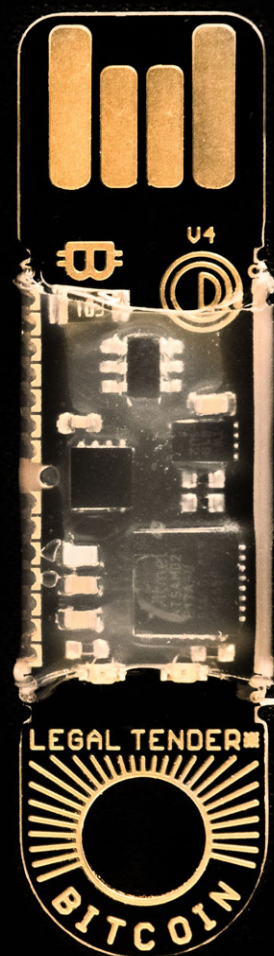


Future Money Playbook



Compiled by Rohas Nagpal

Edition 2.3 dated 20 April 2021

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....

(c) 2021 Rohas Nagpal. All rights reserved.

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



Don't forget to buy me a
coffee...
...if you like my book
😊

Contents

- A. Money - Past, Present & Future.....07**
- B. Crypto valuation using R.O.H.A.S.....28**
- C. The Crypto Ecosystem.....34**
 - C1. Cryptocurrencies.....38
 - AAVE.....46
 - BAT.....48
 - BNB.....50
 - BTC.....52
 - CHZ.....54
 - DOT.....56
 - ENJ.....58
 - ETH.....60
 - ETN.....62
 - LINK.....64
 - MATIC.....66
 - SNX.....68
 - SOL.....70
 - STPT.....72
 - SUSHI.....74
 - SXP.....76
 - THETA.....78
 - UNI.....80
 - VET.....82
 - YFI.....84

C2. Stablecoins.....	86
C3. Central Bank Digital Currency.....	95
C4. Non-Fungible Tokens.....	102
C5. Tokenized stocks.....	121
C6. Crypto Wallets.....	123
C7. Oracles.....	141
C8. Public Blockchains.....	143
C9. Technical Crypto Concepts.....	147
D. The Bitcoin Ecosystem.....	177
E. The Ethereum Ecosystem.....	196
F. Crypto Investing.....	206
F1. Decentralized finance (DeFi)	207
F2. How to profit from crypto.....	221
F3. Crypto Exchanges.....	236
F4. How to keep your crypto safe.....	241
F5. Crypto Resources.....	248
F6. Invest W.I.S.E.L.Y in crypto.....	263
F7. Crypto Indexes.....	265
F8. Hybrid Finance (HyFi)	267
References & sources.....	275
About the author.....	276

A

Money - Past, Present & Future

A. Money - Past, Present & Future

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 (Gol 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.

Virtual currency is different from **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.

Did you know?

Before the USA, only 5 powers had enjoyed the coveted "reserve currency" status, going back to the mid-1400s:

- + Portugal,
- + Spain,
- + the Netherlands,
- + France and
- + Britain.

Those reigns lasted 94 years on average.
The US dollar’s run has crossed 100 years.

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

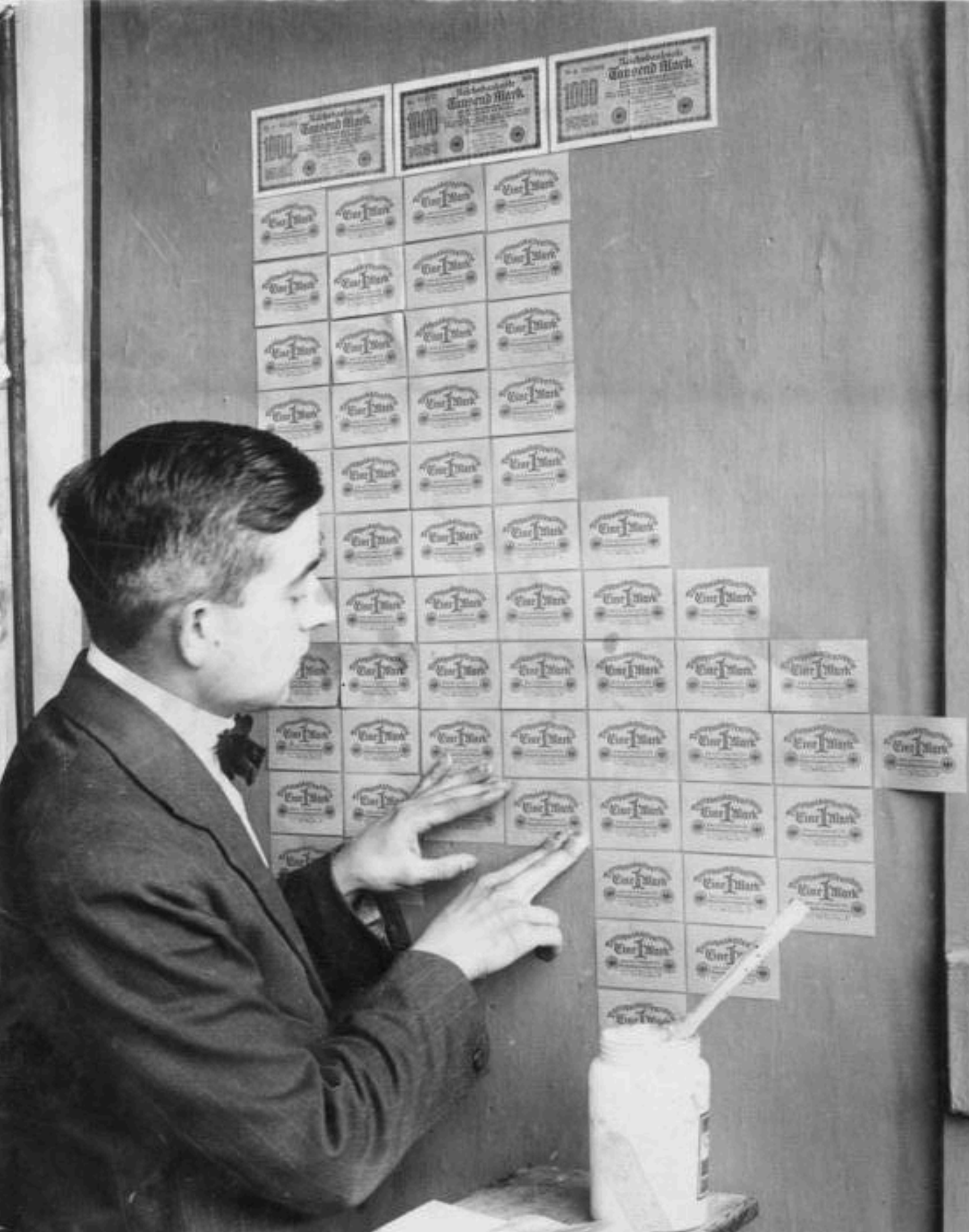
On June 5, 1933, the US went off the gold standard,
when its Congress enacted a joint resolution
nullifying the right of creditors to demand payment in gold.

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>

9 pages that disrupted money forever

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:

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

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

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

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), Aricoïn (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: 157fRqAKrDyGHR1Bx3yDxeMv8Rh45aUet

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. 😊



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

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 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).

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.

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.

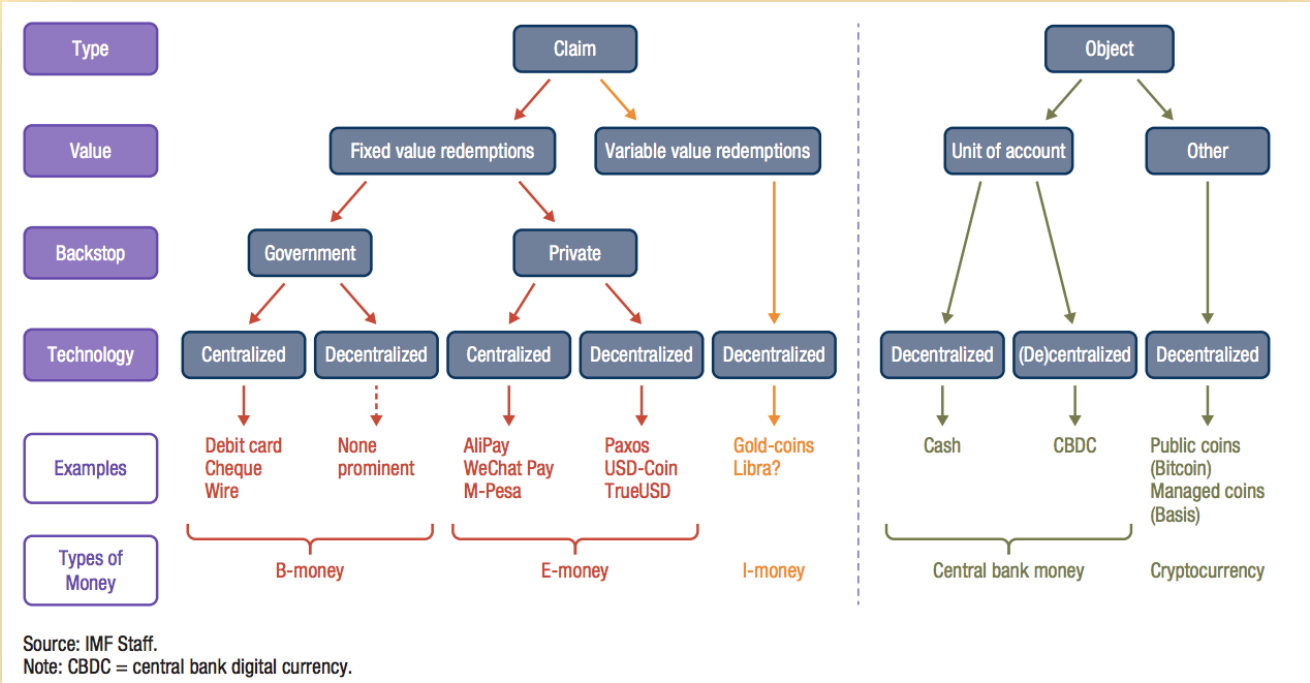
Developers could for instance allow users to determine the goods that e-money could purchase—a useful feature for remittances or philanthropic donations.

- **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.

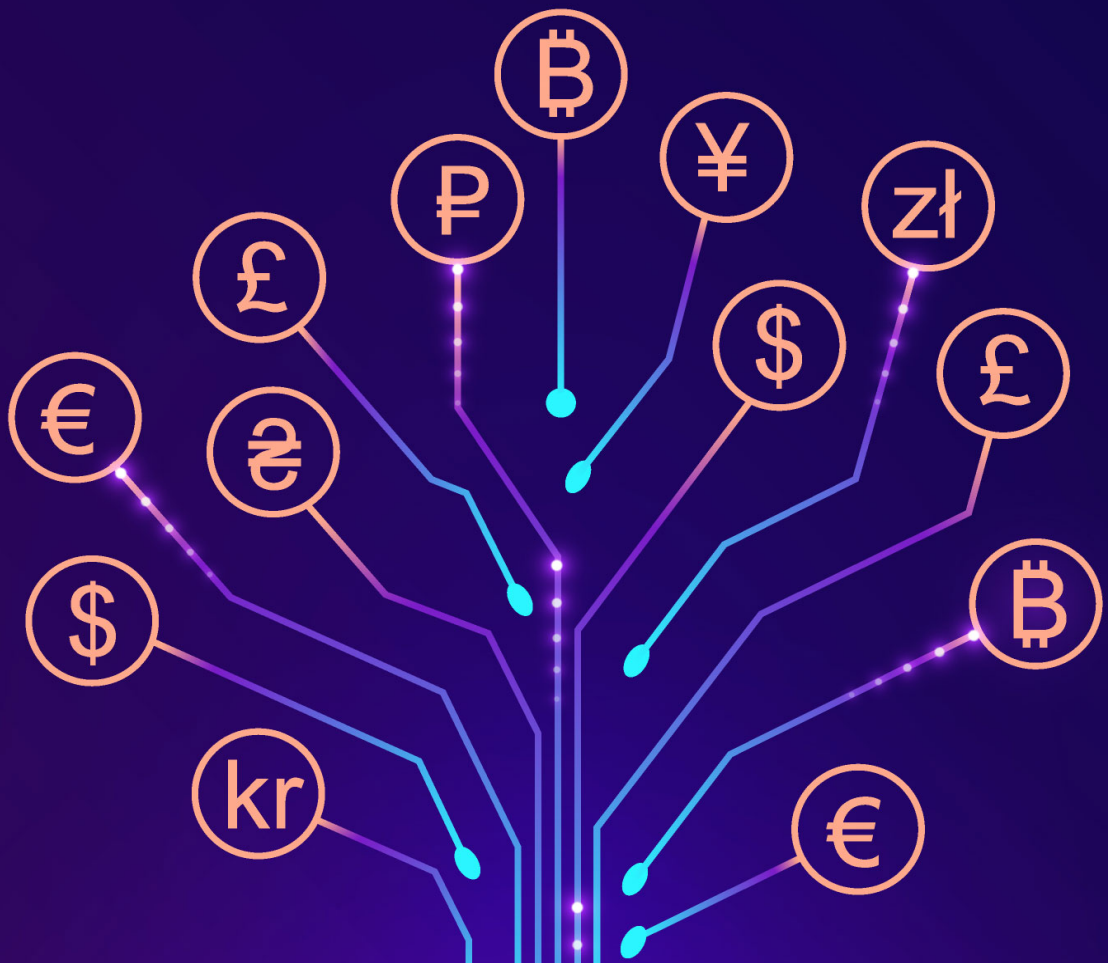
As a result, people might even agree to sell their car for an e-money payment, as the funds would immediately show up in their account, without any settlement lag and corresponding risks.

- **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.

Money Trees

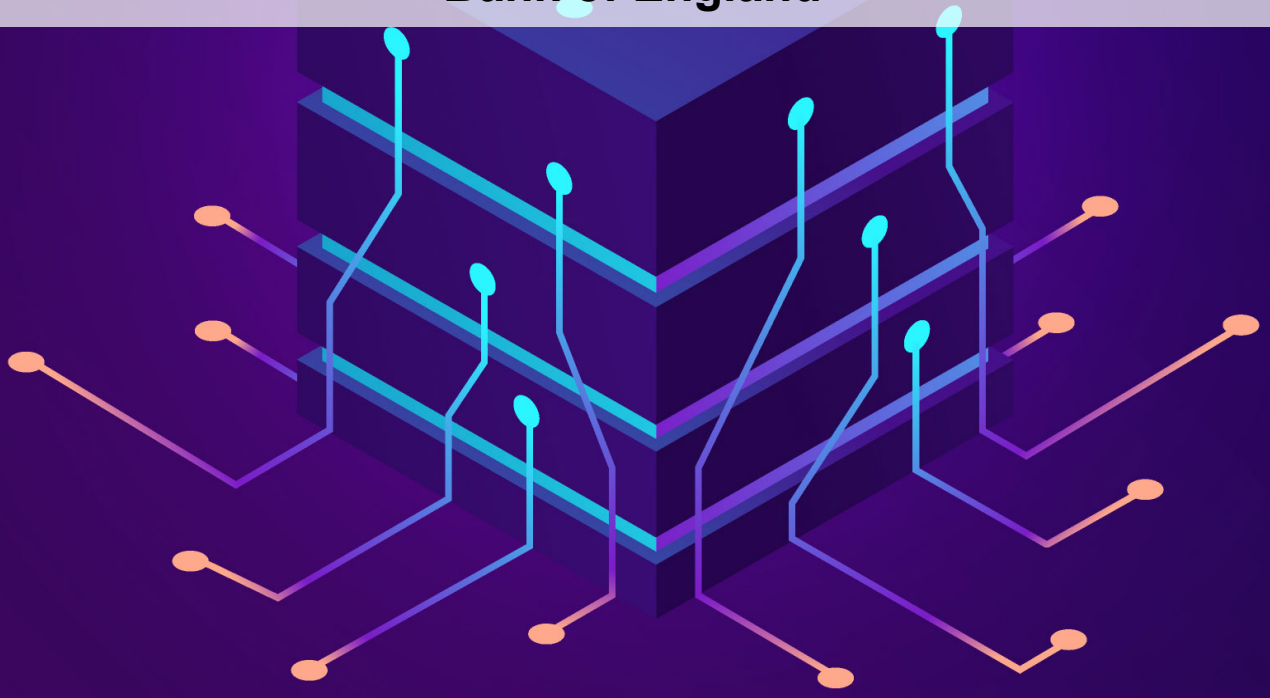


Source: IMF



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



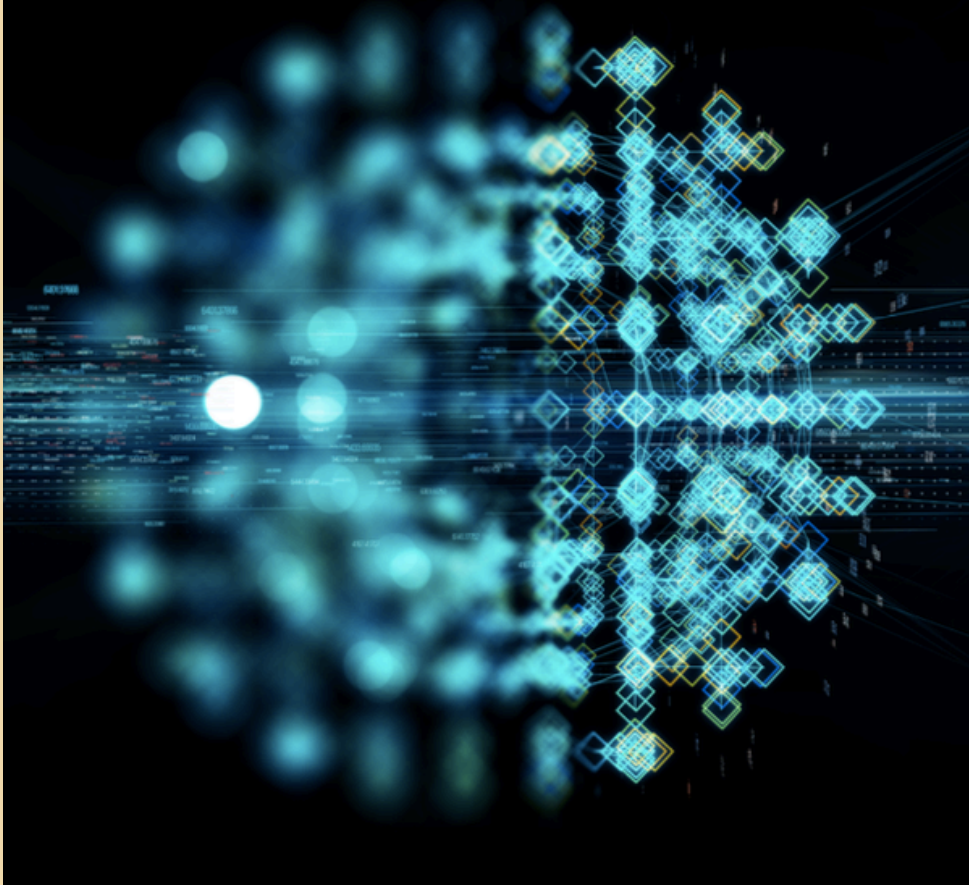
Global Future Council on Cryptocurrencies



Crypto, What Is It Good For?

An Overview of Cryptocurrency Use Cases

DECEMBER 2020



Crypto, What Is It Good For?

An Overview of Cryptocurrency Use Cases

[http://www3.weforum.org/docs/WEF Cryptocurrency Uses Cases 2020.pdf](http://www3.weforum.org/docs/WEF%20Cryptocurrency%20Uses%20Cases%202020.pdf)

How much money is there in the world? (18th February 2021)

(Figures are in trillions of US dollars)

Silver	0.044
Gold	10.9
Bitcoin	0.9
All cryptocurrencies	1.59

Coins & Bank Notes	6.6
IN currency	0.377
US Currency	2.05
World's Billionaires	8.0

Stock markets	89.5
Real Estate	280.6

Derivatives (Market Value)	11.6
Derivatives (Notional Value)	558.5
Derivatives (Notional Value High end)	1000.0

Primary source:

<https://www.visualcapitalist.com/all-of-the-worlds-money-and-markets-in-one-visualization-2020/>

How much U.S. currency is in circulation?:

https://www.federalreserve.gov/faqs/currency_12773.htm

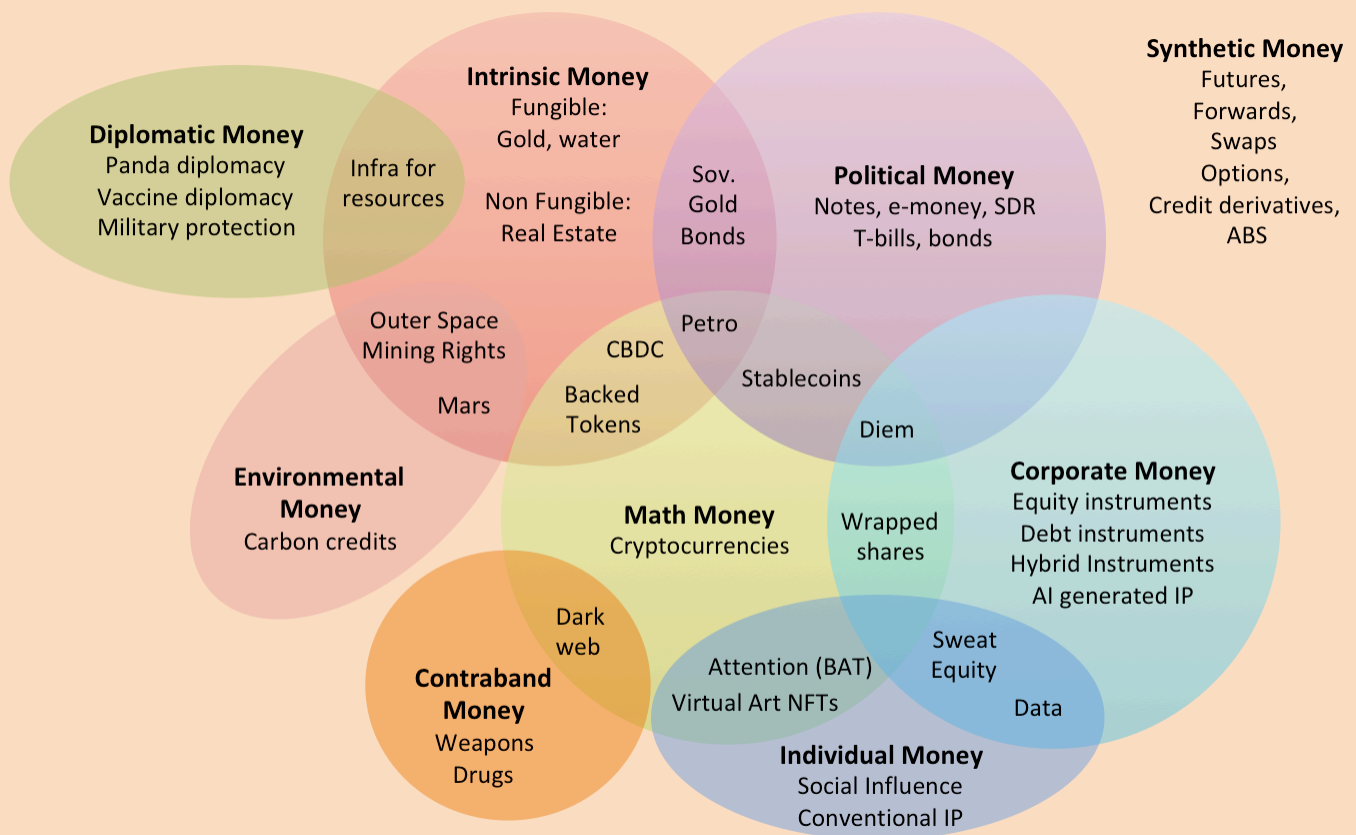
Future Money

Conventionally, money is defined as a matter of functions four - a medium, a measure, a standard, a store. This definition has served us well through the days of commodity and fiat money.

But we now live in the age of vaccine diplomacy, complex derivatives, cryptocurrencies, and mega social influencers. It's time we changed the definition of money.

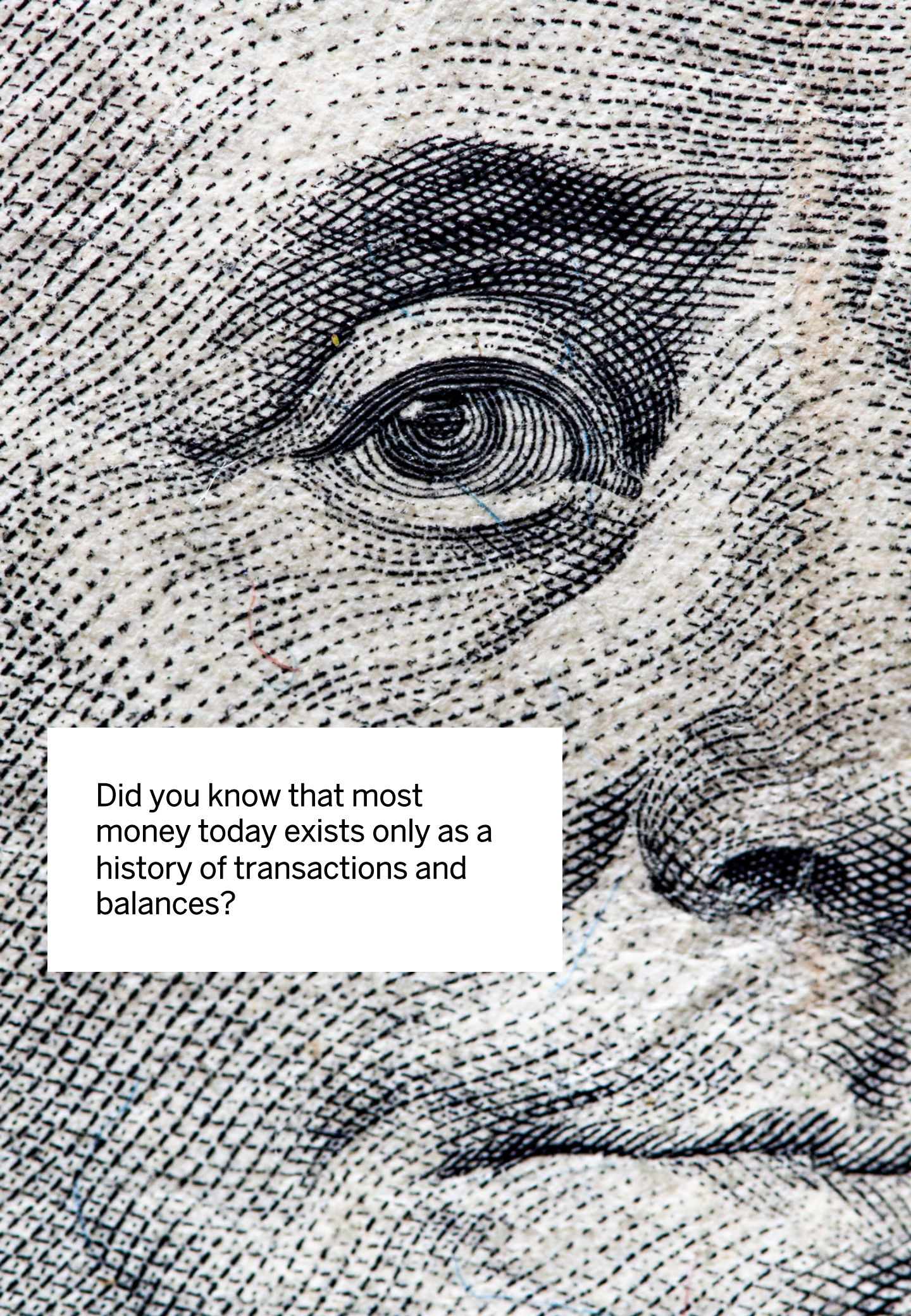
I define Future Money as "something you can give in exchange for something that you want".

The components of Future Money are displayed in the mindmap below:



Future Money comprises (in alphabetical order):

1. Contraband Money
2. Corporate Money
3. Diplomatic Money
4. Environmental Money
5. Individual Money
6. Intrinsic Money
7. Math Money
8. Political Money
9. Synthetic Money

A close-up photograph of a banknote, likely a Euro, showing a highly detailed and textured illustration of a human eye. The eye is rendered with fine, concentric lines and a dense, cross-hatched pattern around it, giving it a three-dimensional, almost woven appearance. The surrounding paper of the banknote has a visible, coarse texture. A white rectangular box is overlaid on the lower-left portion of the image, containing text.

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

B

Crypto & Innovation valuation
using R.O.H.A.S

B. Crypto valuation using R.O.H.A.S

Valuing crypto assets and other innovations is not easy. I propose the R.O.H.A.S method. That's an acronym for:

- Revenue model
- Organization
- History
- Algorithm
- Social engagement

R = revenue model

How's the project going to make money for itself and for investors? Is the crypto a medium of exchange? Is it a platform / security / transactional / utility / governance token?

O = organization

Who's the team behind the project? How respected, experienced and qualified are they? Who are the partners and other ecosystem members?

H = history

Have the project milestones been achieved on time? How's the price fluctuated in the past? How's the liquidity been?

A = algorithm

The technology platform, consensus mechanism and other tech issues are critical. Is the project developing a new blockchain? Is it using a tried and tested one? How scalable is the platform?

S = social engagement

How large and vibrant is the community? How active are they? Do they regularly engage? How many fanatics?



”

R.O.H.A.S. Cryptocurrency Valuator

Value crypto coins & tokens using Revenue, Organization, History,
Algorithm & Social parameters.

R.O.H.A.S. Cryptocurrency Valuator
<https://www.rohasnagpal.com/ROHAS.php>

The ROHAS Valuator takes into account the following:

- r1. Economic impact
- r2. Circulating supply
- r3. Maximum supply
- r4. Total supply
- r5. Category
- r6. Market share
- r7. Public information
- r8. Team
- r9. The ecosystem
- r10. Milestone achievements
- r11. Performance history & liquidity
- r12. Consensus mechanism
- r13. Source code
- r14. Dev pool
- r15. Community & Social engagement

Some of the other methods are:

- ☐ The Net Cost Model
- ☐ Network Value to Transaction Model
- ☐ Monte Carlo Simulation

See: <http://bit.ly/2ZyVrlj>

- ☐ Store of Value Thesis
- ☐ Token Velocity Thesis
- ☐ INET & Crypto J-Curve Thesis
- ☐ Daily active addresses/users (DAA)

See: <http://bit.ly/3aAP0F3>

- ☐ Modified cost of production (Draft)

See: <https://bit.ly/3qJHgWw>

- ☐ Metcalfe's Law
- ☐ Crypto-networks as Small Emerging Economies

See: <http://bit.ly/3s5PAjl>

- ☐ Black-Scholes Option Theory

See: <http://bit.ly/37rbhmr>

- ☐ Quantity Theory of Money
- ☐ National Currency Comparisons
- ☐ Pure Store of Value: Percent of Net Worth

See: <https://www.lynalden.com/cryptocurrencies/>

Also see:

A Review Of Cryptoasset Valuation Frameworks

<https://blog.coinfabrik.com/a-review-on-cryptoasset-valuation-frameworks/>

Cryptoasset Valuation

<https://bit.ly/2NFSMDH>

Under the **BITT 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.

C

The Crypto Ecosystem

C. The Crypto Ecosystem

According to the FATF report on Virtual Currencies - Key Definitions and Potential AML/CFT Risks, a 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.

A **crypto coin** is a cryptocurrency that operates on its own blockchain e.g. Bitcoin (BTC). A **crypto token** is a cryptocurrency that operates on a parent blockchain e.g. BAT is a token that operates on Ethereum.

Circulating Supply: The number of coins that are circulating in the market and are in public hands.

Maximum Supply: The maximum number of coins that will ever exist in the lifetime of the cryptocurrency.

Total Supply: The number of coins that have been already created, minus any coins that have been burned.

Bitcoin, the big daddy of crypto, is the world's first cryptocurrency. All other cryptocurrencies are called "alternative coins" or "altcoins". There are more than 8,000 altcoins!

Did you know that Bitcoin isn't 100% anonymous. All its transactions are recorded on its publicly available Blockchain.

That's what led to the birth of privacy coins - some of which are private by default, while others let the users decide if they want to activate the functionality or not. Some known privacy coins so are

1. Monero (XMR)
2. Zcash (ZEC)
3. Grin (GRIN)
4. Zcoin (XZC)
5. Verge (XVG)
6. Ghost (GHOST)

Also see:

A Guide to Crypto Collectibles and Non-fungible Tokens (NFTs)

<http://bit.ly/2OSWMSH>

ERC-20 standard

<https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>

ERC-721 standard

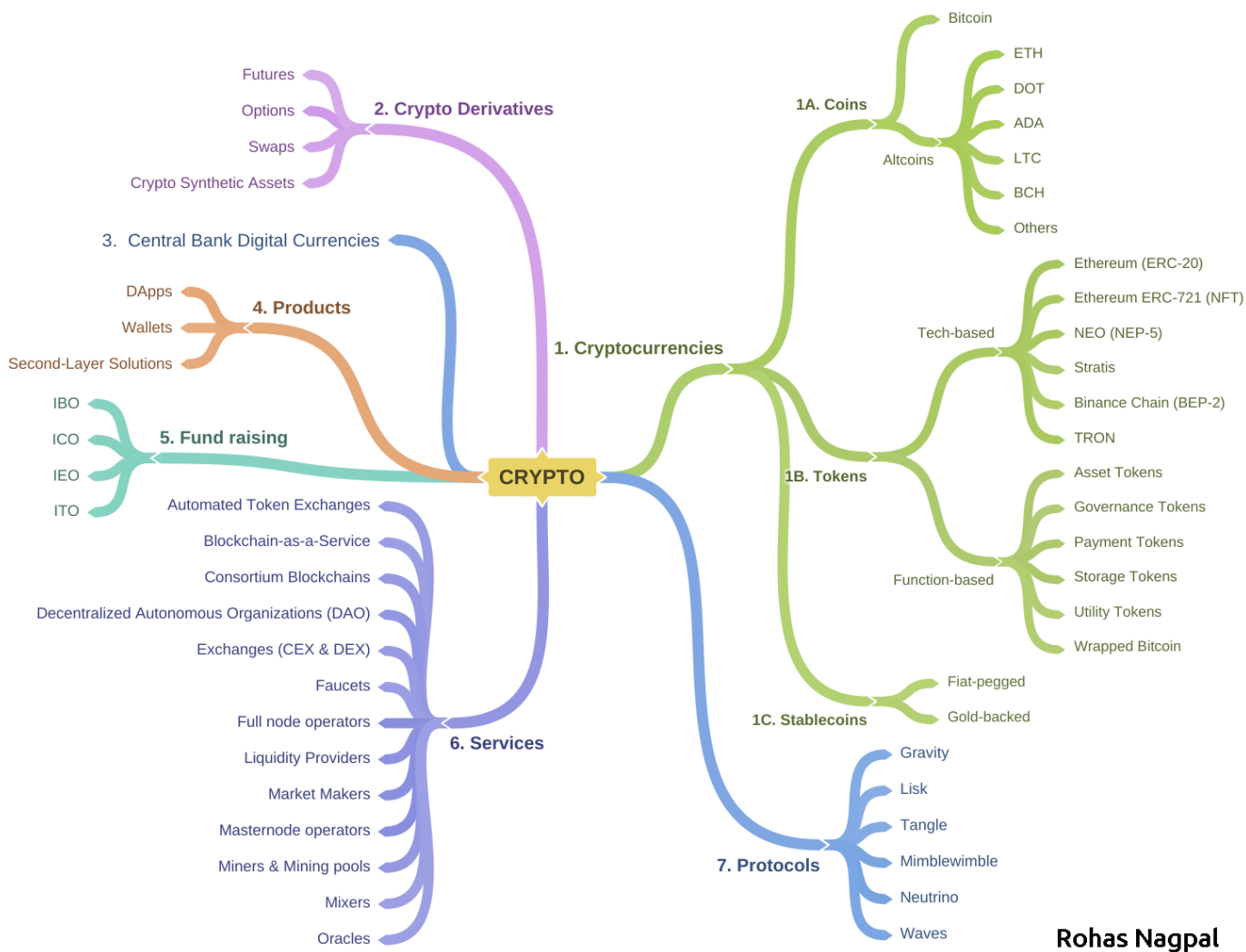
<https://ethereum.org/en/developers/docs/standards/tokens/erc-721>

BEP-2 standard

<https://academy.binance.com/en/glossary/bep-2>

BEP-20 standard

<https://academy.binance.com/en/glossary/bep-20>



Rohas Nagpal

Mindmap of the Crypto Ecosystem

C1. Cryptocurrencies

The popular categories of cryptocurrencies are:

1. Automated Market Maker Tokens

- Uniswap (UNI)
- Bancor (BNT)
- Balancer (BAL)

2. Centralized Exchange Tokens

- Binance Coin (BNB)
- FTX Token (FTT)
- Huobi Token (HT)

3. Collectibles & NFTs

- THETA (THETA)
- Chiliz (CHZ)
- Enjin Coin (ENJ)

4. DAO Tokens

- Dash (DASH)
- Compound (COMP)
- 0x (ZRX)

5. Decentralized Exchange Tokens

- PancakeSwap (CAKE)
- SushiSwap (SUSHI)
- THORChain (RUNE)

6. DeFi Tokens

- Uniswap (UNI)
- Chainlink (LINK)
- Aave (AAVE)

7. Derivatives Tokens

- UMA (UMA)
- Serum (SRM)
- Injective Protocol (INJ)

8. Enterprise Solutions Tokens

- Bitcoin Cash (BCH)
- EOS (EOS)
- Tezos (XTZ)

9. Governance Tokens

- Uniswap (UNI)
- Aave (AAVE)
- Maker (MKR)

10. Identity Tokens

- Ontology (ONT)
- Energy Web Token (EWT)
- Civic (CVC)

11. IoT Tokens

- VeChain (VET)
- IOTA (MIOTA)
- DigiByte (DGB)

12. Lending / Borrowing Tokens

- Kava.io (KAVA)
- RAMP (RAMP)
- bZx Protocol (BZRX)

13. Logistics Tokens

- VeChain (VET)
- OriginTrail (TRAC)
- Morpheus.Network (MRPH)

14. Marketplace Tokens

- Bitcoin Cash (BNB)
- Hedera Hashgraph (HBAR)
- UNUS SED LEO (LEO)

15. Medium of Exchange Tokens

- XRP (XRP)
- Litecoin (LTC)
- Stellar (XLM)

16. Payments Tokens

- Dogecoin (DOGE)
- Crypto.com Coin (CRO)
- TRON (TRX)

17. Platform Tokens

- Solana (SOL)
- Cosmos (ATOM)
- BitTorrent (BTT)

18. Privacy Tokens

- Monero (XMR)
- Dash (DASH)
- Zcash (ZEC)

19. Rebase Tokens

- Ampleforth (AMPL)
- Empty Set Dollar (ESD)
- DIGG (DIGG)

20. Services Tokens

- Synthetix (SNX)
- Nexo (NEXO)
- Dent (DENT)

21. Smart Contract Tokens

- Ethereum (ETH)
- Cardano (ADA)
- Chainlink (LINK)

22. Stablecoins

- Tether (USDT)
- USD Coin (USDC)
- Wrapped Bitcoin (WBTC)

23. State Channels Tokens

- Polygon (MATIC)
- OMG Network (OMG)
- Celer Network (CELR)

24. Storage Tokens

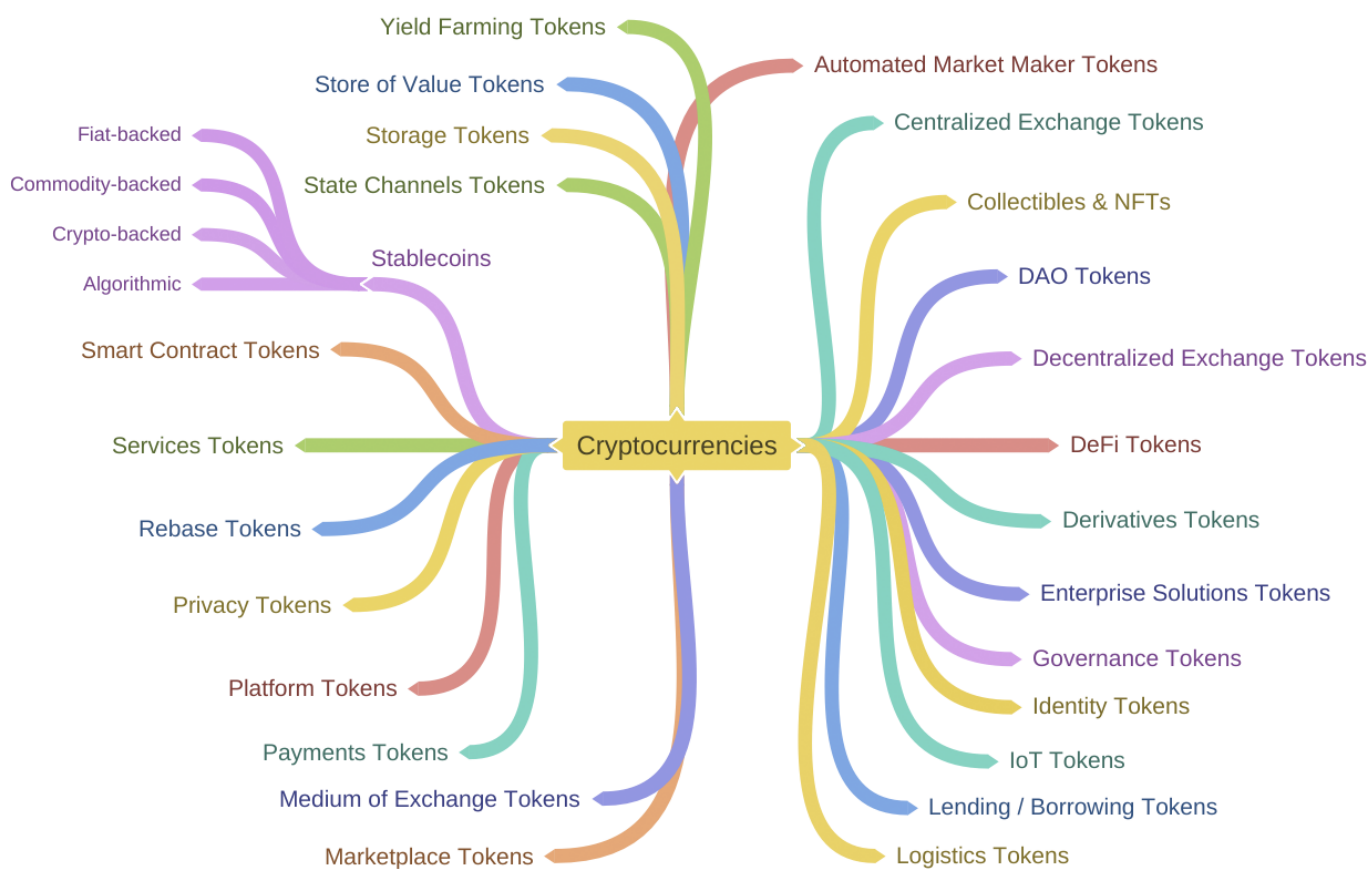
- Filecoin (FIL)
- BitTorrent (BTT)
- Holo (HOT)

25. Store of Value Tokens

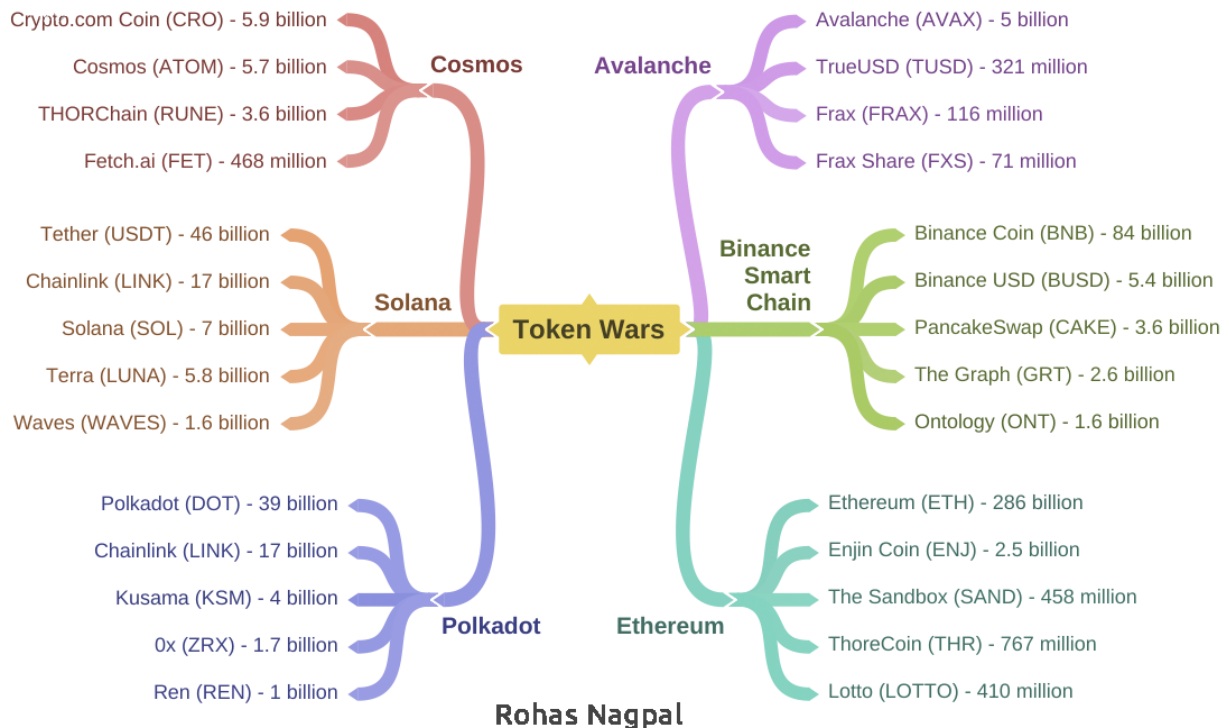
- Bitcoin (BTC)
- Bitcoin SV (BSV)
- Decred (DCR)

26. Yield Farming Tokens

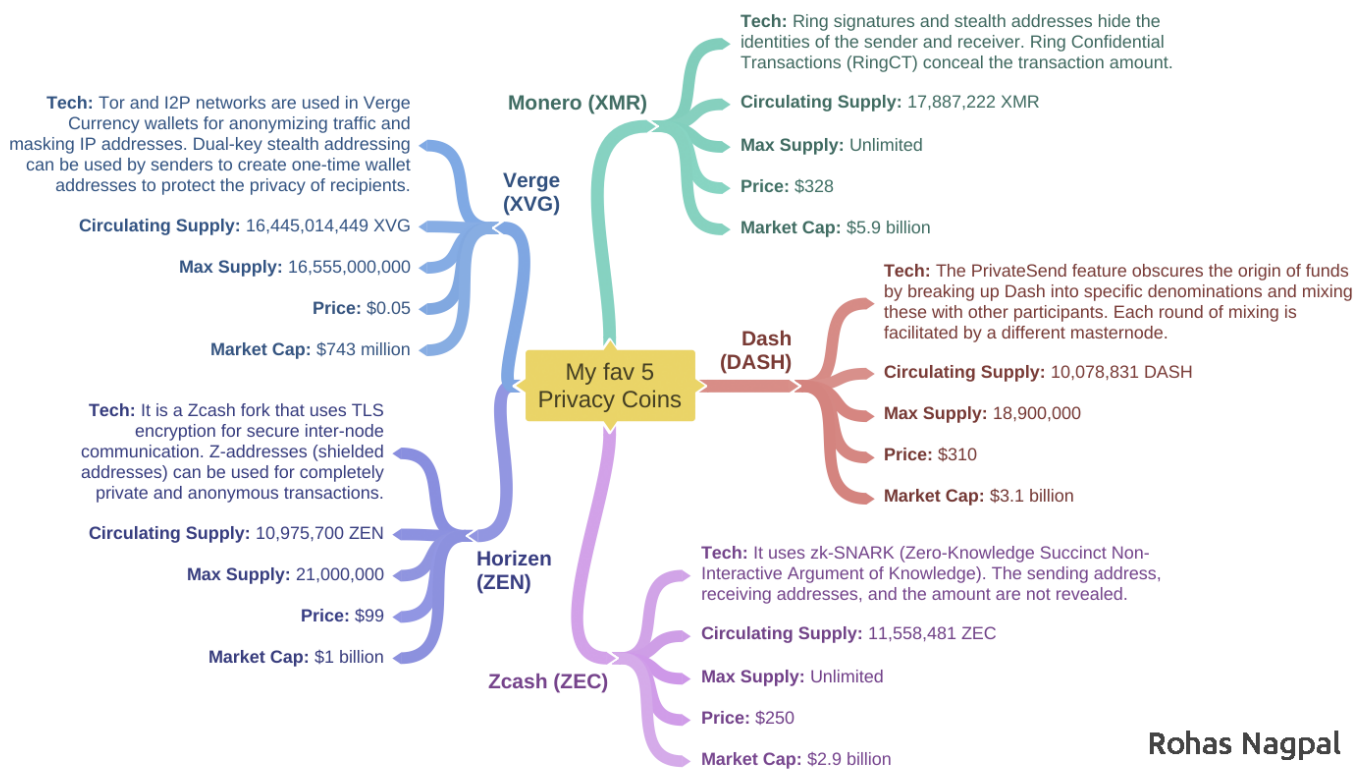
- yearn.finance (YFI)
- Curve DAO Token (CRV)
- Venus (XVS)



Mind map of the types of cryptocurrencies



This mindmap shows the market caps (in US\$)
of the most important tokens across 6 blockchains



Rohas Nagpal

Mindmap of my top 5 favourite privacy coins

The 20 cryptos to watch for in 2021

(In alphabetical order)

1. Aave (AAVE)
2. Basic Attention Token (BAT)
3. Binance Coin (BNB)
4. Bitcoin (BTC)
5. Chiliz (CHZ)
6. Polkadot (DOT)
7. Enjin Coin (ENJ)
8. Ethereum (ETH)
9. Electroneum (ETN)
10. Chainlink (LINK)
11. Polygon (MATIC)
12. Synthetix (SNX)
13. Solana (SOL)
14. Standard Tokenization Protocol (STPT)
15. SushiSwap (SUSHI)
16. Swipe (SXP)
17. THETA (THETA)
18. Uniswap (UNI)
19. VeChain (VET)
20. yearn finance (YFI)

1. AAVE

Aave is a decentralized non-custodial liquidity market protocol.

Users can deposit their preferred asset and earn passive income which is based on the market borrowing demand.

Depositing assets allows users to borrow by using their deposited assets as collateral.

User's funds are allocated in a smart contract and can be exported in tokenized versions (aTokens). These aTokens can be traded like cryptographic assets on Ethereum.

Aave interest bearing tokens (aTokens for short) are minted upon deposit and burned when redeemed. The aTokens are pegged 1:1 to the value of the underlying asset that is deposited in Aave protocol. ATokens, such as aDai, can be freely stored, transferred, and traded.

While the underlying asset is loaned out to borrowers, ATokens accrue interest in real time, directly in your wallet! Seriously, you can watch your balance grow every minute.

In its Nov 2017 ICO, US\$16.2 million was raised by selling 1 billion AAVE tokens @ \$0.0162. 23% of AAVE tokens were assigned to its founders and project.

AAVE tokens have been built based on the ERC-20 standard, and they are designed to be deflationary. In the event of a shortfall in the DeFi protocol, staked tokens would be used as collateral as a last resort.

In 2020, there was a token swap in which 1.3 billion AAVE tokens in circulation were swapped for the newly minted AAVE cryptocurrency at a ratio of 1:100, creating a total supply of 16 million AAVE.

Consensus:	Ethereum ERC 20 token
Max supply	16,000,000 (16 million)
Official website	https://aave.com/
Details:	https://coinmarketcap.com/currencies/aave/



2. BAT

Basic Attention Token (BAT) powers a blockchain-based digital advertising platform that rewards users for their attention, and provides advertisers with a better return on their ad spend.

This experience is delivered through the Brave Browser, where users can earn BAT for watching privacy-preserving ads. BAT is the unit of reward in this advertising ecosystem, and is exchanged between advertisers, publishers and users.

BAT has seen good results since its integration into the Brave browser's first global private ad platform:

- 22.2 million monthly active users,
- 7.4 million daily active users,
- 1 million verified creators accepting BAT,
- millions of wallets created,
- thousands of ad campaigns with leading brands, and
- growing utility in the most innovative names in blockchain gaming.

In its 2017 ICO, a total of 1 billion BAT tokens were sold to investors. 200 million tokens were locked in a development pool, and 300 million BAT was reserved for the user growth pool.

Consensus	Ethereum ERC 20 token
Max supply	-
Official website	https://basicattentiontoken.org/
Details:	https://coinmarketcap.com/currencies/basic-attention-token/



CoinMarketCap

3. BNB

Binance Coin (BNB) was launched through an ICO in 2017, 11 days before the Binance cryptocurrency exchange went online. BNB was originally issued as an ERC-20 token. Later, the ERC-20 BNB coins were swapped with BEP2 BNB on a 1:1 ratio in April 2019 with the launch of the Binance Chain mainnet, and they are now no longer hosted on Ethereum.

BNB can be used as a payment method, a utility token to pay for fees on the Binance exchange and for participation in token sales on the Binance Launchpad. BNB also powers the Binance DEX (decentralized exchange).

Consensus:	Byzantine Fault Tolerance (BFT)
Max supply	170,532,785
Official website	https://www.binance.com/
Details:	https://coinmarketcap.com/currencies/binance-coin/



4. BTC

According to its whitepaper, Bitcoin (BTC) started out as a medium of exchange - "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party".

Over time BTC has grown into a store of value.

Bitcoin's total supply is limited by its software to 21 million. New coins issued as rewards to "miners". On launch, the reward was 50 bitcoins per block: this number gets halved with every 210,000 new blocks mined — which takes around 4 years. As of 2021, the block reward is 6.25 bitcoins.

Bitcoin has not been pre-mined, meaning that no coins have been distributed between the founders before Bitcoin became available to the public.

Consensus	Proof of work
Max supply	21,000,000 (21 million)
Official website	https://bitcoin.org
Details:	https://coinmarketcap.com/currencies/bitcoin



5. CHZ

Chiliz (CHZ) powers Socios.com which enables sports and esports fans to crowd-manage their favorite teams, games, leagues, and events.

Chiliz is one of the largest blockchains for esports and gaming crowdfunding and was officially launched in 2019.

Chiliz and Socios.com allow sports fans to participate in the management of their favorite teams. By buying fan tokens, users secure voting rights and participate in votes announced by the teams on Socios.com. This further boosts the decentralization features offered by the Chiliz blockchain.

Chiliz (CHZ) has a total and maximum supply of 8,888,888,888 tokens.

Of the total CHZ token supply, 34.5% were distributed through a pre-sale event and additional token sales. Another 20% of tokens were set aside as a user base reserve, dedicated for future users of the Socios.com platform. Around a sixth of all tokens were directed towards strategic acquisitions. About 7.5% of CHZ tokens were given as an incentive to seed investors. Finally, 5% of tokens were given as a reward to the team and 3% were distributed among the advisors of the project.

Consensus:	Proof-of-authority (PoA)
Max supply	8,888,888,888 \$CHZ (8.8 Billion)
Official website	https://www.chiliz.com/
Details:	https://coinmarketcap.com/currencies/chiliz/



6. DOT

Polkadot facilitates the cross-chain transfer of all data and asset types. It connects public and private chains, permissionless networks, oracles and future technologies. This allows independent blockchains to trustlessly share information and transactions through the Polkadot relay chain.

DOT is Polkadot's native token and provides network governance & operations, and creating parachains (parallel chains).

There are currently a little over 918 million DOT tokens.

Some of the important features of Polkadot are:

- enabling cross-blockchain transfers of any type of data or asset, not just tokens;
- economic scalability by enabling a common set of validators to secure multiple blockchains;
- custom blockchains can be created in minutes using the Substrate framework;
- upgrade without hard forks to integrate new features or fix bugs;

Consensus:	NPoS (nominated proof-of-stake)
Max supply	-
Official website	https://polkadot.network/
Details:	https://coinmarketcap.com/currencies/polkadot-new/



7. ENJ

Enjin Coin (ENJ) is a project of Enjin, which provides an ecosystem of interconnected, blockchain-based gaming products.

Enjin's flagship offering is the Enjin Network, a social gaming platform through which users can create websites and clans, chat, and host virtual item stores.

Enjin allows game developers to tokenize in-game items on the Ethereum blockchain. It uses ENJ, an ERC-20 token, to back the digital assets issued using its platform. This ensures that items can be bought, sold and traded with real-world value.

Every token minted with Enjin Platform, is directly backed by ENJ, giving in-game items real-world liquidity.

ENJ uses a series of smart contracts to which game developers send ENJ to mint new, unique fungible or non-fungible ERC-1155 tokens. These tokens can be traded on the Enjin Marketplace, or exchanged for their backing ENJ at any time.

As more custom tokens are minted, more ENJ is removed from the ecosystem, thus making it scarcer.

Consensus:	Nominated Proof-of-Stake (NPoS)
Max supply	1,000,000,000 (1 billion)
Official website	https://enjin.io/
Details:	https://coinmarketcap.com/currencies/enjin-coin/



8. ETH

Ethereum is a decentralized open-source blockchain system for decentralized applications. Its native cryptocurrency is Ether (ETH).

Ethereum has pioneered the concept of a blockchain smart contract platform.

Ethereum's blockchain hosts other cryptocurrencies, called "tokens" through the use of its ERC-20 standard. More than 300,000 ERC-20-compliant tokens have been launched.

As of March 2021, there are over 115 million ETH coins in circulation. 72 million coins were issued in the genesis block.

The total supply of ETH is not limited.

Ethereum will be transitioning from a Proof-of-Work blockchain to a Proof-of-Stake algorithm.

Consensus:	Ethash proof-of-work algorithm
Max supply	-
Official website	https://www.ethereum.org/
Details:	https://coinmarketcap.com/currencies/ethereum/



9. ETN

Electroneum is a mobile-phone-based crypto platform that offers an instant payment system. It was launched in September 2017 after completing a \$40 million ICO.

Electroneum's goal is to provide the quickest and safest crypto transactions with minimal fees for the world's unbanked population. In April 2018, it secured a patent for instant crypto transactions.

Electroneum's total and circulating supply is limited to 21 billion.

Electroneum's miners are hand-picked by the project to ensure that there are only reliable miners in the Electroneum network. Electroneum's proof-of-responsibility algorithm reduces the amount of energy required for the mining process. Hash rates are less than half a kilo hash on the network.

Consensus:	Proof-of-responsibility
Max supply	21,000,000,000 (21 billion)
Official website	http://electroneum.com
Details:	https://coinmarketcap.com/currencies/electroneum/



10. LINK

Chainlink is a decentralized oracle network which connects smart contracts with data from the real world. It bridges the gap between blockchain technology-based smart contracts and real world applications. Since blockchains cannot access data outside their network, oracles are needed to function as data feeds in smart contracts.

Oracles provide external data (e.g. temperature, weather) that trigger smart contract executions upon the fulfillment of predefined conditions.

It raised \$32 million in a 2017 ICO with a total supply of 1 billion LINK tokens.

LINK is used to pay node operators. The Chainlink network has a reputation system. Node providers that have a large amount of LINK can be rewarded with larger contracts, while a failure to deliver accurate information results in a deduction of tokens.

Consensus:	Ethereum ERC 20 token
Max supply	1,000,000,000 (1 billion)
Official website	https://chain.link/
Details:	https://coinmarketcap.com/currencies/chainlink/



11. MATIC

Polygon (formerly Matic Network) is an Ethereum scaling and infrastructure development platform.

Polygon can be used to create:

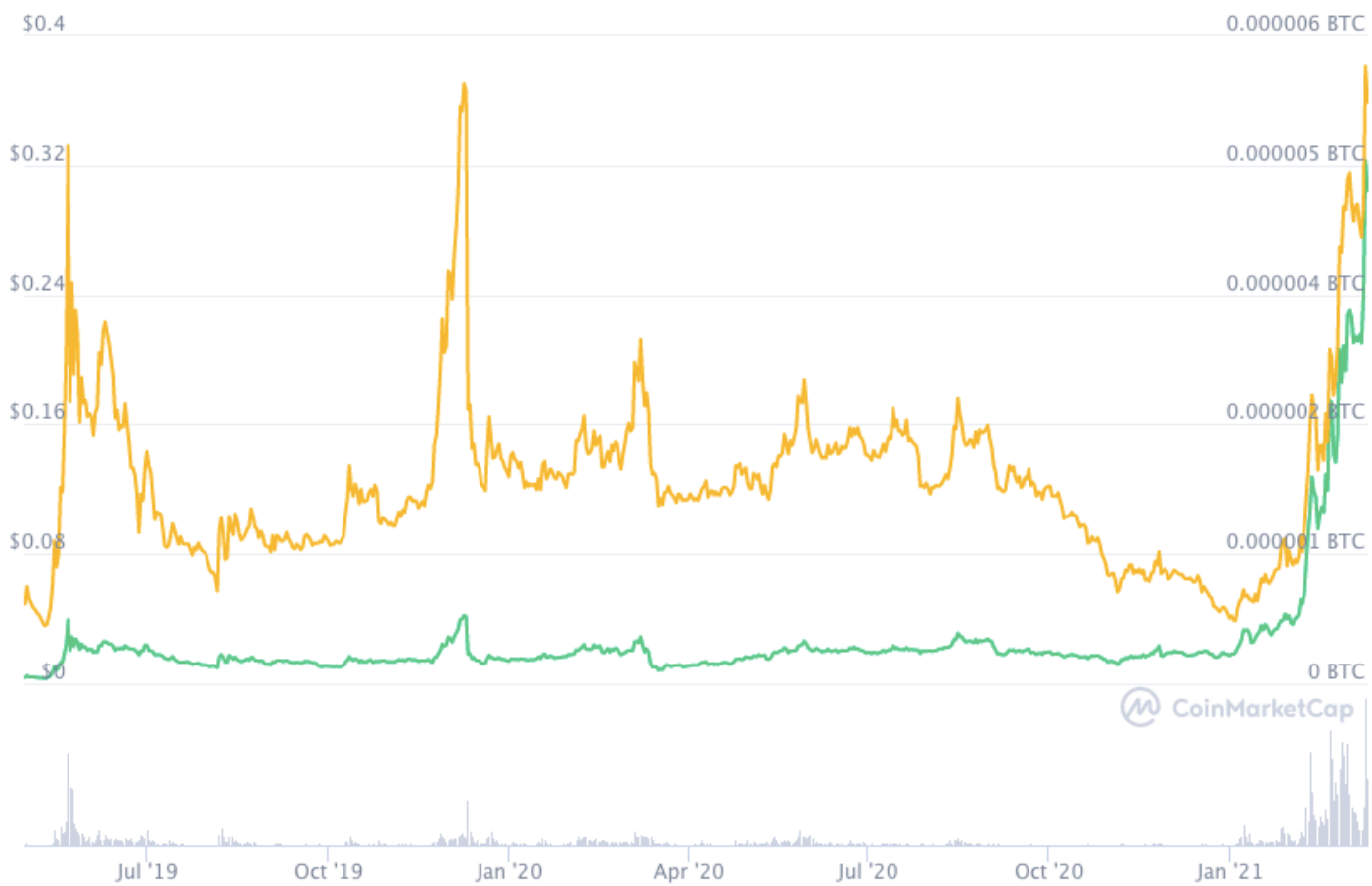
- optimistic rollup chains,
- ZK rollup chains,
- stand alone chains

Polygon effectively transforms Ethereum into a full-fledged multi-chain system like Polkadot, Cosmos, Avalanche, etc.

Polygon supports 65,000 transactions per second on a single side chain, along with a block confirmation time of less than 2 seconds.

MATIC, an ERC-20 token, is the native token of Polygon. MATIC is used for payment services on Polygon and as a settlement currency between users who operate within the Polygon ecosystem. The transaction fees on Polygon sidechains are also paid in MATIC tokens.

Consensus:	Ethereum ERC 20 token
Max supply	10,000,000,000 (10 billion)
Official website	https://matic.network
Details:	https://coinmarketcap.com/currencies/polygon



12. SNX

Synthetix is an Ethereum based decentralized finance (DeFi) protocol. It provides on-chain exposure to a variety of crypto and non-crypto assets.

It offers users access to highly liquid synthetic assets (synths). Synths track and provide returns on the underlying asset without directly hold the asset. The underlying assets are tracked using oracles.

Synthetix allows users to autonomously trade and exchange synths. It also has a staking pool where holders can stake their SNX tokens and are rewarded with a share of the transaction fees on the Synthetix Exchange.

SNX tokens are used as collateral for the synthetic assets that are minted. Whenever synths are issued, SNX tokens are locked up in a smart contract.

The Synthetix network is secured through proof-of-stake (PoS) consensus.

At the seed round and token sale stages, Synthetix sold more than 60 million tokens and raised \$30 million.

Consensus:	Ethereum ERC 20 token
Max supply	212,424,133 (~ 212 million)
Official website	https://www.synthetix.io
Details:	https://coinmarketcap.com/currencies/synthetix-network-token



13. SOL

The Solana protocol is designed to facilitate decentralized app (DApp) creation. It aims to improve scalability by introducing a proof-of-history (PoH) consensus combined with the underlying proof-of-stake (PoS) consensus of the blockchain.

Proof-of-history (PoH) is the main component of the Solana protocol, as it is responsible for the bulk of transaction processing. PoH records successful operations and the time that has passed between them, thus ensuring the trustless nature of the blockchain.

The proof-of-stake (PoS) consensus is used as a monitoring tool for the PoH processes, and it validates each sequence of blocks produced by it.

The combination of two consensus mechanisms makes Solana unique.

Solana's hybrid protocol allows for decreased validation times for both transaction and smart contract execution. The protocol is designed to have low transaction costs while guaranteeing scalability and fast processing.

Consensus:	Proof-of-history (PoH) consensus combined with proof-of-stake (PoS)
Max supply	488,630,611 (~ 489 million)
Official website	https://solana.com
Details:	https://coinmarketcap.com/currencies/solana



14. STPT

The Standard Tokenization Protocol Standard defines how ownership of tokenized assets are generated, issued, sent, and received while complying with the necessary regulations.

Some of the characteristics are:

- Enabling the issuance and trading of synthetic assets and indices on Polkadot.
- Anyone can tokenize an asset by locking up collateral in the form of stablecoin.
- Burning the amount initially issued to receive the locked collateral amount.
- Anyone can create their own basket of assets by locking up collateral in the form of stablecoin.

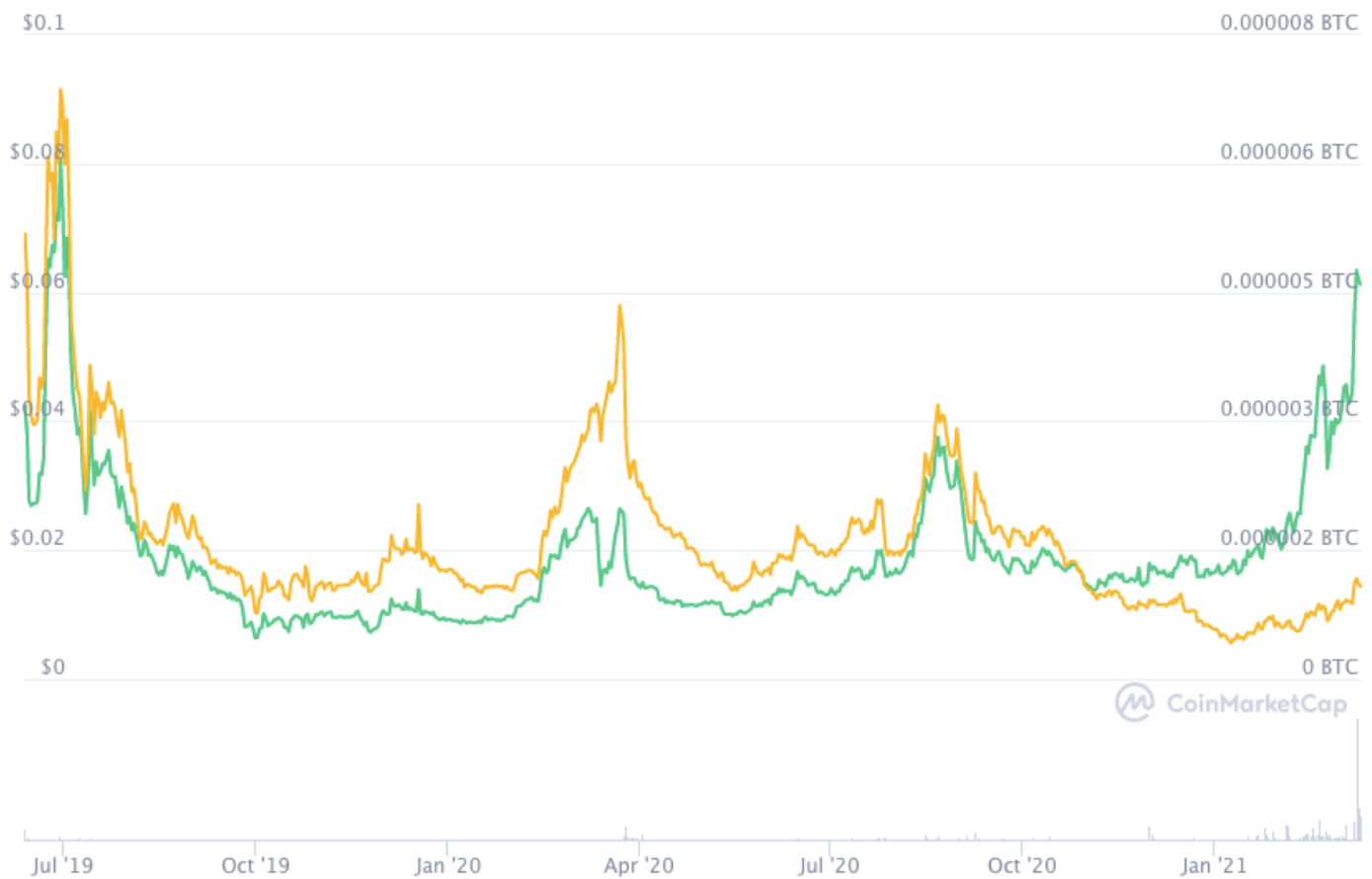
The STPT token is used on several platforms and it allows users to participate in events like airdrops, bounties, Micro Token Offerings, and virtual staking. Additionally, STPT is used as a payment currency for services within the ecosystem which comprises projects, service providers, issuers, and investors.

STP DAO is the mechanism for decentralized governance in which STPT holders will help dictate the direction of important protocol decisions including USTP and the respective DeFi platforms that utilize USTP. Users stake STPT in the STP DAO in order to create and vote on proposals.

USTP is a stablecoin designed for usage in the STP Ecosystem. It will allow users to earn yield, leverage lucrative DeFi strategies and transact across multiple platforms both within and outside our ecosystem.

USTP is over 100% backed by STPT. A greater collateral amount is required in order to reduce the risk of liquidation in case of price volatility.

Consensus:	Ethereum ERC 20 token
Max supply	-
Official website	https://stp.network/
Details:	https://coinmarketcap.com/currencies/standard-tokenization-protocol/



15. SUSHI

SushiSwap is an automated market maker (AMM) - a decentralized exchange which uses smart contracts to create markets for any given pair of tokens.

It was launched in September 2020 as a fork of Uniswap.

SushiSwap has added additional features, not previously present on Uniswap, such as increased rewards for network participants via its token, SUSHI.

The platform takes a 0.3% share from transactions occurring in its liquidity pools, while the SUSHI token is used to reward users portions of those fees. SUSHI also entitles users to governance rights.

SUSHI is created at a rate of 100 tokens per block. The first 100,000 blocks had a block reward of 1,000 SUSHI. The supply of SUSHI will depend on the block rate.

Consensus:	Ethereum ERC 20 token
Max supply	250,000,000 (250 million)
Official website	https://stp.network/
Details:	https://coinmarketcap.com/currencies/standard-tokenization-protocol/



16. SXP

Swipe is a platform that bridges the fiat and cryptocurrency worlds with 3 products:

- the Swipe multi-asset mobile wallet,
- the Swipe cryptocurrency-funded debit card and
- the Swipe Token (SXP).

The Swipe wallet can be used to:

- store and manage cryptocurrencies and fiat currencies
- manage the Swipe debit card.

The debit card allows users to spend their cryptocurrencies at Visa payment terminals.

The Swipe Token (SXP) functions as the fuel for the Swipe Network, and is used for paying transaction fees. Users need to hold a fixed minimum amount of SXP to be eligible to purchase a Swipe Sky, Steel or Slate debit card.

SXP can also be used for creating and voting on governance proposals, allowing holders to help shape the development of the Swipe ecosystem.

Consensus:	Ethereum ERC 20 token
Max supply	289,266,978 (~ 289 million)
Official website	https://swipe.io/token
Details:	https://coinmarketcap.com/currencies/swipe/



17. THETA

Theta is a blockchain powered network to decentralize video streaming, data delivery and edge computing, making it more efficient, cost-effective and fair for industry participants

The Theta mainnet operates as a decentralized network in which users share bandwidth and computing resources on a peer-to-peer (P2P) basis.

Google, Binance, Blockchain ventures, Gumi, Sony Europe and Samsung are Enterprise Validators.

The network runs on a native blockchain, with two native tokens:

- Theta (THETA), and
- Theta Fuel (TFUEL).

Theta's native cryptocurrency token THETA performs various governance tasks. TFUEL is used to power transactions. Its total supply is 5 billion.

Theta's benefits are:

- viewers get rewarded with better quality streaming service,
- content creators improve their earnings and
- video platforms save money on building infrastructure and increase advertising and subscription revenues.

Consensus:	Proof-of-Stake and multi-level Byzantine Fault Tolerance (BFT)
Max supply	1,000,000,000 (1 billion)
Official website	https://www.thetatoken.org/
Details:	https://coinmarketcap.com/currencies/theta/



18. UNI

Uniswap is an automated market maker (AMM). It aims to keep token trading automated and completely open to anyone who holds tokens, while improving the efficiency of trading versus that on traditional exchanges.

By automating the process of market making, Uniswap incentivizes activity by limiting risk and reducing costs for all parties. The mechanism also removes identity requirements for users, and technically anyone can create a liquidity pool for any pair of tokens.

In September 2020, Uniswap created and awarded its own governance token, UNI, to past users of the protocol. The total supply of UNI is 1 billion units and this will become available over 4 years. After this Uniswap will introduce a "perpetual inflation rate" of 2% to maintain network participation.

Consensus:	Ethereum ERC 20 token
Max supply	1,000,000,000 (1 billion)
Official website	https://uniswap.org/blog/uni
Details:	https://coinmarketcap.com/currencies/uniswap



19. VET

VeChain is a blockchain-powered platform that uses distributed governance and Internet of Things (IoT) technology to solve some of the major problems with supply chain management.

It aims to boost the efficiency, traceability and transparency of supply chains while reducing costs and placing more control in the hands of individual users.

VeChain has two in-house tokens: VeChain (VET) and VeThor (VTHO).

The dual-token system is designed to avoid fee fluctuations and network congestion.

VET is the token used for transactions and other activities, while VTHO provides fee payments and functions as a "gas token".

VET holders automatically generate a small amount of passive income in VTHO, while 70% of the VTHO used in a VET payment is destroyed. VTHO is generated based on VET holdings.

Consensus:	Proof of Stake & Proof of Authority
Max supply	86,712,634,466 (~86 billion)
Official website	https://www.vechain.org/
Details:	https://coinmarketcap.com/currencies/vechain/



20. YFI

Yearn.finance is an aggregator service that simplifies the decentralized finance (DeFi) industry. It was earlier known as iEarn.

The target market for yearn.finance is investors who do not have the time to study the increasingly complex DeFi phenomenon from scratch, or who wish to optimize their returns.

The platform uses various tools to act as an aggregator for DeFi protocols including Curve, Compound and Aave for bringing cryptocurrency stakers the highest possible yield.

Yearn.finance makes a profit by charging withdrawal fees and gas subsidization fees.

Yearn.finance's in-house token is YFI, which was the first cryptocurrency to become worth more than Bitcoin (BTC) per unit.

Users of yearn.finance earn YFI through providing liquidity, while token holdings dictate governance privileges.

Consensus:	Proof of Stake & Proof of Authority
Max supply	36,666 (~ 36 thousand)
Official website	https://yearn.finance
Details:	https://coinmarketcap.com/currencies/yearn-finance



CoinMarketCap

C2. 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.

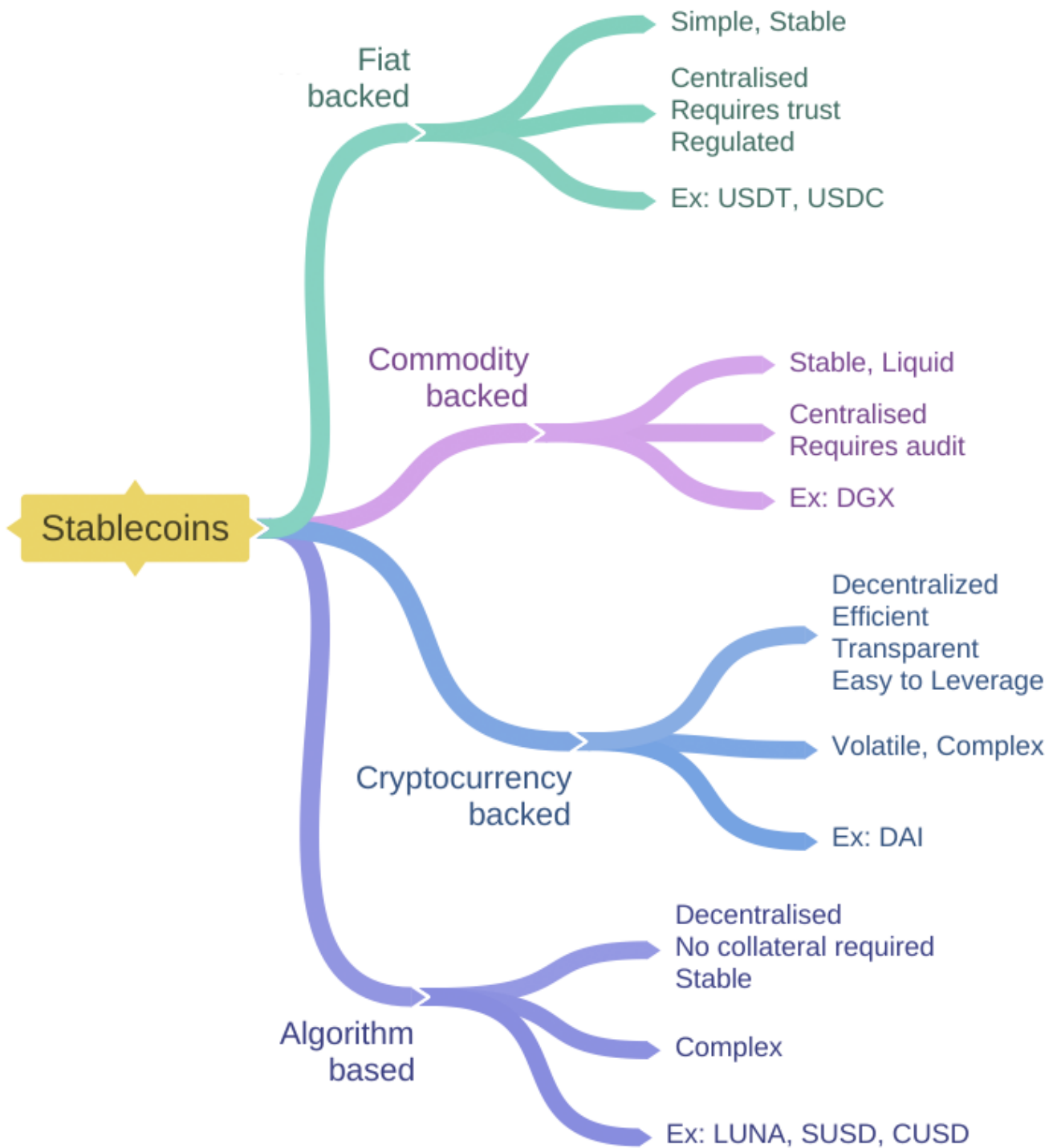
Conventional payment systems involve the movement of E-money across multiple private databases (of banks, money transfer organizations etc.). This is why typical cross-border payments involve high cost and time.

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.



Mindmap of the types of stablecoins

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>

Binance USD Charts



For the latest prices, see:

<https://coinmarketcap.com/currencies/binance-usd/>

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 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.

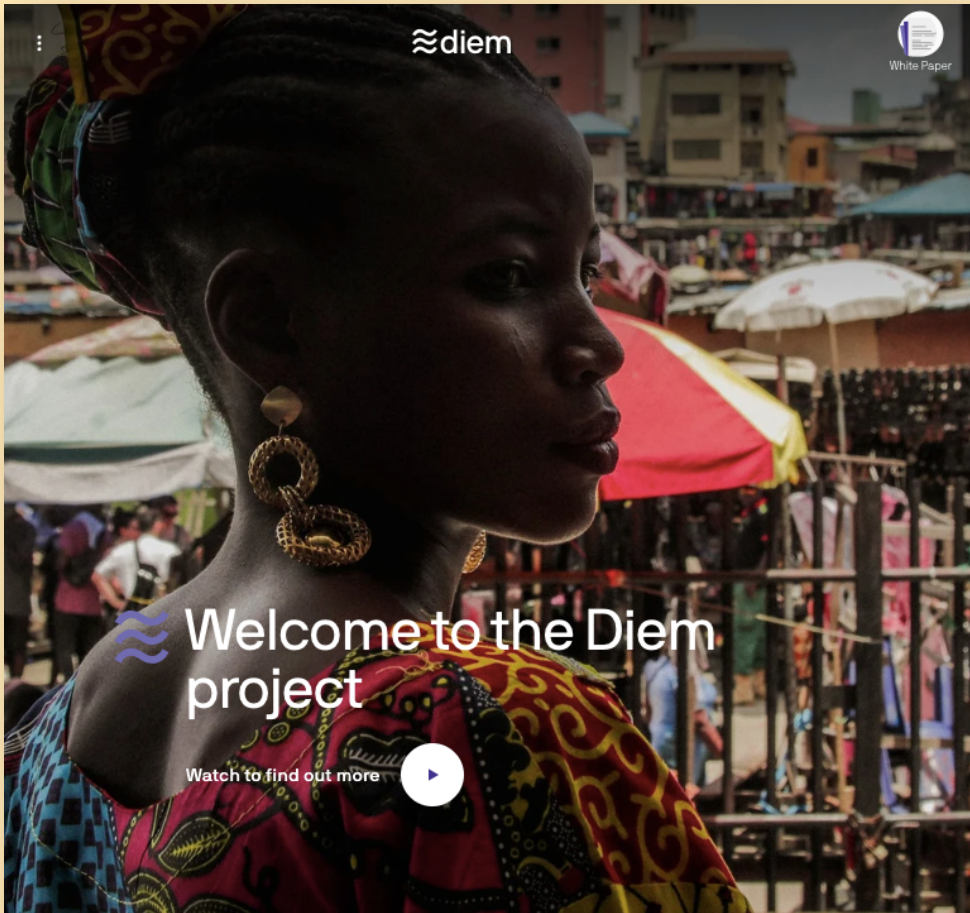
Initially, Libra was planned to be a permission-less blockchain. This would have made it easy for criminals to use it for money laundering. Since there was huge opposition from Governments and regulators, Diem will now be a permissioned blockchain. Diem will also enable Know Your Customer (KYC) for all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



Welcome to the Diem project

Watch to find out more

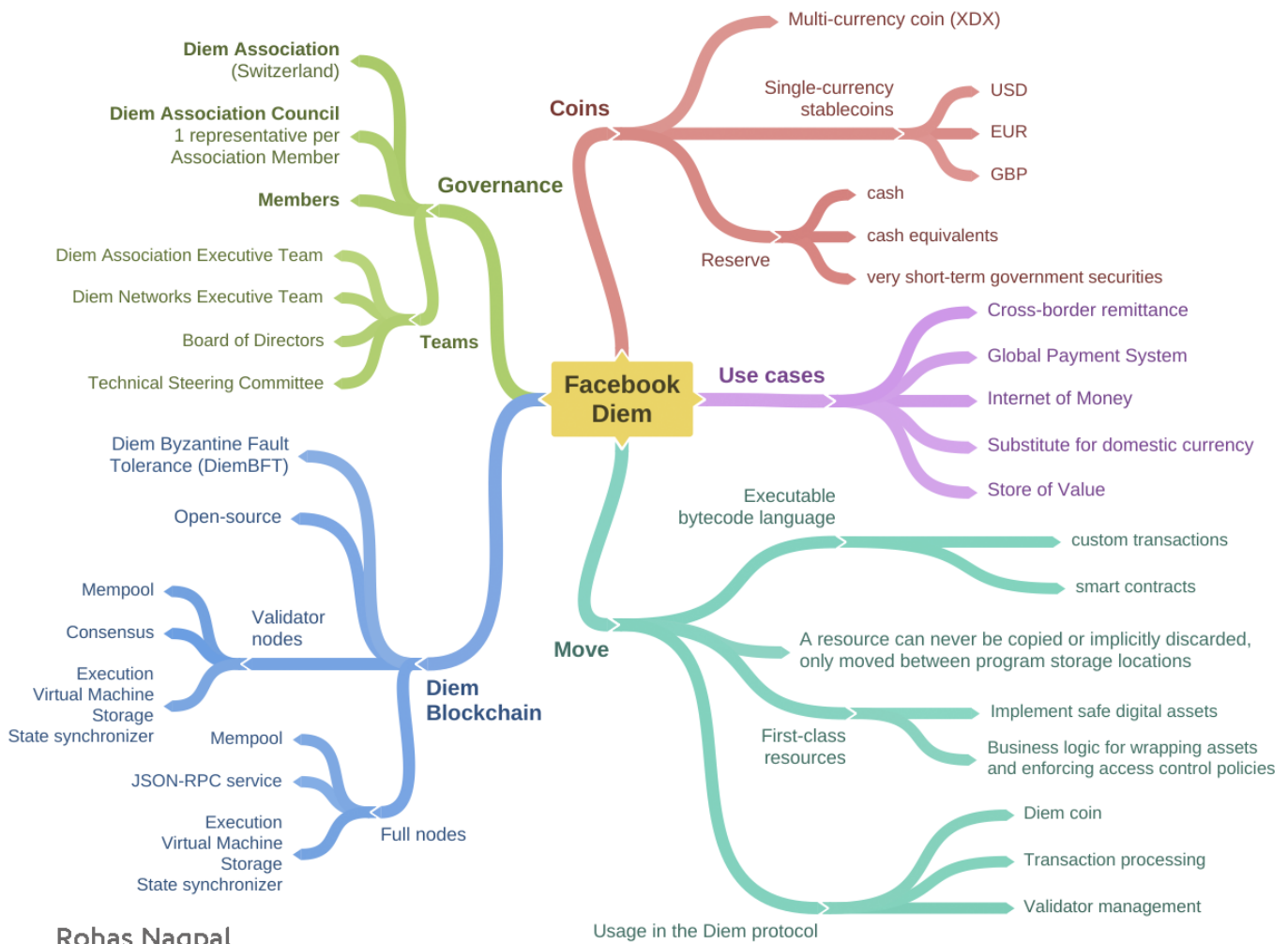


The Diem mission

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

Mindmap of Facebook Diem



**Interpretive Letter 1174
January 2021**

**OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association
Authority to Use Independent Node Verification Networks and Stablecoins for Payment
Activities**

January 4, 2021

I. Introduction and Summary Conclusion

This letter addresses the legal permissibility of certain payment-related activities that involve the use of new technologies, including the use of independent node verification networks (INVNs or networks) and stablecoins, to engage in and facilitate payment activities. National banks and Federal savings associations (collectively referred to as "banks") may use new technologies, including INVNs and related stablecoins, to perform bank-permissible functions, such as payment activities.

An INVN consists of a shared electronic database where copies of the same information are stored on multiple computers. One common form of an INVN is a distributed ledger.¹ Cryptocurrency transactions are recorded on these ledgers.² An INVN's participants, known as nodes, typically validate transactions, store transaction history, and broadcast data to other nodes.³

¹ See OCC Interpretive Letter 1170 (Jul. 22, 2020) (IL 1170) (describing distributed ledger technology as a shared electronic database where copies of the same information are stored on multiple computers. This shared database functions as both a mechanism to prevent tampering and as a way to add new information to the database. Information will not be added to the distributed ledger until consensus is reached that the information is valid. INVNs represent one of the key technologies that support the novel exchange mechanism underlying cryptocurrency. The other key technology is advanced cryptography.).

² The OCC described many features of cryptocurrency in IL 1170. In addition, the OCC recently addressed the permissibility of a national bank holding reserves for stablecoins that are backed by fiat currency on at least a 1:1 basis in situations where there is a hosted wallet. See OCC Interpretive Letter 1172 (Sept. 21, 2020) (IL 1172).

³ Nodes are generally either full nodes or light nodes. Full nodes verify transactions, maintain consensus between other nodes, and contain a full copy of the ledger's entire history. Light nodes generally consist of wallets that download only the headers of blocks to validate their authenticity and save hard drive space for users by not storing a full copy of the ledger's history. One example of a light node may be a customer's digital wallet on the customer's mobile phone. See, e.g., Josh Evans, Blockchain Nodes: An In-Depth Guide, Nodes.com (Sept. 22, 2020), available at <https://nodes.com/>; Blockchain: What are nodes and masternodes?, Medium.com (Sept. 22, 2020), available at <https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a420d938f>. A bank may want to serve as a full node on an INVN due to the wider range of capabilities on a full node as compared to a light node, as described above.











The United States Office of the Comptroller of the Currency (OCC) has allowed national banks and federal savings associations to participate in independent node verification networks (INVN) and use stablecoins to conduct payment activities and other bank-permissible functions.

See:

<https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf>

Top stablecoins by market capitalisation ⓘ

Market capitalisation is the total number of tokens that exist multiplied by the value per token. This list is dynamic and the projects listed here are not necessarily endorsed by the ethereum.org team.

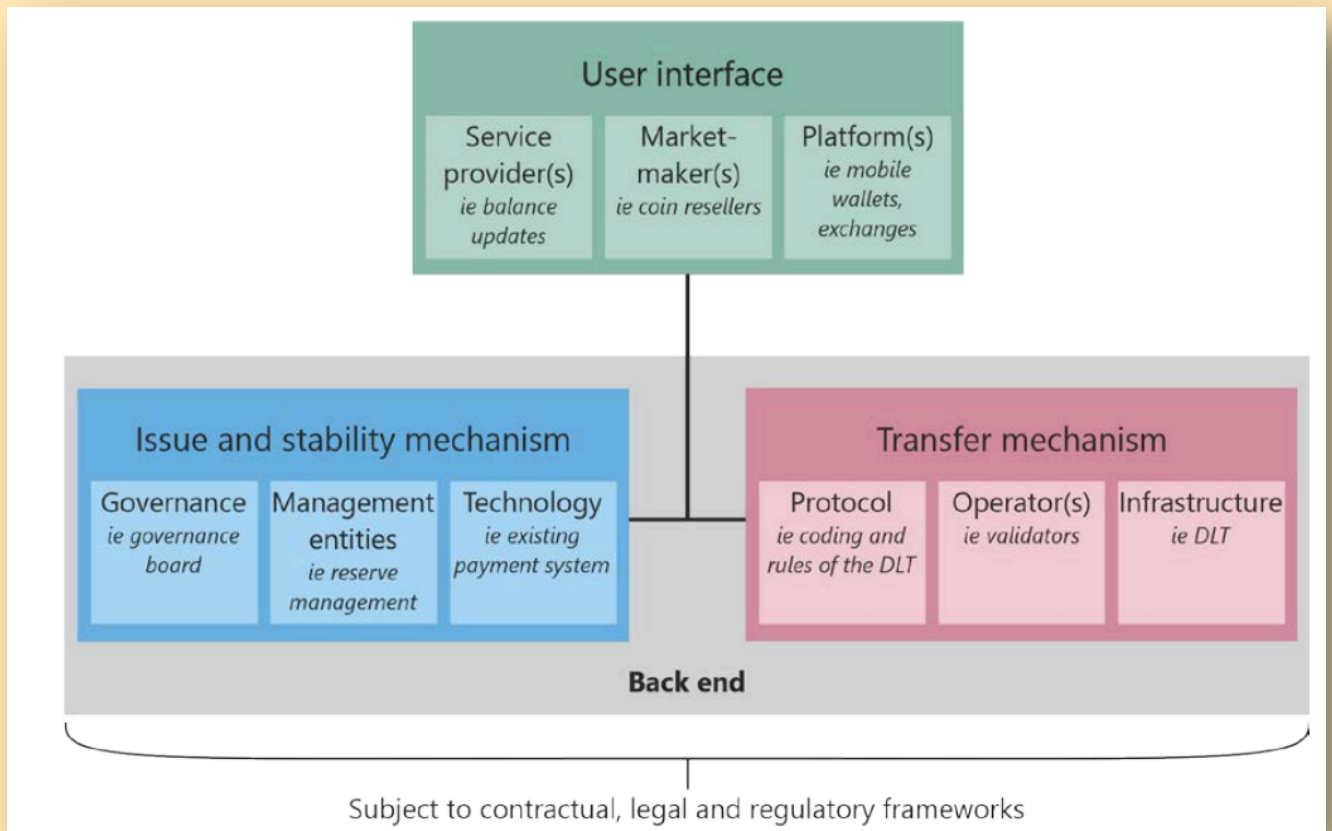
CURRENCY	MARKET CAPITALIZATION	COLLATERAL TYPE	↗
 Tether	\$33,052,072,203	Fiat	↗
 USD Coin	\$7,309,541,967	Fiat	↗
 Dai	\$2,265,280,314	Crypto	↗
 Binance USD	\$1,727,610,160	Fiat	↗
 Paxos Standard	\$705,401,915	Fiat	↗
 Ampleforth	\$502,845,771	Algorithmic	↗
 HUSD	\$500,626,376	Fiat	↗
 TrueUSD	\$320,585,214	Fiat	↗
 sUSD	\$262,173,215	Crypto	↗
 PAX Gold	\$128,346,181	Precious metals	↗

As on 18-Feb-2021

<https://ethereum.org/en/stablecoins/#explore>

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>

C3. Central Bank Digital Currency (CBDC)

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>

[Home](#)[About Us](#) ▾[Individual](#)[Merchants](#)[Fin-Tech](#)[Media Room](#) ▾[FAQ's](#)[Contact Us](#)

Digital Bahamian Dollar

Inclusive | Convenient | Secure

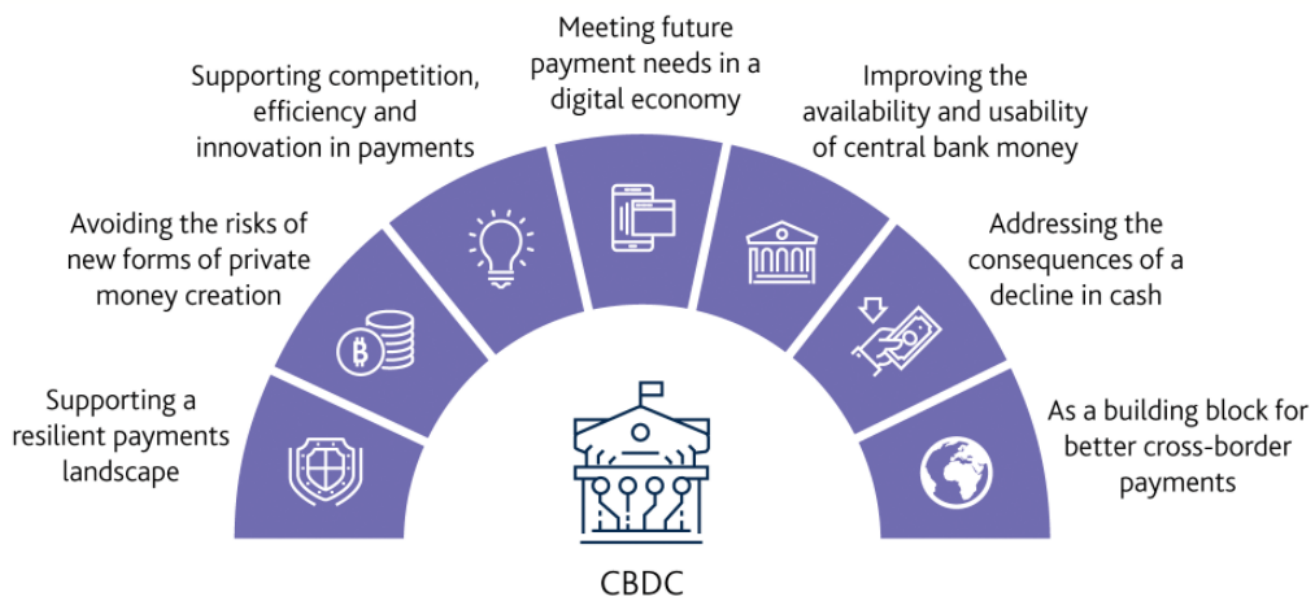
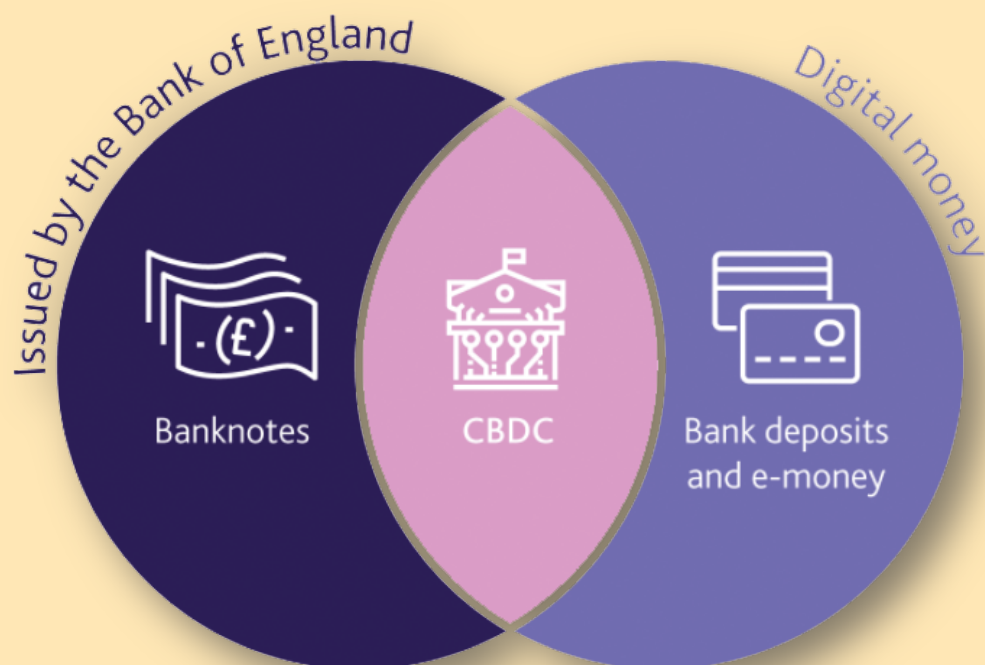


This site uses cookies: [Find out more](#)

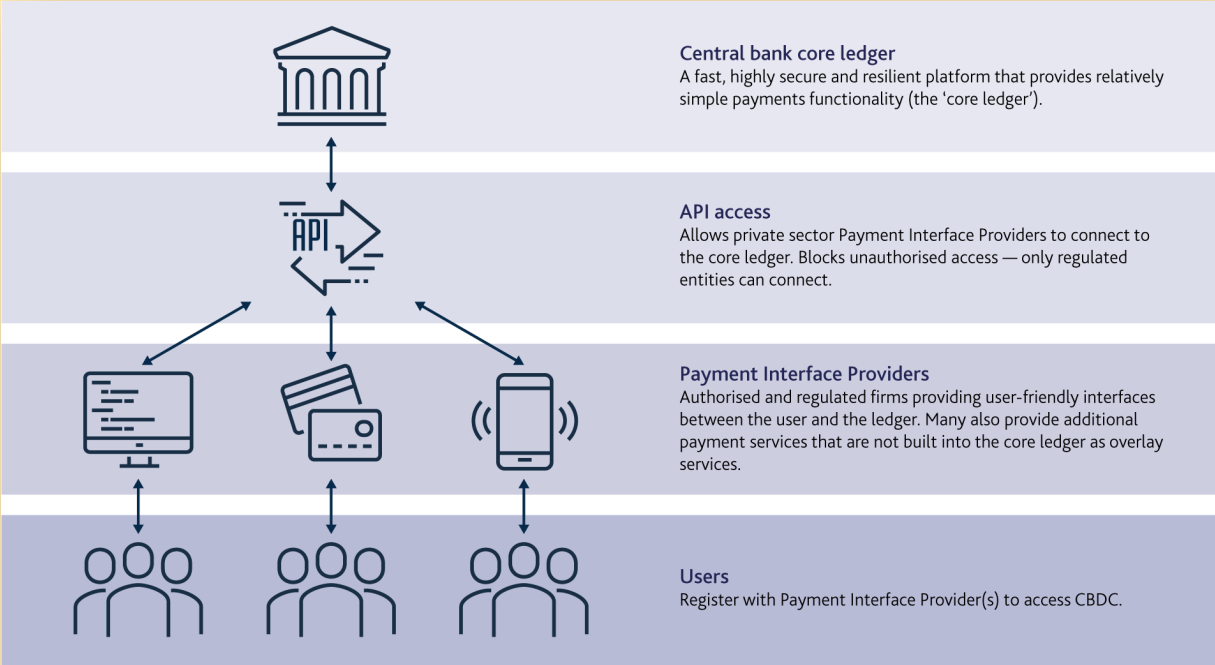
Okay, Thanks

Sand Dollar is the digital version of the Bahamian dollar (B\$).
Like cash, Sand Dollar is issued by the Central Bank of The Bahamas
through authorised financial institutions (AFIs).

<https://www.sanddollar.bs>



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.

PwC CBDC global index

1st Edition

April 2021



The PwC Global CBDC Index measures central banks' level of maturity in deploying their own digital currency.

<https://pwc.to/3dAmaWs>

C4. Non-Fungible Token (NFT)

The INR balance in your mobile wallet is fungible - every rupee is exactly the same as another rupee. Any one rupee can be exchanged for another one rupee. Things like real estate and art are non-fungible because no two of them are identical.

Non-Fungible Tokens (NFT) are the crypto versions of things like art, and real-estate. They are used as digital proof-of-ownership of the underlying asset.

Let's answer some frequently asked questions.

1. What is a Non-Fungible Token (NFT)?

An NFT is a unique token on a blockchain. It can be attached to any asset (tangible or not) to verify its authenticity and ownership.

Example: When you buy a book, you can read it. But you cannot translate it into another language and start selling the translated version. With an NFT, the author can give you translation and other rights.

2. What is minting?

Minting is the process of tokenizing an asset and creating the NFT. This can be done by the creator of the work or an authorized person.

3. What are the legal rights of a buyer of an NFT?

Depending upon the NFT, the buyer may get the rights to own, sell, lend, monetize, etc.

4. Why do we need NFTs

Intellectual property markets have complex licensing & paperwork requirements. NFTs enable quick tokenization and monetization of IP.

5. What are the types of NFTs

NFTs can be of many types, including:

- art,
- collectibles (trading cards, sneakers)
- domains,
- financial instruments
- IP assets - trademarks, patents etc
- music,
- photos,
- tokenized assets (cars, land, oil)
- videos of iconic events
- virtual game items (avatars, skins, weapons, etc)

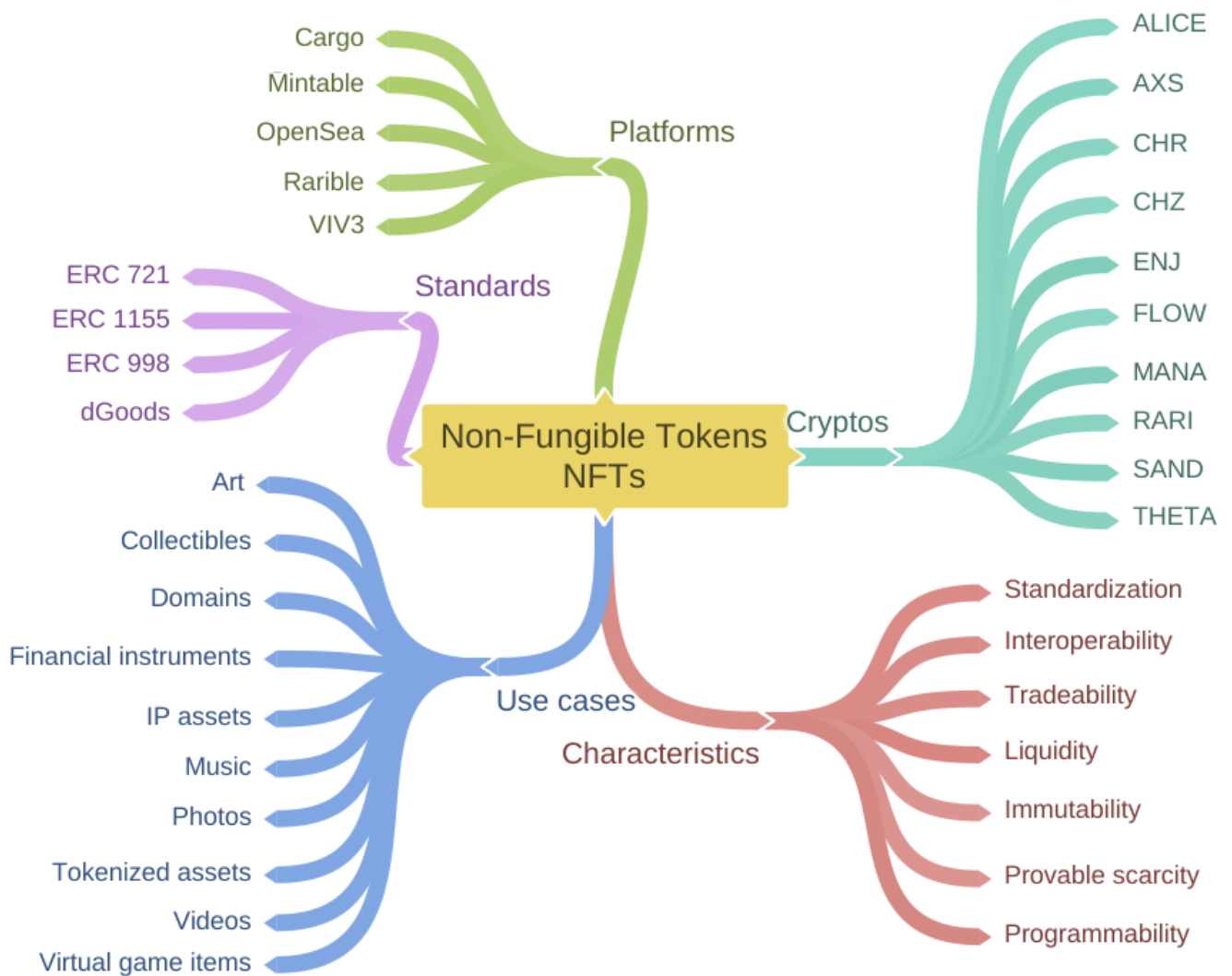
6. Which are some NFT platforms?

Ethereum: Cargo, Mintable, OpenSea, Rarible

Flow: VIV3

According to OpenSea's NFT Bible, the characteristics of NFTs are:

1. **Standardization:** Conventional digital assets (in-game collectibles, event tickets, domain names, etc) are very different from each other. But when they are represented as NFTs on public blockchains, they can have common, reusable, and inheritable standards for ownership, transfer, and access control.
2. **Interoperability:** NFTs can easily move across multiple ecosystems, different wallet providers. They are tradeable on marketplaces and can be displayed inside virtual worlds.
3. **Tradeability:** NFTs enable digital assets to move outside their original environments and into marketplaces with sophisticated trading capabilities e.g. eBay-style auctions, bidding, bundling, and the ability to sell in any currency.
4. **Liquidity:** Instant tradeability of NFTs leads to higher liquidity.
5. **Immutability & provable scarcity:** Smart contracts enable the placing of hard caps on the supply of NFTs and the enforcement of persistent properties that cannot be modified.
6. **Programmability:** NFTs are fully programmable and have complex mechanics like forging, crafting, redeeming, random generation, etc.



Mindmap of NFTs

NFT Standards

ERC-721

<https://ethereum.org/en/developers/docs/standards/tokens/erc-721/>

ERC-1155

<https://eips.ethereum.org/EIPS/eip-1155>

ERC-998

<https://github.com/ethereum/eips/issues/998>

dGoods

<https://dgoods.org/>

Metadata

NFT metadata can be stored on-chain or off-chain.

In the case of on-chain storage, the metadata is baked directly into the smart contract representing the tokens. The benefits are:

- the metadata permanently resides with the token,
- the metadata can change in accordance with on-chain logic.

In the case of digital art, keeping the metadata on-chain ensures that it will persist even if the original website does not.

In most cases, metadata is stored off-chain because of the storage limitations of Ethereum. In this case, the metadata can be stored on centralized servers (e.g. cloud servers) or InterPlanetary File System (IPFS)

– see: <https://ipfs.io/>

10 NFTs to watch for in 2021

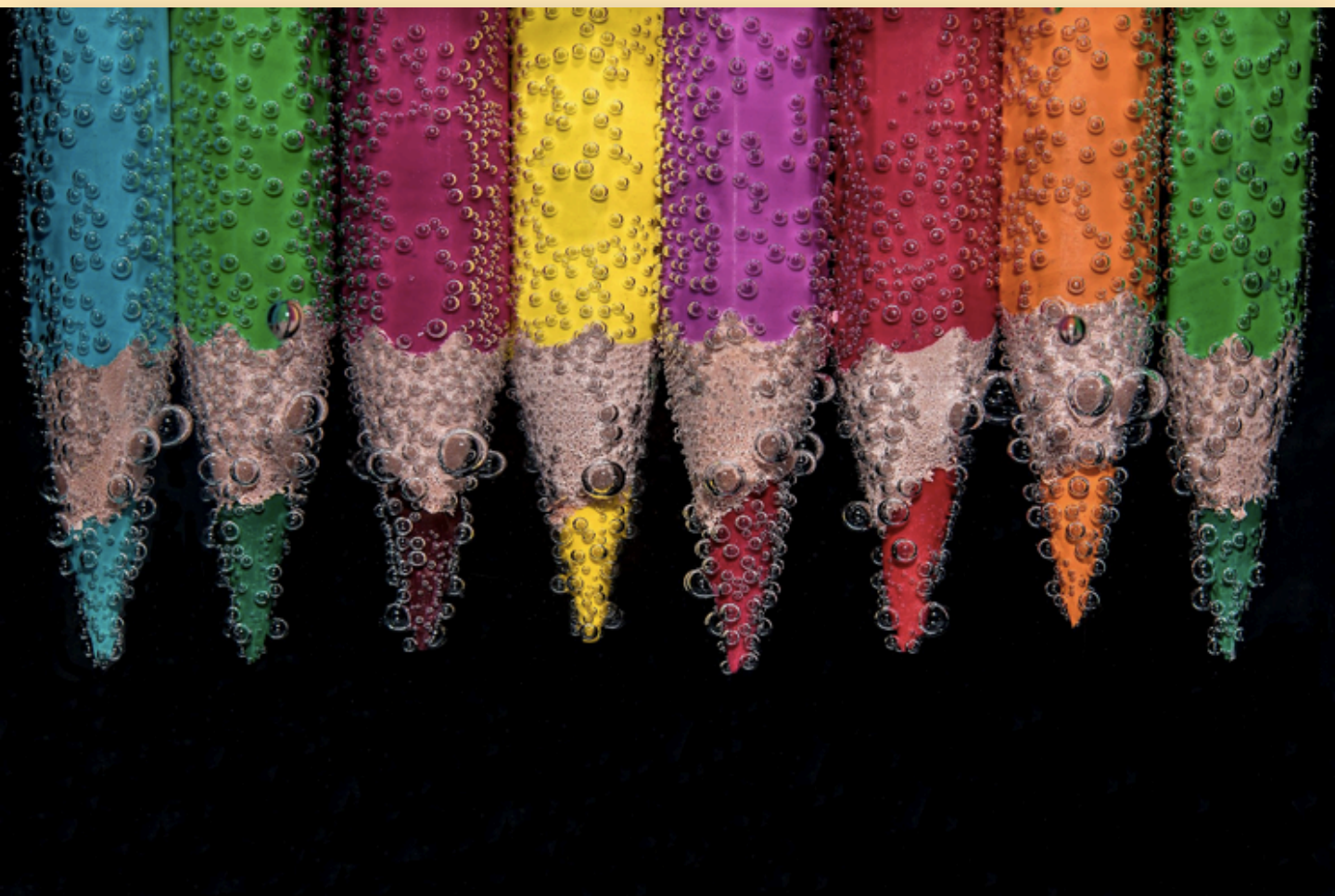
1. MyNeighborAlice (ALICE)
2. Axie Infinity (AXS)
3. Chromia (CHR)
4. Chiliz (CHZ)
5. Enjin Coin (ENJ)
6. Flow (FLOW)
7. Decentraland (MANA)
8. Rarible (RARI)
9. The Sandbox (SAND)
10. THETA (THETA)



Webinar on NFTs (Non-Fungible Tokens)

Rohas Nagpal

<https://youtu.be/kycdsq6550E?t=60>



Guide to Non-Fungible Tokens (NFT)

<https://www.linkedin.com/pulse/guide-non-fungible-tokens-nft-rohas-nagpal>



CryptoKitties

Collect and breed furrever friends!



Get your own Kitty

- 👤 Buy & sell cats with our community
- 🧩 Crack puzzles alongside other players
- 📁 Create collections & earn rewards
- 🎮 Chase limited edition Fancy cats
- 🌱 Breed adorable cats & unlock rare traits
- 🎮 Play games in the KittyVerse



What is CryptoKitties?

CryptoKitties is a game centered around breedable, collectible, and oh-so-adorable creatures we call CryptoKitties! Each cat is one-of-a-kind and 100% owned by you; it cannot be replicated, taken away, or destroyed.

Your place to create, share, sell and buy digital collectibles.

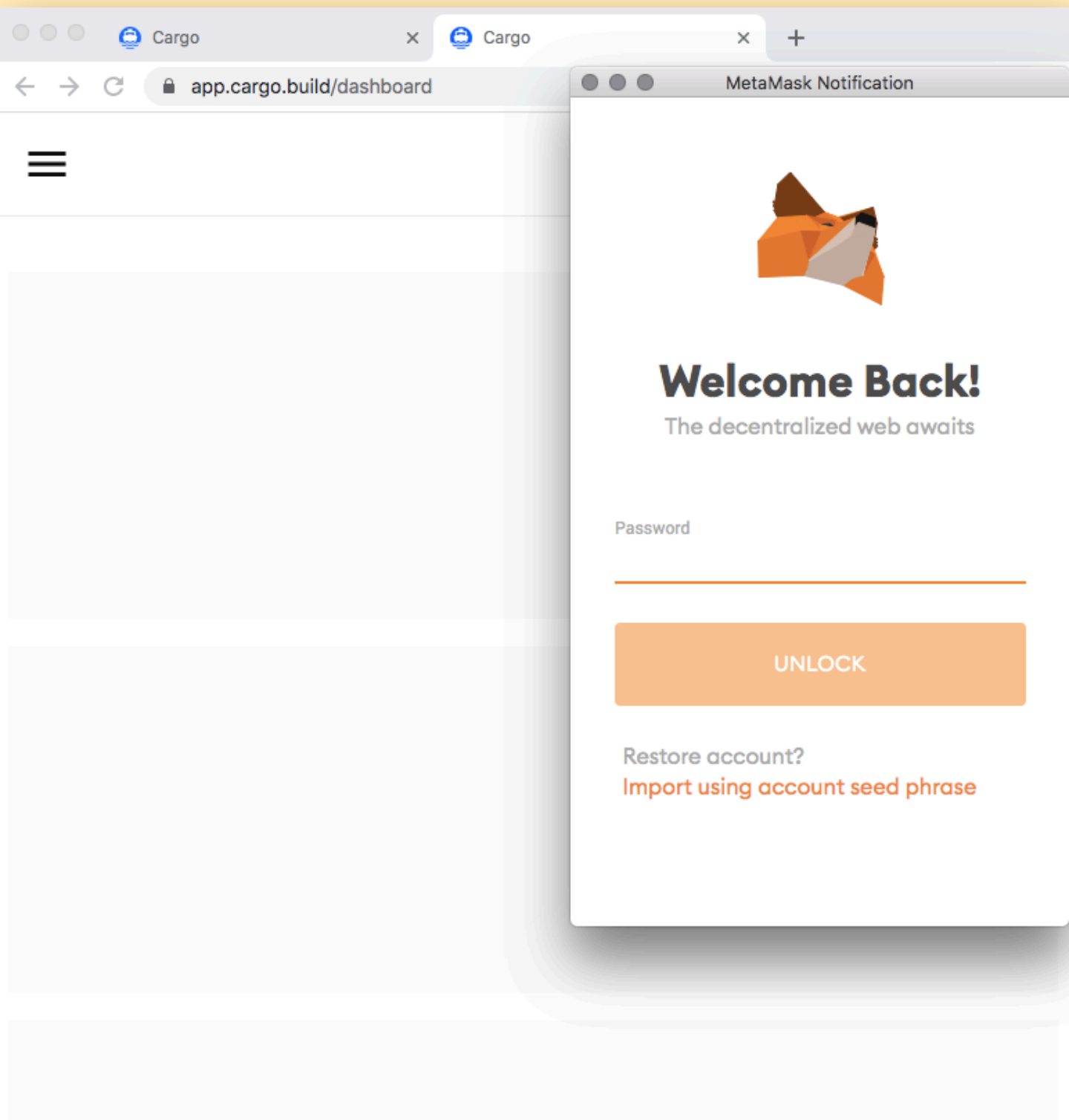
Securely manage and sell your digital
collectibles all in a single place.

Browse the Marketplace





Start Creating






<https://cargo.build/>



Navigation

 [Dashboard](#) [Projects](#) [Showcases](#) [Profile Page](#) [Orders](#) [Log out](#)

More

 [Marketplace](#) [Gem Portal](#) [Proposals](#) [Docs](#)

Your Projects

[Learn more](#)[View all](#)[+ Create your first project](#)

Your Showcases

[Learn more](#)[View all](#)[+ Create a showcase](#)

More Tools

Magic Minting

Gas free NFT creation. Sell, or transfer immediately. NFTs are held in a secure custodial wallet. Cost: Pay \$1.99 with a credit card.

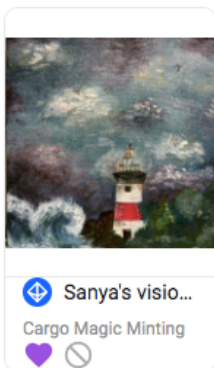
[Create](#)[Learn more](#)

Single NFT

Create a new ERC-721 NFT on Ethereum in Cargo's shared smart contract. Cost: 1 Cargo Credit + ETH Gas Fees.

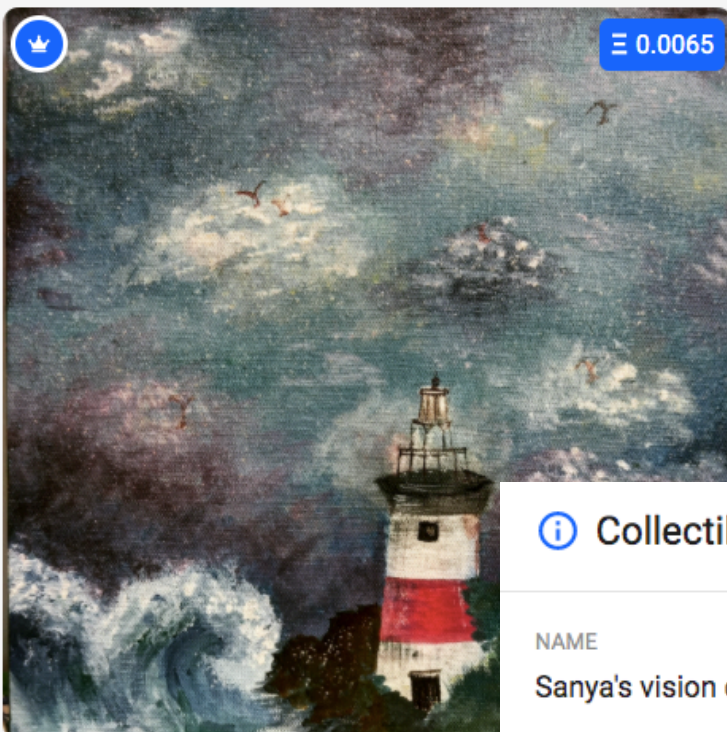
[Create](#)

Your NFTs

[View by collection](#)

Sanya's vision of "To the lighthouse"

[View public page](#)



Transfer

Details

Sell

Collectible Details

NAME

Sanya's vision of "To the lighthouse"

DESCRIPTION

Digital image of an acrylic on canvas painting titled "To the lighthouse" by Sanya Nagpal

COLLECTIBLE ID

718

COLLECTION ADDRESS

0x728d...9dA2



COLLECTION NAME

Cargo Magic Minting

Locked Files

[Unlock and download files](#)

Collectible Metadata

```
{
  "name": "Sanya's vision of \"To the lighthouse\" ",
  "description": "Digital image of an acrylic on canvas painting titled \"To the lighthouse\" by Sanya Nagpal ",
  "image":
    "https://assets.cargo.build/a44b2eadd3b54578bd5f1d0c4680ff03_preview.jpeg",
  "creator": "cobasnagpal"
}
```



Search by code or collection



Welcome to the crypto stamp!

The crypto stamp is the world's first ever blockchain stamp. This makes Österreichische Post AG the first postal company to introduce a stamp that can be used for postage purposes but is also saved as a digital image within the blockchain. Crypto stamp 1.0 was issued in 2019 and bears a unicorn, the heraldic beast of the Ethereum community. Crypto stamp 2.0 came out in June 2020 and depicted no fewer than four different animal motifs! And stay tuned, because Österreichische Post AG is already hard at work on Crypto stamp 3.0!



Crypto stamp

<https://crypto.post.at>

welcome to the world
of programmable art
living art created to change over time

View Gallery

what is async art?

▶ watch the video

Subscribe to our newsletter for updates on upcoming events, promotions, and new features.

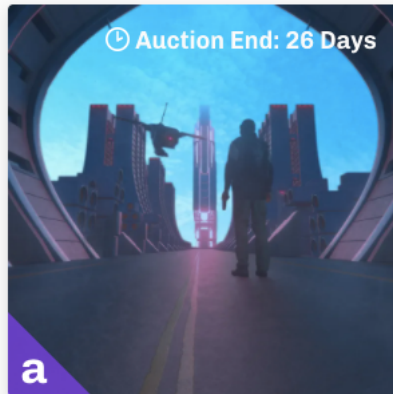
your@email.com

Submit

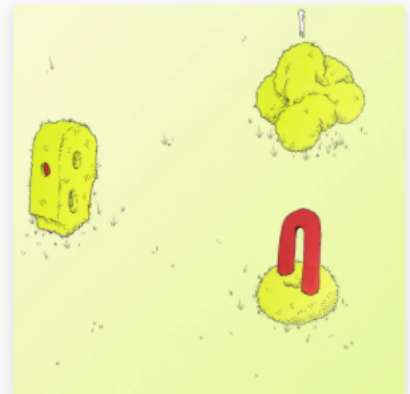
New and Notable



What is your biggest Current Bid: US\$1,483
Natacha Einat Reserve: US\$2,224



January 1st 2021 - On Current Bid: US\$593
Brian



Tarrying with Topiary Open To Bids
Mark Zlotzky Prev. US\$3,489

More Notable Picks

<https://async.art/>



Mintbase

Virtual Economy Starter Pack / NFT Factory

- Markets
- [Test on NEAR](#)
- Get Started

1,031 stores 2,492 bought 83,147 transactions 144.4 earned

Art | Tickets | Photography | You Decide



By using this website, you agree to our [privacy policy](#)

See All Markets

N

Minting NFTs on Mintbase, entrance to the virtual economy.

Full Node

New Store

Settings

Share Market

Watch later

Share

Fresh Mint

Mint

Burn

Transfer

Mint

Burn

Transfer

Mint

Burn

Transfer

Mint

Burn

Transfer

Tokyo Month Pass

Available: 3

2.0 ETH

\$463.62

Global Pass

Available: 9

1.0 ETH

\$231.81

Flex Desk

Available: 72

1.0 ETH

\$231.81

San Francisco Pass

Available: 6

1.2 ETH

\$278.17

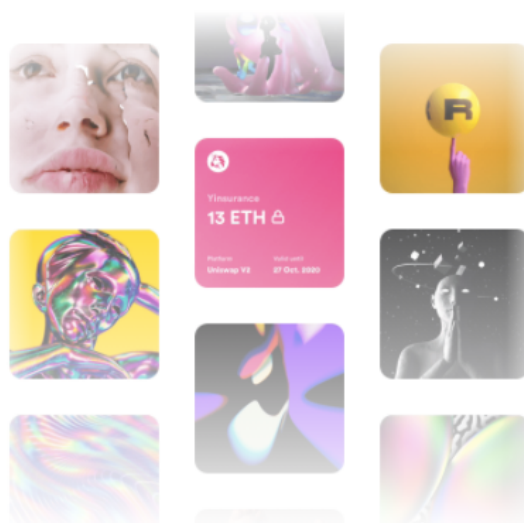


Rarible is the first community-owned NFT marketplace

Create, sell or collect digital items secured with blockchain

Create

Explore



Join 20,000+ creators and collectors



**No code
Required**



**Community
Driven**



**Flexible
Royalties**



**Verified
Creators**



**Multiple
Minting**



**Unlockable
Items**



**Auction
Functions**



**RARI
Rewards**

<https://rarible.com/>



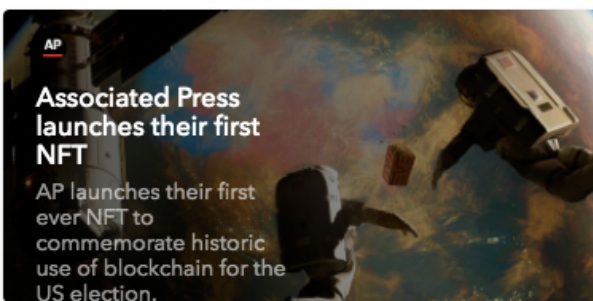
Search items, collections, and accounts

New Art Domain Names Virtual Worlds Trading Cards Collectibles Sports Utility

The largest NFT marketplace

Buy, sell, and discover rare digital items

Explore



DIGITAL ART

VIEW ALL >



Flips! Balancetherium

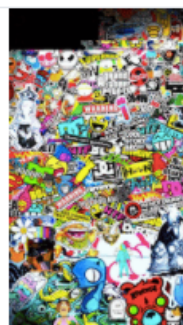
Price
Ξ0.09



Rarible Polkadot BaseBall Cap (Special)

Price
Ξ0.218

Last Ξ0.263



CanvasLife CanvasLife #167

Price
Ξ0.2

3 days left

<https://opensea.io/>



Type ▾ 🔍



Ethereum ▾

Art

Collectibles

Game Items

Music

Domains

Templates

Videos

Create it. Mint it. Earn Crypto.

Turn any creation into a blockchain item

Trade digital items on **Mintable** to easily earn crypto



Start Selling

List item for sale



Join our discord community

Top ranked items

Beautiful



Most Liked



Innovative!



Must Buy!



Underpriced



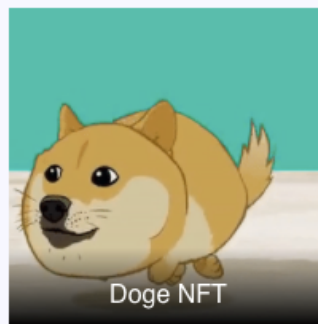
Thumbs down



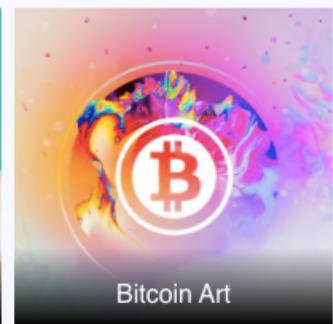
Overpriced



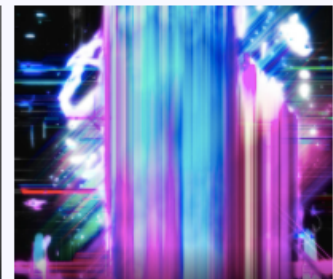
Digital City Art



Doge NFT



Bitcoin Art



<https://mintable.app/>

Collect **SuperRare** Digital Artworks

[START COLLECTING](#)[LEARN MORE](#)

SuperRare Art Market Weekly Report

Featured Editorial | March 1, 2021

SuperRare Art Market Weekly Report

[READ THE ARTICLE](#)

How To Collect Digital Art.

DISCOVER TOKENIZED DIGITAL ART.

Artists issue authenticated single edition digital artworks. These are certified on the Ethereum blockchain to prevent forgery and provide historical provenance.

BUYING & SELLING

Purchase at the asking price or make an offer by placing a bid. Once you own a piece you can resell it in the secondary market to other collectors.

SHOWCASE YOUR COLLECTION

Customize your profile to show off your art collection to patrons around the world. Display your works in a VR gallery, digital display, or anywhere else you like.

[START COLLECTING](#)<https://superrare.co/>

C5. Tokenized stocks

Tokenized stocks are tokenized derivatives representing shares in:

- publicly traded companies
- Exchange Traded Funds
- Indexes
- baskets of securities

Some of the benefits of tokenized stocks are:

- fractional ownership of securities,
- 24/7 trading
- ease of trading in foreign stocks

Holders are also entitled to dividends and stock splits on the underlying shares.

Bittrex Global is one of the exchanges that enables trading in tokenized stocks. It lists tokens representing derivative contracts collateralized by the underlying equities. These tokens cannot be withdrawn from Bittrex Global or redeemed for the underlying shares. The underlying is custodied by licensed banks and traded on fully regulated exchanges through regulated brokers.

GET TOKENIZED STOCKS

GameStop, AMC, BlackBerry, Nokia and iShares Silver Trust all available now 24/7.

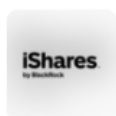


GameStop

\$110.00

+2.65%

[Buy GME Now](#)



iShares Silver Trust

\$23.54

0%

[Buy SLV Now](#)







AMC Entertainment

\$8.13

+2.74%

[Buy AMC Now](#)

Name	Price	24hr Volume	24hr	
 TSLA Tesla	\$606.32	\$1,502,929.08	-7.57%	Buy
 PFE Pfizer	\$34.24	\$299,554.99	-2.05%	Buy
 BILI Bilibili	\$121.88	\$138,444.13	-8.94%	Buy
 BNTX BioNTech	\$97.12	\$120,724.94	-2.05%	Buy

C6. Crypto Wallets

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

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 respective 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>


 [Wallet](#) [Exchange](#) [Explorer](#) [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](#)

[All Blockchains](#) [Search](#)


There are 2 blockchains with result(s) to your search 1AHr3RDS7v8ruFLbVoxXsgVeGqYqALqQ8 :


 BTC


Address


 BCH

Address

Explorer >  Bitcoin Explorer > Address


Search your transaction, 


Address 





Payment Request


Donation Button


Address	1AHr3RDS7v8ruFLbVoxXsgVeGq... 
Format	BASE58 (P2PKH)
Transactions	0
Total Received	0.00000000 BTC
Total Sent	0.00000000 BTC
Final Balance	0.00000000 BTC

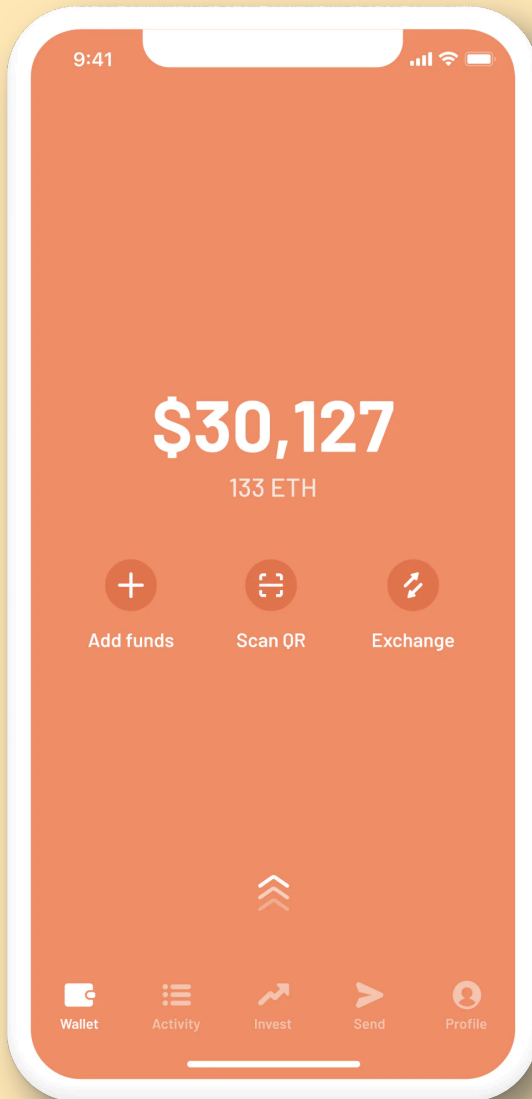
Explorer >  Bitcoin Cash Explorer > Address

Search your transaction, 

Address 



Address	qpj73wdjxays94h4vtp209cw3v2a0... 
Format	CASHADDR (P2PKH)
Transactions	0
Total Received	0.00000000 BCH
Total Sent	0.00000000 BCH
Final Balance	0.00000000 BCH

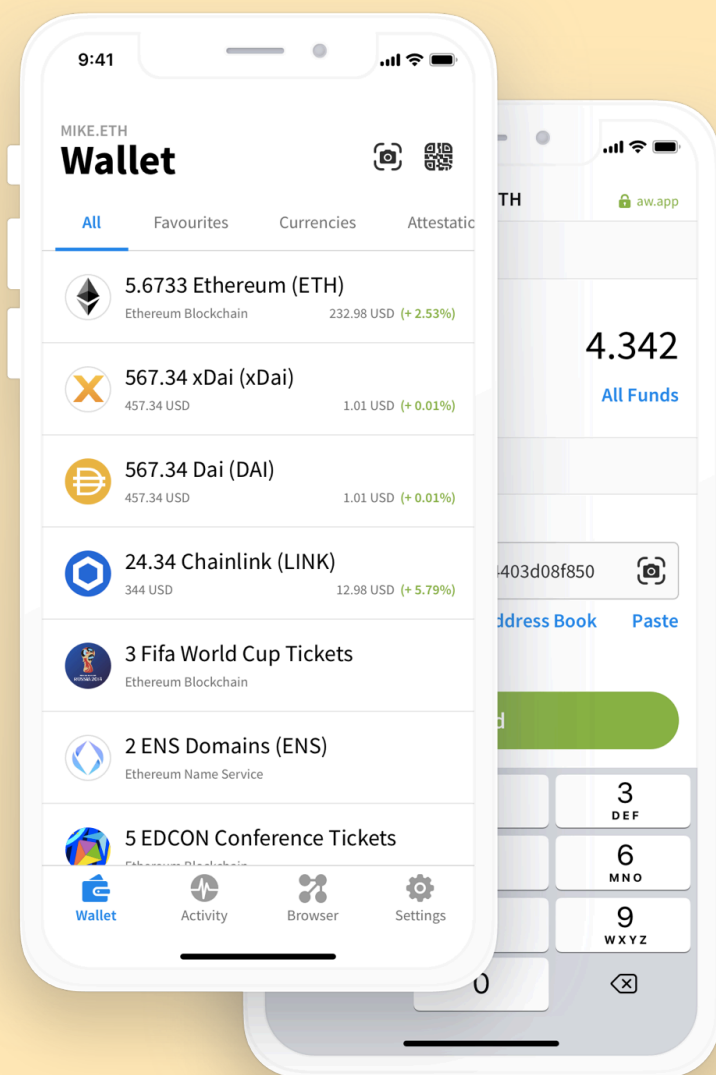


Argent

Argent is a crypto wallet that can be used to:

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

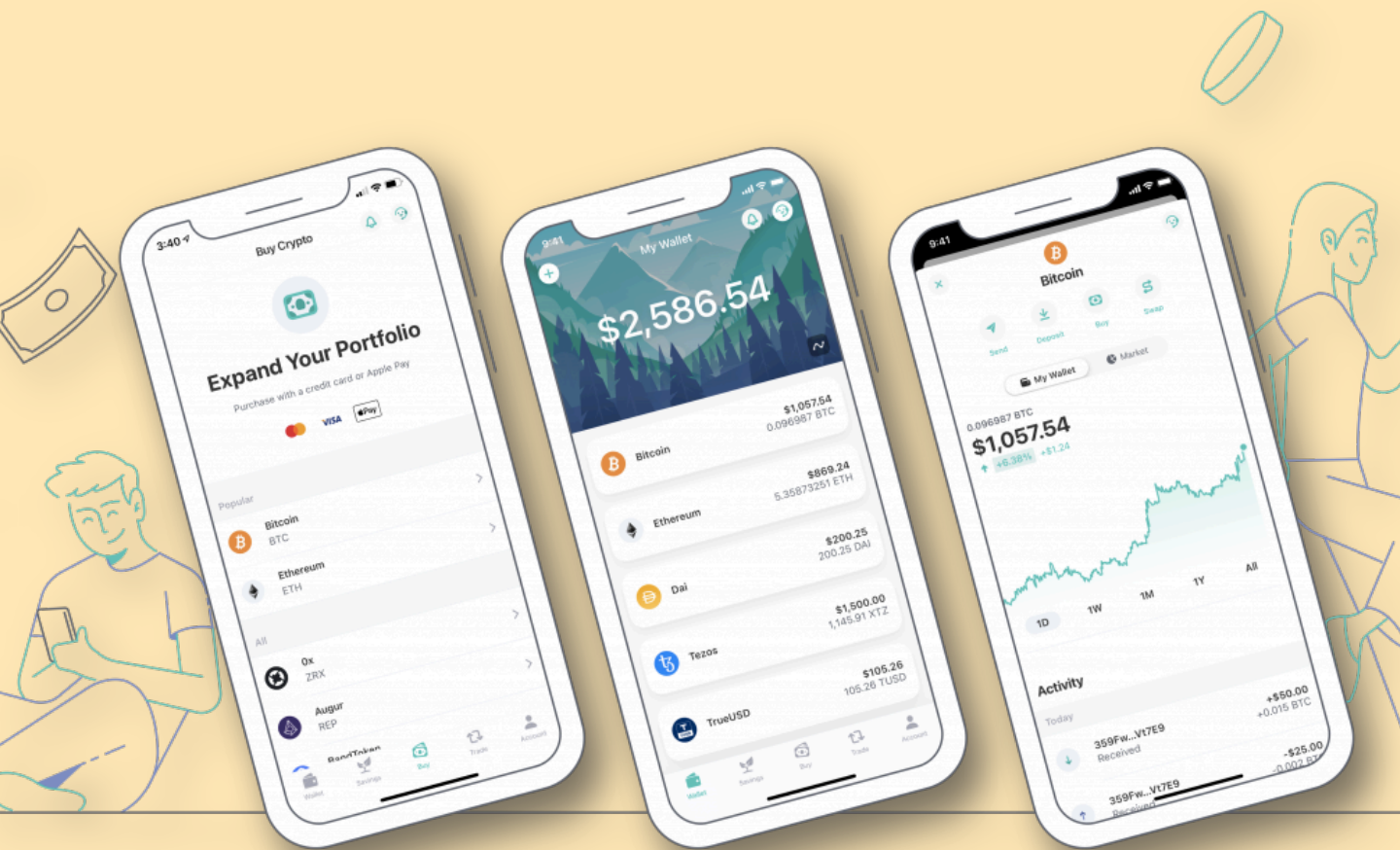
<https://www.argent.xyz>



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>

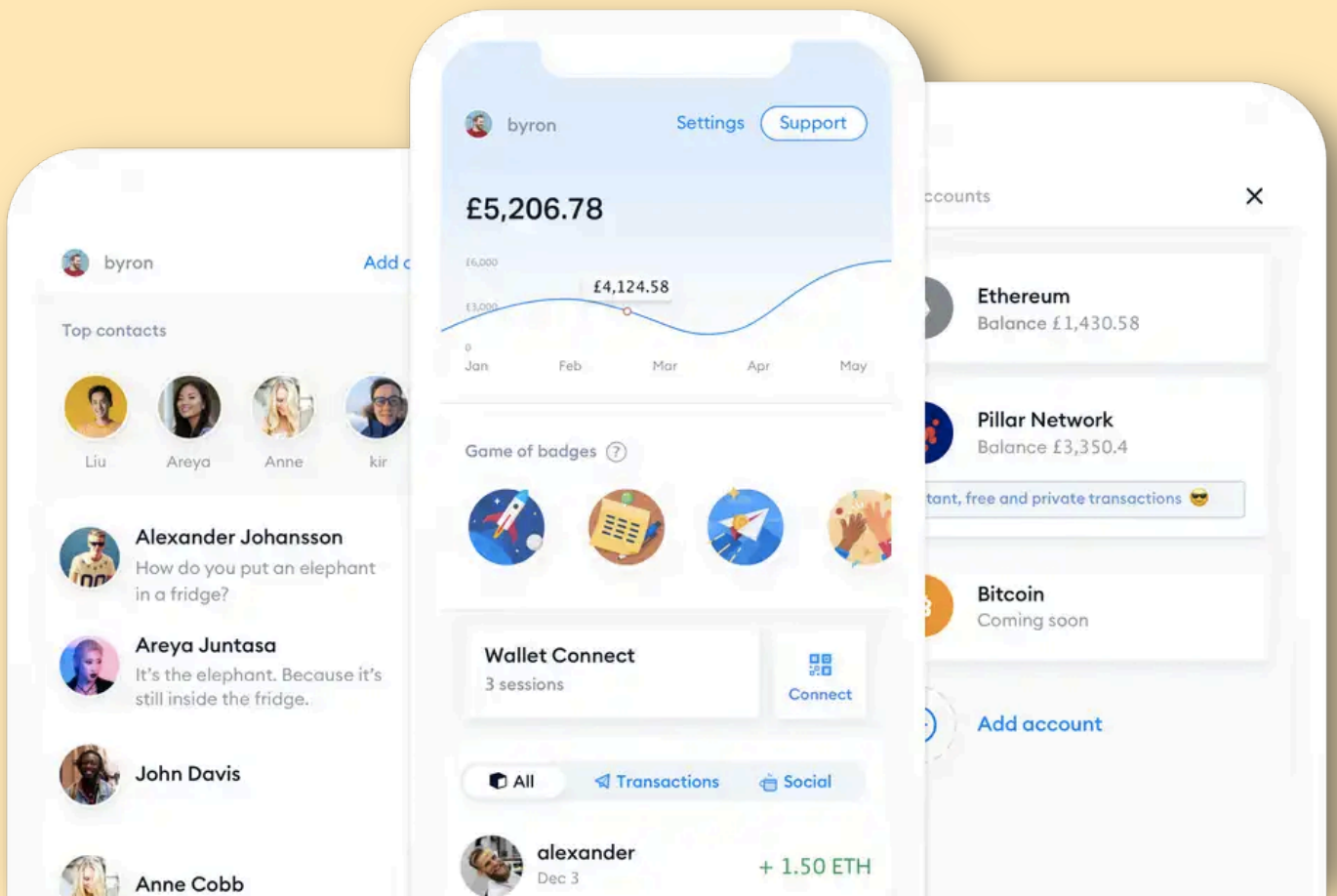
Pillar

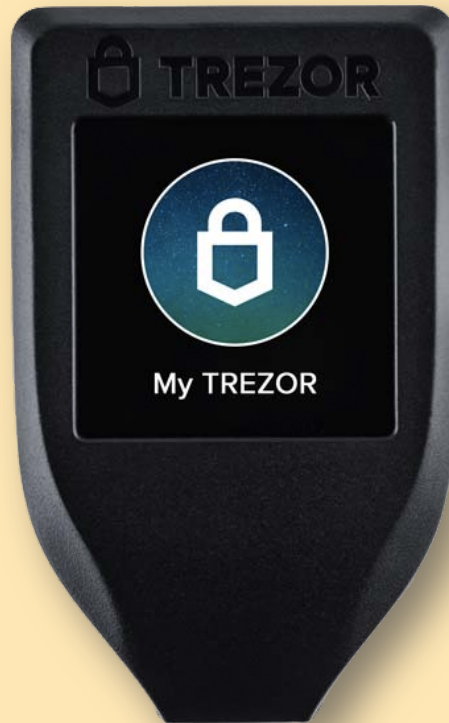
Pillar is a non-custodial, community-owned wallet with its own L2 Payment Network.

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>





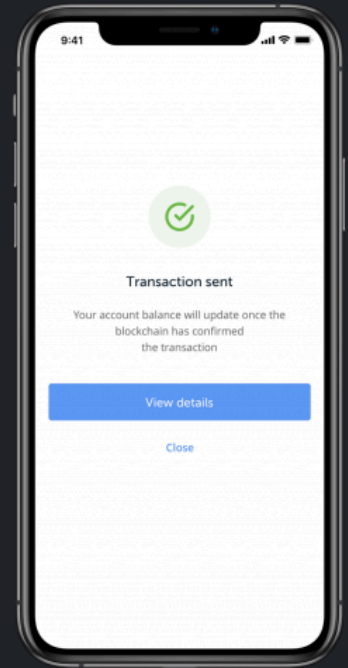
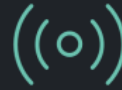
The Trezor Model T is a cryptocurrency hardware wallet for coins, passwords and other digital keys. Its features include:

- ☐ 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>

Ledger Nano X & Bluetooth



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>

Generating new Address...

MOVE your mouse around to add some extra randomness...

OR type some random characters into this textbox

Skip »

You may skip this step if you do not plan to use the random key generator.

Step 1. Generate new address

Choose your currency and click on the "Generate new address" button.

Step 2. Print the Paper Wallet

Click the Paper Wallet tab and print the page on high quality setting. **Never save the page as a PDF file to print it later since a file is more likely to be hacked than a piece of paper.**

Step 3. Fold the Paper Wallet

Fold your new Paper wallet following the lines.



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.

Ethereum's Original Wallet

MyEtherWallet (our friends call us MEW) is a free, client-side interface helping you interact with the Ethereum blockchain. Our easy-to-use, open-source platform allows you to generate wallets, interact with smart contracts, and so much more.



Create A New Wallet

Generate your own unique Ethereum wallet. Receive a public address (0x...) and choose a method for access and recovery.

Get Started →



Quick Help



Access My Wallet

Connect to the blockchain using the wallet of your choice.

- Send and Swap ETH & Tokens
- Sign & Verify Messages
- Interact with Contracts, ENS, Dapps, and more!

Access Now →

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

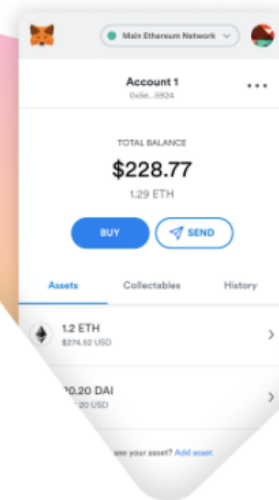
It can be used for generating wallets, and interacting with smart contracts.

<https://www.myetherwallet.com>

A crypto wallet & gateway to blockchain apps

Start exploring blockchain applications in seconds. Trusted by over 1 million users worldwide.


Download now



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>


 Trust Wallet


AssetsStakingEarn +7.21% APRDApp BrowserLanguage

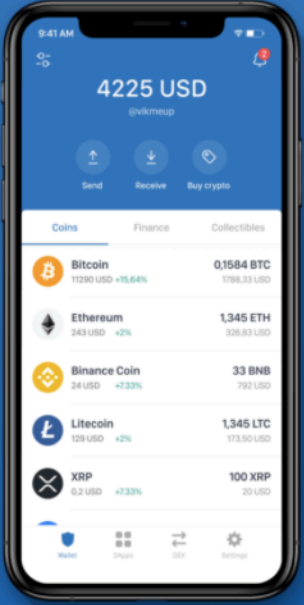
The most trusted & secure crypto wallet

Buy, store, exchange & earn crypto. Join 5 million+ people using Trust Wallet.

 DOWNLOAD ON THE App Store

 GET IT ON Google Play

 DOWNLOAD APK 6.0+



The smartphone screen shows the Trust Wallet app interface. At the top, it displays the balance as 4225 USD. Below this are three circular buttons: 'Send', 'Receive', and 'Buy crypto'. The main section is titled 'Coins' and lists several cryptocurrencies with their current prices and percentage changes: Bitcoin (11290 USD, +15.64%), Ethereum (243 USD, +2%), Binance Coin (24 USD, +7.33%), Litecoin (129 USD, +2%), and XRP (0.2 USD, +7.33%). To the right of these, it shows the quantity of each coin held in the wallet. At the bottom, there are icons for 'Wallet', 'Swap', 'DEX', and 'Settings'.

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>

C7. Oracles

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 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.

 Chainlink Labs is hiring. Come [join an industry-leading team.](#)

Connect your smart contract to the outside world

Chainlink's decentralized oracle network provides reliable, tamper-proof inputs and outputs for complex smart contracts on any blockchain.

[Develop with Chainlink](#)[Explore solutions](#)AAVE 

SYNTHETIX

 celsius

Ampleforth

Nexus  Mutual ENS

Start building your universally connected smart contract

[Price Feeds](#)[Randomness](#)[Any API](#)

C8. Public Blockchains

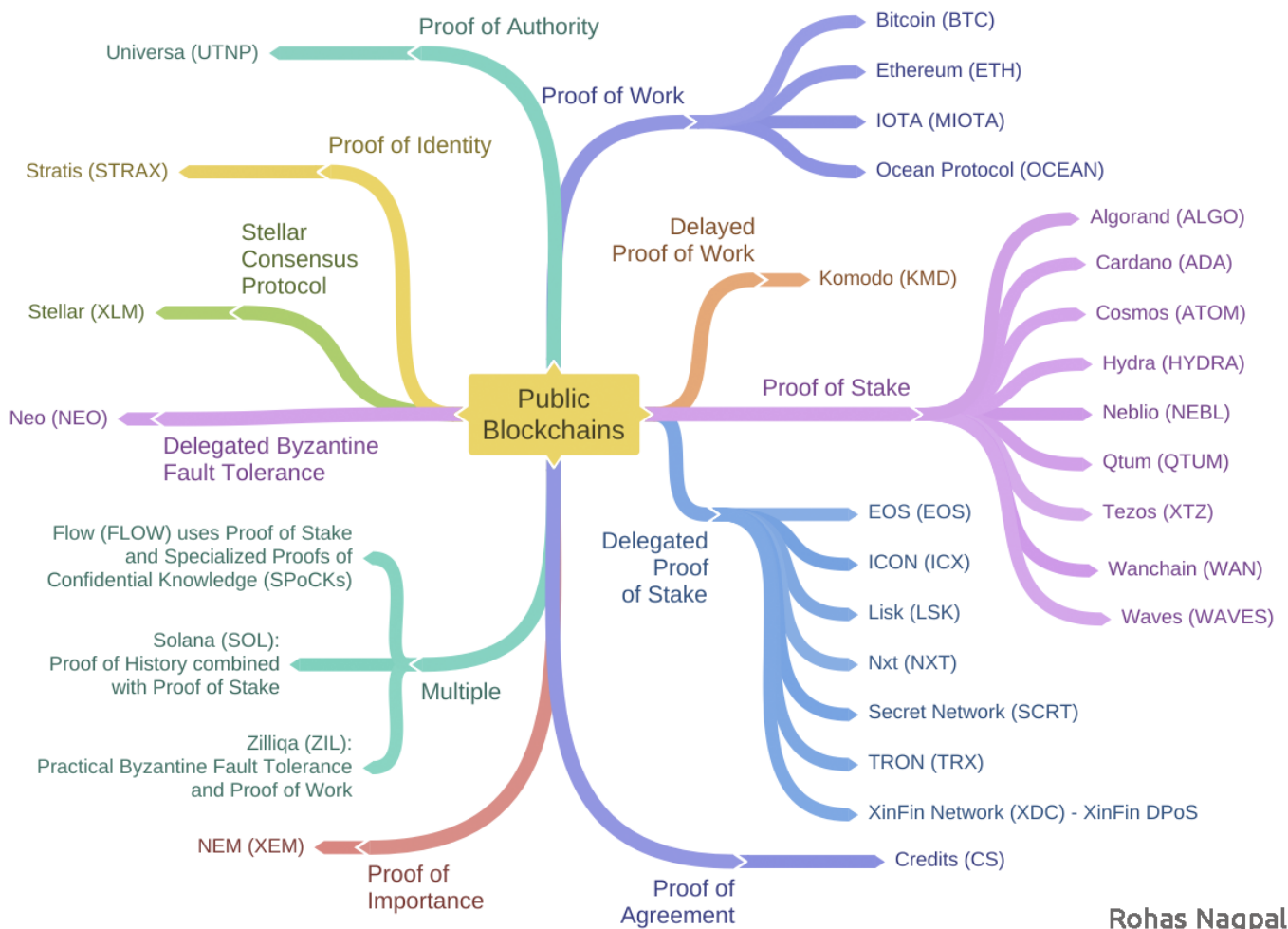
The list of popular public blockchains and their native assets are:

1. Algorand (ALGO)
2. Bitcoin (BTC)
3. Cardano (ADA)
4. Cosmos (ATOM)
5. Credits (CS)
6. EOS (EOS)
7. Ethereum (ETH)
8. Flow (FLOW)
9. Hedera Hashgraph (HBAR)
10. Hydra (HYDRA)
11. ICON (ICX)
12. IOTA (MIOTA)
13. Komodo (KMD)
14. Lisk (LSK)
15. Neblio (NEBL)
16. NEM (XEM)
17. Neo (NEO)

18. Nxt (NXT)
19. Ocean Protocol (OCEAN)
20. Qtum (QTUM)
21. Secret Network (SCRT)
22. Solana (SOL)
23. Stellar (XLM)
24. Stratis (STRAX)
25. Tezos (XTZ)
26. TRON (TRX)
27. Universa (UTNP)
28. Wanchain (WAN)
29. Waves (WAVES)
30. XinFin Network (XDC)
31. Zilliqa (ZIL)

Private blockchains are usually built using:

- ConsenSys Quorum
- R3 Corda
- Hyperledger (Besu, Burrow, Fabric, Indy, Iroha, and Sawtooth)
- Multichain by Coin Sciences



Mindmap of 30 public blockchains categorize on their consensus mechanisms

Blockchain Wars

Blockchain Wars is a research project to identify the best public blockchains.



Algorand (78%)

Algorand is the world's first pure proof-of-stake blockchain with Smart Contracts, Standard Assets, Atomic Transfers, and Rekeying in Layer 1. Its native cryptocurrency is ALGO.

🕒 MONDAY, 22ND MARCH, 2021



Bitcoin (89%)

Bitcoin is the world's most popular, most audited, and probably most secure blockchain. It follows a proof of work consensus and its native cryptocurrency is BTC.

🕒 MONDAY, 22ND MARCH, 2021



CARDANO

Cardano (75%)

Cardano is a proof-of-stake (Ouroboros protocol) blockchain whose primary goals is to "bring reliable, secure financial services to those people who do not currently have access". Its native cryptocurrency is ADA.

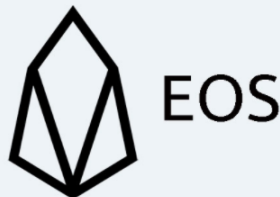
🕒 MONDAY, 22ND MARCH, 2021



Credits (51%)

Credits is a Proof-of-Agreement (PoA) blockchain with 0.5 second transactions and java-based smart contracts. Its native cryptocurrency is CS.

🕒 MONDAY, 22ND MARCH, 2021



EOS (56%)

EOS uses a delegated proof-of-stake consensus mechanism and its native cryptocurrency is EOS.

🕒 TUESDAY, 23RD MARCH, 2021

Ethereum



Ethereum (88%)

Ethereum is the first blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "smart contracts". Its native cryptocurrency is ETH.

🕒 TUESDAY, 23RD MARCH, 2021

Blockchain Wars is a research project to identify the best public blockchains.

https://www.rohasnagpal.com/blockchain_wars.php

C9. Technical Crypto Concepts

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-----
iQHgBD5vDDEBBAC+UMHkR9YL1W0OYzL9gK/
AERegEtzoFiveSzbeFQtNhxDIOSPJc60Y8v2nTecl0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPApi
OFXhUrkhHF0DmrmEpa5UpHjpO3sD+HlvG84N6jHjAIRMINMAyrg/
e4i6ABGzAuxYbJC6ax9mxdrFAQARAQABAwvtDcK53Fr7j9Ss3v83ZR7g1DgFFy3oo97XWb
mJ02BdRGy/
C+aluu3wMRNqmPo5w1i8VVCjjM02eqSr0+8mbLLX0Dwqbn33QitGW34Upt6EI+fv0ObKbJRi2
Hc628l3mi+jjsskxvQ8oavtSJL2j/
xTEtL+vvqObcFxllyjPH5N1wY7xQ5BPSNjYLFZr99MXycFhee14V2YdQv0iPZFrJnvCQFWXL
AiX1L9AH5DgwmXLtNCPblQnRwyLPyWSOT4yH8e6ibqlBvMhpGe4WOAzuccHL6jjZrokVrBB
u50Z6EqGFkzS8X6iygvSATOjr3L/
X9EW7Fw098CcVK3IDB93rpeXR+tU370nV+0FgXQqUzQ3SJ6vZwdlwy6cmjZOWmd/
YrbGLOyyW+zFFSZFdiG480ELozMfmSq3OJvElvhRgS/tbA/
94jpOtzhWV9Du0pd7otCBBYmhpbmF2IEJoYXR0IDxhYkBhc2lhbmxhd3Mub3JnPp0B4AQ+b
wwwAQQAmmkdApHtWspZdNfqeEROxctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLRnW+N4QUAgm
+eNNsTrqZZjJUP526dOTK8RmxV4QJeh2Q0bsLPs6SXTIPwfBWPpt+U/
kfrSt8ZJF5lWR0jaiJG2hE3dBiuszPa+6cJUDuQnYCVCHZARCKLcAEQEAAQPT8PBQW4y8b
4C7BvhjnGAATQliwRajv6uWmfUFcl+DPdtAZh3yb9EKWmS8vSkSzn+pWG1dEkuURyvBGJM
Dxs/
FB+CMouTQejhA11Ho5tblas8HnoNPeQv1x9Xas+lrs1j2AmfrLWwKEQAuH9di+d9DRU6YHxy1
oclHZELXR9ECsSP0C1iSeuJn+u4HLP3y4uBHcGRdihLRIUSCJ0tXd2meRAXw4dsZlIDAeb21i
2Tj+I0SngTEzFj8fSuvAxoXRv30gq5VLbH5WDbJah5n688THMAUIUC5dlG8MMXMgmUe887l
wKEqSvLqCk5ymHmCdZiJQQEpAxVbXb9bkKs2UhxN1zRnug4OcR411XOqlvIBwsk121yY760
6mZ7r+icnXvLLEVezmegXsN8mlhAnb+p629HPZSMFOSHgX3CwhlwTKDaMxZBft94Fk8w3l/
NBuwQJYg===Emf5
-----END PGP PRIVATE KEY BLOCK-----
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQCNBD5vDDEBBAC+UMHkR9YL1W0OYzL9gK/
AERegEtzoFiveSzbeFQtNhxDIOSPJc60Y8v2nTecl0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPApi
OFXhUrkhHF0DmrmEpa5UpHjpO3sD+HlvG84N6jHjAIRMINMAyrg/
e4i6ABGzAuxYbJC6ax9mxdrFAQARAQABtCBBYmhpbmF2IEJoYXR0IDxhYkBhc2lhbmxhd3
Mub3JnPokAtAQQAQIAHgUCPm8MMQUJAeKFAAgLAWklBwIBCglZAQUBAwAAAAAKCRDR
PtuuStKFCIJwA/9t1Cjpi+hjVaWjJx1BZpoGv4b+t/
Qb03J9ABFUatbypUX5jmMmCUT7h3TgiCgT5F4imvijm4+uCDeoHz0Uj+nPfvW8guMd805s/
+3oU+FT4R2qYvEX6MAQVex67TJ0pHvmiV55Mn/
apNvTdvgsXJbQfHuza9u1QPEUm+LIVdOZx7kAjQQ+bwwwAQQAmmkdApHtWspZdNfqeERO
xctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLRnW+N4QUAgm+eNNsTrqZZjJUP526dOTK8RmxV4Q
Jeh2Q0bsLPs6SXTIPwfBWPpt+U/
kfrSt8ZJF5lWR0jaiJG2hE3dBiuszPa+6cJUDuQnYCVCHZARCKLcAEQEAAAYkAqAQYAQIAEg
UCPm8MMgUJAeKFAAUbDAAAAAAKCRDRPtuuStKFCADiA/
0csZOSY9Ztyvw2iVSJqf9g4u3z+ePmEcwy2RK5tuOXU2p7HvEBMKeLIG9Dxg0xwy7cVvHejjA
n4LxMPG9j26TinLCAfqHs7C1og8an1tHstrM4lcw7pWx5fIRLiqQLqEc/
RVFLBKU3nMAJgu0E9wjHicWFwsxUfeF5qD9kAsl0Og===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 $\phi = (p-1)(q-1)$.
4. Select e such that $1 < e < \phi$ and the greatest common divisor of e and ϕ is 1. That means e and ϕ are coprime.
5. Compute d such that $1 < d < \phi$ and $ed \equiv 1 \pmod{\phi}$. This means that the value of d must be such that $ed-1$ should be completely divisible by ϕ or $(ed-1) / \phi$ 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
 $c = m^e \pmod{n}$.

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 $\phi = (p - 1) * (q - 1) = 2 * 10 = 20$
4. Choose e such that $1 < e < \phi$ and e and ϕ are coprime. Let $e = 7$
5. Compute a value for d such that $1 < d < \phi$ and $ed \equiv 1 \bmod \phi$.
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.

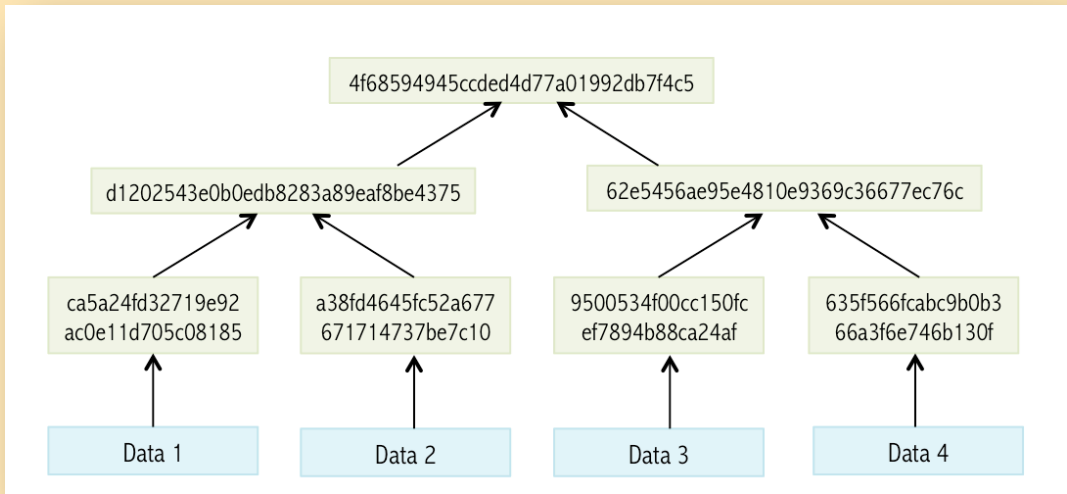
This **digital signature** is unique to the message. The signer then sends the message and the digital signature to the receiver. The receiver re-computes the hash from the message. The receiver also computes another string using the digital signature and the signer's public key (using the relevant algorithm).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

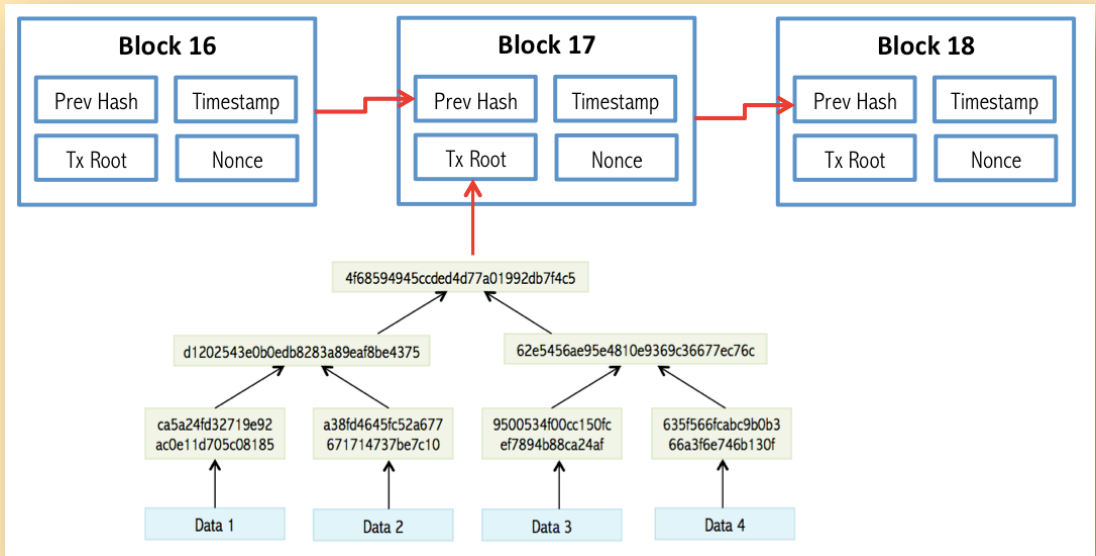


`4f68594945ccded4d77a01992db7f4c5` is the merkle root of the 4 transactions (or pieces of data) in the illustration above.

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.

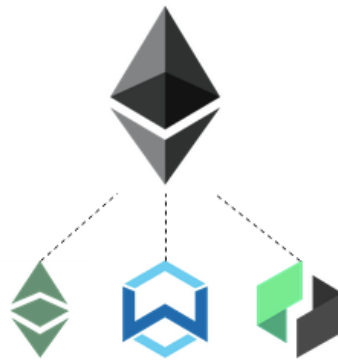
Hard forks are the result of network changes that are so extensive that every node participating in the network must upgrade their software in order to be compatible with the new processes.

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 Ethereum Forks



List of Ethereum Forks

- **Ethereum (ETH)**

- Ethereum Classic (ETC) is technically the original Ethereum blockchain while Ethereum is the fork, however the majority of the Ethereum community has followed the direction of Ethereum over Ethereum Classic.
- Wanchain (WAN)
- Ubiq (UBQ)

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 (BTCPrv)
 - 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)
 - Groestlcoin (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)

Consensus algorithms

Consensus algorithms are the heart of blockchains. They enable network participants to agree on the contents of a blockchain in a distributed and trust-less manner.

The world's first consensus algorithm was Bitcoin's Proof of Work (PoW).

Today there are 75 algorithms divided into 10 categories:

1. Chain-based Proof of Work
2. Chain-based Proof of Stake
3. Chain-based Proof of Capacity/Space
4. Chain-based Hybrid models
5. Chain-based Proof of Burn
6. Chain-based Trusted computing algorithms
7. Chain-based PBFT and BFT-based Proof of Stake
8. Chain-based others
9. Chain-based DAG
10. Magi's proof-of-work (mPoW)

The detailed list is provided below:

Note: For each of these, see details at: <http://bit.ly/2NnUQR0>

Chain-based Proof of Work

1. Proof of Work (PoW)
2. Proof of Meaningful Work (PoMW)
3. Hybrid Proof of Work (HPoW)
4. Proof of Work time (PoWT)
5. Delayed Proof of Work (dPoW)
6. Proof of Edit Distance
7. ePoW: equitable chance and energy-saving.
8. Semi-Synchronous Proof of Work (SSPoW)

Chain-based Proof of Stake

1. Delegated Proof-of-Contribution (DPoC)
2. Secure Proof of Stake (SPoS)
3. Hybrid PBFT/Aurand
4. Proof of Stake (PoS)
5. Delegated Proof of Stake (DPoS)
6. Proof of Stake Time (PoST)
7. Proof of stake Boo (PoS Boo)

8. High Interest Proof of Stake (HiPoS)
9. Asset PoS (APoS)
10. Traditional Proof of Stake / Tiered Proof Of Stake (TPOS)
11. Casper the Friendly Finality Gadget (FFG)
12. Correct By Construction (CBC) Casper
13. Variable Delayed Proof of Stake (vDPOS)
14. Proof of Stake Velocity
15. Magi's Proof of Stake (mPoS)
16. Leased Proof of Stake (LPoS)
17. Delegated Proof of Importance (DPoI)
18. Leasing Proof of Stake (PoS/LPoS)

Chain-based Proof of Capacity/Space

1. Proof of Process
2. Proof of capacity (PoC)
3. Proof of Signature (PoSign)
4. Proof of Retrievability (POR)
5. Proof of Location
6. Proof of Reputation (PoR)
7. Proof of Proof (PoP)
8. Proof of History
9. Proof of Existence
10. Proof of Research (DPoR)
11. Proof of Activity
12. Proof of Weight (PoWeight)
13. Proof of Zero (PoZ)
14. Proof of Importance
15. Proof of Care (PoC)
16. Raft
17. Proof of Value (PoV)
18. Proof of Participation (PoP)
19. Proof of Believability
20. Proof of Stake (POS) / Proof of Presence (PoP)
21. Proof of Ownership
22. Proof of Quality (PoQ)
23. Proof of Space (PoC)

Chain-based Hybrid models

1. GHOST-based Recursive ANcestor Deriving Prefix Agreement
2. Proof of authority (PoA)
3. Ethereum Proof of Authority
4. Limited Confidence Proof-of-Activity (LCPoA)

5. Proof of Work (PoW) / Nexus Proof of State (nPoS) or Nexus Proof of Holding (nPOH)
6. Proof of Activity
7. Proof of Work (PoW) / Proof of Stake (PoS) / Proof Of Care (PoC)
8. Proof of work (PoW) / High Interest Proof of Stake (HiPoS)
9. Proof of Work (PoW) / PoM / PoSII

Chain-based Proof of Burn

1. Proof of Processed Payments (PoPP)
2. Proof of Burn (PoB)
3. Proof of Time
4. Proof of Stake (PoS) / Proof of Disintegration (PoD)

Chain-based Trusted computing algorithms

Proof of Elapsed Time (PoET)

Chain-based PBFT and BFT-based Proof of Stake

Chain-based others

1. Proof of Trust (PoT)
2. Proof of Devotion
3. Snowglobe
4. Avalanche
5. Serialization of Proof-of-work Events (Spectre)
6. Script-adaptive-N (ASIC resistant)

Chain-based DAG

1. BlockFlow
2. Direct Acyclic Graph Tangle (DAG)
3. Hashgraph
4. Block-lattice - Directed Acyclic Graphs (DAGs)

Magi's proof-of-work (mPoW)

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.

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.

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 February 2021, some of the 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);

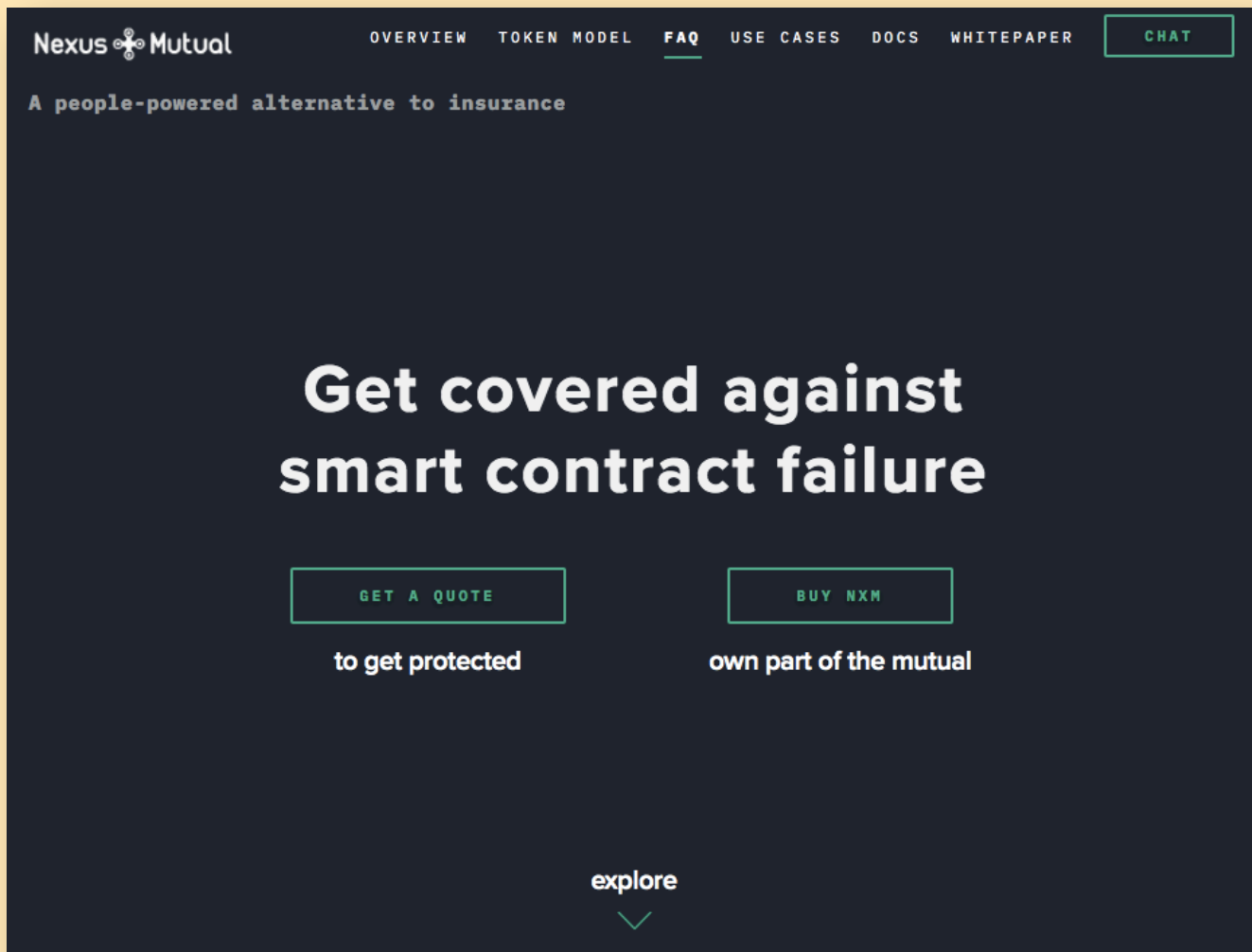
    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() public {
        minter = msg.sender;
    }

    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>



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>

Blockchain Security

26th February 2021

Rohas Nagpal

Tech terms

Install a blockchain

Basic commands

Secure Blockchain

Security Controls

For a dive into Blockchain Tech Terms & Security, see:

The first 90 minutes of this video:

<https://www.youtube.com/watch?v=3xmhRRHJjg>

The Blockchain Security Presentation

<https://bit.ly/38cHU7K>

Primechain Technologies

Blockchain Security Controls



Primechain-BSC

Version 1.2 dated 26th February, 2021

Blockchain Security Controls
<https://bit.ly/37OWW3H>

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

This website uses cookies to ensure
you get the best experience on our
website. [Learn More](#)

GOT IT!

Betting today is broken & exploitative.

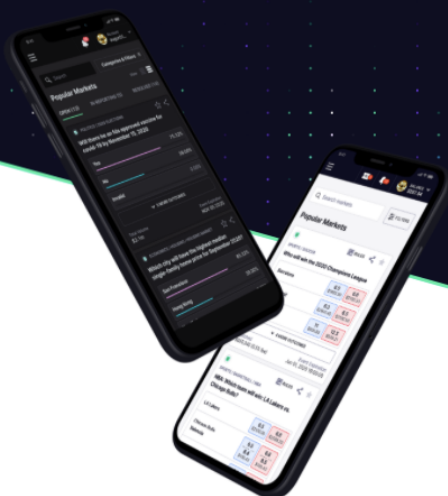
Today's betting Industry trades on promises of getting rich
quick, using every trick in the book to **extract the maximum
value from customers.**

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 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>

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

**Bitstamp**

400+ more

Bitcoin 51,719.77 USD ▲ 214.88 (0.42%)

Ethereum 1,894.32 USD ▲ 80.29 (4.43%)

Binance Coin 189.53 USD ▲ 56.08 (42.02%)

Litecoin 233.06 USD ▲ 10.83 (4.87%)

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

<https://www.bitgo.com>

Bitgo custody services include:

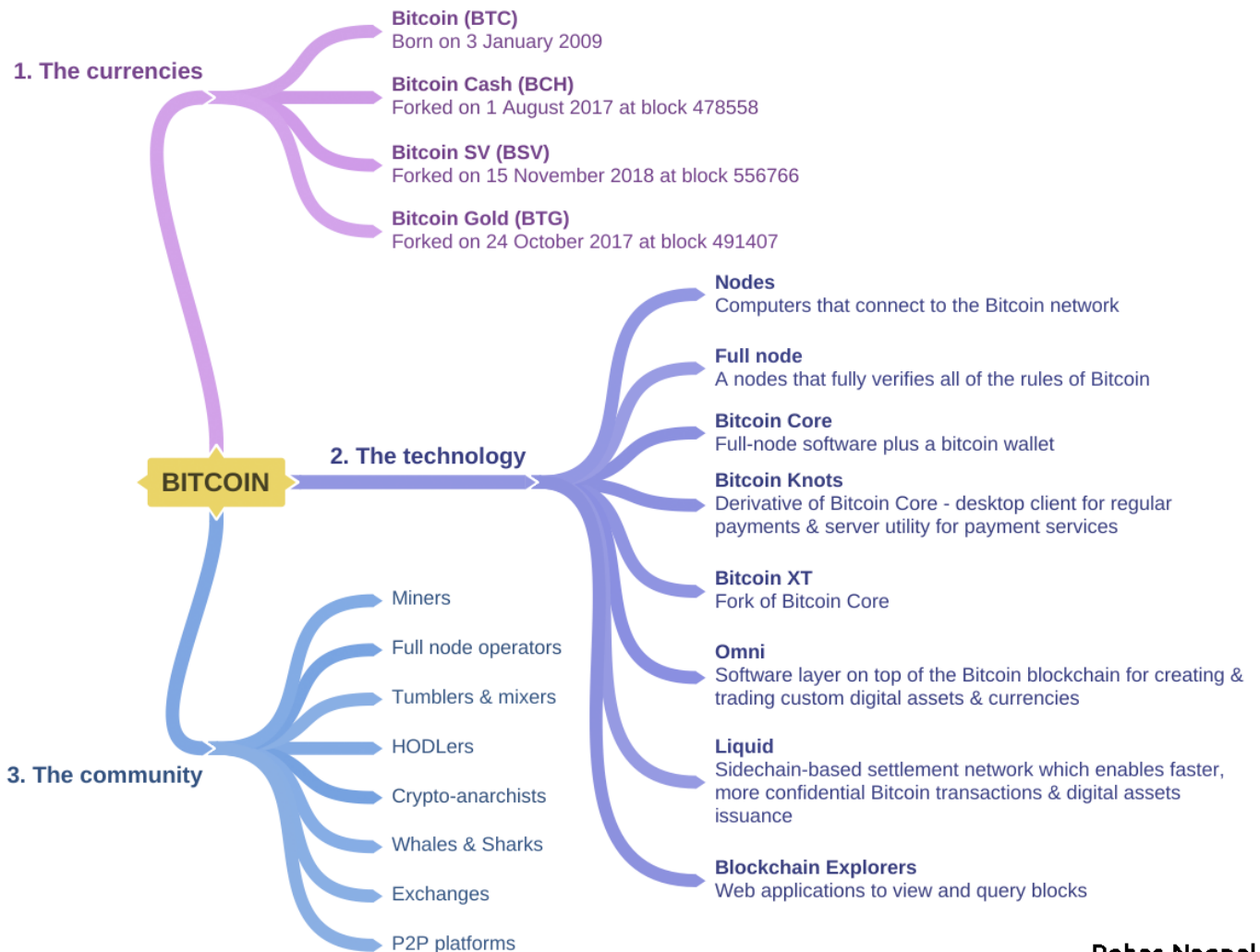
- Wallet Platform - hot, warm, and cold wallet solutions.
- Qualified Custody - insured cold storage for digital assets.
- Self-Managed Custody - secure your keys locally.

D

The Bitcoin Ecosystem

D. The Bitcoin Ecosystem

If you thought that Bitcoin is just 1 lonely cryptocurrency, you are in for a surprise. Check out this mindmap to understand what Bitcoin really is.



Rohas Nagpal

Running A Full Node

Support the Bitcoin network by running your own full node

What Is A Full Node? ▾

Setup a Full Node ▾

Costs And Warnines ▾

What Is A Full Node? ▾

Setup a Full Node ▾

Costs And Warnings ▾

Initial Block Download(IBD) ▾

Linux Instructions ▾

Windows Instructions ▾

Mac OS X Instructions ▾

Upgrading Bitcoin Core ▾

Network Configuration ▾

Configuration Tuning ▾

Report An Issue

Edit On GitHub

What Is A Full Node?

A full node is a program that fully validates transactions and blocks. Almost all full nodes also help the network by accepting transactions and blocks from other full nodes, validating those transactions and blocks, and then relaying them to further full nodes.

Most full nodes also serve lightweight clients by allowing them to transmit their transactions to the network and by notifying them when a transaction affects their wallet. If not enough nodes perform this function, clients won't be able to connect through the peer-to-peer network—they'll have to use centralized services instead.

Many people and organizations volunteer to run full nodes using spare computing and bandwidth resources—but more volunteers are needed to allow Bitcoin to continue to grow. This document describes how you can help and what helping will cost you.

For details on running a Bitcoin full node, see:
<https://bitcoin.org/en/full-node#what-is-a-full-node>

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.

Bitcoin Charts



For the latest prices, see:
<https://coinmarketcap.com/currencies/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

Enter amount

Exit

Enter amount

Select payment method

Review offer

Start the trade

Select the amount you'd like to spend and your preferred currency.

AMOUNT

1400.58

Indian Rupee (INR)

Show in Bitcoin

Select payment method

English

PAXFUL

Select payment method

Exit

Enter amount

Select payment method

Review offer

Start the trade

Bank Transfers

Online Wallets

Debit/Credit Cards

Gift Cards

Back

Review offer

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](#)

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

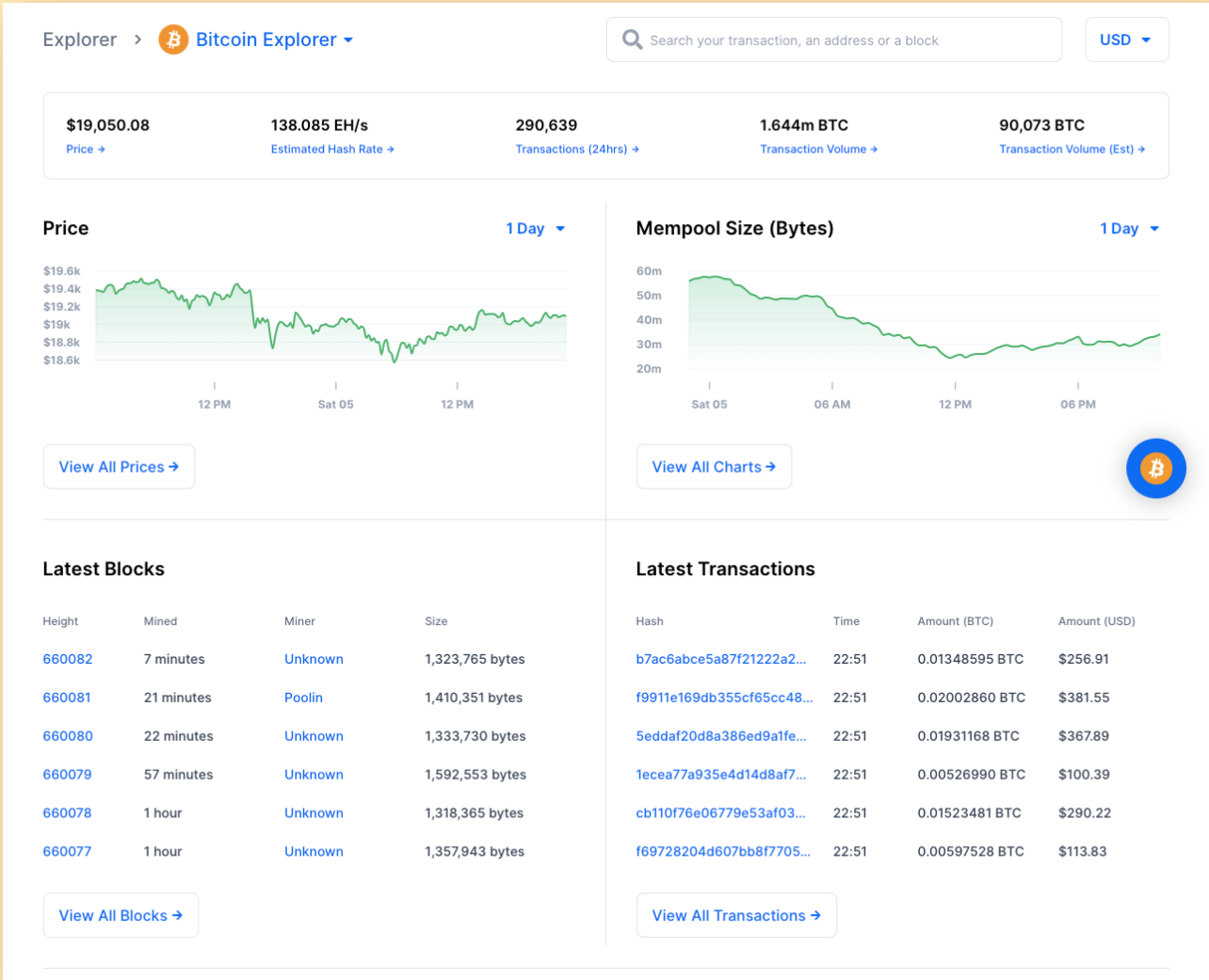
Search

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
aruntauus18 (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: 1AHR3RDS7v8ruFLbVoxXsgVeGqYqALqQ8

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.

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.

Bitcoin Cash Charts



For the latest prices, see:

<https://coinmarketcap.com/currencies/bitcoin-cash/>

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.

Bitcoin SV Charts



For the latest prices, see:
<https://coinmarketcap.com/currencies/bitcoin-sv/>



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>



Bitcoin ATM Near Me Search.

Select operation:

☒ Buy

☐ Sell

Select cryptocurrency:

☒ Bitcoin (BTC)

☐ Lightning BTC (LBTC)

☐ Bitcoin Cash (BCH)

☐ Ether (ETH)

☐ Dash (DASH)

☐ Litecoin (LTC)

☐ Zcash (ZEC)

☐ Monero (XMR)

☐ Dogecoin (DOGE)

☐ Tether (USDT)

☐ Ripple (XRP)

Address or location:

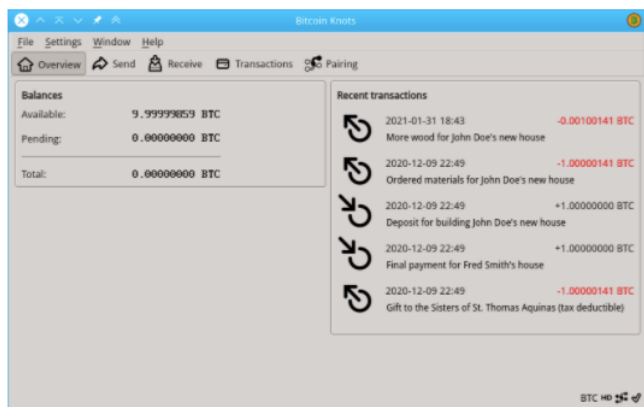
Search by address...

x



[ABOUT](#)[DOWNLOAD](#)

Bitcoin Knots is a combined Bitcoin node and wallet. Not only is it easy to use, but it also ensures bitcoins you receive are both real bitcoins and really yours.



Features:

- You hold your own bitcoins
- Full verification of payments
- Easy to send and receive
- Backup your wallet just like saving a document
- Optional expert control for advanced users
- Pair with your phone wallet to upgrade its security

Latest version: 0.21.0.knots20210130

[release notes](#)



Download Bitcoin Knots for macOS



Download digital signature

Show other downloads (advanced)

<https://bitcoinknots.org/>

Omni Layer

An open-source, fully-decentralized asset platform on the Bitcoin Blockchain



THE WALL STREET JOURNAL

YAHOO!
FINANCE

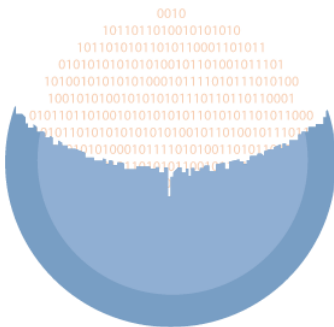
Forbes

BITCOIN
MAGAZINE

coindesk

Built on top of the Bitcoin blockchain

Omni is a platform for creating and trading custom digital assets and currencies. It is a software layer built on top of the most popular, most audited, most secure blockchain -- Bitcoin. Omni transactions are Bitcoin transactions that enable next-generation features on the Bitcoin Blockchain. Our reference implementation, Omni Core is an enhanced Bitcoin Core that provides all the features of Bitcoin as well as advanced Omni Layer features.



Easily create custom currencies

With Omni it's simple to create tokens to represent custom currencies or assets and to transact these via the Bitcoin blockchain. The power and simplicity offered by Omni has helped to make it the leading Bitcoin based token protocol.

[Click here](#) to see a list of all created tokens.

<https://www.omnilayer.org/>



Faster, more confidential Bitcoin transactions.

Liquid is a sidechain-based settlement network for traders and exchanges, enabling faster, more confidential Bitcoin transactions and the issuance of digital assets.

[GET A LIQUID WALLET](#)[Help Center](#)

LIQUID NETWORK

<https://blockstream.com/liquid/>

11X

Bitcoin Futures with 100X Leverage
Register & Get 110 USDT Bonus

JOIN NOW

Sponsored Content

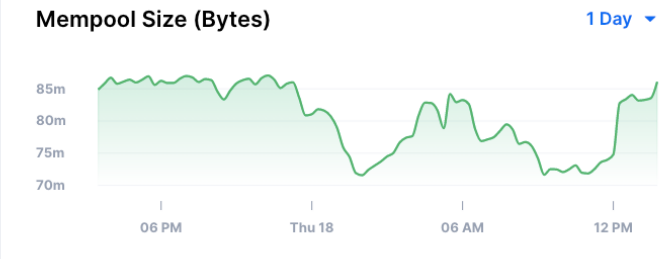
\$51,774.40
Price

155.564 EH/s
Estimated Hash Rate

328,431
Transactions (24hrs)

2.331m BTC
Transaction Volume

150,076 BTC
Transaction Volume (Est)



FAIRSPIN
BLOCKCHAIN CASINO

PRO GAMBLING TOOL

PLAY NOW

Latest Blocks

Height	Mined	Miner	Size
671109	11 minutes	Unknown	1,302,072 bytes
671108	16 minutes	Unknown	1,336,236 bytes
671107	21 minutes	Unknown	1,459,315 bytes
671106	24 minutes	Unknown	1,342,563 bytes
671105	1 hour	Unknown	1,402,823 bytes
671104	1 hour	Unknown	1,354,733 bytes

View All Blocks

Latest Transactions

Hash	Time	Amount (BTC)	Amount (USD)
fff9e318911be2af1f9e0c7...	15:18	0.72434937 BTC	\$37,502.75
e7d9b23c6a3835213ed11...	15:18	0.18190162 BTC	\$9,417.85
521ca3e3a22d0e35c7296...	15:18	1.62737098 BTC	\$84,256.16
06ee4fe430b58a4f314f0...	15:18	2.94233720 BTC	\$152,337.74
047cbd3afa1d2cb0eb4e7f...	15:18	0.00042074 BTC	\$21.78
619bd3711d76b4d12727e...	15:18	0.00400841 BTC	\$207.53

View All Transactions

<https://www.blockchain.com/explorer>



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.

E

The Ethereum Ecosystem

E. The Ethereum Ecosystem

Ethereum is not a blockchain. It's not a cryptocurrency either. It's actually a **protocol** (a set of rules or procedures).

There are multiple independent "networks" that conform to the Ethereum protocol. These networks do not interact with each other.

When most people talk about Ethereum, they are talking about **Mainnet** - the primary public Ethereum production blockchain. This is where actual-value transactions occur on the blockchain.

An Ethereum **account** works across different networks but the account balance and transaction history do not.

Ether (ETH) is Ethereum's native cryptocurrency.

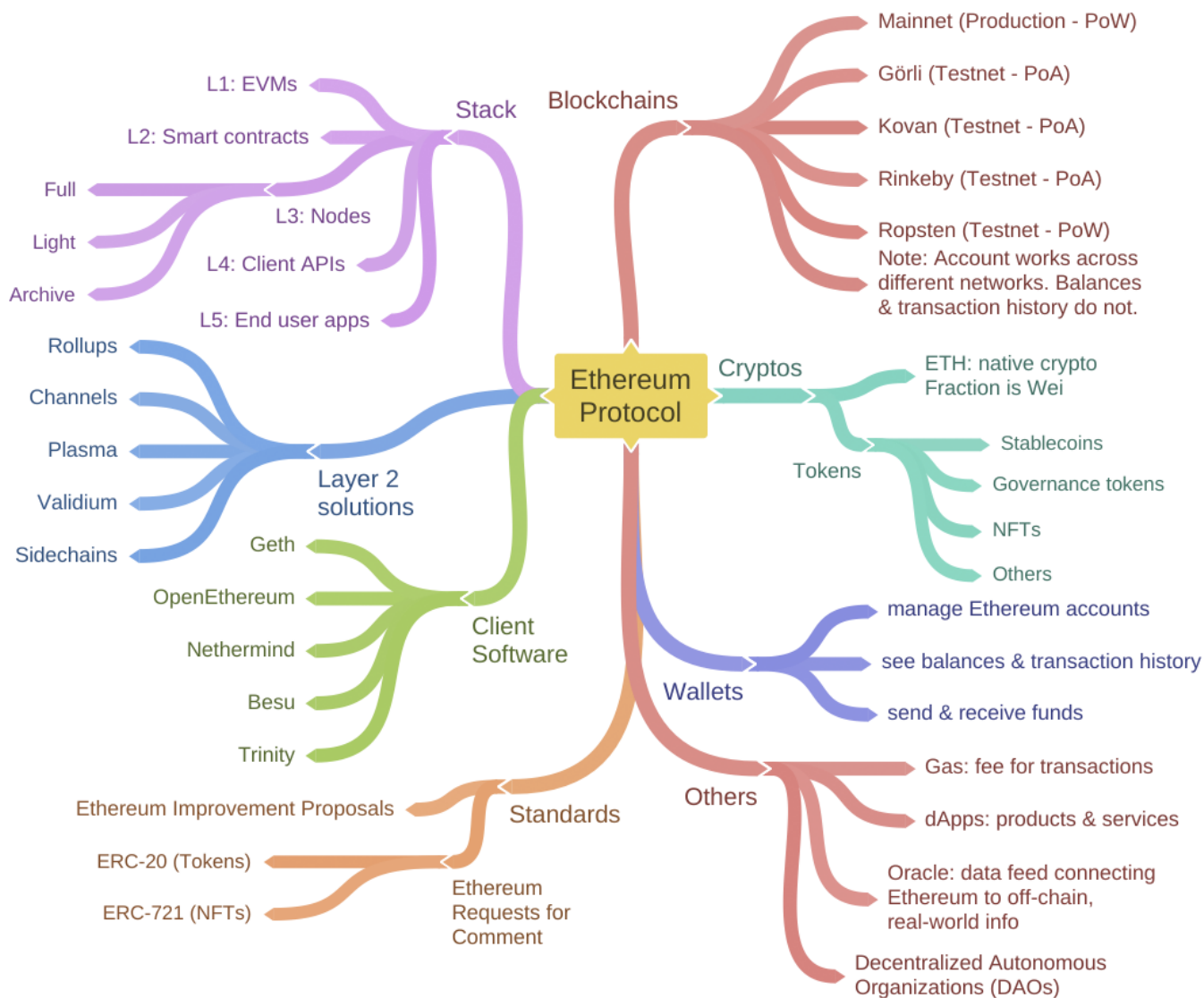
Gas is the fee, measured in Gwei (0.000000001 ETH), that is required to successfully conduct a transaction on Ethereum.

Wei is the smallest fraction of an Ether. One ETH equals 1000000000000000000 Wei.

Anyone can access, read, create and validate transactions on **the Ethereum Public Networks**. There are 5 public networks:

- Mainnet,
- Görli,
- Kovan,
- Rinkeby, and
- Ropsten.

Görli, Kovan, Rinkeby, and Ropsten are testnets used for testing protocol upgrades and potential smart contracts before deployment to mainnet.



Ethereum mindmap

Mainnet and Ropsten use proof-of-work. Görli, Kovan, and Rinkeby use proof-of-authority.

An **Ethereum node** is an implementation of Ethereum client software (such as Geth, OpenEthereum, Nethermind, Besu, or Trinity) that verifies all transactions in each block. A node can be of 3 types:

- full node,
- light node and
- archive node.

An Ethereum **Wallet** is a tool to manage an Ethereum account, see balances & transaction history, and send & receive funds.

Ethereum **dApps** are products and services that run on Ethereum.

An **Oracle** is a data feed connecting Ethereum to off-chain, real-world information for querying data in smart contracts.

Decentralized Autonomous Organizations (DAOs) leverage Ethereum technology for collaboration such as controlling membership, voting on proposals, managing pooled assets, etc.

Layer 2 solutions enable scaling of applications by handling transactions off the main Ethereum chain (Layer 1). Some examples are:

- **Rollups:** They bundle sidechain transactions into a single transaction and generate a cryptographic proof that is submitted to the main chain.
- **Channels:** Participants open a channel by locking an ETH deposit into a multisig contract. They transact quickly and freely off-chain and submit a final on-chain transaction unlocking the state.
- **Plasma:** Separate blockchain anchored to the main Ethereum chain.
- **Validium:** Doesn't store data on the main chain.
- **Sidechains:** Separate blockchains running in parallel to mainnet and operating independently with their own consensus algorithms.

Ethereum standards include:

- Ethereum Improvement Proposals (EIPs)
- Ethereum Requests for Comment (ERC)
- ERC-20 standard interface for tokens
- ERC-721 standard interface for non-fungible tokens

The Ethereum stack comprises 5 levels:

- **Level 1:** Ethereum Virtual Machine (EVM) is the runtime environment for smart contracts in Ethereum.
- **Level 2:** Smart contracts are programs that run on the Ethereum blockchain.
- **Level 3:** Ethereum nodes are computers running Ethereum client software.
- **Level 4:** Ethereum client APIs enable end user applications to connect to the Ethereum blockchain.
- **Level 5:** End user apps are web and mobile applications.

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/>

ETH

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 Charts



For the latest prices, see:

<https://coinmarketcap.com/currencies/ethereum/>

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.

Ethereum Classic Charts



For the latest prices, see:

<https://www.coindesk.com/price/ethereum-classic>



Staking has arrived! If you're looking to stake your ETH, [confirm the deposit contract address](#).



HOW TO STAKE YOUR ETH

Stake your ETH to become an Ethereum validator

Staking is a public good for the Ethereum ecosystem. You can help secure the network and earn rewards in the process.

[Start staking](#)

<https://ethereum.org/en/eth2/staking/>

TOKEN STANDARDS



Last edit: [@jamespfarrell](#) , October 25, 2020

See contributors

Edit page

On this page >

INTRODUCTION

One of the many Ethereum development standards focus on token interfaces. These standards help ensure smart contracts remain composable, so for instance when a new project issues a token, that it remains compatible with existing decentralized exchanges.

PREREQUISITES

- [Ethereum development standards](#)
- [Smart contracts](#)

TOKEN STANDARDS

Here are some of the most popular token standards on Ethereum:

- [ERC20 - A standard interface for tokens](#)
- [ERC721 - A standard interface for non-fungible tokens](#)

<https://ethereum.org/en/developers/docs/standards/tokens/>

ETHEREUM DEVELOPMENT TUTORIALS

Welcome to our curated list of community tutorials.

Submit a tutorial

AAVE (1) ALCHEMY (3) BLOCKCHAIN (1) CLIENTS (3) COMPOSABILITY (1)

COMPOUND (1) CONTINUOUS INTEGRATION (1) CREATE-ETH-APP (2)

DEFI (1) DEPLOYING (2) ERC-20 (2) ERC-721 (1) ETH2 (1)

ETHERS.JS (3) EVENTS (1) FACTORIES (1) FORMAL VERIFICATION (1)

FRONTEND (2) FUZZING (1) GANACHE (2) GETH (2)

GETTING STARTED (6) HARDHAT (1) JAVASCRIPT (5) MOCKING (2)

NODES (4) PYTHON (1) QUERYING (3) REACT (1) REMIX (3)

SABLIER (1) SECURITY (7) SMART CONTRACTS (21) SOLIDITY (21)

STATIC ANALYSIS (1) STORAGE (1) SUBSCRIPTION (1) TESTING (8)

THE GRAPH (2) TOKENS (4) TRANSACTIONS (2) TRUFFLE (3)

UNISWAP (1) WAFFLE (3) WEB3.JS (4) WEB3.PY (1) WEBSOCKETS (1)

<https://ethereum.org/en/developers/tutorials/>

F

Crypto Investing

F1. Decentralized finance (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.

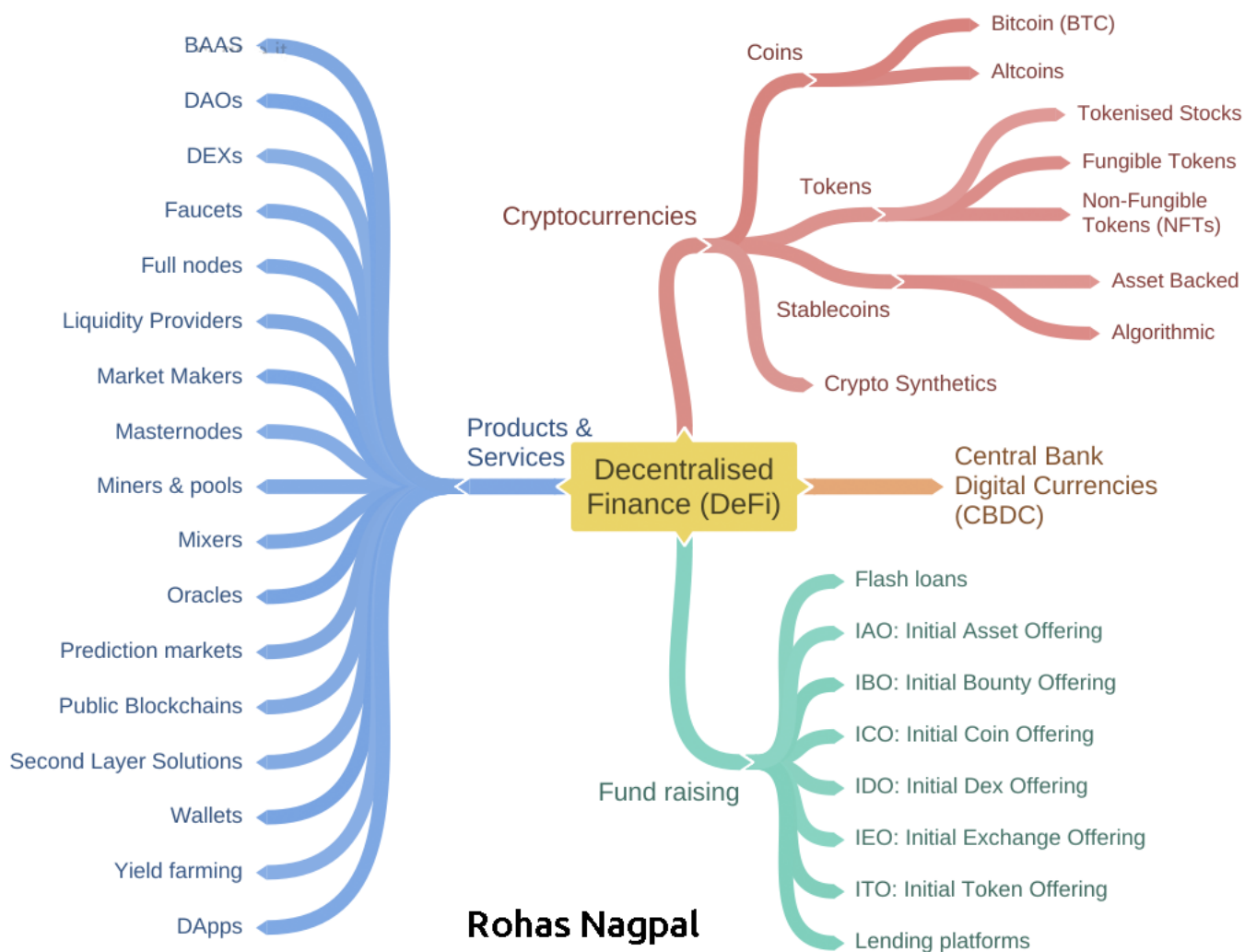
5. **Prediction markets**, which are markets for betting on future events e.g. elections.
6. **Yield farming**, where users scan through multiple DeFi tokens in search of opportunities for larger returns.

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.

DeFi protocols include:

- Uniswap
- AAVE
- Decentraland
- Gnosis
- Balancer
- Synthetix



DeFi mindmap

Protocol Analytics

Search Uniswap pairs and tokens...



ETH Price: \$589.04

Volume (24hrs)

\$262,685,895**-13.07%**

Total Liquidity

\$1.66b**+0.51%**

Liquidity ▾

Liquidity

\$1.66b **+0.51%**

\$4b

\$3b

\$2b

\$1.66b

\$1b

5

Jun

Jul

Aug

Sep

Oct

Nov


Dec



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>

Also see: <https://uniswap.org/docs/v2/protocol-overview/how-uniswap-works>


V2 | V1

[About](#)
[Aave Protocol](#)
[FAQ](#)
[Documentation](#)
[Security](#)

THE LIQUIDITY PROTOCOL

\$ 1,898,185,944.28

Aave is an open source and non-custodial liquidity protocol for earning interest on deposits and borrowing assets.

Enter app

USD

Native

Assets


Market size

Total borrowed

Deposit APY

Variable Borrow APR

Stable Borrow APR



USD Coin (USDC)

\$ 122.03M

\$ 103.85M

6.62%

Past 30D Avg. 6.00%


7.62%

Past 30D Avg. 7.15%

9.17%

Deposit

Borrow



TrueUSD (TUSD)

\$ 113.01M

\$ 49.65M

1.41%

Past 30D Avg. 2.17%


3.20%

Past 30D Avg. 3.94%

—

Deposit

Borrow



USDT Coin (USDT)

\$ 141.48M

\$ 90.69M

4.36%

Past 30D Avg. 6.20%


5.99%

Past 30D Avg. 7.74%

7.77%

Deposit

Borrow



sUSD

\$ 3.43M

\$ 549.74K

0.29%

Past 30D Avg. 11.16%


1.80%

Past 30D Avg. 13.14%

—

Deposit

Borrow



Binance USD (BUSD)

\$ 25.55M

\$ 14.8M

2.26%

Past 30D Avg. 3.69%


3.90%

Past 30D Avg. 3.69%

—

Deposit

Borrow



Ethereum (ETH)

\$ 264.42M

\$ 29.1M

0.16%

Past 30D Avg. 9.35%

1.35%

Past 30D Avg. 1.42%

4.69%

Deposit

Borrow

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 over-collateralized (perpetually) or under-collateralized (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.

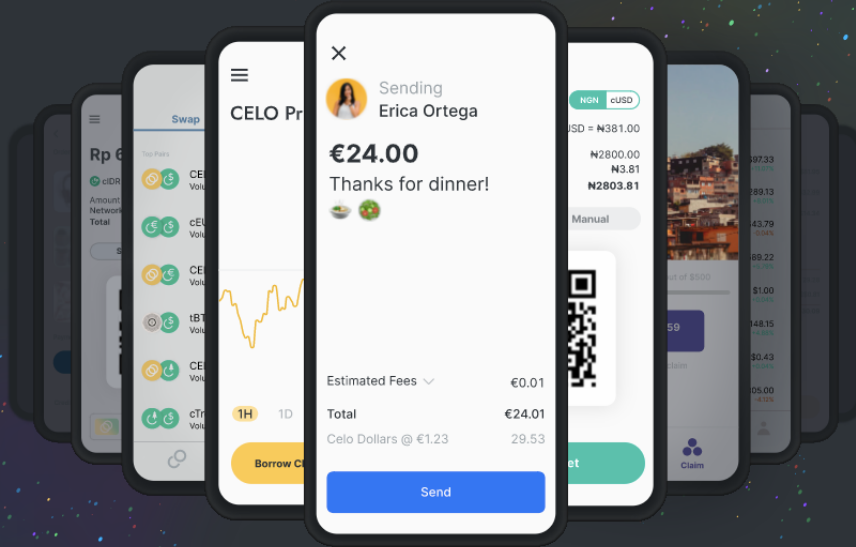
There are also transaction fees for Ethereum Blockchain usage, which depend on the network status and transaction complexity.



Global payments infrastructure built for mobile

Thousands of organizations and individuals are developing, growing, and governing Celo, an open-source platform that enables anyone to build borderless applications

Start Building



The Builders Platform



Mobile

Hyper-efficient light client and full node incentives allowing for scalability to 6 billion smartphones. Full EVM compatibility making it easy to get started.

[Make it mobile with DappKit >](#)



Stable

Growing family of native stablecoins, like Celo Dollars, which follow the value of fiat currencies. Pay transaction fees with stablecoins or your own tokens.

[Learn more about Celo Dollars >](#)




Usable

Users can easily send currency to any mobile number, enabled by Celo's decentralized phone verification protocol, and get access to a growing ecosystem of global cash-in cash-out options.

[See it in action with Valora >](#)

Build the Internet of Finance

Avalanche is an open-source platform for launching **highly decentralized applications**, new **financial primitives**, and new **interoperable blockchains**.

Build 

Community

Explore some useful links:

Avalanche

Mainnet

Avalanche Explorer
Avalanche Wallet
AVAX Public Sale Info
(Closed)

Developers

Documentation
GitHub
Avalanche Forum
Avalanche-X
Athereum
Whitepapers



Learn & Get Help

Why Avalanche?
Solutions
Roadmap
Blog
Support

Get Involved

Propose a Grant
Explore Open Grants
Social
News



The internet of

Avalanche democratizes financial markets and bridges all blockchain platforms together into one interoperable ecosystem.

Build your own custom blockchains or digitize any assets with arbitrarily complex rulesets.

```
> ~ cd avalanchego
> avalanchego git:(master) ./scripts/build.sh
> avalanchego git:(master) ./build/avalanche --db=true --require_staking=true

INFO [01-05 | 15:07:34] /node/node.go#292: Initializing RPC server
INFO [01-05 | 15:07:34] /node/node.go#292: Initializing Statistics Plugin
INFO [01-05 | 15:07:34] /node/node.go#292: Initializing Admin RPC Service
INFO [01-05 | 15:07:34] /node/node.go#292: Initializing Wallet Plugin
INFO [01-05 | 15:07:34] /node/node.go#292: Initializing Avalanche Plugin

...
```

<https://www.avalabs.org/>

Announcing the Solana x Serum DeFi Hackathon

Register today and join leaders from Circle, Aave, SushiSwap, and more!

[LEARN MORE →](#)

Build Crypto Apps that Scale

Solana is a fast, secure, and censorship resistant blockchain providing the open infrastructure required for global adoption.

[START BUILDING →](#)[CONTACT US](#)

11,835,389,152
Total Transactions

587ms
Block Time

\$0.00001
Avg. Fee Per Transaction

643
Global Validators

<https://solana.com/>

COSMOS

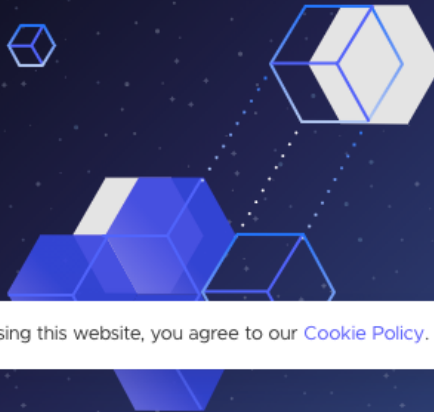


THE FOUNDATION FOR A NEW TOKEN ECONOMY

Join the **most customizable**
ecosystem of connected blockchains

WATCH VIDEO ↗

LEARN MORE ↓



By using this website, you agree to our [Cookie Policy](#).



<https://cosmos.network/>

The Builder's fastest path to market

NEAR is an open source platform that accelerates the development of decentralized applications.



Build your first app in 5 min. Try it!

```
# Make sure you have Node.js installed.  
# Run this in your CLI to initialize a web app and follow  
instructions from there  
npx create-near-app your-awesome-project
```

<https://near.org/>

[AVATARS](#)[MARKETPLACE](#)[BUILDER](#)[DOCS](#)[EVENTS](#)[DAO](#)[BLOG](#)[GET STARTED](#)

Welcome to Decentraland

thejoeart
Create, explore and trade in the first-ever virtual
baus
world owned by its users.

[GET STARTED](#)

Jessie

Guest-3a11dd

Explore

Lose yourself in an amazing, evolving world

Explore LANDs owned by users to experience incredible scenes and structures. From a space adventure to a medieval dungeon maze to entire villages crafted from the minds of community members.

[START EXPLORING](#)



Gnosis builds new market mechanisms for decentralized finance. Our three interoperable product lines allow you to securely **create**, **trade**, and **hold** digital assets on Ethereum.

Build on Gnosis

The Gnosis Developer Portal provides introductions, technical documentation, and tutorials, and the **Gnosis Ecosystem Fund (GECO)** provides teams with mentoring, marketing, and funding up to \$100,000 to build on Gnosis.

[Get Started](#)[Visit Forum](#)

Participate in GnosisDAO


GnosisDAO is the prediction market-driven collective, stewarding the Gnosis ecosystem through futarchy: governance by prediction markets.

Balancer is a protocol for
programmable liquidity

WHITEPAPER

EXCHANGE



 Balancer

0xeF83...43e7

Shared Pools

Private Pools

ETH

WRAP

Keep some ETH unwrapped for transaction fees

WETH

Max

UNWRAP

MY WALLET

ETH

11.8085

BAL

6.6661



DAI

1004.8252

MKR





0.002

My Liquidity

Pool Address	Assets	Swap Fee	Liquidity	My Liquidity	Trade Vol. (24h)
0x6b98...52E2	 • 50.00% BAL • 50.00% WETH	0.95%	\$ 4,215,909.63	\$ 1,117.53	\$ 64,400.81
0x95f0...d2Db	 • 75.00% LINK • 25.00% WETH	0.2%	\$ 306,770.56	\$ 1,354.44	\$ 4,119.62

Shared Pools

Create Pool

Pool Address	Assets	Swap Fee	Liquidity	My Liquidity	Trade Vol. (24h)
0x72Cd...1d2C	 • 50.00% USDC • 50.00% mUSD	0.05%	\$ 17,463,269.74	\$ -	\$ 342,545.24
0x454c...8A3B	 • 90.00% RPL • 10.00% WETH	0.05%	\$ 11,216,955.86	\$ -	\$ 92,387.35
0x59A1...6fB4	 • 80.00% BAL • 20.00% WETH	0.15%	\$ 10,146,390.76	\$ -	\$ 469,485.78
0x9866...1fC3	 • 60.00% MKR • 40.00% WETH	0.2%	\$ 9,501,898.97	\$ -	\$ 169,370.10

<https://balancer.finance/>

THE DERIVATIVES LIQUIDITY PROTOCOL

Synthetix is the backbone for derivatives trading in DeFi, allowing anyone, anywhere to gain on-chain exposure to a vast range of assets.

LEARN MORE

TOTAL VALUE LOCKED IN SYNTHETIX
\$2,536,386,726

<https://synthetix.io/>

F2. How to profit from crypto

1. Airdrops

An airdrop is a marketing activity by a new crypto project. A small amount of crypto is sent out for "free" to increase awareness. It's not entirely "free" as you may need to do some promotional work like retweeting a post, sharing a link with your network, etc. If you want to bypass this work, you can sign up for automated services like AirDrop Alert:

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

2. Bug bounties

Many projects pay serious money if you find bugs in their platform/code. This requires a ton of "hacking" talent.

3. Learn and Earn

Some cryptos pay you to learn about them. This is great because you are getting paid to learn interesting stuff! It usually requires you to watch a few videos and take a quiz or two. Head over to <https://coinmarketcap.com/earn> to get started.

4. HODL

HODL is an acronym for "Hold on for Dear Life". Most bitcoin investors I know fall under this category. So while they don't "book" profits, their net worth has been skyrocketing. You really need to be a "believer" and a long-term player for this.

5. Dividends

Some crypto assets pay dividends similar to how companies pay dividends to shareholders. An example is KuCoin, a crypto exchange that pays 50% of all trading fees as dividends to Kucoin Shares (KCS) holders.

6. Staking

Bitcoin uses "mining" to validate transactions. This costs a huge amount of electricity and computational power. Many other cryptos (e.g. TRX, XTZ, ATOM, VET, ALGO) use a more eco-friendly way of validating transactions - proof of stake. This requires you to temporarily "lock" your crypto in a wallet or exchange.

7. Day trading

People "gamble" on a lot of things - horse races, dog races, lotteries, and even cockroach races! In fact, there are many "prediction markets" out there for gamblers. Well, day traders gamble on cryptos. This is probably the riskiest way to "try" to make money. Most day traders I know barely break even.

8. Smart investing

This is what savvy investors do. First, they identify great projects using the R.O.H.A.S. method by analyzing the Revenue models, Organization, History, Algorithms, and Social engagement levels. Then they buy at the right time and hold for the medium to long term. Then they sell at the right time. To be honest this is not as simple as it sounds. But it's one of the best ways to profit from crypto.

9. Sit at the other side of the table

This is the ultimate way to profit from crypto. The really serious players don't just invest or trade in crypto. They run their own exchanges, DeFi platforms, blockchains, stablecoins, and cryptocurrencies. They also provide liquidity and market making. You can also raise funds through Initial Coin Offerings (ICOs), Initial Exchange Offerings (IEOs) and Initial Token Offerings (ITOs).

If this is what you want to do, get in touch with me :-)



Make passive income from Crypto!

Are you looking for ways to create passive income? Congratulations, you have discovered the right place, Best Crypto Dividends provides information and detailed calculators that allow you to discover which cryptocurrency investment is best for you.

[View coins & tokens below](#)

Cryptocurrency dividends calculators

Use our free and easy dividends calculators to explore which cryptocurrency will provide you with the best return on investment.



Kucoin
Shares
KCS



Bibox
BIX



Coss
COSS



BitMax
BTMX



Bitsdaq
BQQQ



Neo
NEO



Ontology
ONT



Beaxy
BXY

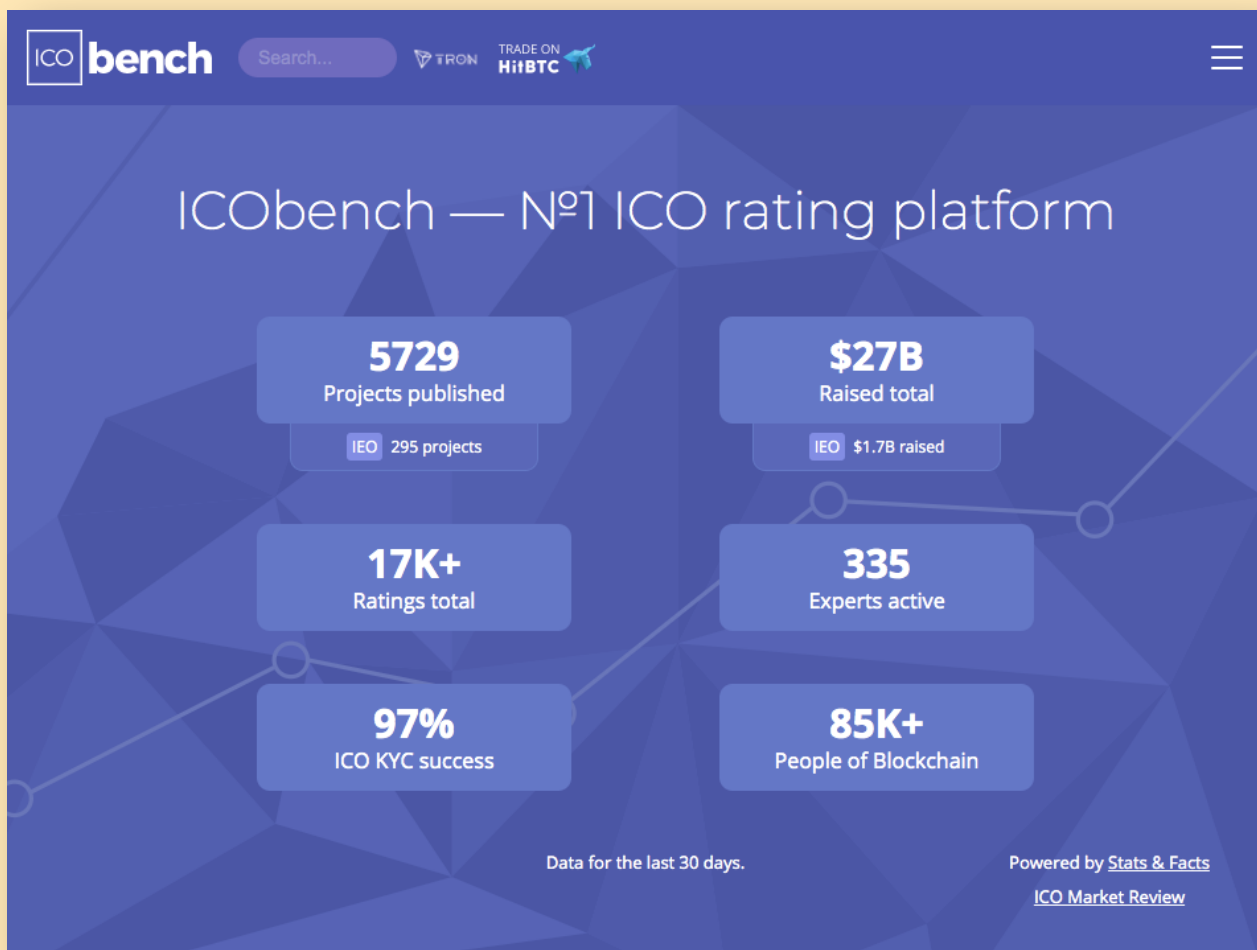


Best Cryptocurrency Dividends provides calculators for fee share tokens, masternode payouts and bonuses.

<https://www.bestcryptodividends.com>

Also see:

<http://www.thelazycryptoinvestor.com>



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>

[ICO LIST](#)
[GUIDES](#)
[STATISTICS](#)

Welcome to the ICO Watch List!

Discover the best ICO (initial coin offering) opportunities. Review this list daily to stay on top of the exponentially growing cryptocurrency & blockchain ecosystem. The projects on the ICO list are scanned and updated regularly, to help crypto token buyers make better decisions.

Positions on this page such as gold & silver are sponsored and are **NOT** an indicator of the quality of the ICO. [Here](#) is more info on how to use our platform.

LIVE ICOs

UPCOMING ICOs

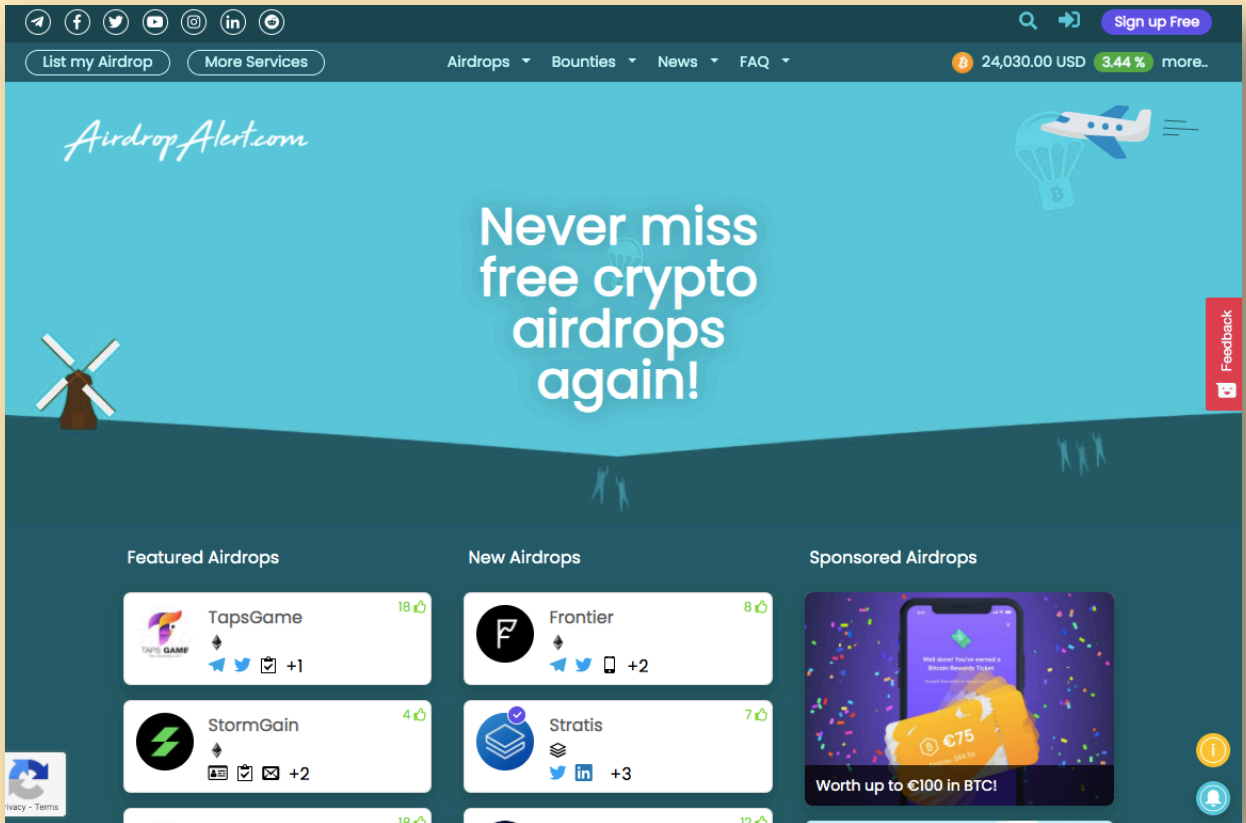
FINISHED ICOs

PROJECT	INFO	TIME	TIMELINE	
 <small>NETWORK/COMMUNICATIONS</small>	With over 1 million location-verifying beacons already in the world, XYO is blockchain's first crypto-location oracle network.	ENDS IN: 30 07 56 <small>Days Hours Minutes</small>	 3%	ICO Details
 <small>BLOCKCHAIN PLATFORM</small>	4th Generation Blockchain with a Multidimensional Structure (POS).	PRESALE ENDS IN: 10 22 55 <small>Days Hours Minutes</small>	 64%	ICO Details
 <small>ENTERTAINMENT</small>	BunnyToken is a payment solution for the \$103 billion adult industry.	PRESALE ENDS IN: 33 23 55 <small>Days Hours Minutes</small>	 18%	ICO Details
 <small>DATA/COMPUTING/AI</small>	Crowd Machine is powering the next generation of decentralized blockchain applications.	PRESALE ENDS IN: 10 23 55 <small>Days Hours Minutes</small>	 81%	ICO Details
 <small>PAYMENTS/WALLETS</small>	Branded debit cards and secure payment infrastructure for all companies and ICOs that issue cryptocurrencies.	ENDS IN: 24 00 56 <small>Days Hours Minutes</small>	 22%	ICO Details

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>

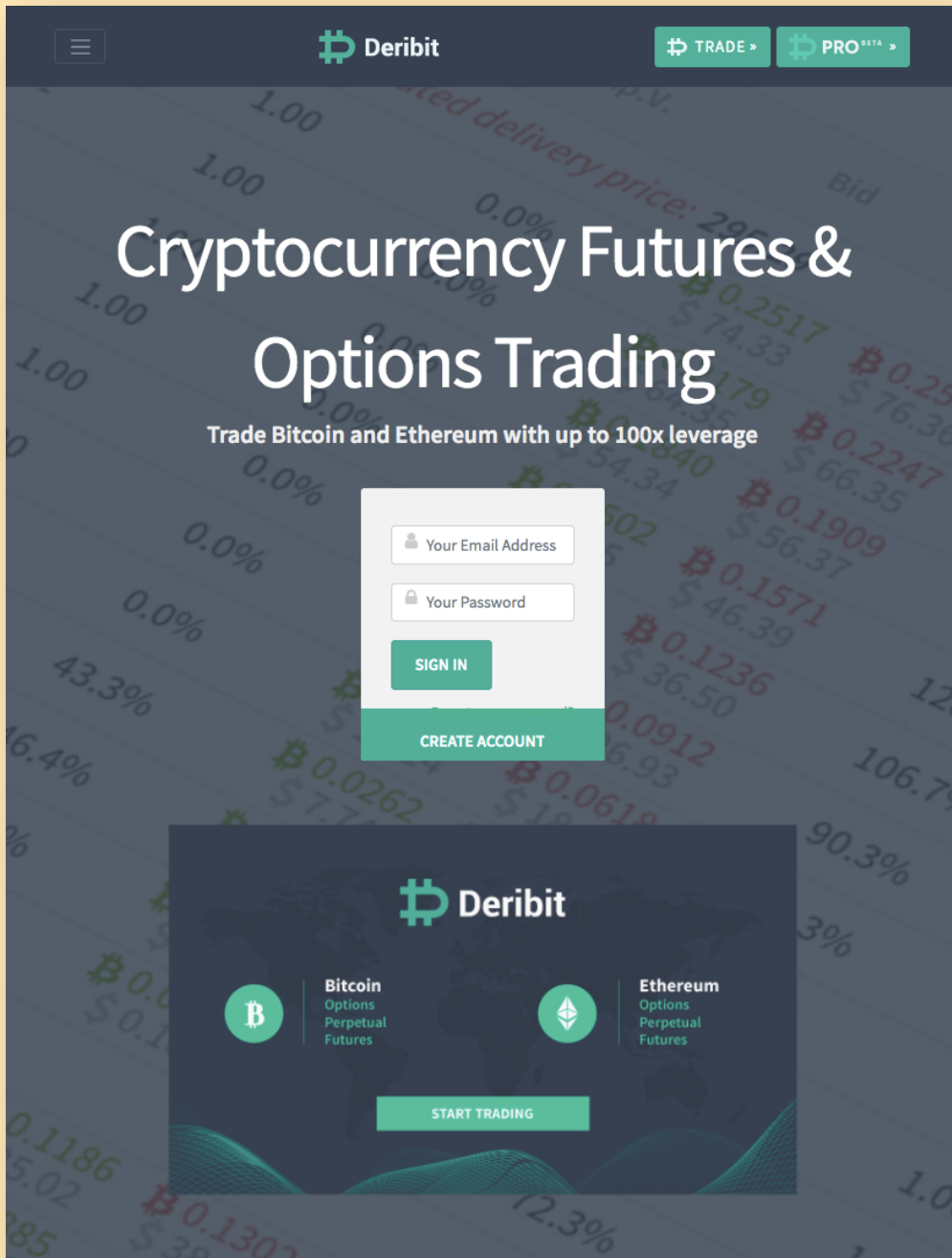
Get FREE cryptocurrency coins



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>



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



Earn Passive Income With Crypto

Staking Rewards is the leading data provider for staking and crypto-growth tools. We are currently tracking **156** yield-bearing assets with an average reward rate of **21.27%** and **1693** qualified providers.



Claim this ad space



Staking Marketcap \$135,483,547,228 3.15%



Allnodes Earn up to 47.24%



Top 10 Crypto Assets by Score

Asset	Price	Reward	Adj. Reward	Market Cap	24h Volume	Total Staked
-------	-------	--------	-------------	------------	------------	--------------

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>



How to use candlesticks when trading cryptocurrency

<https://blog.liquid.com/how-to-use-candlesticks-when-trading-cryptocurrency>

CRYPTO EARN

Up to 6.5% p.a. on Your Crypto *

Up to 12% p.a. for Stablecoins

Simple interest paid weekly in your crypto (e.g. BTC deposit, interest paid in BTC)

Compare Staking and Non-Staking Benefits

With 5,000 or Less
CRO Stake



With 50,000 or More
CRO Stake



	Supported Coins	Supported Stablecoins	CRO
3-month	up to 6.5% p.a.	12% p.a.	6% p.a.
1-month	up to 4.5% p.a.	10% p.a.	4% p.a.
Flexible	up to 2% p.a.	8% p.a.	2% p.a.

For the latest rates, please check the Crypto.com App.

Bonus: Users that stake 500,000 CRO or more earn an additional 2% p.a. on fixed term deposits (paid in CRO). Not applicable to CRO deposits.

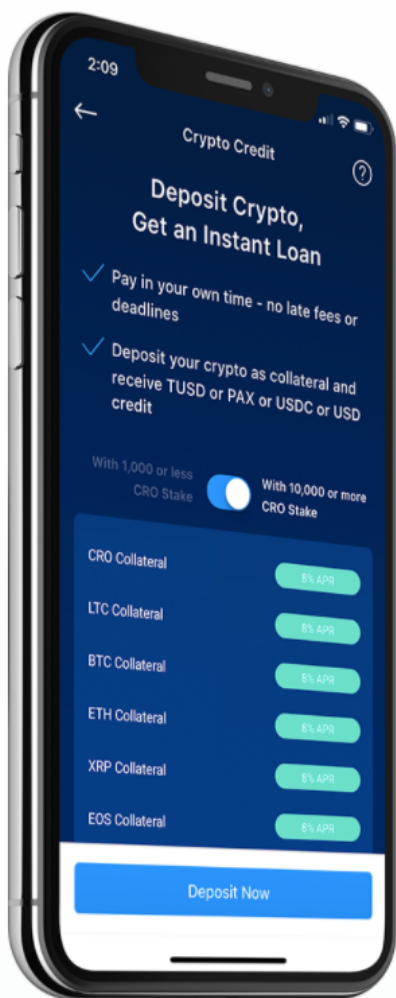
<https://crypto.com/en/earn.html>

NOT YET AVAILABLE IN UNITED STATES

CRYPTO CREDIT

Deposit Crypto, Get an Instant Loan

- ✓ Instant credit, ready to spend
- ✓ No credit check required
- ✓ No repayment deadline



<https://crypto.com/en/credit.html>

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>

The World's First Tokenized

Cryptocurrency Index Fund



FUND VALUE	TOKEN NAV	C20 MOVEMENT
\$24,088,149	\$0.88163	-1.68% ^{1h} -6.81% ^{24h} -3.85% ^{1w}



Fact Sheet



White Paper

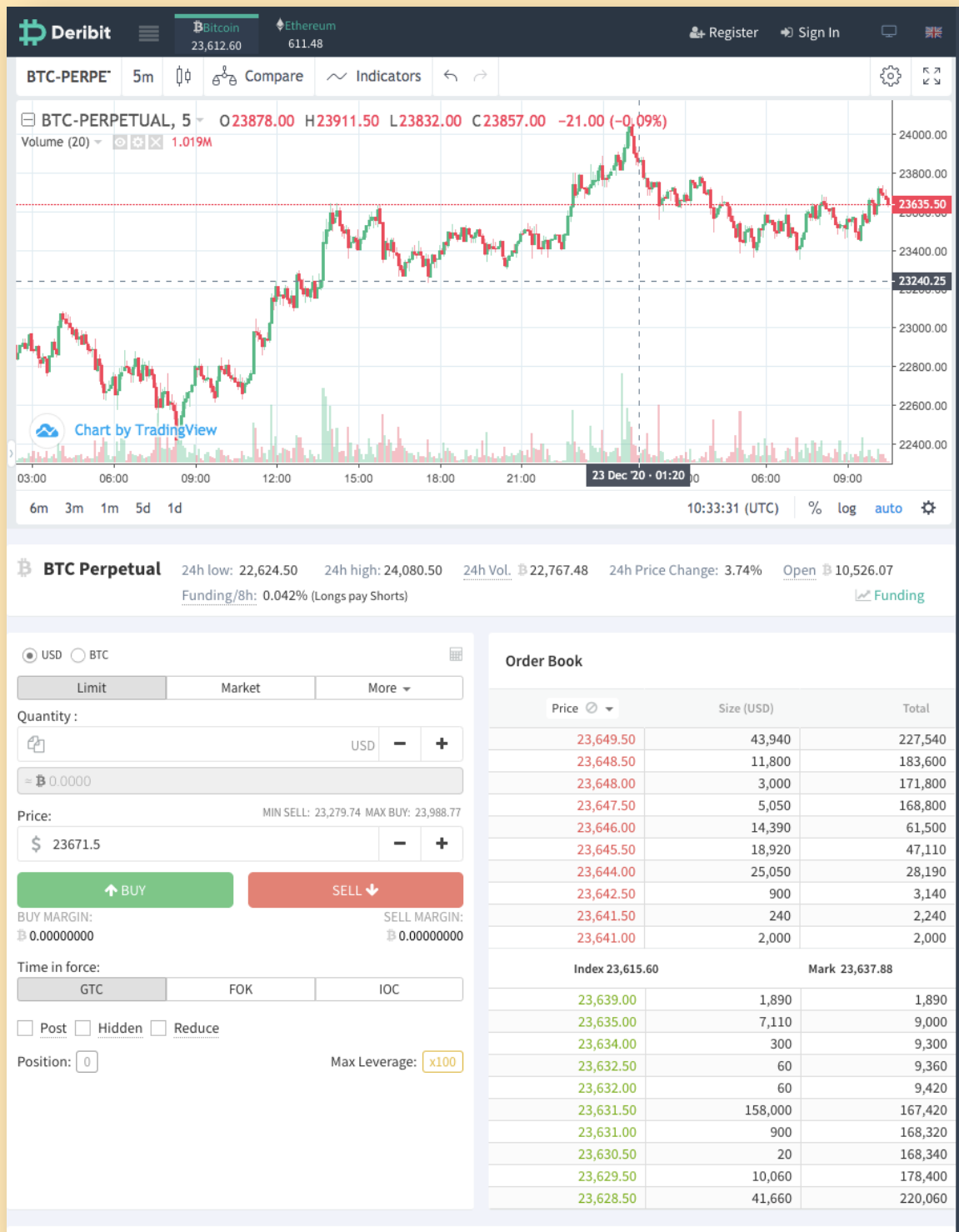


Q3 Report 2020

CRYPTO20 is an autonomous cryptocurrency index fund.

<https://www.crypto20.com/en>

Deribit



Deribit enables Cryptocurrency Futures & Options Trading.
This allows trading of Bitcoin and Ethereum with up to 100x leverage.

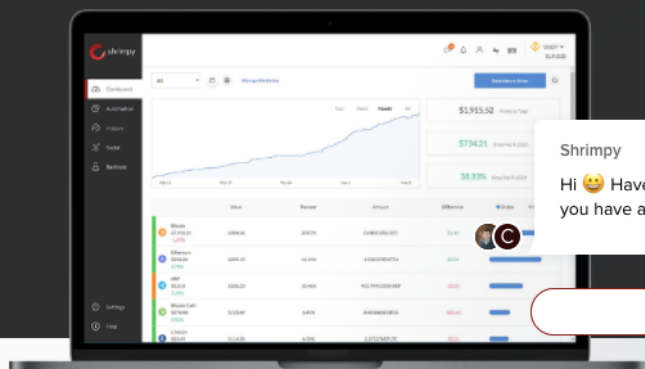
<https://www.deribit.com>

The Social Trading Platform for Cryptocurrency

Simplify the way you manage your portfolio by automating your trading strategy.

Demo

Get Started



Shrimpy

Hi 😊 Have a look around! Let us know if you have any questions.

✉ Write a reply



Automate A Strategy For The Long-Term

Connect Shrimpy to all your crypto exchange accounts to automate trading strategies that can improve performance and reduce risk in the long-term.

Copy The World's Best Traders

Automatically copy the top crypto traders on the only social trading platform that was built for simple portfolio management.



F3. Crypto Exchanges

Some of the top **Spot** (instant settlement) Crypto Exchanges are:

1. Binance
2. Huobi Global Huobi
3. Coinbase Pro
4. Kraken
5. Bitfinex
6. Bitstamp
7. KuCoin
8. bitFlyer
9. Bittrex
10. Coinone

Some of the top Cryptocurrency **Derivatives** Exchanges:

1. Binance
2. Huobi Global Huobi
3. Bybit
4. OKEx
5. FTX
6. Bitget
7. BitZ
8. BitMEX
9. ZBG
10. Deribit

Some of the top Cryptocurrency **Decentralized** Exchanges are:

1. Uniswap
2. PancakeSwap
3. SushiSwap
4. BurgerSwap
5. 1inch Exchange
6. Compound
7. Curve Finance
8. Tokenion
9. Balancer
10. dYdX

Binance

The screenshot shows the Binance website's landing page for India. At the top, there's a dark header with the 'BINANCE APP' logo and a download button. Below this is a navigation bar with the Binance logo, a grid icon, and links for 'Buy Crypto' (with a USD dropdown), 'Markets', 'Trade', 'Derivatives', and 'Finance'. A 'Register' button is on the right. The main banner features the text 'Buy Bitcoin with INR' and 'Join the world's largest crypto exchange. Designed for India'. It includes an input field for an email address and a 'Register Now' button. The background of the banner shows the Indian Parliament building and a large Indian Rupee symbol. Below the banner, there are four market cards for BTC/BUSD, ETH/BUSD, BNB/BUSD, and XRP/BUSD, each displaying the current price, volume, and percentage change.

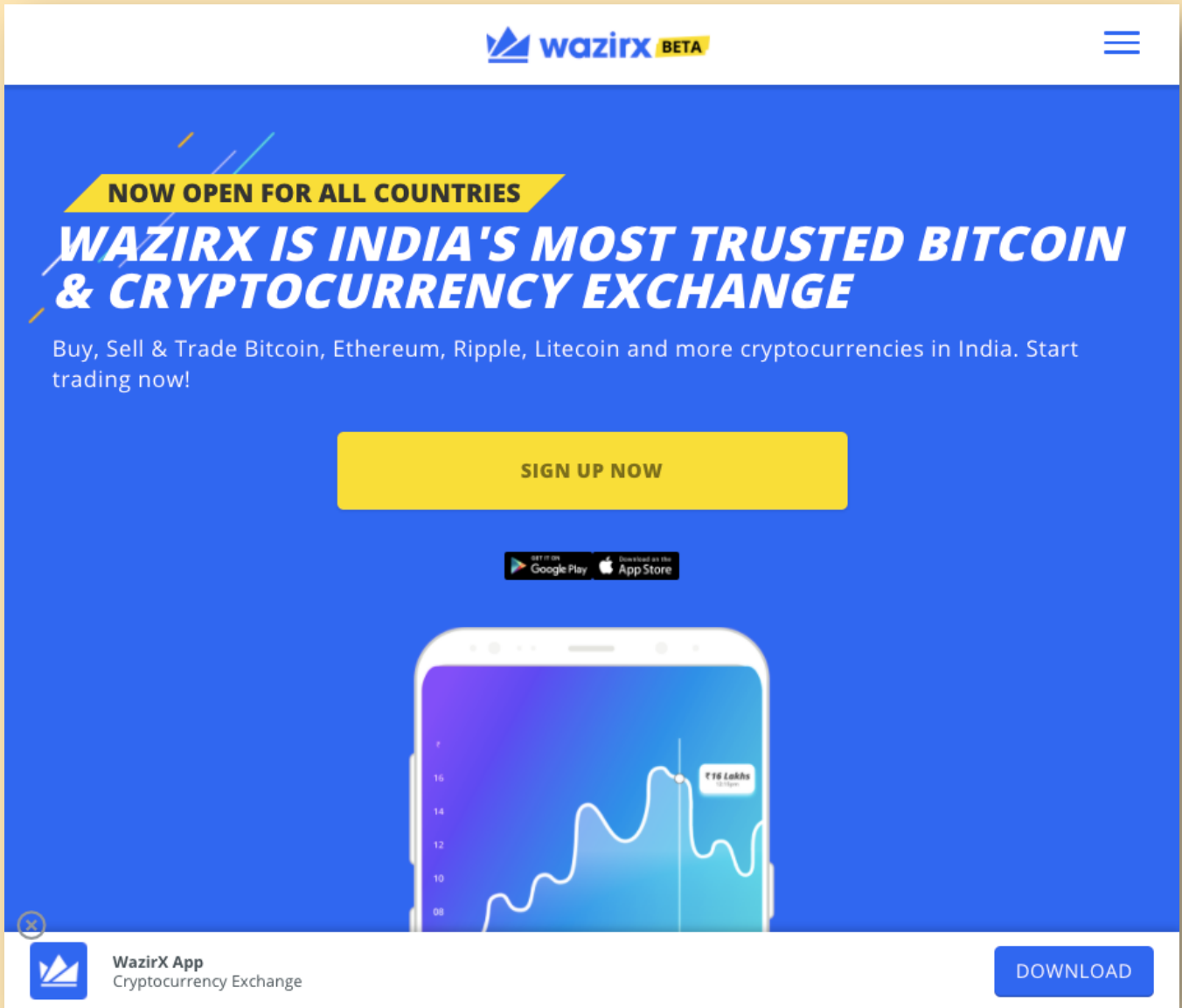
Pair	Current Price	Volume	Change
BTC / BUSD	23,394.50	311,500,093.48 BUSD	+2.97%
ETH / BUSD	600.77	221,678,765.60 BUSD	-0.48%
BNB / BUSD	32.1470	19,688,150.97 BUSD	+1.53%
XRP / BUSD	0.31381	84,994,307.63 BUSD	-33.51%

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/en/register?ref=HB4ZZL5H>

WazirX



The banner features a blue background with a yellow header bar containing the WazirX logo and 'BETA' text. A yellow diagonal bar on the left contains the text 'NOW OPEN FOR ALL COUNTRIES'. The main headline is 'WAZIRX IS INDIA'S MOST TRUSTED BITCOIN & CRYPTOCURRENCY EXCHANGE' in large, bold, white letters. Below this, a line of text says 'Buy, Sell & Trade Bitcoin, Ethereum, Ripple, Litecoin and more cryptocurrencies in India. Start trading now!'. A large yellow button in the center says 'SIGN UP NOW'. Below the button are icons for Google Play and the App Store. At the bottom, there is a smartphone displaying a line graph with a peak labeled '₹16 Lakhs'. The bottom left corner has the WazirX App logo and text 'WazirX App Cryptocurrency Exchange'. The bottom right corner has a blue button that says 'DOWNLOAD'.

WAZIRX IS INDIA'S MOST TRUSTED BITCOIN & CRYPTOCURRENCY EXCHANGE

Buy, Sell & Trade Bitcoin, Ethereum, Ripple, Litecoin and more cryptocurrencies in India. Start trading now!

SIGN UP NOW

GET IT ON Google Play Download on the App Store

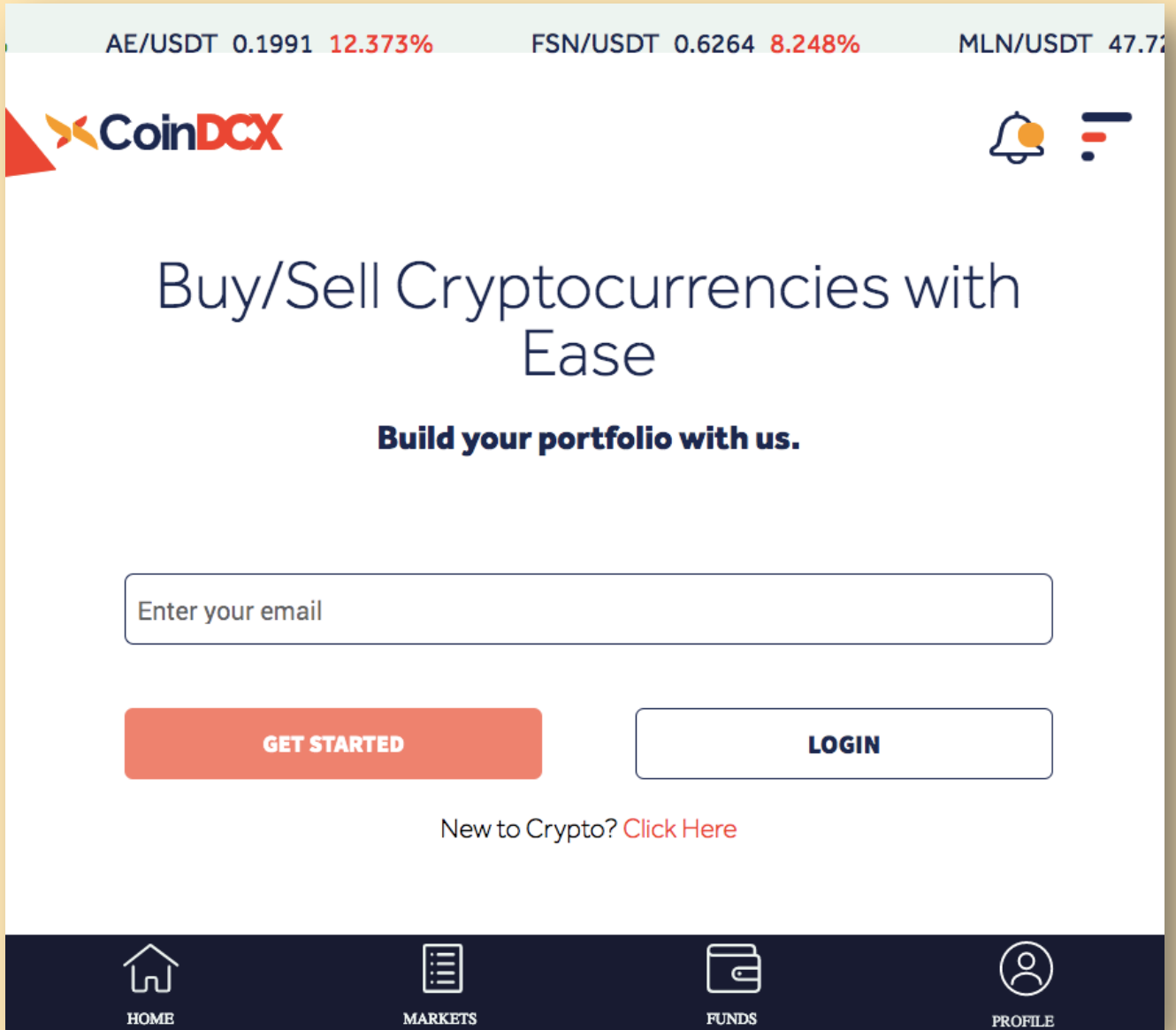
₹16 Lakhs

WazirX App
Cryptocurrency Exchange

DOWNLOAD

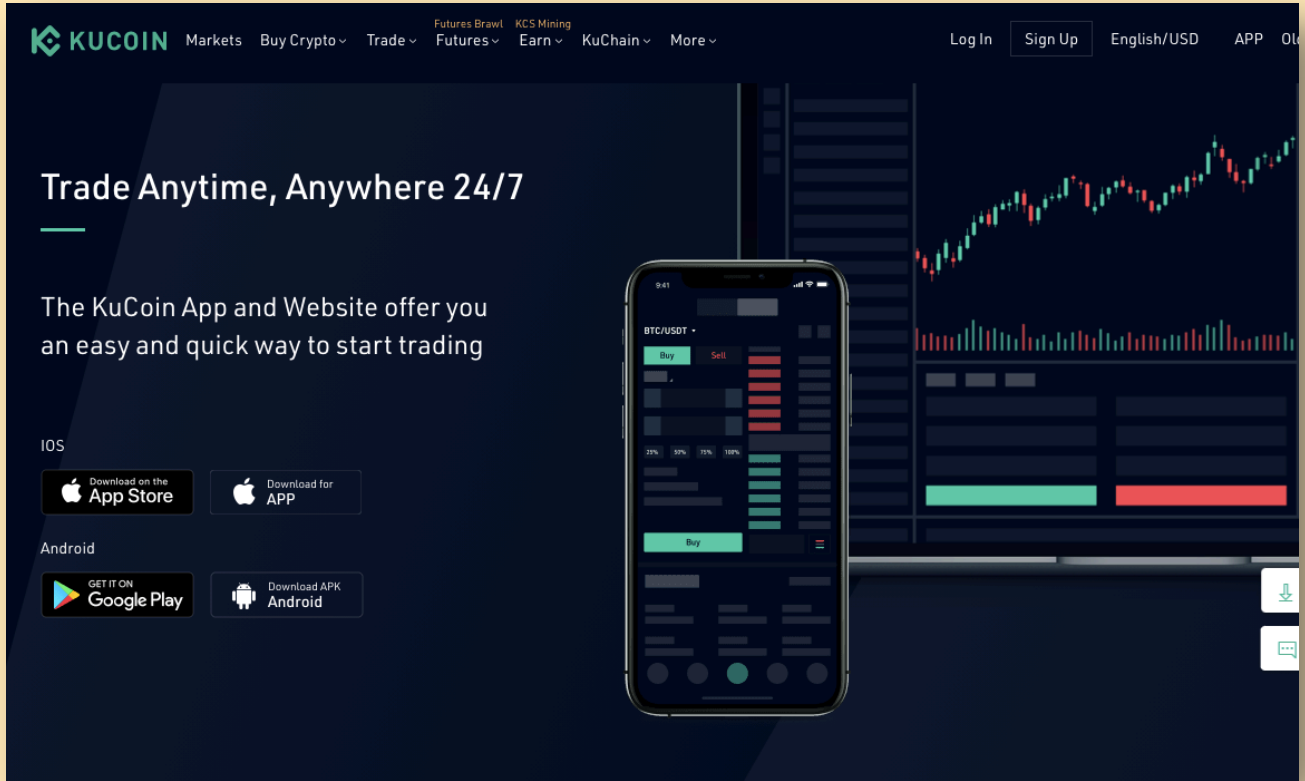
WazirX is a leading Indian crypto exchange.
<https://wazirx.com/invite/dtha8t87>

CoinDCX



CoinDCX is a leading Indian crypto exchange.
[https://coindcx.com/signup?r=09625454\\$\\$\\$Olexp](https://coindcx.com/signup?r=09625454$$$Olexp)

Kucoin



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>

F4. 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.

F5. 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>

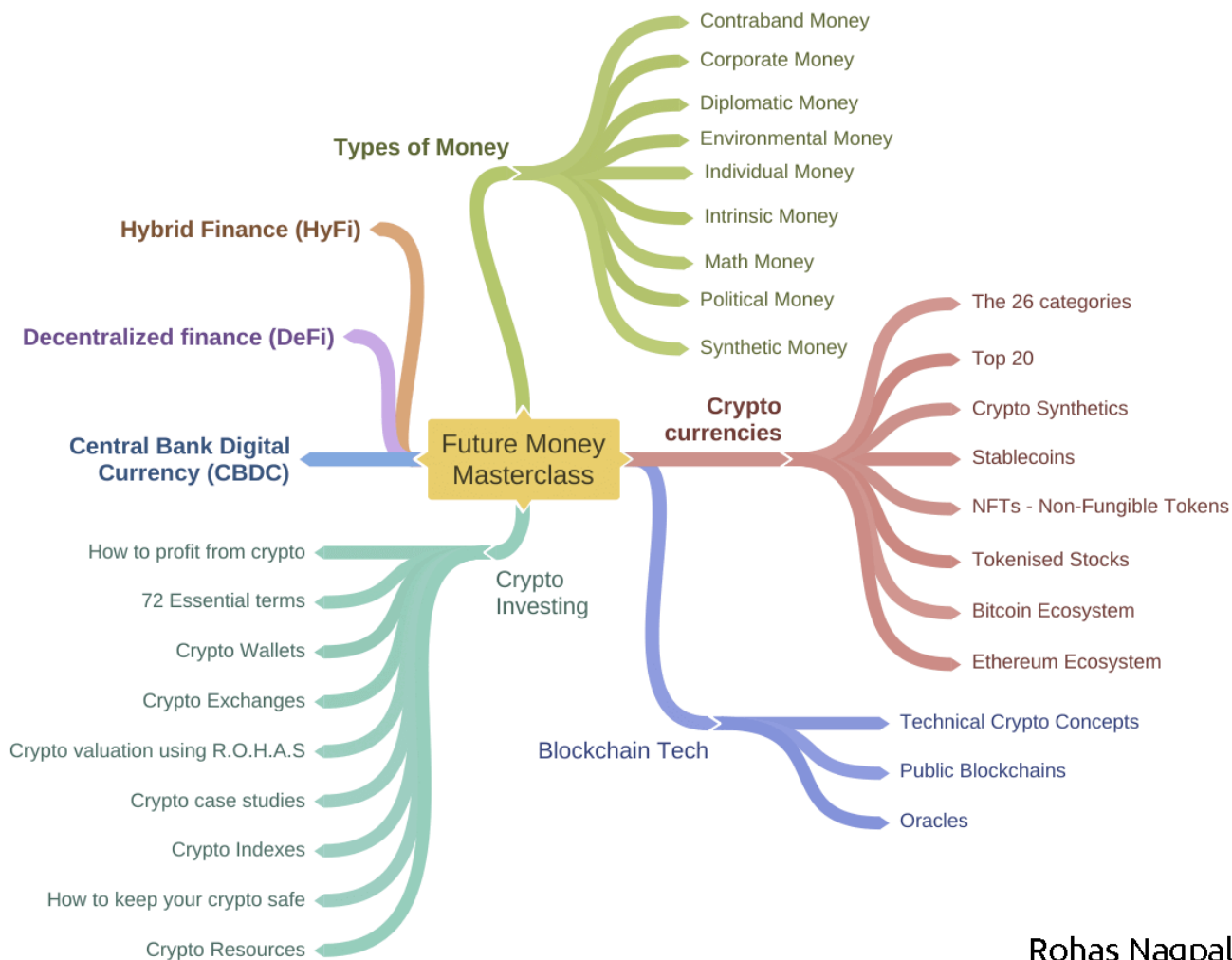
CUSTOM GOOGLE SEARCH ENGINE FOR CRYPTOS

Searching for crypto information online can be a pain.

For example, searching for BAT (Basic Attention Token) will show results for cricket bats and the scary mammal. So, to make the search easier and faster, check out this custom Google search engine maintained by Sanya.

You can access it at:

<https://cse.google.com/cse?cx=421011fe27d8822e3>



Rohas Nagpal

Future Money Masterclass

<https://www.asianlaws.org/future-money-masterclass.php>

Future
Money
Newsletter

NEWSLETTER

The Future Money Newsletter

For those who want to know what the future of money looks like



By **Rohas Nagpal**
Future Money Evangelist

Published weekly
6,036 subscribers

Subscribed

Share

Editions 24

Published 1 week ago



Framework for valuing cryptocurrencies

Rohas Nagpal on LinkedIn

20

Your dream
job is closer
than you
think

See jobs

LinkedIn

[About](#) [Accessibility](#) [Help Center](#)

[Privacy & Terms](#) [Ad Choices](#)

[Advertising](#) [Business Services](#)

[Get the LinkedIn app](#) [More](#)

LinkedIn LinkedIn Corporation © 2021



Messaging

Future Money Newsletter
<http://bit.ly/38d83Dw>

Bitcoin Forum

simple machines forum




December 23, 2020, 04:11:56 PM

Welcome, **Guest**. Please login or register.

News: [Bitcointalk Community Awards results](#)

[HOME](#)
[HELP](#)
[SEARCH](#)
[LOGIN](#)
[REGISTER](#)
[MORE](#)





















Bitcoin Forum

Bitcoin			
	Bitcoin Discussion General discussion about the Bitcoin ecosystem that doesn't fit better elsewhere. News, the Bitcoin community, innovations, the general environment, etc. Discussion of specific Bitcoin-related services usually belongs in other sections. <i>Moderator: hilariousandco</i>	2295466 Posts 92635 Topics	Last post by sapnu in Re: Is bitcoin difficult... on Today at 04:10:21 PM
Child Boards: Legal, Press, Meetups, Important Announcements			
	Development & Technical Discussion Technical discussion about Satoshi's Bitcoin client and the Bitcoin network in general. No third-party sites/clients, bug reports that do not require much discussion (use github), or support requests. <i>Moderators: gmaxwell, achow101</i>	266003 Posts 21512 Topics	Last post by ruzyysmartt in Re: Recover wallet from ... on Today at 01:42:21 PM
Child Boards: Wallet software			
	Mining Generating bitcoins. <i>Moderators: gmaxwell, frodocooper</i>	1019831 Posts 26321 Topics	Last post by philipma1957 in Re: Mining hardware on Today at 03:45:55 PM

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>


Top 100 Coins by Market Cap

<div> <div>USD ▾</div> <div>Filter</div> <div>★ Portfolio</div> <div>🌐 Explore All Coins</div> <div>● Recently Added</div> <div>Market</div> <div>All-Time High</div> <div>Developer</div> <div>Social</div> <div><</div> <div>></div> </div>									
#	Coin		Price	1h	24h	7d	24h Volume	Mkt Cap	Last 7 Days
☆ 1	 Bitcoin	BTC	\$23,972.17	2.4%	2.8%	22.9%	\$41,934,260,630	\$445,379,340,771	
☆ 2	 Ethereum	ETH	\$622.16	3.0%	1.2%	5.1%	\$15,547,615,891	\$70,895,638,285	
☆ 3	 Tether	USDT	\$1.01	0.1%	-0.4%	0.1%	\$62,609,146,122	\$20,642,468,739	
☆ 4	 XRP	XRP	\$0.359646	8.4%	-26.1%	-23.5%	\$14,512,061,248	\$16,258,005,527	
☆ 5	 Litecoin	LTC	\$112.67	5.8%	4.3%	38.2%	\$8,308,784,151	\$7,428,039,644	
☆ 6	 Bitcoin Cash	BCH	\$299.77	3.7%	-5.8%	3.5%	\$4,467,967,725	\$5,577,916,090	
☆ 7	 Binance Coin	BNB	\$33.12	2.7%	1.0%	11.7%	\$734,193,241	\$4,898,230,245	
☆ 8	 Chainlink	LINK	\$12.18	1.9%	-1.5%	-4.6%	\$1,023,277,991	\$4,841,312,733	
☆ 9	 Polkadot	DOT	\$5.01	0.2%	-1.1%	-5.3%	\$322,987,266	\$4,741,300,290	
☆ 10	 Cardano	ADA	\$0.150307	2.4%	-5.0%	-3.0%	\$977,114,413	\$4,676,415,768	

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>



COINTELEGRAPH
 The future of money


BTC	ETH	LTC	XRP	BCH	EOS
\$23,613	\$608	\$107.72	\$0.33	\$293	\$2.65
+0.79%	-1.63%	-2.14%	-31.59%	-7.65%	-9.28%

ENGLISH
 ADVERTISE
 CAREERS

News ▾ Markets ▾ Magazine ▾ People ▾ Cryptopedia ▾ Industry ▾ Consulting ▾ Video ▾ CFC St. Moritz

Discovering Institutional Demand for Digital Assets in DACH region
 Industry Report by Cointelegraph Consulting

Explore Insights



New Bitcoin price highs revive old misconceptions about BTC and crypto

EDITOR'S CHOICE


HOT STORIES

Bitcoin price drops to \$23K in minutes despite huge new Grayscale buy-in

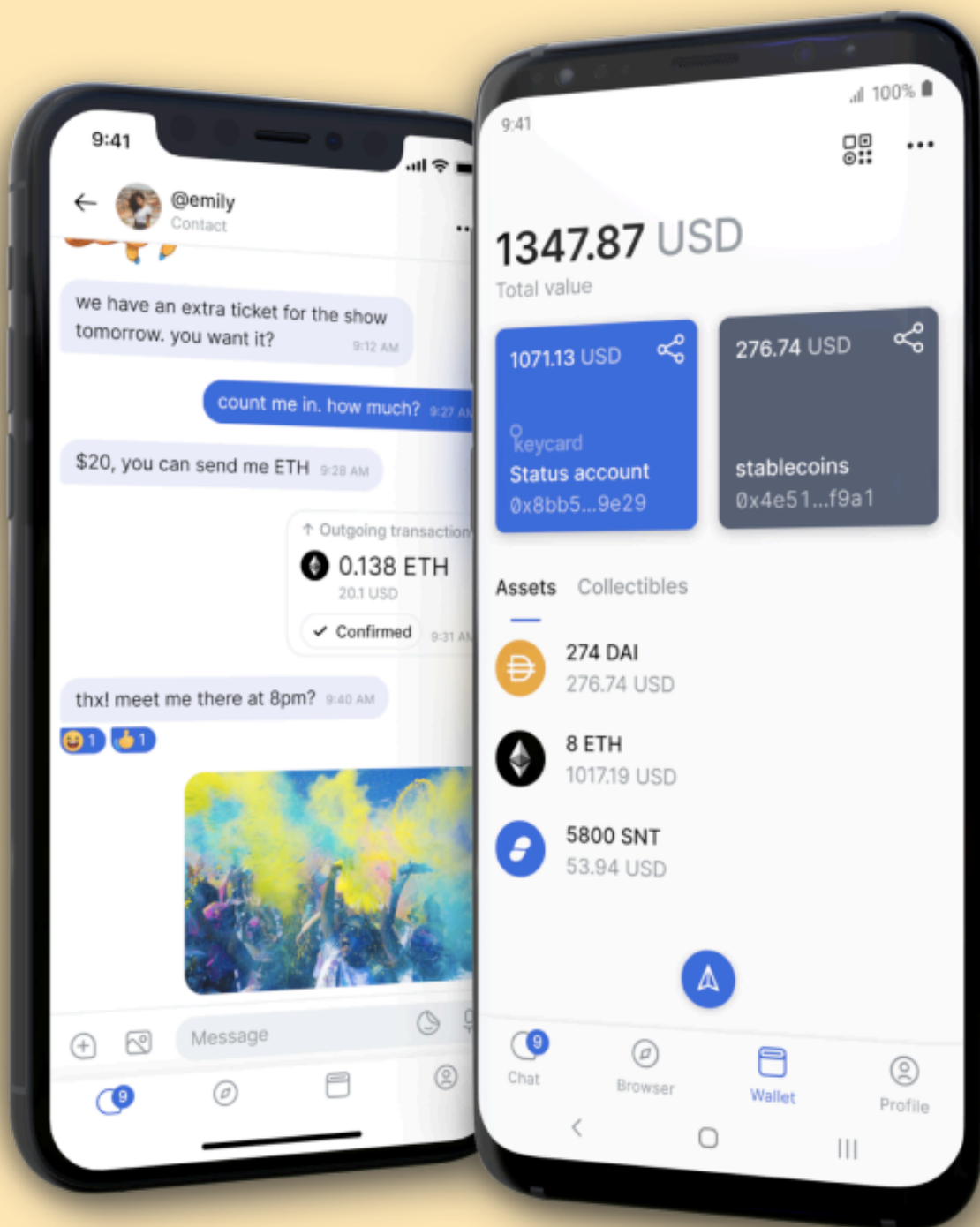
Scaramucci's SkyBridge BTC fund launches with \$25 million investment

New Bitcoin price highs revive old misconceptions about BTC and crypto

Notorious crypto figures are... 2020

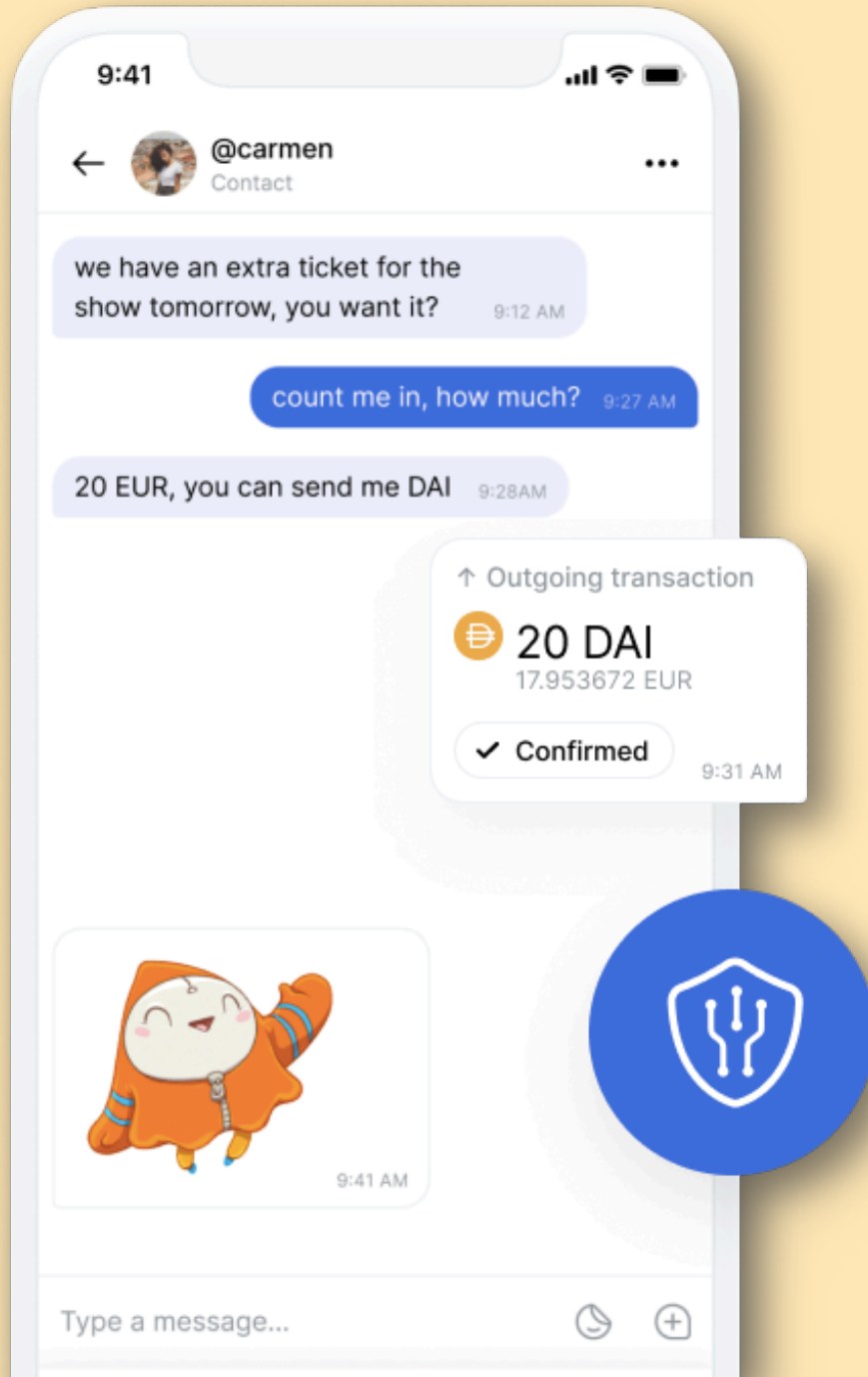


Coin Telegraph is a reputed crypto news site.
<https://cointelegraph.com>



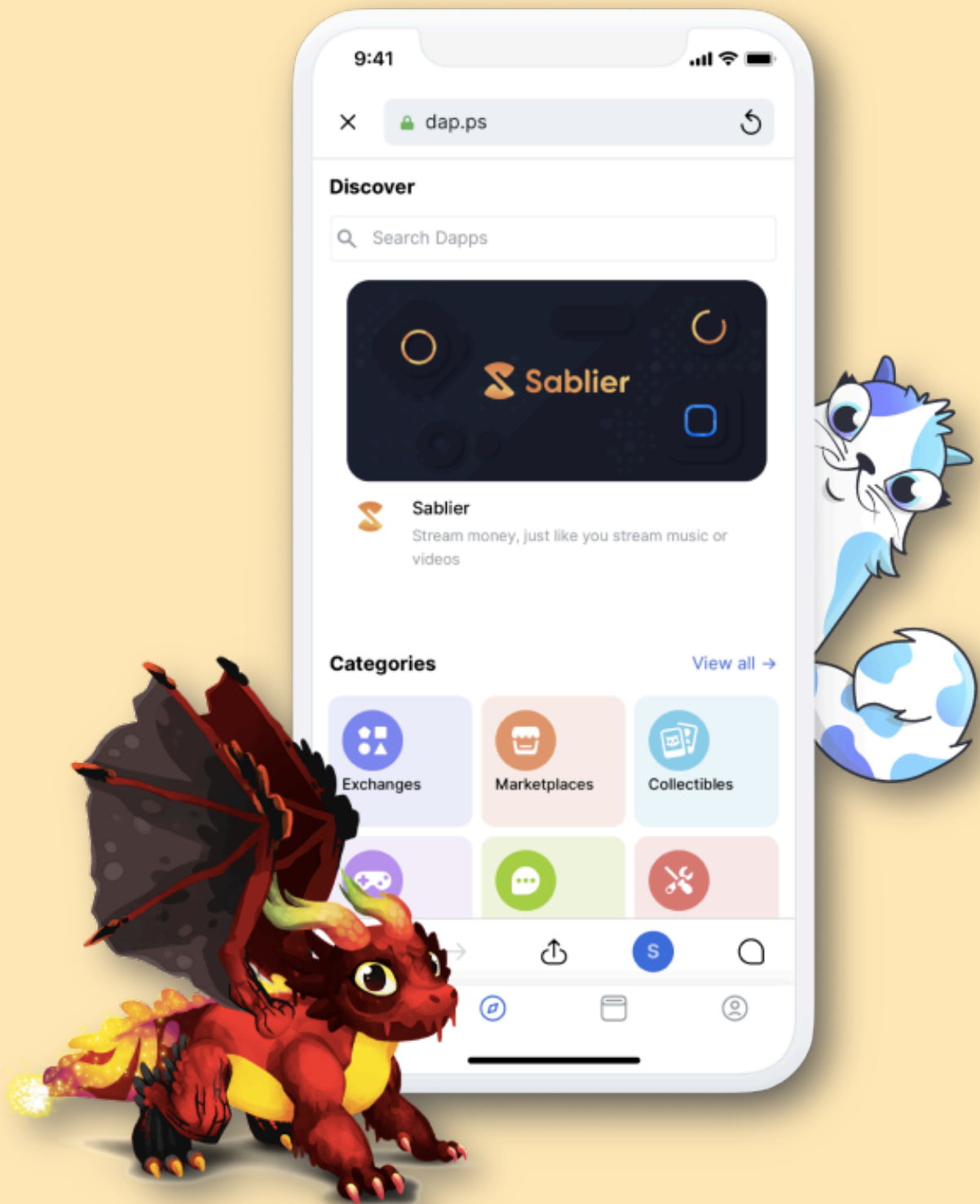
Status is a secure messaging app,
crypto wallet, and Web3 browser.

<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.

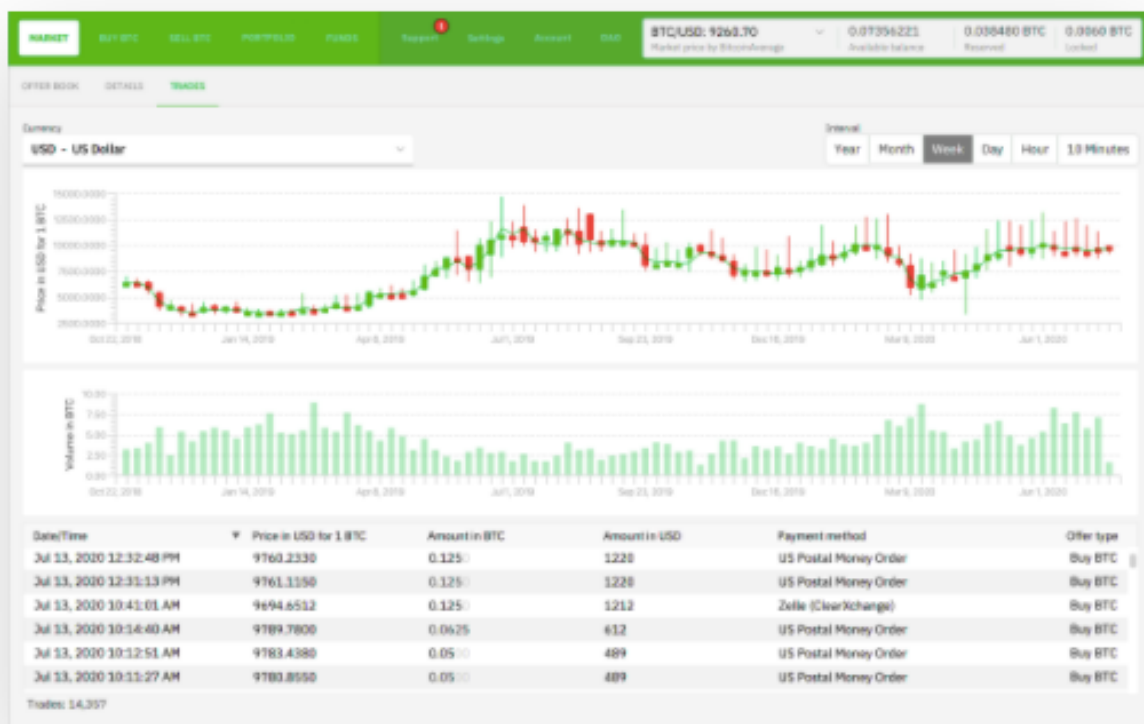
<https://status.im/web-three-browser>

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.



COIN360 is a cryptocurrency and crypto exchange live data aggregator.

<https://coin360.com>

CoinMarketCap

Q

≡

Market Cap: \$569,086,019,801 • 24h Vol: \$112,858,940,707 • BTC Dominance: 62.6% • Cryptocurrencies: 7,875 • Markets: 33,950

Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is \$569.09B, a ▲0.79% increase over the last day. [Read more](#)

Take a quiz!

Earn \$HNT and \$OXT

Make a Prediction

\$10,000 in BTC to Be Won!

Alert

A Div

☆ Watchlist

Cryptocurrencies

Derivatives

DeFi

Storage ●

Yield Farming

Show rows

100 ▾

⚙️ Filters

	#▲	Name	Price	24h	7d	Market Cap	Volu
☆	1	<div><div></div>Bitcoin BTC</div>	59.95	▲ 0.57%	▲ 3.57%	\$355,813,564,006	\$26,340,696,41,374,328 E
☆	2	<div><div></div>Ethereum ETH</div>	93.27	▲ 0.38%	▲ 2.06%	\$67,438,561,088	\$12,443,275,020,985,149 E
☆	3	<div><div></div>XRP XRP</div>	16495	▲ 1.43%	▼ 1.93%	\$27,402,056,587	\$8,703,437,614,399,073,233 J
☆	4	<div><div></div>Tether USDT</div>	97571	▼ 0.29%	▲ 0.00%	\$19,695,248,081	\$41,569,036,441,541,097,688 US

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>



Regulation of Cryptocurrency Around the World



ICO/Crypto Rating is a number that can have the following values:

☆☆☆☆☆ unknow (0),

☆☆☆☆☆ prohibited (1), when crypto is officially prohibited you can obviously not run an ICO.

☆☆☆☆☆ mostly unfavorable (2), officially discouraged to invest in crypto or no ICO ever run in that country.

☆☆☆☆☆ mostly favorable (3), when there is no official warning nor ICO law in that country.

☆☆☆☆☆ favorable (4), no law (but may be pending) but crypto and ICO are executed in that country

☆☆☆☆☆ legalized (5) are for country with clearly defined ICO / crypto laws.

- | | | |
|-----------------------------|---|---|
| • ☆☆☆☆☆ Afghanistan | • ☆☆☆☆☆ Germany | • ☆☆☆☆☆ Northern Mariana Islands |
| • ☆☆☆☆☆ Åland Islands | • ☆☆☆☆☆ Ghana | • ☆☆☆☆☆ Norway |
| • ☆☆☆☆☆ Albania | • ☆☆☆☆☆ Gibraltar | • ☆☆☆☆☆ Oman |
| • ☆☆☆☆☆ Algeria | • ☆☆☆☆☆ Greece | • ☆☆☆☆☆ Pakistan |
| • ☆☆☆☆☆ American Samoa | • ☆☆☆☆☆ Greenland | • ☆☆☆☆☆ Palau |
| • ☆☆☆☆☆ Andorra | • ☆☆☆☆☆ Grenada | • ☆☆☆☆☆ Palestinian Territory, Occupied |
| • ☆☆☆☆☆ Angola | • ☆☆☆☆☆ Guadeloupe | • ☆☆☆☆☆ Panama |
| • ☆☆☆☆☆ Anguilla | • ☆☆☆☆☆ Guam | • ☆☆☆☆☆ Papua New Guinea |
| • ☆☆☆☆☆ Antarctica | • ☆☆☆☆☆ Guatemala | • ☆☆☆☆☆ Paraguay |
| • ☆☆☆☆☆ Antigua and Barbuda | • ☆☆☆☆☆ Guernsey | • ☆☆☆☆☆ Peru |
| • ☆☆☆☆☆ Argentina | • ☆☆☆☆☆ Guinea | • ☆☆☆☆☆ Philippines |
| • ☆☆☆☆☆ Armenia | • ☆☆☆☆☆ Guinea-Bissau | • ☆☆☆☆☆ Pitcairn |
| • ☆☆☆☆☆ Aruba | • ☆☆☆☆☆ Guyana | • ☆☆☆☆☆ Poland |
| • ☆☆☆☆☆ Australia | • ☆☆☆☆☆ Haiti | • ☆☆☆☆☆ Portugal |
| • ☆☆☆☆☆ Austria | • ☆☆☆☆☆ Heard Island and McDonald Islands | • ☆☆☆☆☆ Puerto Rico |
| • ☆☆☆☆☆ Azerbaijan | • ☆☆☆☆☆ Holy See | |

<https://ico.tokens-economy.com/>

F6. 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>

F7. Crypto Indexes

A crypto index is a mathematical method for tracking the performance of a group of cryptocurrencies.

Crypto indexes can be:

- broad-based (covering thousands of cryptos) or
- specialized (covering a category of cryptos e.g. NFTs).

A crypto index can be unweighted (all cryptos are equally represented) or weighted and can be based on price or market capitalization.

ROHAS Cryptocurrency Index

ROHAS Cryptocurrency Index is an unweighted market capitalization index based on these 10 cryptocurrencies:

1. Binance Coin (BNB)
2. Bitcoin (BTC)
3. Bitcoin Cash (BCH)
4. Cardano (ADA)
5. Chainlink (LINK)
6. Ethereum (ETH)
7. Litecoin (LTC)
8. Polkadot (DOT)
9. Tether (USDT)
10. Uniswap (UNI)

https://www.rohasnagpal.com/crypto_index.php

How much Gold can you buy with 1 BTC?

Bitcoin is thought to be very volatile. That's true when compared to fiat currencies (USD, INR etc.). But how volatile is Bitcoin when mapped to Gold?

Get the answer here: https://www.rohasnagpal.com/btc_metal_index.php

F8. Hybrid finance (HyFi)

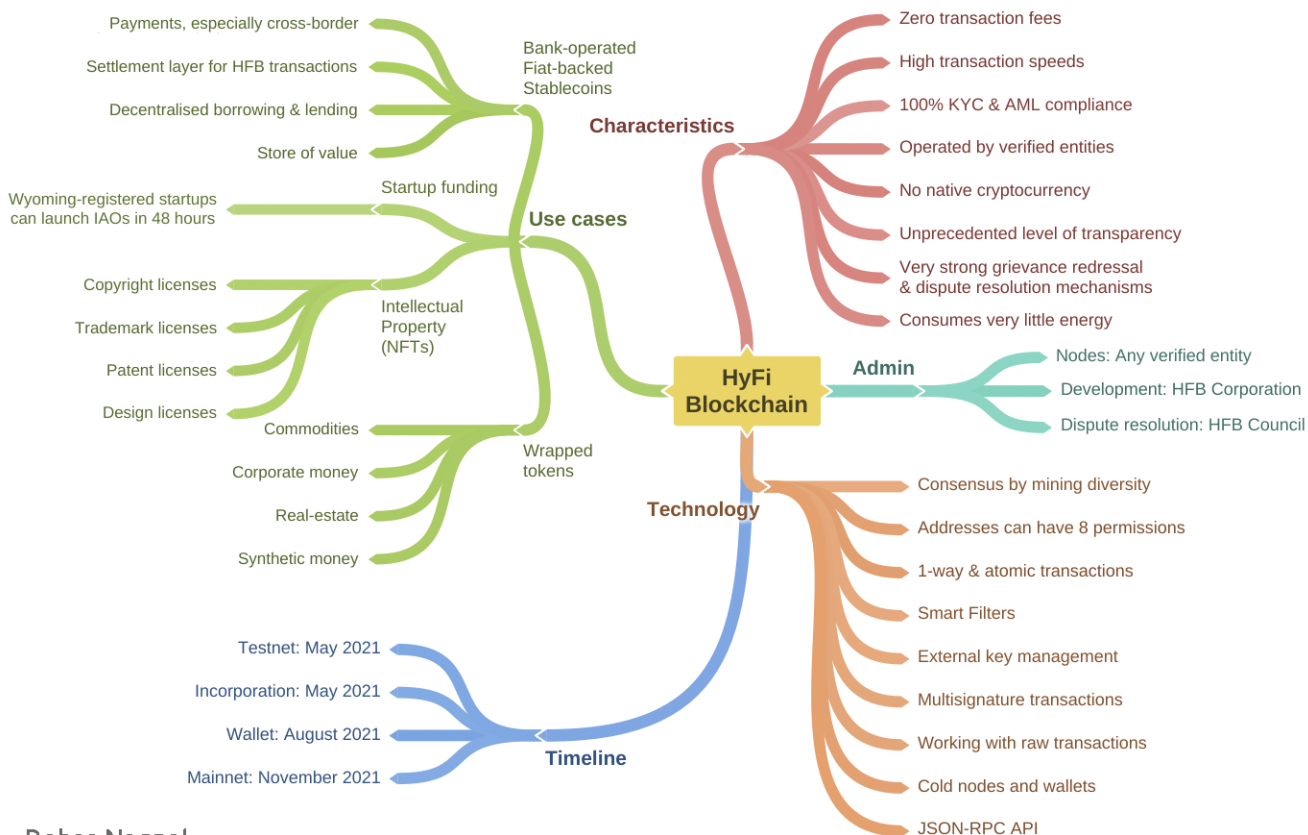
1. Introduction to DeFi

Today, almost every aspect of finance is managed by centralized systems, operated by regulated intermediaries and controlled by Governments. Regular consumers have to deal with a web of financial intermediaries to get access to these systems. This Centralised Finance (CeFi) system suffers from many problems including those of access, efficiency, time, and cost.

DeFi (Decentralised Finance) is an umbrella term for financial applications powered by blockchain technology.

Today, the Internet enables the movement of data (videos, text, photos, and more) globally in milliseconds. But try moving value (money, loyalty points, etc.) and you will be surprised by the costs, inefficiencies, and time delays.

Blockchain is a revolutionary technology that enables "internets of value" that can move value in seconds - money, loyalty points, equity shares, bonds, coupons, votes, intellectual property, and much more.



Rohas Nagpal

HyFi mindmap

2. The limitations of DeFi and most public blockchains

DeFi has become a "wild and lawless" environment where there are virtually no regulators (pun intended). There are many problems that are holding back the decentralized finance system from mass adoption.

2.1 High & unpredictable transaction fees

Public blockchains require fees to be paid using cryptocurrency. As the project becomes more successful, its cryptocurrency becomes more expensive.

Transactions fees are very high & unpredictable, especially in the DeFi market leader Ethereum. The increasing use of DeFi protocols, dApps, and applications built on top of Ethereum has overloaded the network to the point where its fees are almost unsustainable. The average transaction cost on Ethereum has catapulted from less than \$5 in 2020 to about \$40 in February 2021.

An Ethereum based social media token project, Unite, announced on 10 February 2021 that the project was no longer in active development, adding that the original idea for the project had been rendered unfeasible by the recent gas price spike. The average cost of using Ethereum increased 35,600% since January 2020.

2.2 Slow transaction speed

Many public blockchains have slow transaction speeds. See details here: <https://alephzero.org/blog/what-is-the-fastest-blockchain-and-why-analysis-of-43-blockchains/>

2.3 Zero support for KYC (Know Your Customer)

Most public blockchains are permissionless. This means that anyone can read, write and validate. There is zero KYC (Know Your Customer) compliance.

2.4 Zero support for AML (Anti-Money Laundering)

Most public blockchains are permissionless. This means that anyone can read, write and validate. There is zero AML (Anti-Money Laundering) compliance.

2.5 Fake dApps, apps, & wallets

Recently an Apple user lost his life savings of \$600,000 in Bitcoin when he installed a fake Trezor wallet app on his iPhone. Something similar also took place through a fake app on the Google Play Store. In another case, malware that replaced victims' cryptocurrency wallet addresses also spread through a "MetaMask" impersonator app. Such incidents are fairly common.

2.6 Large number of scams and rug pulls

A recent fraud around WoToken cost more than a billion dollars! According to a CipherTrace report, DeFi "rug pulls" and exit scams were the biggest chunk of crypto fraud schemes in 2020. A rug pull begins with criminals minting a new token, hyping it, listing it on Uniswap, and then providing liquidity. Once victims swap their ETH for this new token, the criminals "drain the liquidity pool" and leave the victims with a worthless token.

2.7 Unsustainably high energy consumption

The energy consumption and environmental cost of Proof-of-Work blockchains like Bitcoin and Ethereum are massive.

2.8 Creation of a new set of intermediaries

DeFi was supposed to reduce the cost and time taken for financial activities by removing intermediaries. Instead, it has created a new class of intermediaries such as miners and node operators.

2.9 Duplicate ticker symbols

Duplicate ticker symbols bring in a very high risk of financial loss as an investor can easily end up buying the wrong crypto. An example: BitRewards, BitMoney, and First Bitcoin have the same ticker symbol - BIT.

2.10 Low to zero grievance redressal mechanisms

Many public blockchains have not only anonymous users but also anonymous creators, developers, and managers! In such a scenario, there are very low to zero grievance redressal mechanisms.

2.11 Low to zero consumer protection

Many public blockchains have not only anonymous users but also anonymous creators, developers, and managers! In such a scenario, there are very low to zero customer protection mechanisms.

2.12 No insurance cover

Public blockchains do not have insurance coverage like banks do.

2.13 Vulnerability of Smart Contracts

A small mistake in the code of a smart contract can lead to a huge financial loss. A case in point is the multi-million Ethereum DAO hack of 2016.

2.14 Complexity

DeFi solutions are not easy to use. In many cases, less sophisticated users end up sending assets to the wrong address, leading to huge financial losses.

2.15 Unpredictable yields

DeFi is ruled by highly volatile cryptocurrencies. This adds a huge amount of unpredictability to the yields.

2.16 Regulatory uncertainty

Some jurisdictions are pro-DeFi, some are clearly anti-DeFi and the rest are still making up their minds. This creates a lot of fear, uncertainty, and doubt.

2.17 Usage by criminals and blacklisted entities

The absence of regulators and the high level of anonymity means you could end up transacting with criminals and blacklisted entities.

2.18 Low liquidity

There are thousands of cryptocurrencies out there. A majority of these have low liquidity which means you may get stuck trying to exit or book profits.

2.19 High collateral for loans

Unlike the CeFi world, the collateral requirement for DeFi loans is very high.

2.20 Low level of transparency

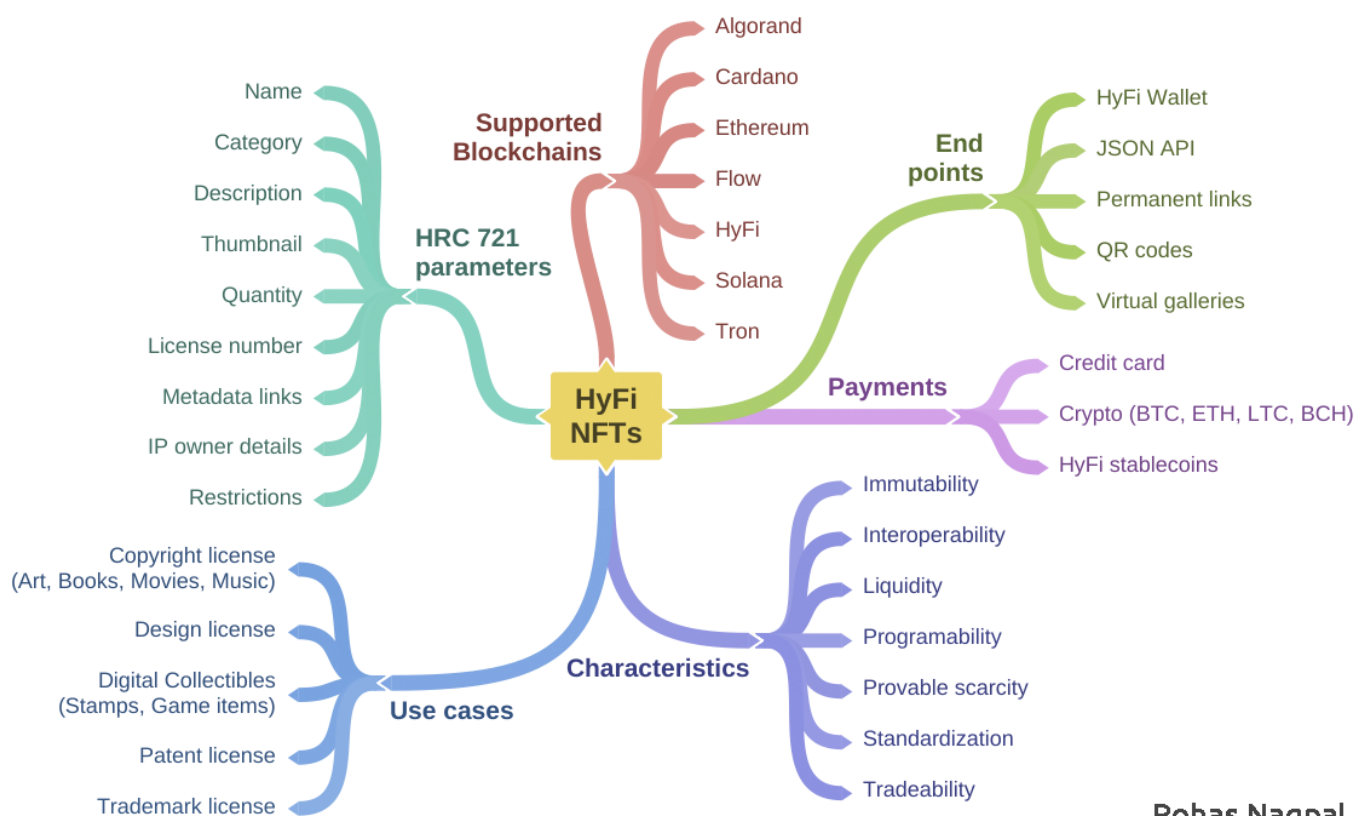
While nodes can be operated by anyone in the world, who is actually managing the project? That's something not answered clearly by most public blockchains.

3. The solution – Hybrid Finance (HyFi)

I believe that the future belongs to Hybrid Finance (HyFi) - which combines the best of both worlds.

A HyFi Blockchain must:

1. have zero transaction fees,
2. have high transaction speeds,
3. support 100% KYC & AML compliance,
4. be operated by verified entities,
5. have no native cryptocurrency,
6. offer an unprecedented level of transparency,
7. have very strong grievance redressal & dispute resolution mechanisms
8. consume very little energy



Rohas Nagpal

Mindmap on the HyFi approach to NFTs

Misc.

References & sources

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 spanned **18 countries** and I have investigated cyber crimes & data breaches for hundreds of organizations across many sectors - aerospace, banking, defense, law & tax enforcement, IT, manufacturing, media, medical, pharmaceuticals, shipping, trading, transportation.

I developed an interest in virtual currencies in **2011** while investigating a case of organized criminals using bitcoin. Since **2015**, I have been working extensively in the blockchain / distributed ledger technology domain.

In 2016, I co-founded **Primechain Technologies Pvt. Ltd.**, a blockchain startup with the mission of "building blockchains for a better world". I co-founded **BankChain** - a community of 37 banks for exploring, building, and implementing blockchain solutions. I am the author of **the Future Money Playbook** and have designed the **R.O.H.A.S. Cryptocurrency Valuator**.



Rohas Nagpal
Future Money Evangelist
www.rohasnagpal.com

Changelog

e2.3

- Added mindmap to E. The Ethereum Ecosystem
- Added a mindmap in C8. Public Blockchains
- Added a mindmap in C2. Stablecoins
- Added section F8. Hybrid Finance (HyFi)
- Added Privacy Coins to C1. Cryptocurrencies

e2.2

- Updated section B – “Crypto & Innovation valuation using R.O.H.A.S”
- Added categories of cryptos, examples of each category and mindmap to C1. Cryptocurrencies
- Updated C8. Public Blockchains
- Added mindmap to F1. Decentralized finance (DeFi)
- Added F7. Crypto Indexes

e2.1

- Updated section B – “Crypto & Innovation valuation using R.O.H.A.S”
- Added section C4 on Non-Fungible Tokens (NFT)
- Added section C5 on Tokenized stocks

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

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