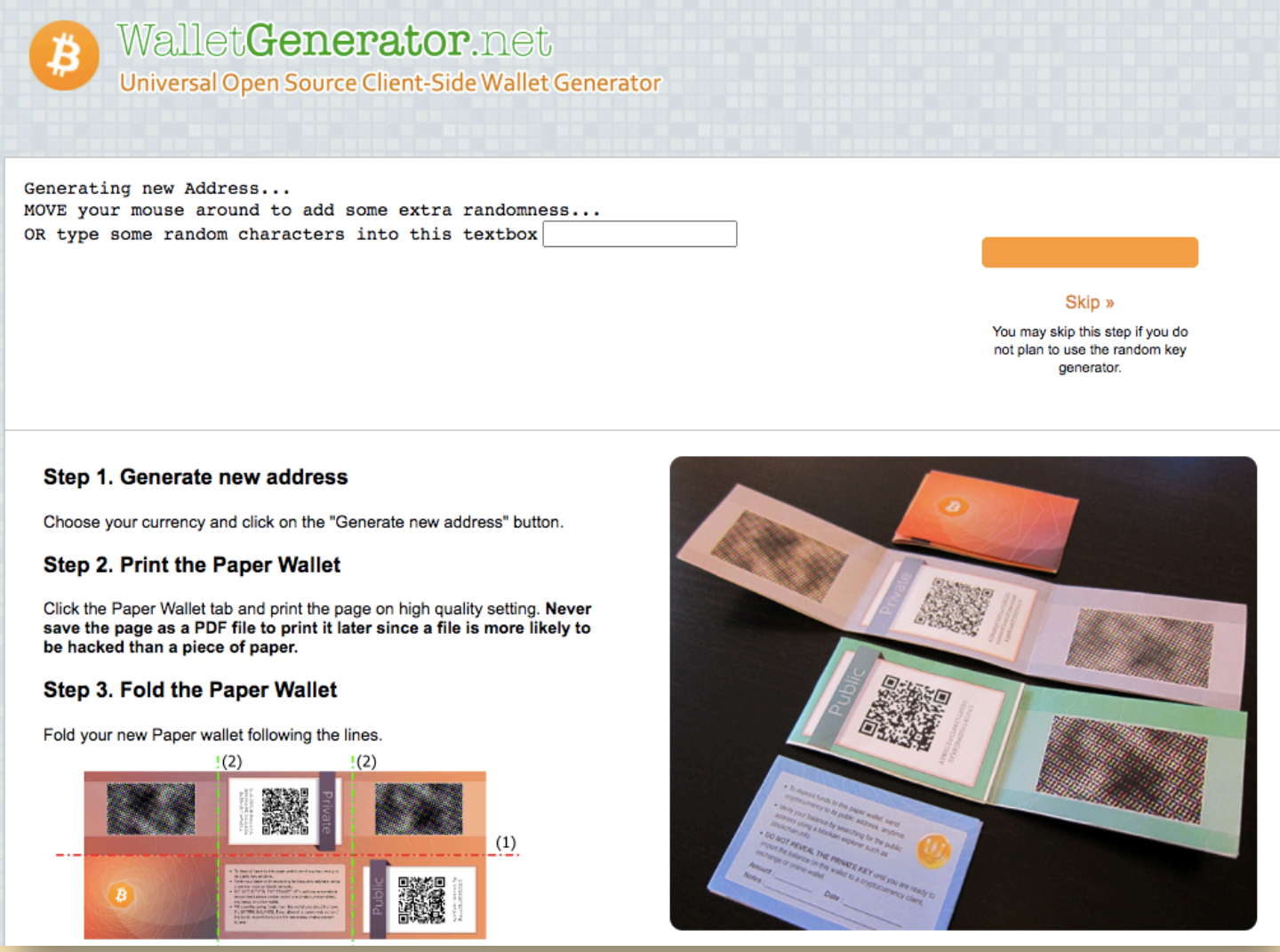
The Ledger Nano X is a hardware wallet that features Bluetooth Low Energy (BLE) connectivity enabling it to be used with Android or iOS devices without the need of a cable.

- ❑ Only public data is transported by Bluetooth; critical data (such as private keys and seed) never leaves the device.
- ❑ The security of the Ledger Nano X relies on the Secure Element which requests consent for any action.
- ❑ The Ledger Nano X Bluetooth implementation uses a Bluetooth protocol which ensures authentication by using pairing. This is numeric comparison based and confidentiality is ensured using AES-based encryption.
- ❑ You can disable the Bluetooth and use the USB type-C cable.
- ❑ Install up to 100 crypto applications at the same time on your Ledger Nano X.
- ❑ More than 1500 coins and tokens are supported.

You can buy Ledger products from:
https://shop.ledger.com/pages/christmas-pack?r=b46acb0ce55e

imKey is a hardware wallet that integrates with CC EAL 6 ＋ secure chip and supports BTC, ETH, COSMOS,EOS and ERC 20 tokens.

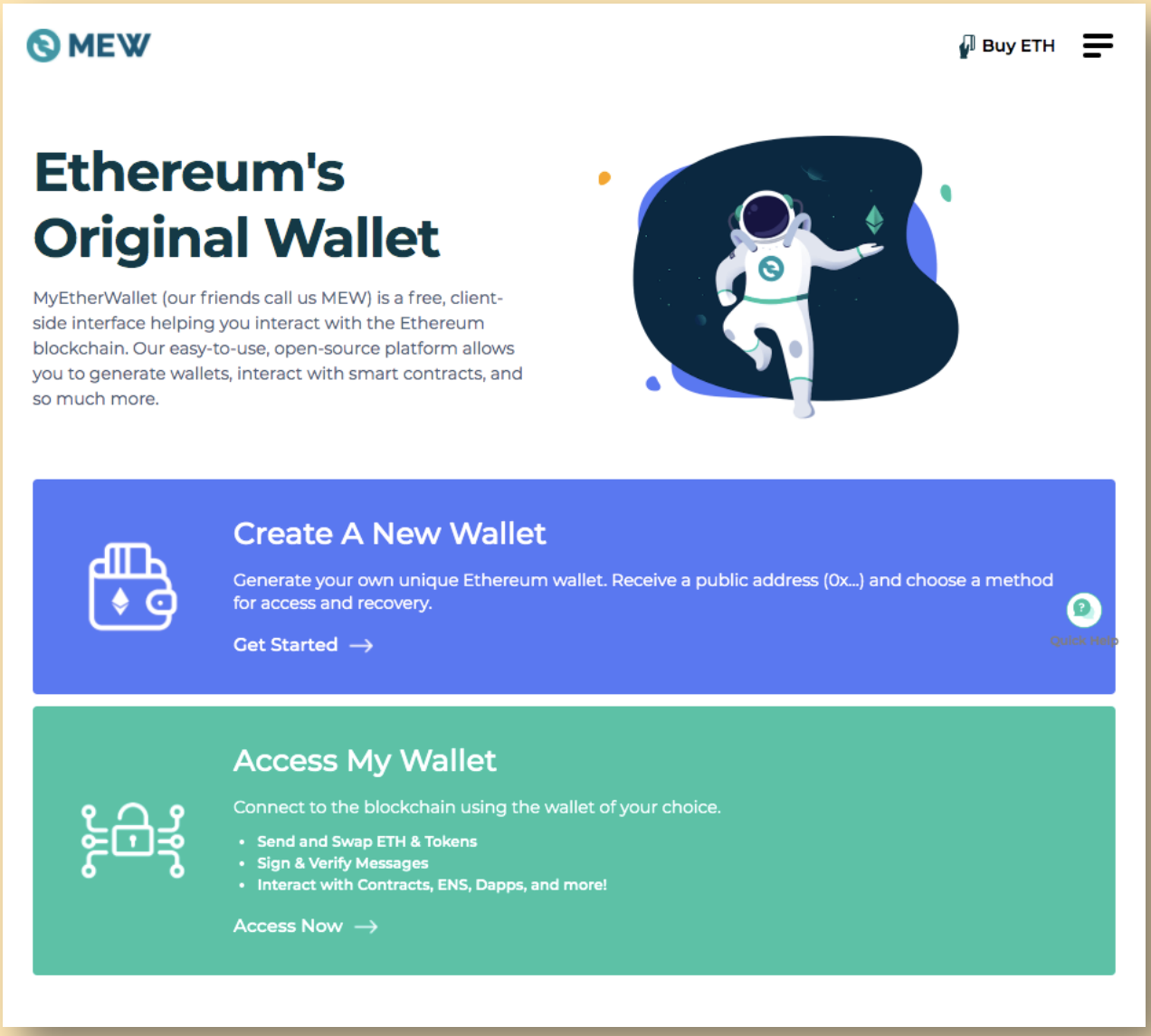
https://imkey.im



You can use https://walletgenerator.net to generate a paper wallet.

Advantages of a paper wallet are:

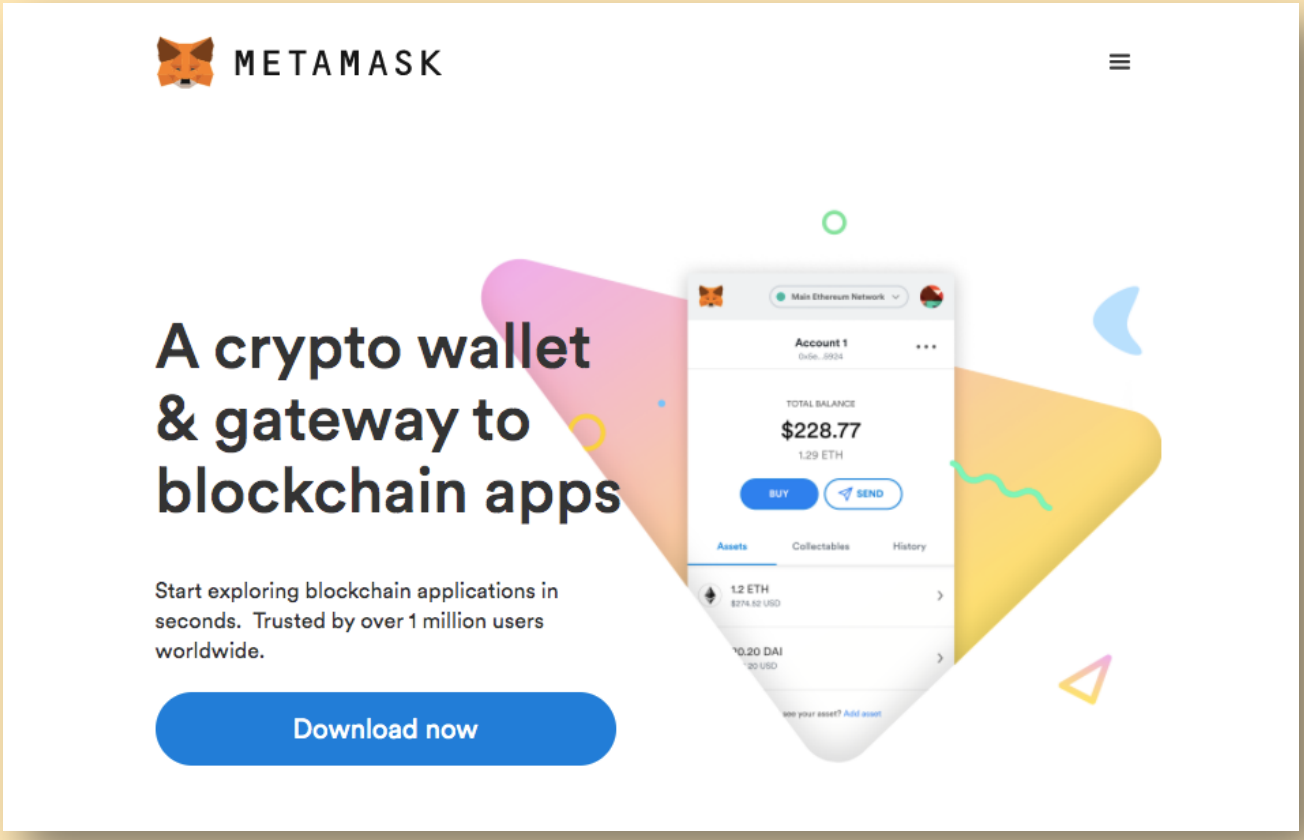
- ❑ They are not subject to malwares and keyloggers.
- ❑ You don’t rely on a third party’s honesty or capacity to protect your coins.
- ❑ You won't lose your coins if your device breaks.



MyEtherWallet (MEW) is a free, client-side interface for interacting with the Ethereum blockchain.

It can be used for generating wallets, and interacting with smart contracts.

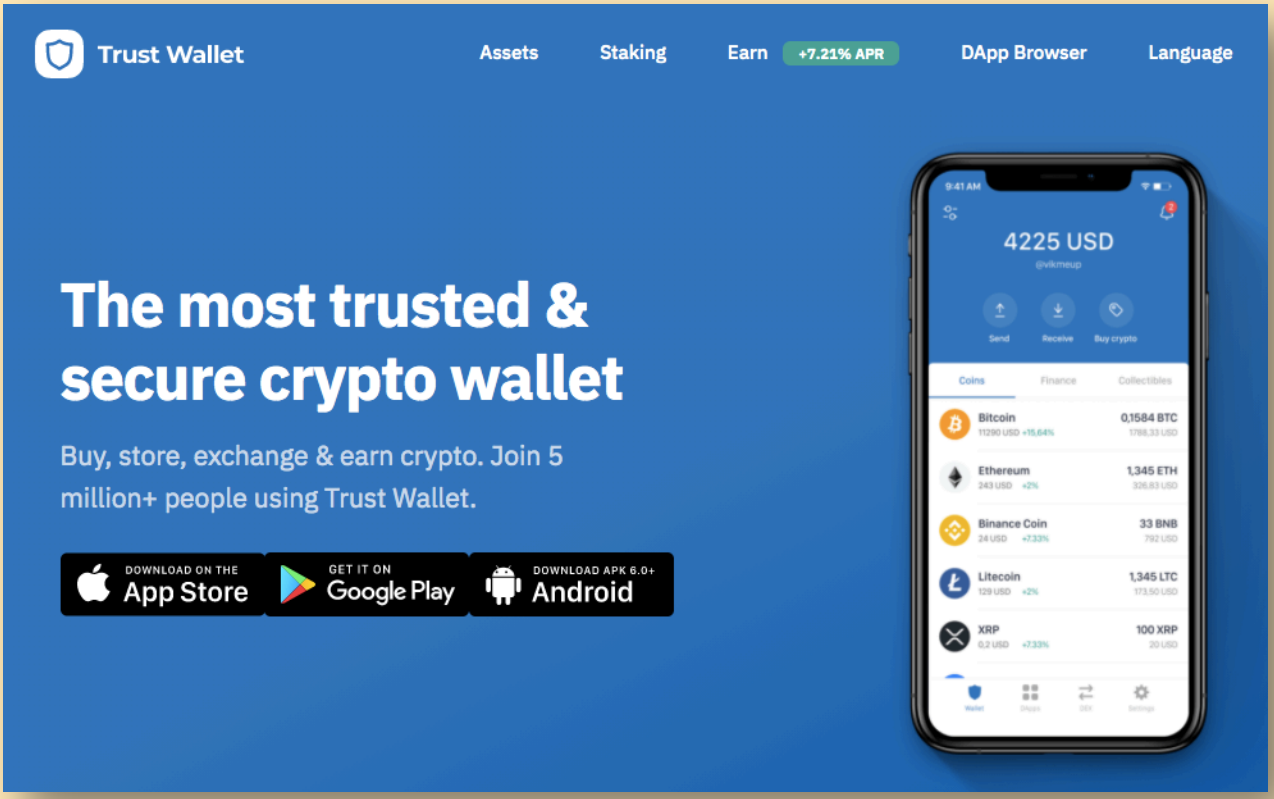
https://www.myetherwallet.com



MetaMask is a crypto wallet that is available as a browser extension and as apps for Android and iOS. It can be used to buy Ethereum with a debit card or Apple Pay.

Key features include a key vault, secure login, token wallet, and token exchange.

https://metamask.io



Some of the features of Trust Wallet are:

- Buy Bitcoin in under 5 minutes
- Easily earn interest on the crypto in your wallet
- See your collectibles, art & non-fungible digital assets in one place
- Exchange your crypto within the app
- Track charts and prices within the wallet

https://trustwallet.com

11. Crypto custody

Bitgo is an institutional digital asset custody, trading, and finance platform.

https://www.bitgo.com

Bitgo custody services include:

- ❑ Wallet Platform - hot, warm, and cold wallet solutions.
- ❑ Qualified Custody - insured cold storage for digital assets.
- ❑ Self-Managed Custody - secure your keys locally.

Other Bitgo services include:

- ❑ Trade digital assets directly and anonymously from insured cold storage at BitGo Trust.
- ❑ Lend and borrow digital assets through BitGo Prime.
- ❑ Portfolio Management - visualize and understand your entire digital asset portfolio.
- ❑ Wallets SDK - Manage multiple digital currencies and wallets through a single, unified interface.
- ❑ Customizable tax configurations and automatic report generation.

BitGo

Institutional digital asset custody, trading, and finance

BitGo enables our clients to navigate the complex landscape of digital assets with a connected, compliant, and secure suite of solutions.

Connect With Us

Explore Services ↓

TRUSTED BY

bitgate BitBay 300+ more

Bitcoin 19,164.77 USD ▲ 184.48 (0.97%) **Ethereum** 596.55 USD ▲ 8.42 (1.43%) **XRP** 0.61 USD ▲ 0.02 (3.

INSTITUTIONAL DIGITAL ASSET PLATFORM

Custody

12. How to keep your crypto safe

When you own crypto, you actually don't own coins. You own private keys.

A cryptocurrency wallet is designed to
- ❑ Store public and private keys
- ❑ Send and receive digital currencies
- ❑ Monitor balances
- ❑ Interact with supported blockchains.

A **hot wallet** is connected to the internet, can be accessed at any time with the requisite keys and is the most vulnerable to hacking e.g. mobile and software wallets, and funds stored on crypto exchanges.

A **cold wallet** is an offline wallet. Since it is not connected to the internet, it is considered more secure e.g. hardware wallets and paper wallets.

Ensure that the exchange you use has a robust verification process that:
- ❑ confirms your email
- ❑ confirms your phone
- ❑ verifies your Government issued ID
- ❑ verifies your address
- ❑ does video verification

It must also have security features like:
- ❑ security questions answers
- ❑ two factor authentication

It must also display:
- ❑ active sessions
- ❑ account activity

How to stay safe

Wallets are a bit of a shift in thinking. Financial freedom and the ability to access and use funds anywhere comes with a bit of responsibility – there's no customer support in crypto.

1. Take responsibility for your own funds

Centralized exchanges will link your wallet to a username and password that you can recover in a traditional way. Just remember you're trusting that exchange with custody over your funds. If that company is attacked or folds, your funds are at risk.

2. Write down your seed phrase

Wallets will often give you a seed phrase that you must write down somewhere safe. This is the only way you'll be able to recover your wallet.

Here's an example:

there aeroplane curve vent formation doge
possible product distinct under spirit lamp

Don't store it on a computer. Write it down and keep it safe.

3. Bookmark your wallet

If you use a web wallet, bookmark the site to protect yourself against phishing scams.

4. Triple check everything

Remember transactions can't be reversed and wallets can't be easily recovered so take care.

(Source: https://ethereum.org/en/wallets)

Common crypto scams

Source: https://bitcoin.org/en/scams

Blackmail

Be wary of blackmail attempts in which strangers threaten you in exchange for bitcoin as a means of extortion. One common execution of this method is by email, where-in the sender transmits a message claiming that he/she has hacked into your computer and is operating it via remote desktop protocol (RDP).

The sender says that a key logger has been installed and that your web cam was used to record you doing something you may not want others to know about. The sender provides two options - send bitcoin to suppress the material, or send nothing and see the content sent to your email contacts and spread across your social networks.

Scammers use stolen email lists and other leaked user information to run this scheme across thousands of people en masse.

Fake Exchanges

As bitcoin has become more popular, more people have sought to acquire it. Unfortunately, nefarious people have taken advantage of this and have been known to set up fake bitcoin exchanges.

These fake exchanges may trick users by offering extremely competitive market prices that lull them into thinking they're getting a steal, with quick and easy access to some cheap bitcoin. Be sure to use a reputable exchange when buying or selling bitcoin.

Free Giveaways

Due to the viral nature of how information spreads on the internet, scammers seek to take advantage of people by offering free giveaways of bitcoin or other digital currencies in exchange for sending a small amount to register, or by providing some personal information.

When you see this on a website or social network, it's best to immediately report the content as fraudulent, so that others don't fall victim.

Impersonation

Unfortunately it's very easy for con-artists to create social media accounts and impersonate people. Often they lie in wait, until the person they're trying to impersonate publishes content.

The impersonator then replies to it with a follow-up message or call to action - like a free giveaway - using an account that looks almost identical to the original poster or author. This makes it seem like the original person is saying it.

Alternatively, impersonators may also try to use these same fake accounts to trick others via private or direct message into taking some kind of action in an attempt to defraud or compromise.

Never participate in free giveaways, and if you receive an odd request via someone in your network, it's best to double check to confirm the authenticity via multiple mediums of communication.

Malware

Hackers have become very creative at finding ways to steal from people. When sending bitcoin, always be sure to double or triple check the address you're sending to.

Some malware programs, once installed, will change bitcoin addresses when they're pasted from a user's clipboard, so that all of the bitcoin unknowingly gets sent to the hacker's address instead.

Since there is little chance of reversing a bitcoin transaction once it's confirmed by the network, noticing this after the fact means it's too late and most likely can't be recovered.

It's a good idea to be super-cautious about what programs you allow to have administrator access on your devices. An up-to-date, reputable virus scanner can also help but is not foolproof.

Meet in Person

When buying or selling bitcoin locally, a counterparty may ask you to meet in person to conduct the exchange. If it isn't a trusted party that you already know, this is a very risky proposition that could result in you getting robbed or injured.

Con-artists have also been known to exchange counterfeit fiat currency in exchange for bitcoin. Consider using a peer-to-peer platform to escrow the funds in place of meeting in person.

Money Transfer Fraud

Do not reply to emails or inbound communications from strangers telling you they need help moving some money, whereafter in exchange for your services, you'll get a portion of the funds.

Phishing Emails

Beware of emails purported to be from services you use soliciting you for action, such as resetting your password, or clicking through to provide some sort of interaction with regard to your account.

It can be very difficult to spot the difference in a fake email that's trying to entice you to compromise your account, and a legitimate one sent on behalf of a product or service that you use.

When in doubt, considering triple-checking the authenticity of the communication by forwarding it to the company, using the contact email address on their website, calling them on the telephone, and/or reaching out to them via their official social media accounts.

Phishing Websites

Phishing websites often go hand-in-hand with phishing emails. Phishing emails can link to a replica website designed to steal login credentials or prompt one to install malware.

Do not install software or log in to a website unless you are 100% sure it isn't a fake one. Phishing websites may also appear as sponsored results on search engines or in app marketplaces used by mobile devices. Be wary that you aren't downloading a fake app or clicking a sponsored link to a fake website.

Ponzi Schemes

Do not participate in offerings where one or more people offer you a guaranteed return in exchange for an upfront deposit. This is known as a ponzi scheme, where-in future depositors' principals are used to pay previous investors. The end result is usually a lot of people losing a lot of money.

Pyramid Schemes

A pyramid scheme promises returns to participants based on the number of people they invite to join. This enables the scheme to grow virally and rapidly, however, it most often doesn't result in any kind of meaningful return for the members and/or those invited who also joined.

Never invite your personal network under the sole goal of accumulating rewards or returns from a product or service, and do not contribute your own capital at the behest of others to accelerate the process.

Prize Giveaways

Similar to free giveaways, prize giveaway scams trick people into taking action or supplying information about themselves.

For example, supplying a name, address, email and phone number in order to claim a prize. This can allow a hacker to attempt to use the information to gain access to accounts by impersonating you.

Pump and Dumps

Do not trust people who entice you or others to invest because they claim that they know what the bitcoin price is going to be. In a pump and dump scheme, a person (or persons) try to artificially drive up or pump the price so that they can dump their holdings for a profit.

Ransomware

This is a type of malware that partially or completely blocks access to a device unless you pay a ransom in bitcoin. It's best to consult the advice of a trusted computer professional for removal assistance, rather than paying the ransom.

Be careful about what programs you install on your devices, especially those that request administrator access. Also be sure to double-check that the application you are downloading isn't a fake one that's impersonating a legitimate one you've used in the past.

Scam Coins

Be careful when investing in alternative coins (altcoins). Amongst altcoins there may be scam coins, enticing users to invest via private sales, or with presale discounts. Scam coins may feature a flashy website and/or boast a large community to create a fear of missing out effect on people who discover it.

This helps early holders pump up the price so that they can dump and exit their positions for a profit. Scam coins without large communities may do airdrops - offering free coins (or tokens) to people in exchange for joining their communities.

This enables scam coins to present their initiatives with inflated traction metrics to make investors feel like they're missing out when it comes time for them to decide if they'd like to buy-in. Scam coins may also use the word Bitcoin in them in an effort to trick or mislead people into thinking there is a legitimate relationship.

13. Exchanges

When you own crypto, you actually don't own coins. You own private keys.

A cryptocurrency wallet is designed to
- ❑ Store public and private keys
- ❑ Send and receive digital currencies
- ❑ Monitor balances
- ❑ Interact with supported blockchains.

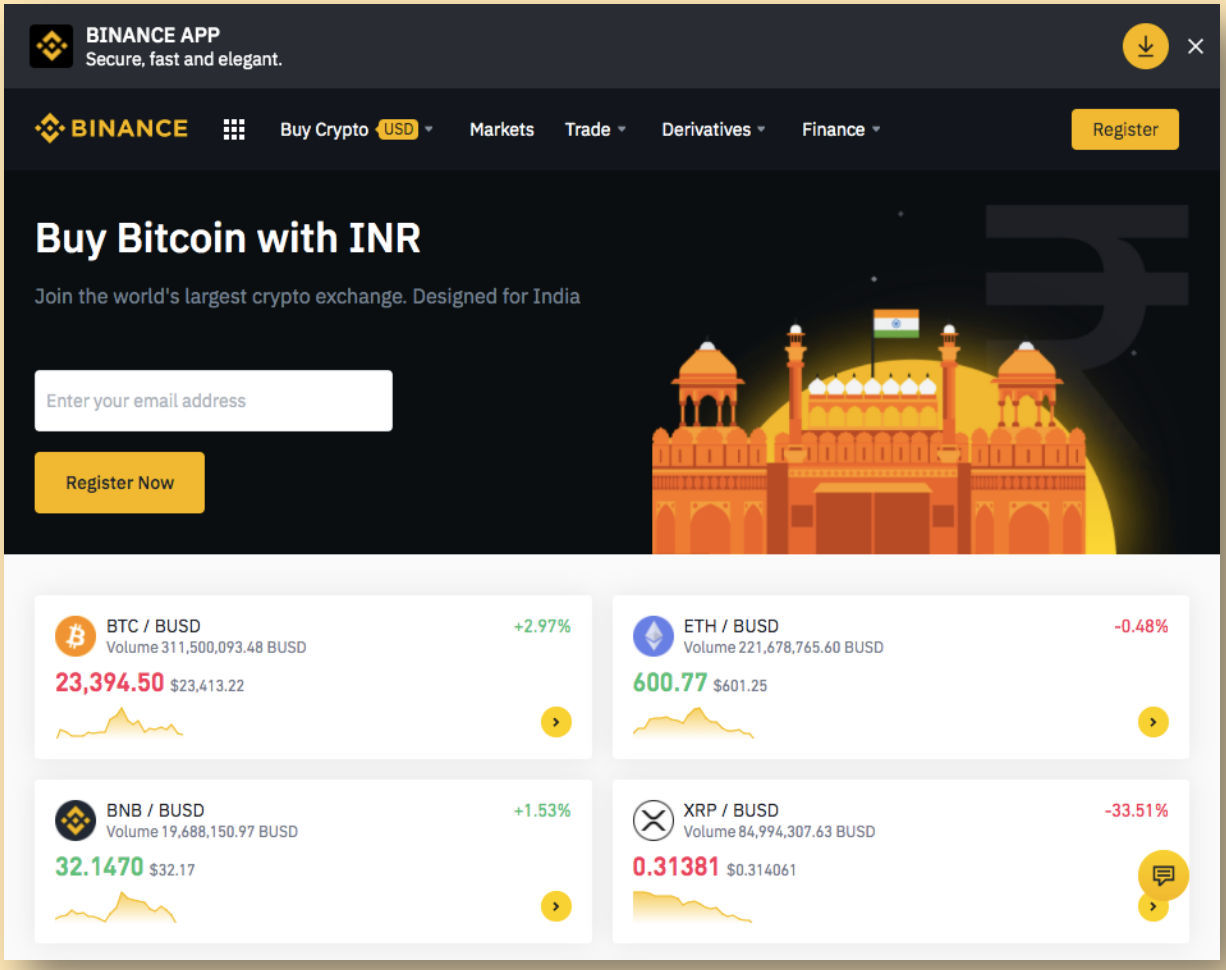
A **hot wallet** is connected to the internet, can be accessed at any time with the requisite keys and is the most vulnerable to hacking e.g. mobile and software wallets, and funds stored on crypto exchanges.

A **cold wallet** is an offline wallet. Since it is not connected to the internet, it is considered more secure e.g. hardware wallets and paper wallets.

Ensure that the exchange you use has a robust verification process that:
- ❑ confirms your email
- ❑ confirms your phone
- ❑ verifies your Government issued ID
- ❑ verifies your address
- ❑ does video verification

It must also have security features like:
- ❑ security questions answers
- ❑ two factor authentication

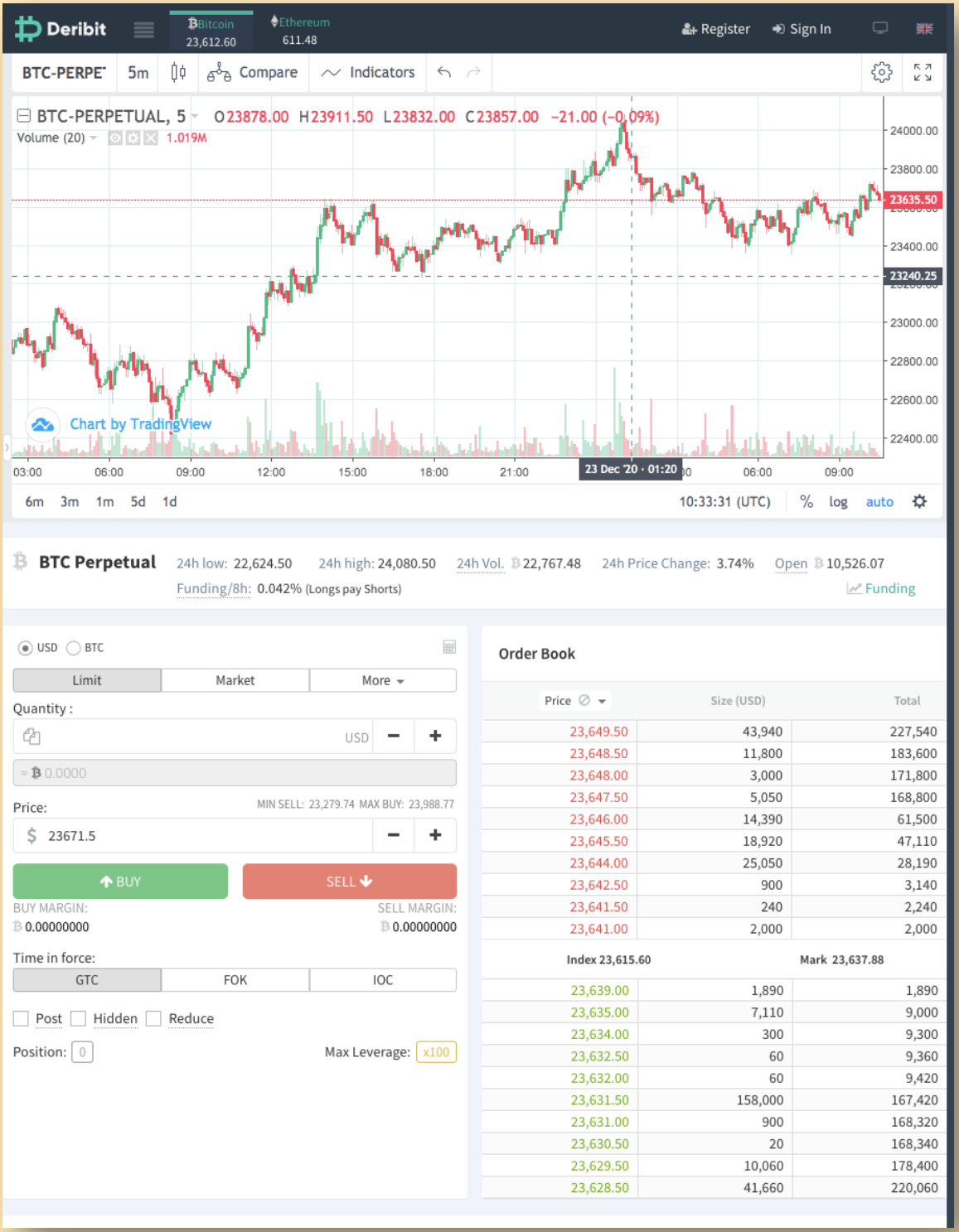
It must also display:
- ❑ active sessions
- ❑ account activity



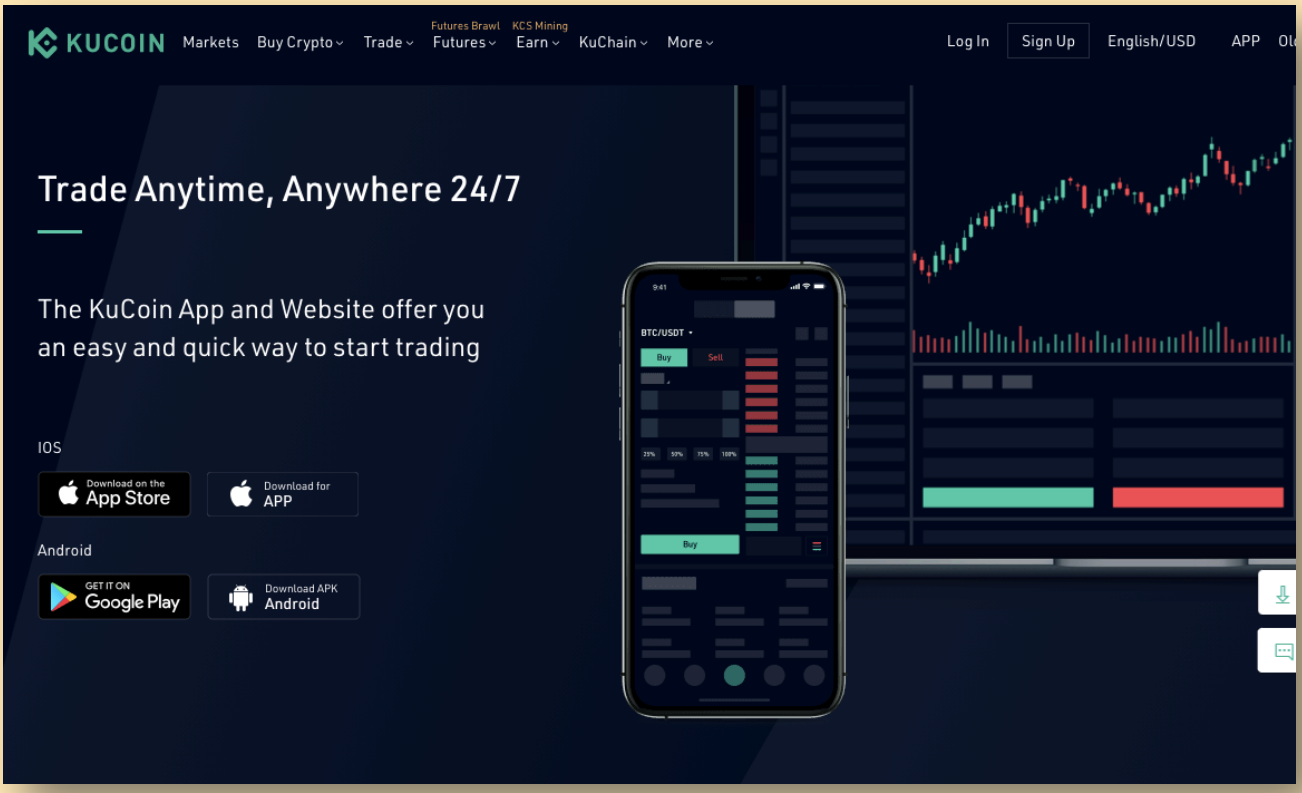
Binance enables:

- Trading in 740 cryptocurrency and fiat pairs.
- Futures trading with 125x leverage.
- Earning interest on idle crypto assets.
- Staking on crypto assets and DeFi.

https://www.binance.com



Deribit enables Cryptocurrency Futures & Options Trading.
This allows trading of Bitcoin and Ethereum with up to 100x leverage.
https://www.deribit.com



Kucoin is a Hong Kong based cryptocurrency exchange that has its own cryptocurrency called KuCoin Shares (KCS). KCS holders receive dividends on a daily basis.

This dividend is based on the amount of tokens they hold and the trades which are completed on the platform. Additionally KCS holders receive exclusive promotions, rewards and offers.

https://www.kucoin.com

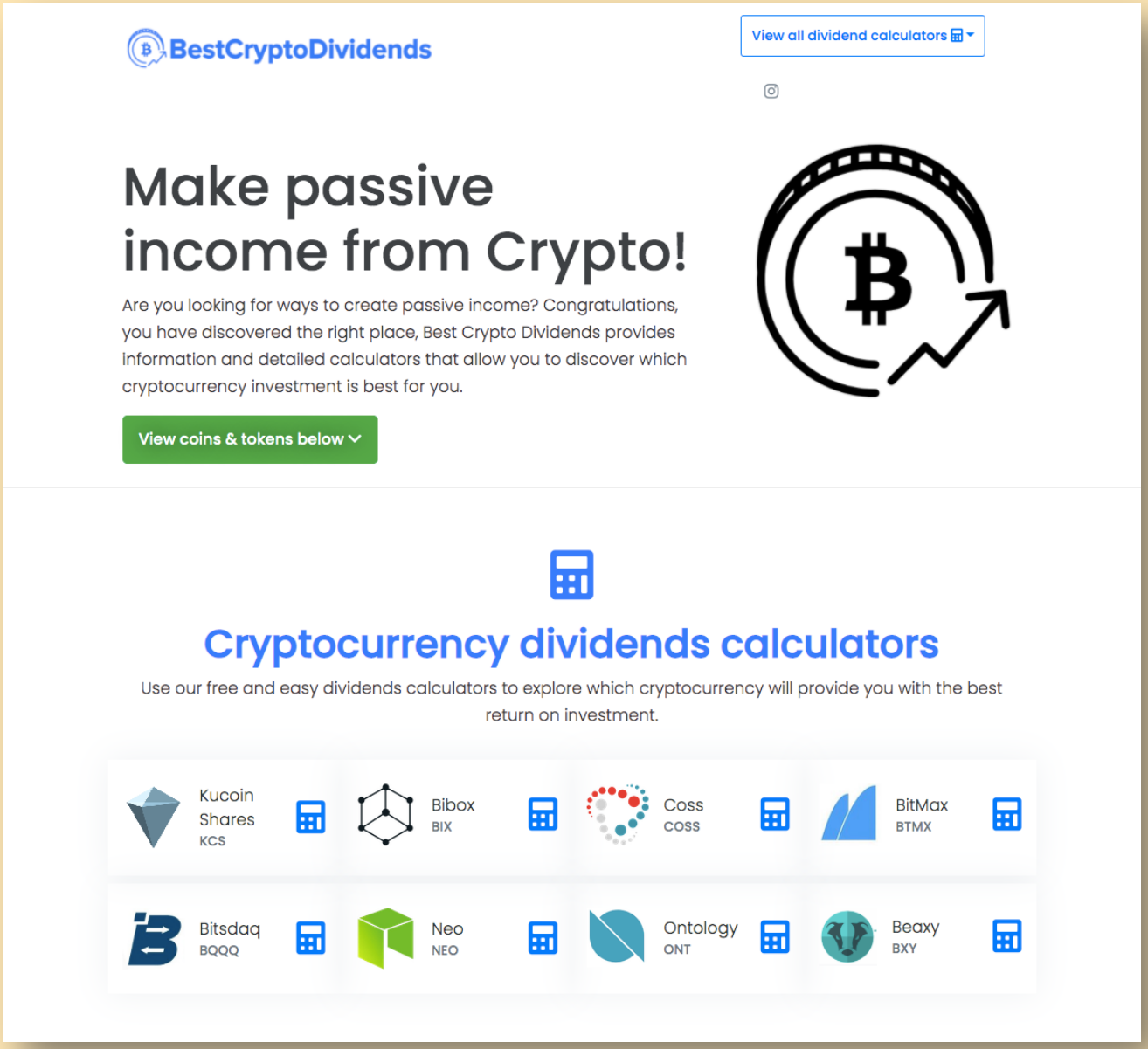
14. Crypto resources

CryptoWithSanya

"Crypto With Sanya" is a web-show about cryptocurrencies by Sanya Nagpal, a tenth grader, amateur boxer, and professional artist. She is also my daughter :-)

YouTube:
https://www.youtube.com/channel/UCapSUnxqtKIBktx3C2yGMPw

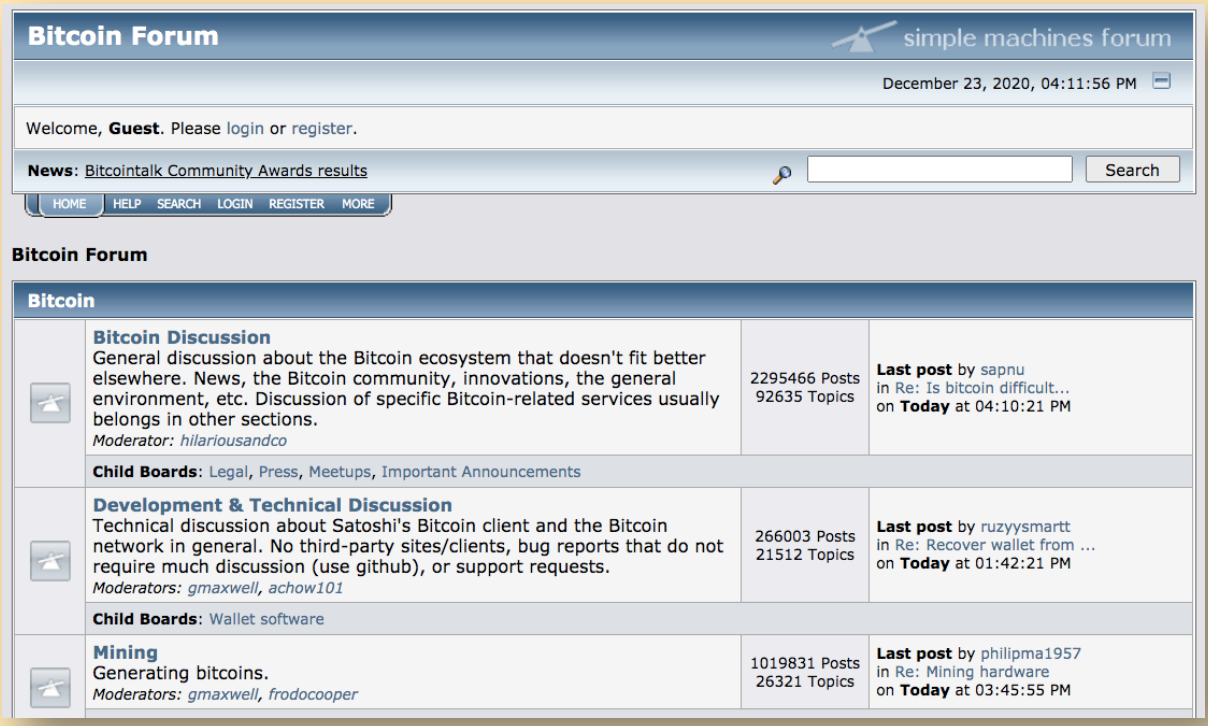
Facebook:
https://www.facebook.com/Crypto.with.Sanya



Best Cryptocurrency Dividends provides calculators for fee share tokens, masternode payouts and bonuses.

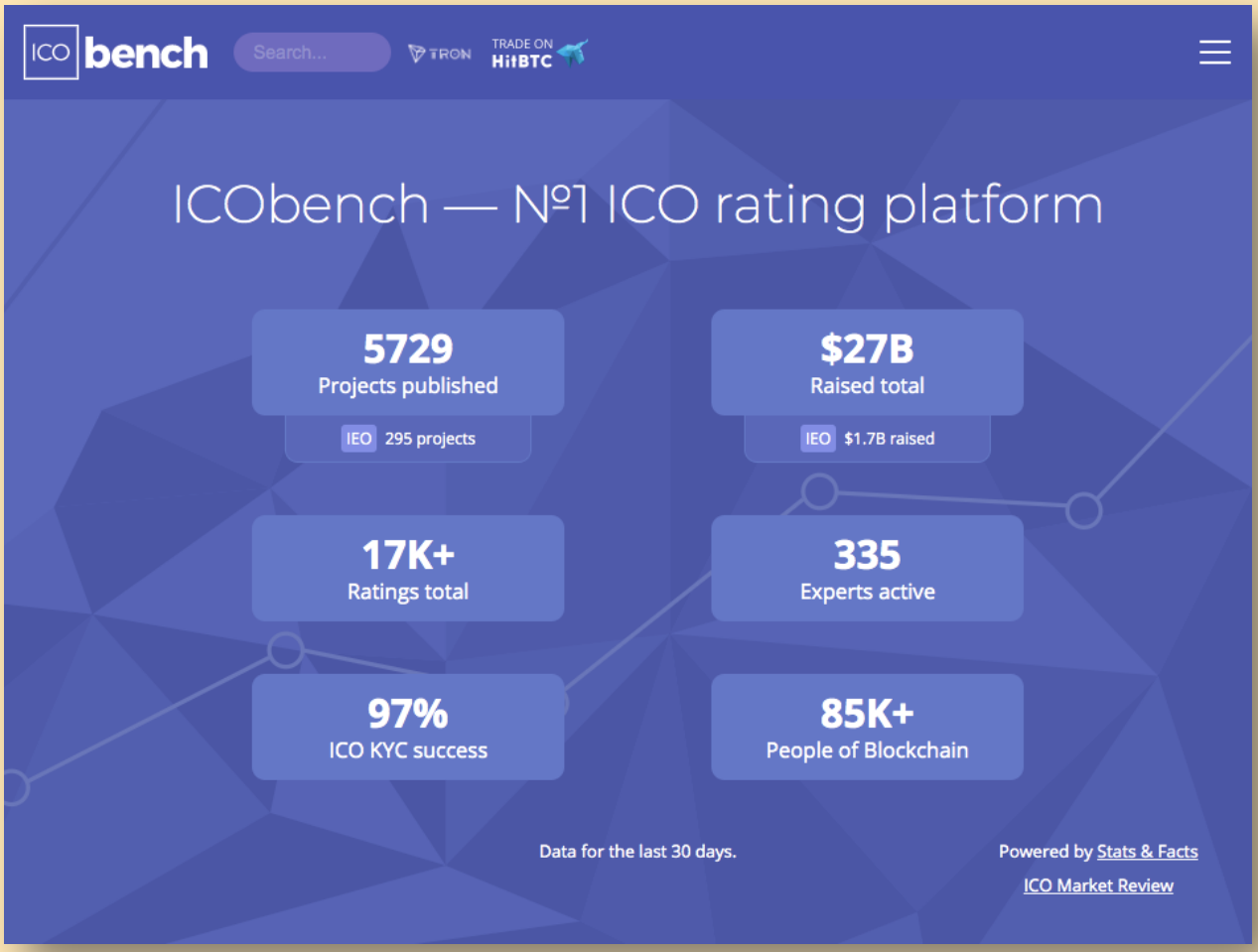
https://www.bestcryptodividends.com

Also see:
http://www.thelazycryptoinvestor.com



Some popular crypto social networks and discussions forums are:

- Bitcointalk: https://bitcointalk.org
- Cryptocurrency talk: https://cryptocurrencytalk.com
- Bitcoingarden: https://bitcoingarden.org
- https://www.reddit.com/r/CryptoCurrency

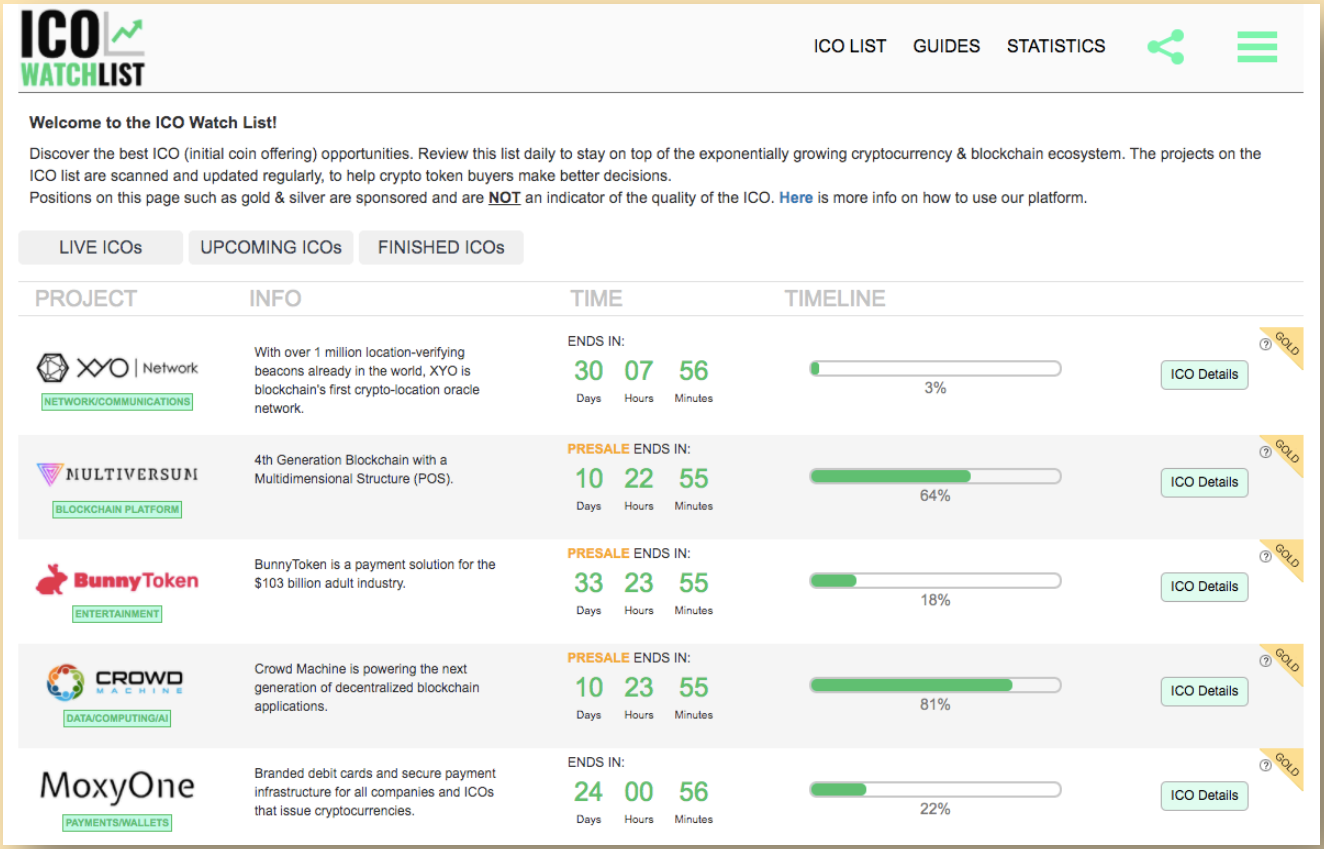


ICObench has detailed updated lists of:

- Initial Exchange Offerings (IEOs)
- Initial Coin Offerings (ICOs)
- Blockchain startups

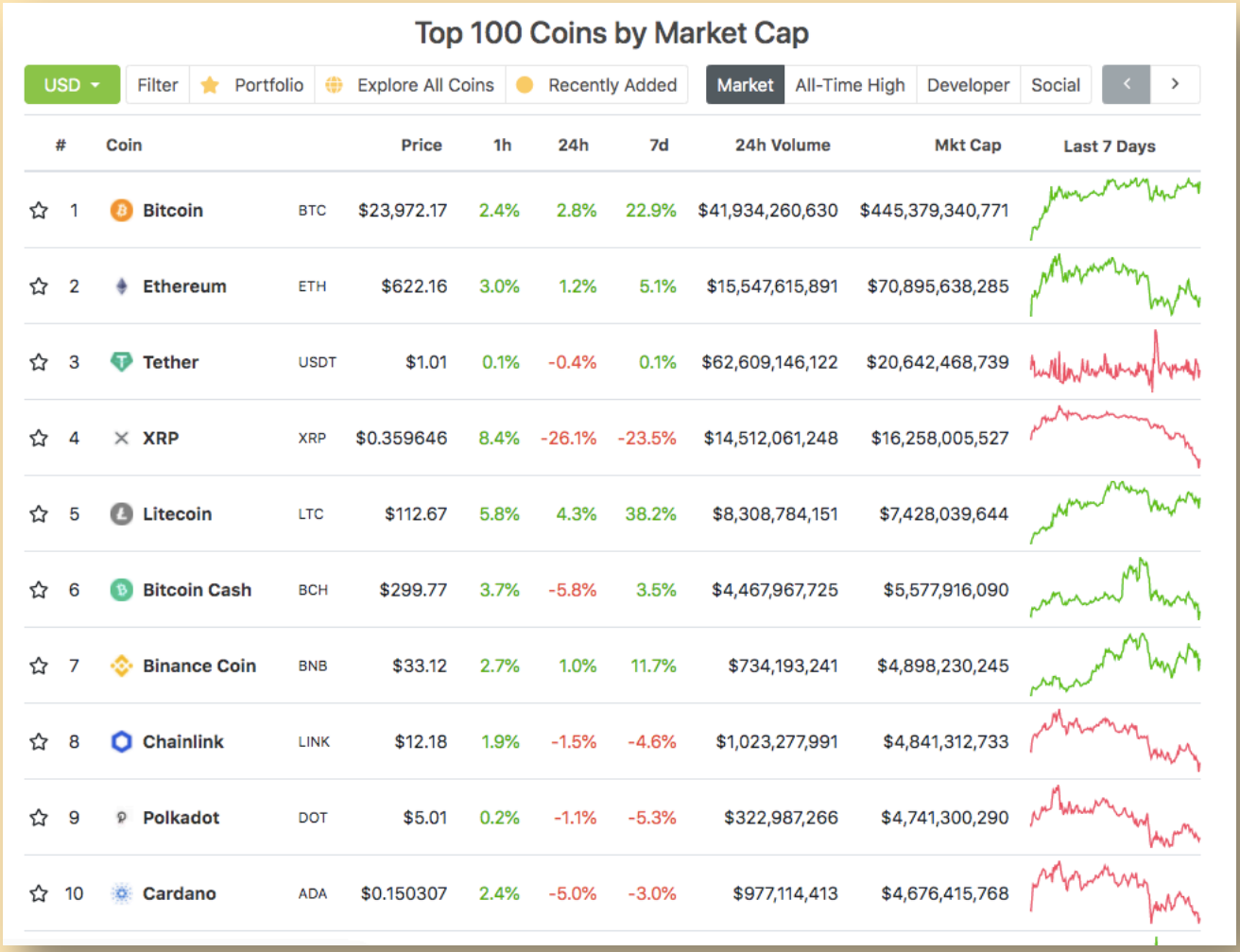
It also offers a premium API service for ICO listings, ratings, and statistics.

https://icobench.com



For the updated list of live and upcoming Initial Coin Offerings (ICOs) see:

- ICO WatchList: https://icowatchlist.com
- ICO Drops: https://icodrops.com
- ICO HotList: https://www.icohotlist.com

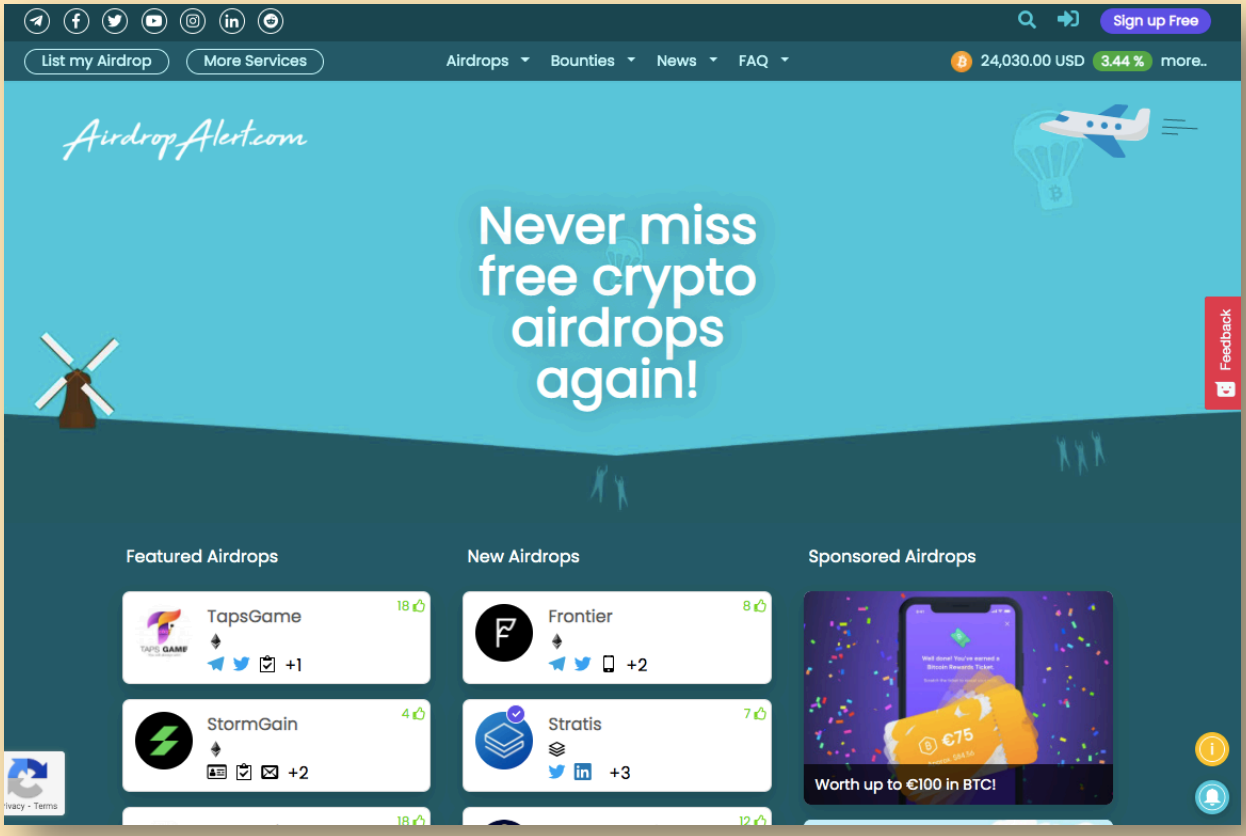


CoinGecko has detailed lists of:

- 6000+ Coins by Market Cap
- Top 100 DeFi Coins by Market Capitalization
- 370+ Spot Exchanges ranked by Trust Score
- 60+ Decentralized Exchanges ranked by Trading Volume
- 40+ Derivative Exchanges by Open Interest & Trade Volume
- 200+ Yield Farming Pools by Value Locked

https://www.coingecko.com/en

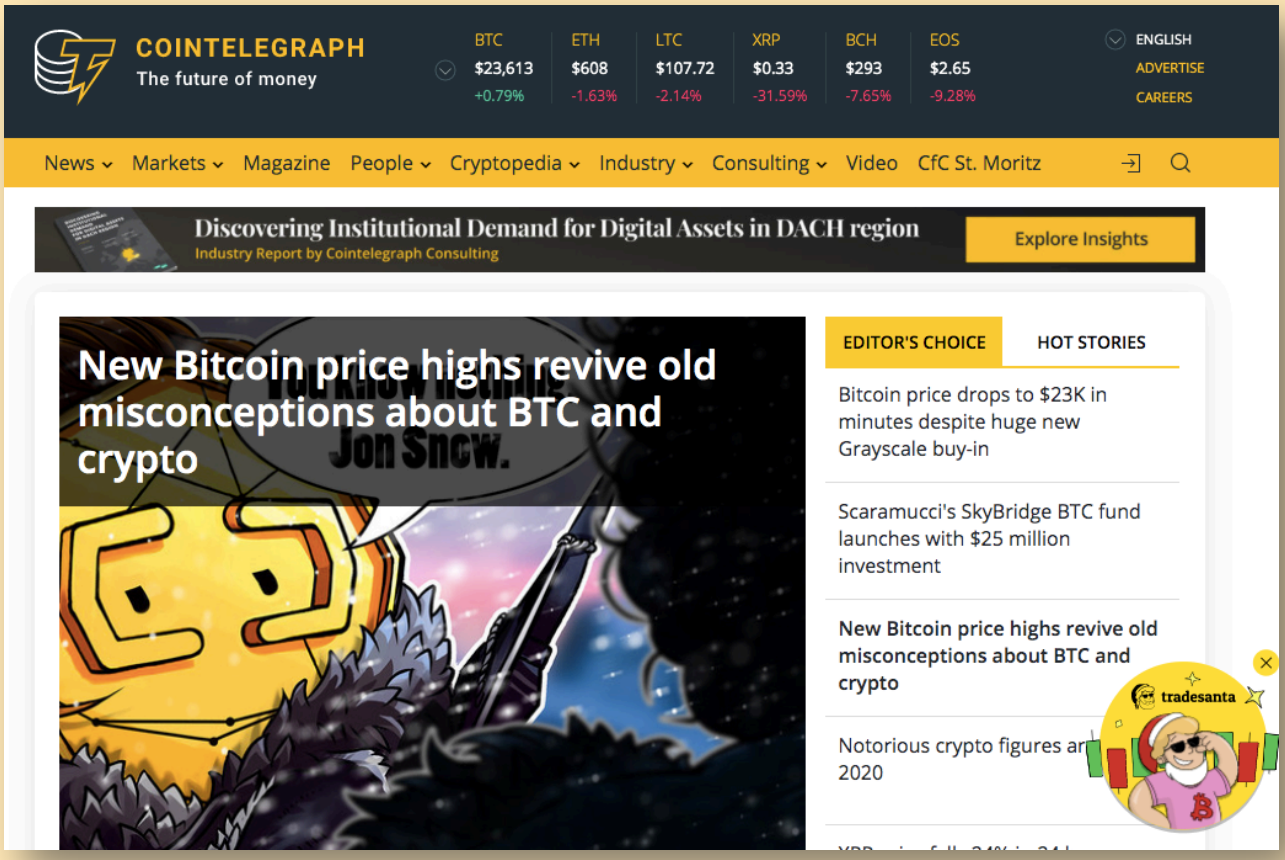
Get FREE cryptocurrency coins



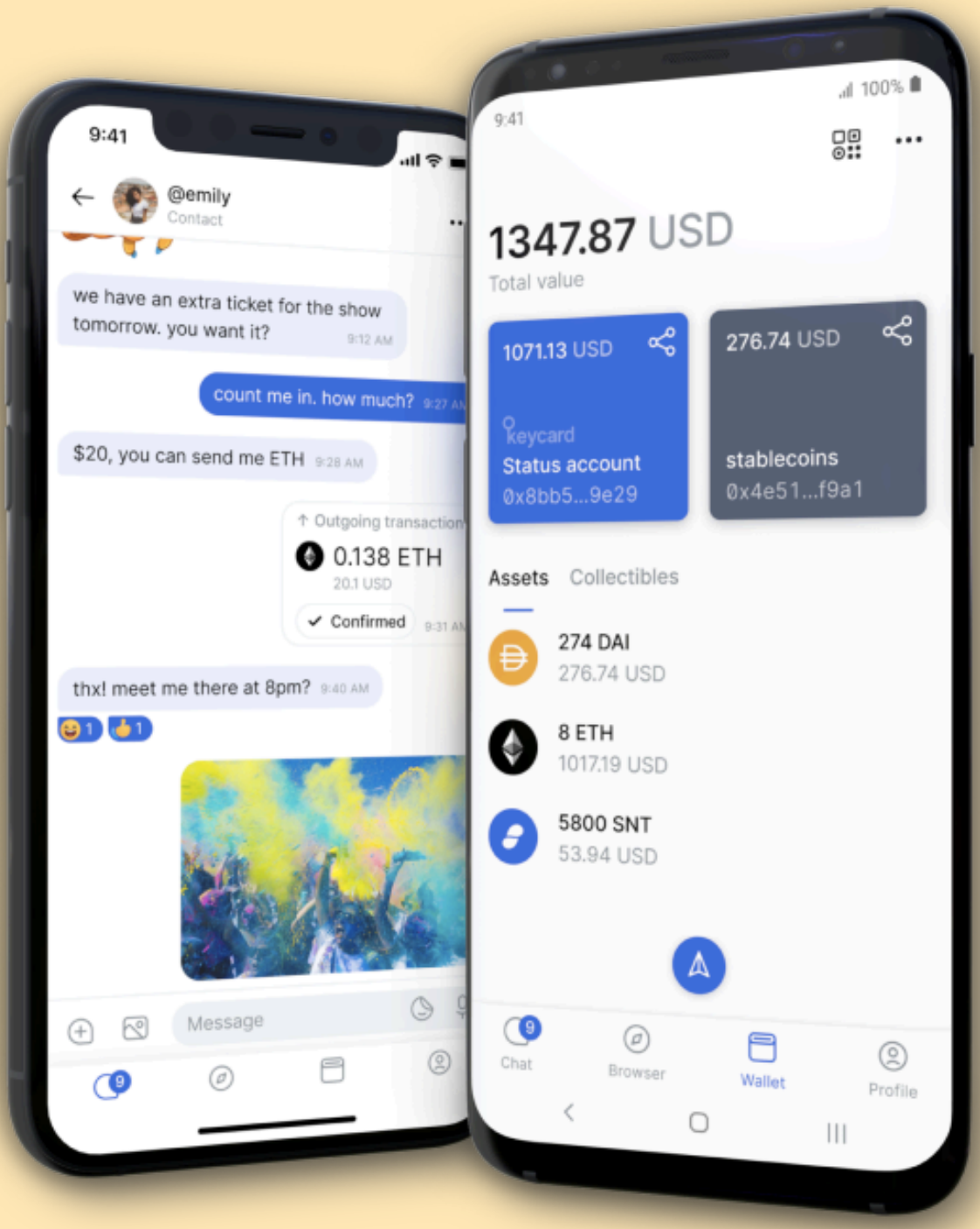
Cryptocurrency airdrops are free coin giveaways. This is done by blockchain startups as a marketing & public relations strategy.

Airdrop Alert is an automated airdrops service.

https://airdropalert.com/pro-plan/0oOGuLc9y

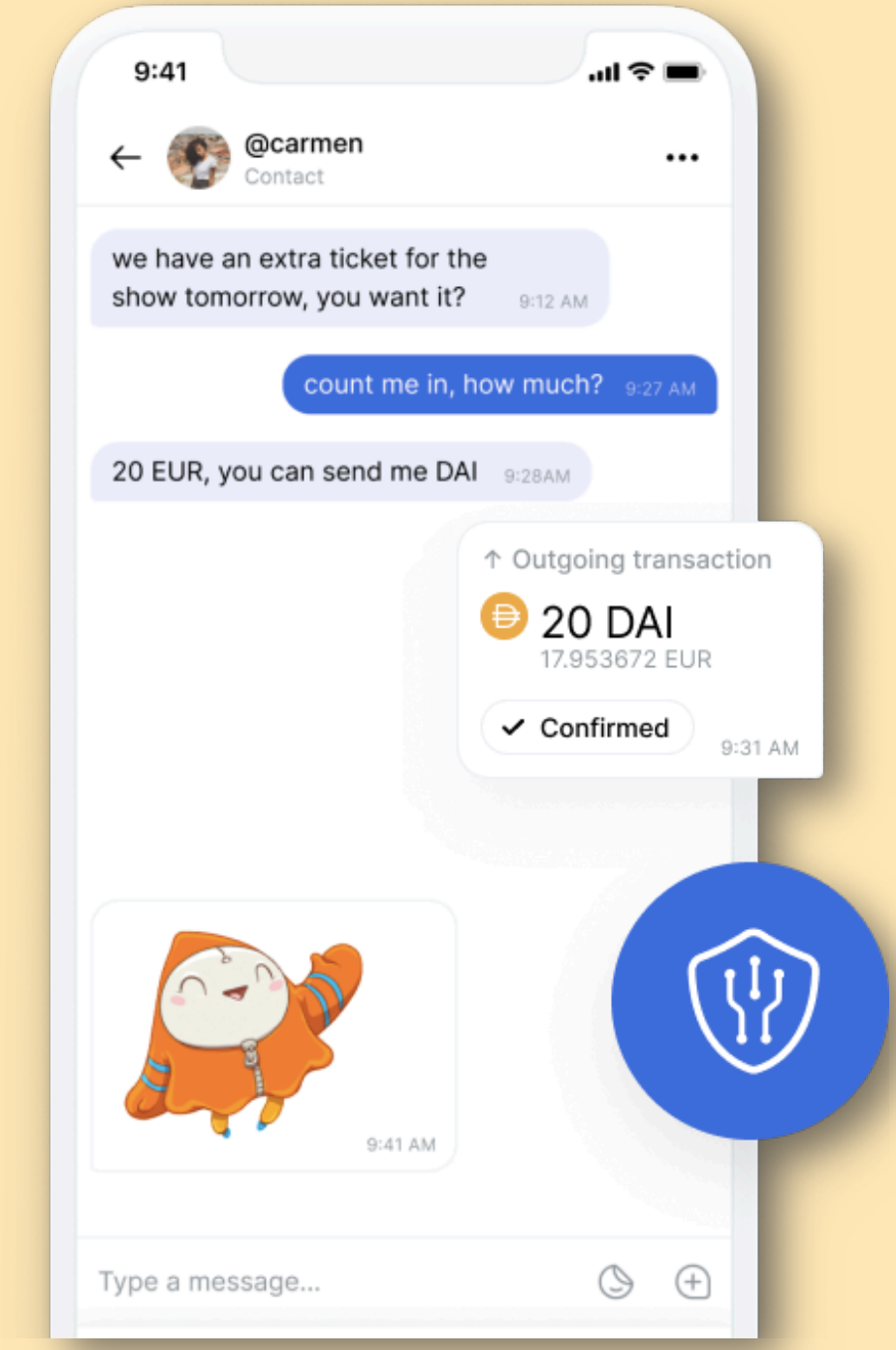


Coin Telegraph is a reputed crypto news site.
https://cointelegraph.com



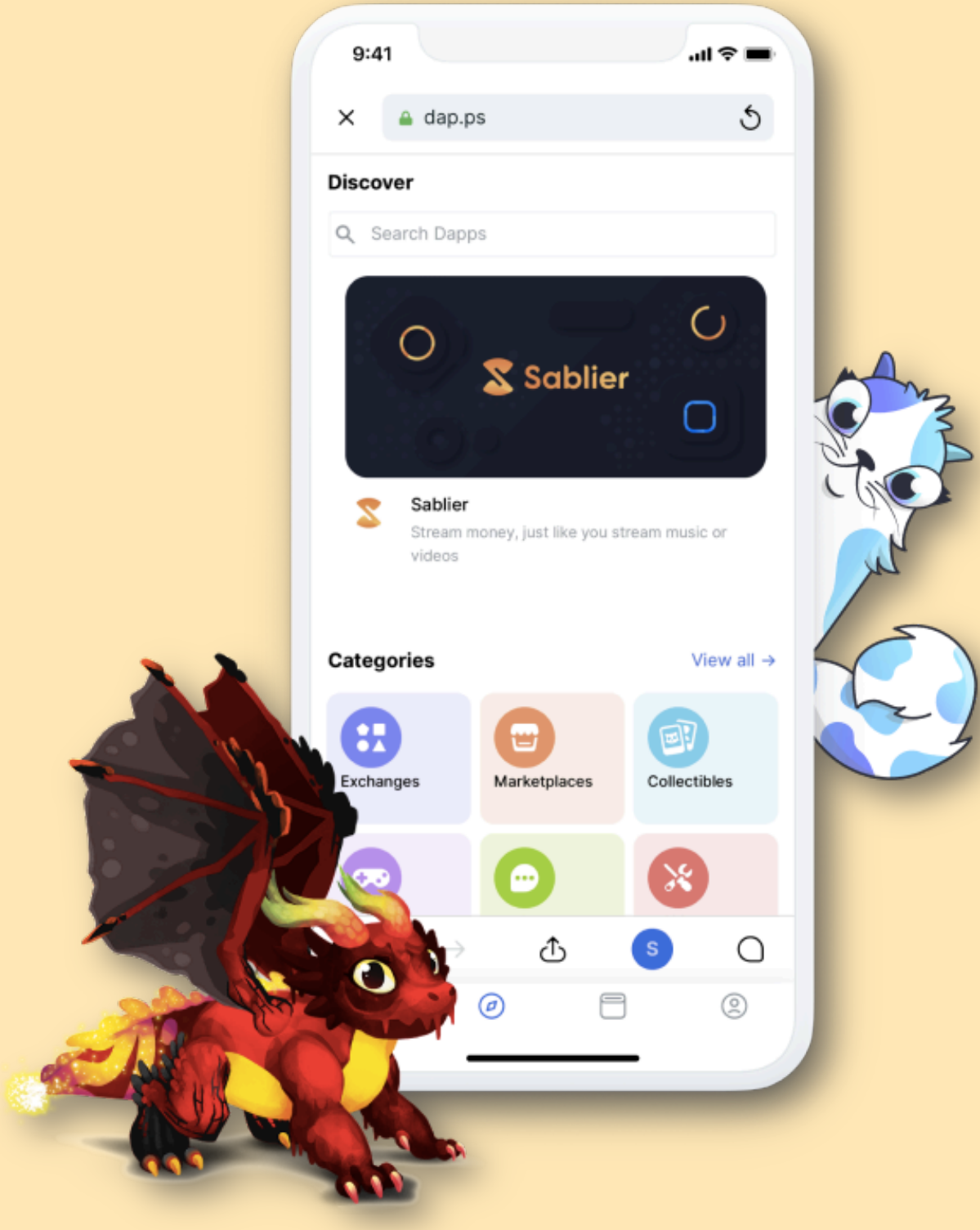
Status is a secure messaging app,
crypto wallet, and Web3 browser.

https://status.im



Status is a "Privacy-First Messenger" for sending private 1:1, group, and public chats. It enables payments globally and is built with peer-to-peer technology to remove "surveilling third parties".

https://status.im/private-messenger/



Status has a private & secure Web3 browser to access the latest defi dapps, exchanges, marketplaces, games and more.

https://status.im/web-three-browser

bisq

En

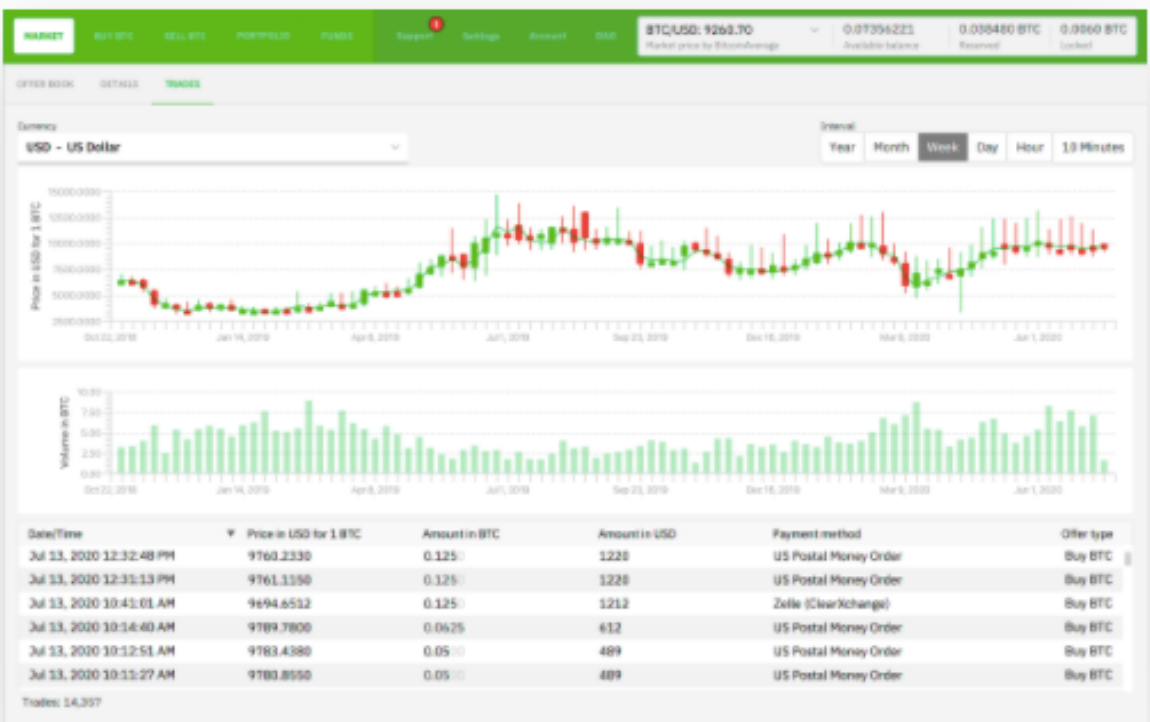
Exchange, Decentralized.

Buy and sell bitcoin for fiat (or other cryptocurrencies) privately and securely using Bisq's peer-to-peer network and open-source desktop software. No registration required.

Downloads

Get Started →

All Downloads | v1.5.0 | You appear to be using a Mac



Bisq

Bisq is a peer-to-peer bitcoin trading network which you run on your own hardware. It's open-source and community-driven.

https://bisq.network

Some of the key features:

- ❑ Bisq does not hold any bitcoin. All bitcoin used for trading is held in 2-of-2 multisignature addresses controlled solely by the trading peers themselves.

- ❑ Bisq does not hold any national currency. National currency is transferred directly from one trader to the other using traditional banking and payment services.

- ❑ All Bisq data is transferred over its own secure peer-to-peer network, which is built on top of the Tor network—no central servers. This means there are no data honeypots, reducing the risk of hacking.

- ❑ Bisq does not know anything about traders who use its network, and no data is stored on who trades with whom.

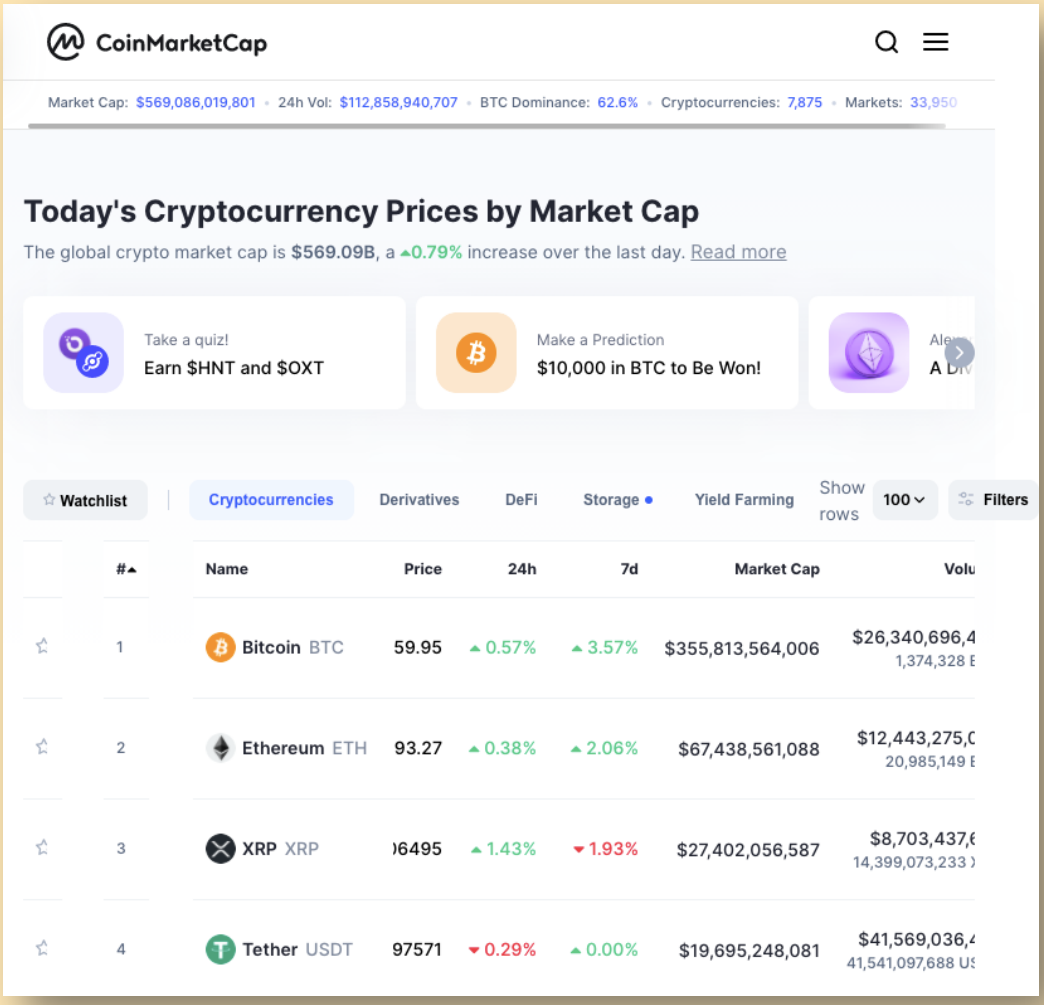
- ❑ Bisq does not require registration. This means user privacy is protected, and it also means there is no waiting period to have your account approved for trading.

- ❑ Bisq is code, not a company. It is an open-source project organized as a decentralized autonomous organization (DAO) built on top of Bitcoin.

Deribit is an institutional grade crypto derivatives platform.
https://www.deribit.com

COIN360 is a cryptocurrency and crypto exchange live data aggregator.

https://coin360.com



CoinMarketCap is a popular price-tracking website for cryptoassets.
https://coinmarketcap.com

For the latest crypto currencies, see:
https://coinmarketcap.com/new

To learn about crypto basics, see:
https://coinmarketcap.com/alexandria/categories/crypto-basics

For Crypto How-to Guides, see:
https://coinmarketcap.com/alexandria/categories/how-to-guides

For a Crypto Glossary, see:
https://coinmarketcap.com/alexandria/glossary

For tech deep-dives, see:
https://coinmarketcap.com/alexandria/categories/tech-deep-dives

Staking Rewards is a leading data provider for staking and crypto-growth tools. It tracks 150+ yield-bearing assets and 1700 qualified providers.

https://www.stakingrewards.com

15. Invest W.I.S.E.L.Y in crypto assets

W.I.S.E.L.Y is an acronym for: Wisdom, Intricacies, Security, Exchanges, Law, Yield.

Wisdom
Crypto-currencies are not for everyone. They are very very very volatile. Another point to remember is that there are thousands of crypto-currencies, most of which have very low liquidity. This means that you may not find a buyer when you decide to book profits or sell.

So be wise. First, understand your risk appetite. Then consider if you should invest in cryptocurrencies. Please DO NOT put your retirement fund into crypto assets. Only invest money that you can afford to lose.

Intricacies
Conventional investments (mutual funds, gold, real estate, bank deposits) are relatively easy to understand. Crypto investments require a lot of technical knowledge.

Make sure you have a strong understanding of addresses, blocks, confirmation, cryptography hash functions, hash rate, mining, multi-sig, nodes, pools, private keys, proof of work (and other algorithms), wallets, etc.

Security
If your online banking or share trading account is hacked, you do have some legal recourse. But if your crypto account/wallet gets hacked, you have almost no legal options. So you must know how to secure your crypto assets using hot, warm, and cold wallets.

While phishing, malware, and scams are usually targeted towards end-users and exchanges, there are many attacks on the crypto networks - 51% attack, cannibalizing pools, DDoS attacks, double-spend attacks, P+Epsilon attacks, Sybil attacks, etc.

Exchanges
Stock exchanges are highly regulated entities. Crypto exchanges in most countries are not regulated. This means they can shut down anytime or even steal your money and there's not much you would be able to do. So make sure you only use highly respected and credible exchanges.

Law
Cryptocurrencies are outright illegal in some countries. Plus the legal and taxation issues are not clear in most jurisdictions. You must understand the money laundering and taxation laws of your country before you trade in crypto.

Yield
There are all sorts of crypto assets today - Utility tokens, Transactional tokens, Electronic cash / decentralized money, Privacy coins, Tokenized version of assets such as land, gold, Mining contracts, Crypto derivatives, etc. Financial models for predicting yields in such assets are very primitive as of today. You need to learn how to calculate yields.

Prefer the video version of this?

https://www.youtube.com/watch?v=r9stGriav-s

15. References

The rise of digital money
https://www.rohasnagpal.com/docs/future-money/IMF-Digital-Money.pdf

FATF report on Virtual Currencies - Key Definitions and Potential Risks
https://www.rohasnagpal.com/docs/future-money/FATF-VC-defn.pdf

Stablecoins: The Next Generation Of Digital Money – Forbes
https://www.forbes.com/sites/tatianakoffman/2019/03/08/stablecoins-the-next-generation-of-digital-money/#37f11e4d23f3

Everything you need to know about 180 world currencies
https://www.travelex.com/currency/current-world-currencies

Wikipedia
https://en.wikipedia.org

Bitcoin developer guide
https://bitcoin.org/en/developer-guide

Ken Shirriff's blog:
www.righto.com

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

https://blockchainhub.net/blockchain-oracles

https://www.ledger.com

https://trezor.io

In 1999, I co-founded the Asian School of Cyber Laws and moved into the super exciting field of cyber law and cybercrime investigation. I have had the privilege of assisting the Government of India in framing draft rules and regulations under the Information Technology Act.

My work has taken me to 18 countries and I have investigated cyber crimes & data breaches for hundreds of organizations.

I developed an interest in virtual currencies in 2011 while investigating a case of organized criminals using bitcoin. I have been working extensively in crypto assets & blockchain since 2013.

I co-founded BankChain - a community of 37 banks for exploring, building, and implementing blockchain solutions.

I led the teams that developed Primechain, a blockchain ecosystem that builds itself in 6 minutes (or less) with a functional web application, mobile Progressive Web App, and a Blockchain REST API service.

Rohas Nagpal
Fintech & Crypto Evangelist
www.rohasnagpal.com

The latest version of the
Future Money Playbook
can be downloaded from:

https://www.rohasnagpal.com/future-money.php