2023/2024 S2

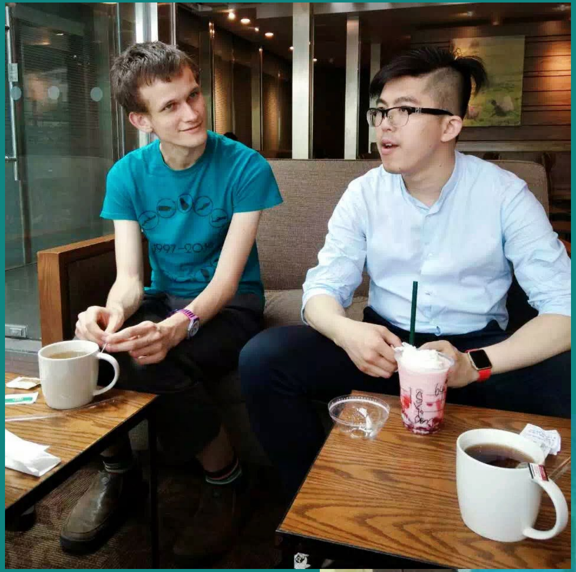
Introduction to Blockchain

Dr. Hui Gong (h.gong1@westminster.ac.uk)

UNIVERSITY OF WESTMINSTER

Module Leader

Hui Gong

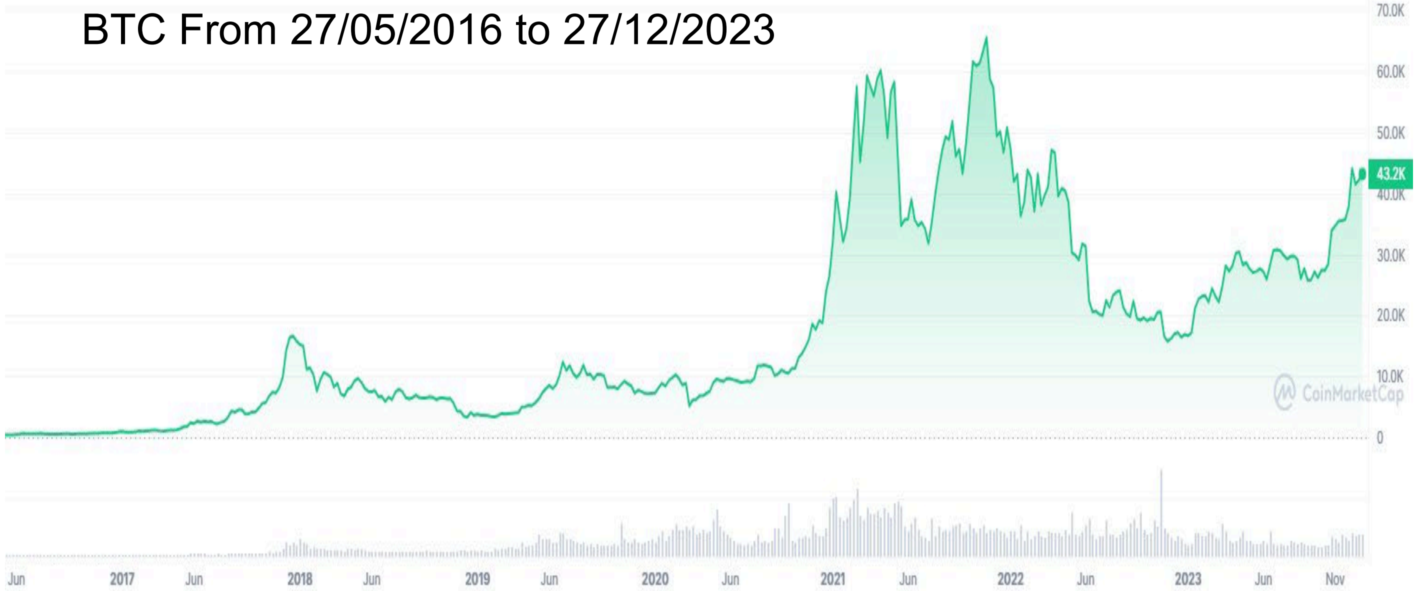


Hui and Vitalik Buterin (born on 31st Jan 1994), founder of Ethereum.

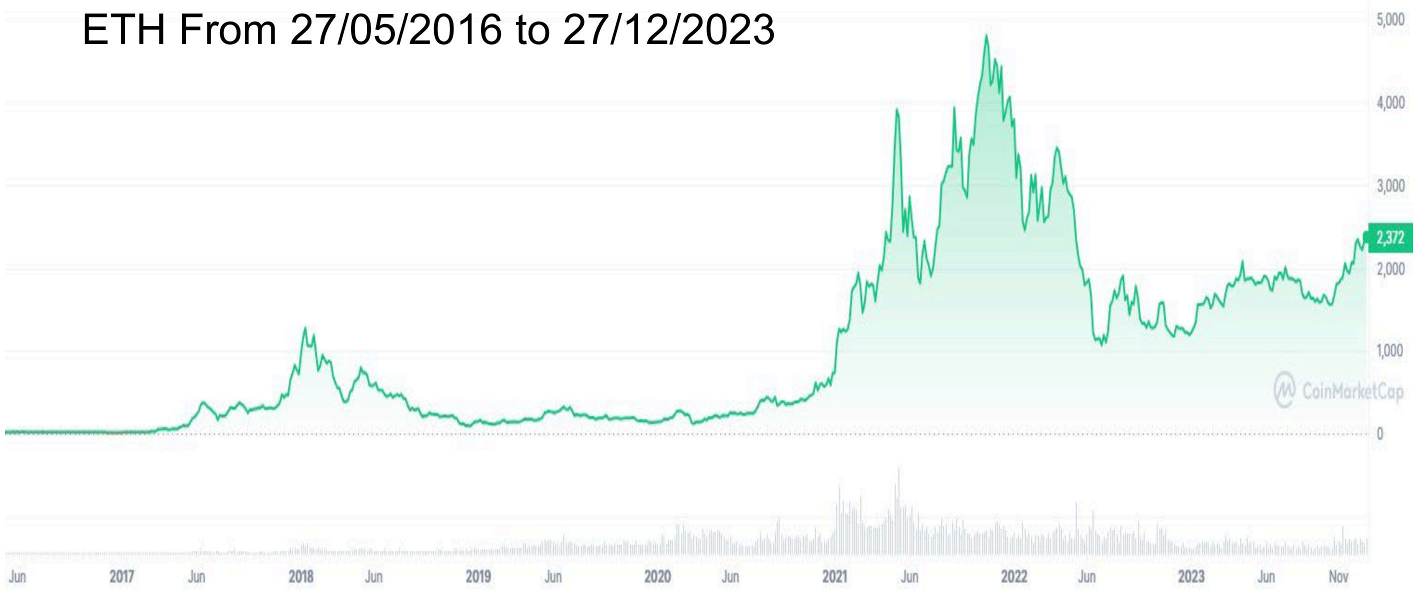
27 May 2016

@Shanghai, China

ETH was $10.7 that day.



BTC From 27/05/2016 to 27/12/2023



ETH From 27/05/2016 to 27/12/2023

Blockchain Technologies and Cryptocurrencies (BTC)

Structure of Our Module

I. Blockchain and Bitcoin

- Brief about Fintech and Blockchain
- Bitcoin I – Mining and PoW
- Bitcoin II – Transaction/Crypto Wallet etc

II. Ethereum and Smart Contract

- Ethereum I – PoS, EVM etc
- Ethereum II – Smart Contract and DApps etc
- Tokenisation of Asset – Solidity and ERC20

III. Crypto Finance

- ICO, STO and its regulation
- CryptoEx and DeFi
- Digital Fiat Currency – CBDC

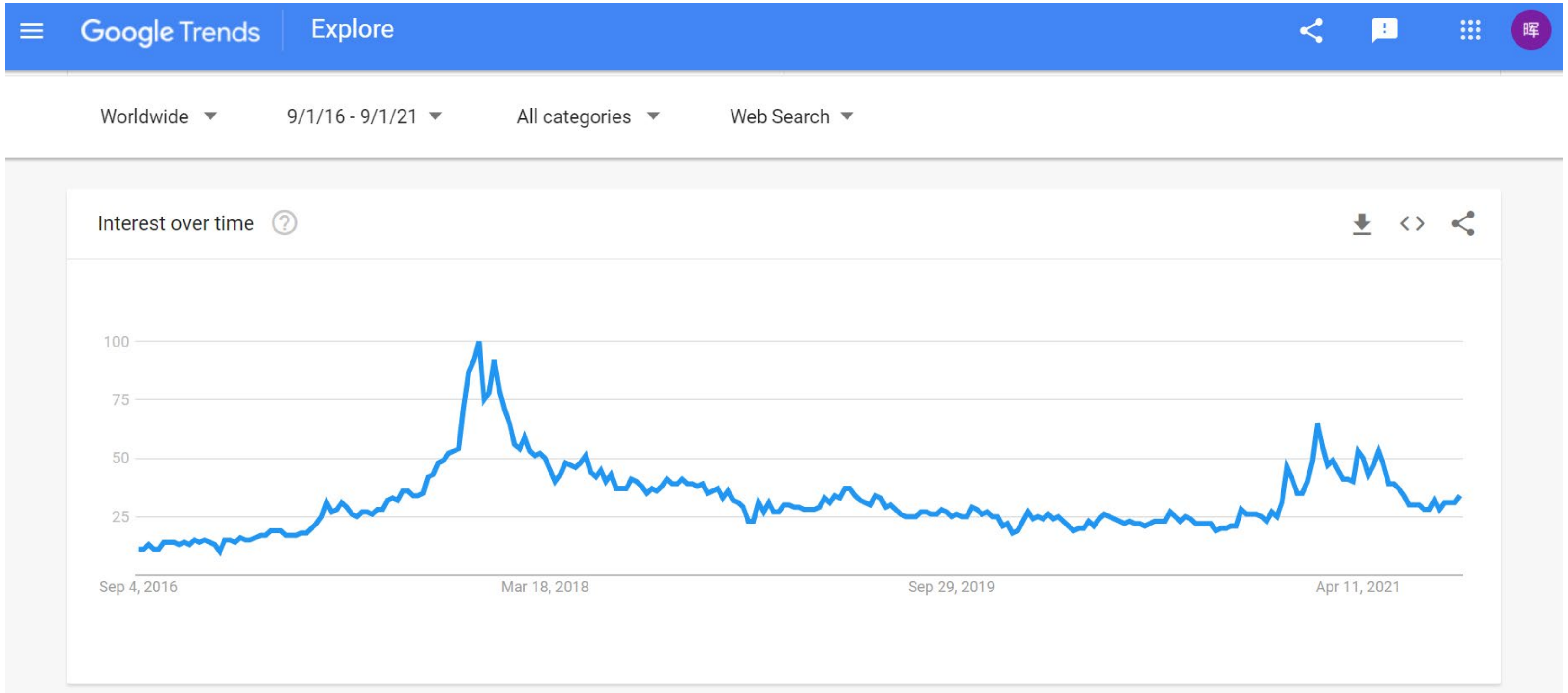
IV. Case Studies

- Case Study I – Metaverse/NFT
- Case Study II – Layer2 & BRC20
- Revision

Block + Chain

Block + chain

Blockchain



- AI is productivity, blockchain is a production relationship, and machines are production tools.
- In the future, AI + blockchain + machines will constitute the main body of the world. When AI has evolved to be sufficiently intelligent, the blockchain written by humans will be carried out by AI, and it is easier for machines to reach ‘consensus’ and abide by ‘consensus’ than between humans.
- ‘Code Is Law’ -- Harvard Magazine

Fintech

Fintech

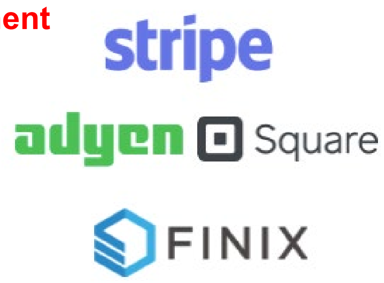
Financial Technologies

- Artificial Intelligence
- Blockchain
- Cloud Computing
- Data / Big Data / Data Analytics

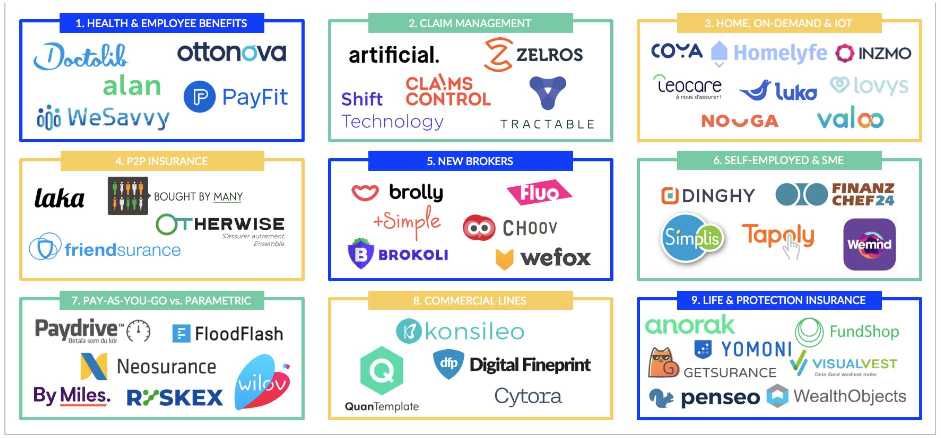
Fintech

Application Scenarios

Payment



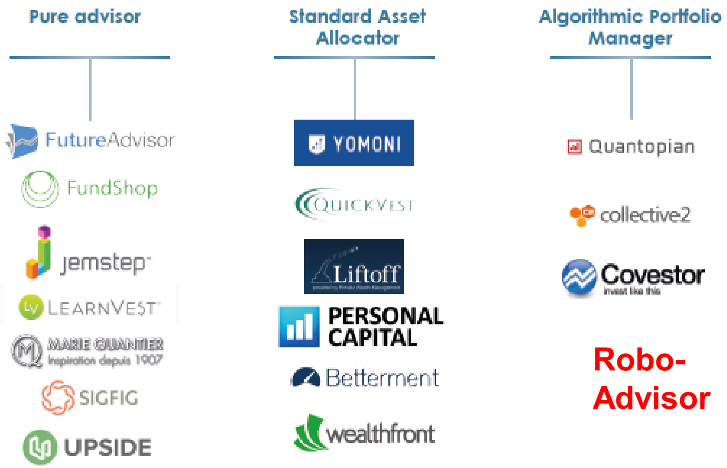
InsurTech



Crowd Funding

1
KICKSTARTER
2
INDIEGOGO
3
Crowdfunder.co.uk
4
AngelList
5
gofundme
6
PATREON
7
Funding Circle
8
SEEDRS
9
crowdrise
10
Give
DEMOCRATIZING GENEROSITY

P2P lending

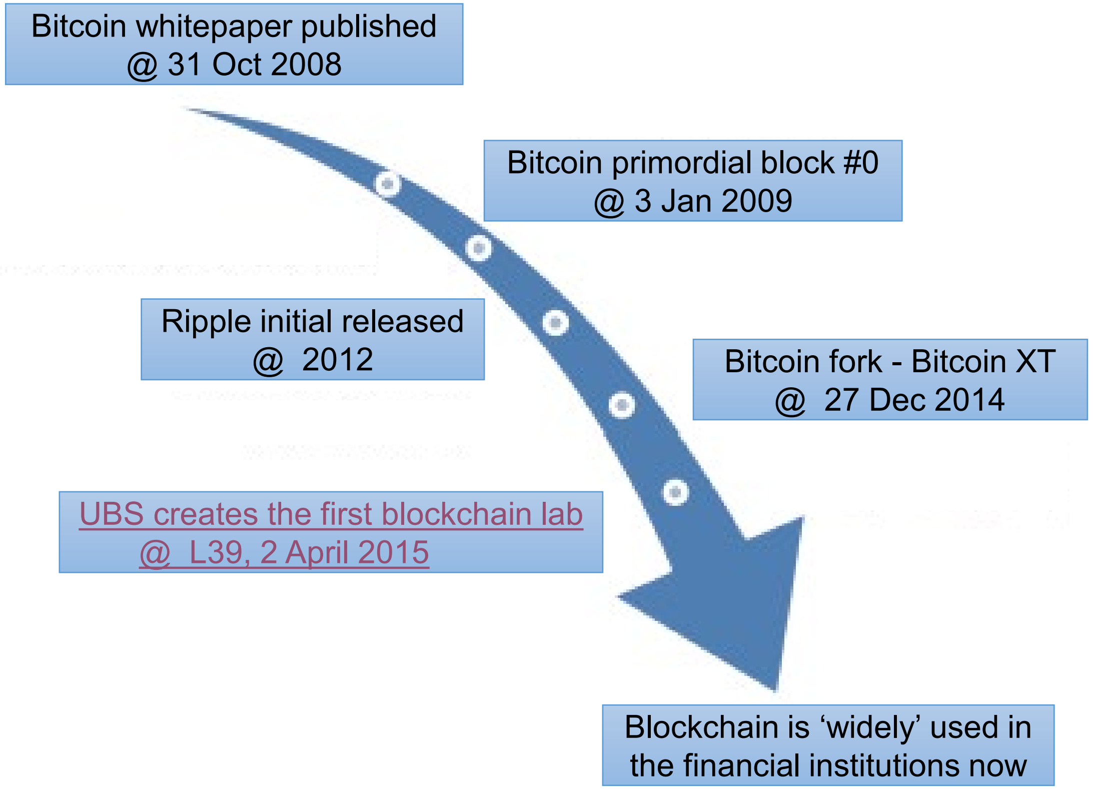


Robo-Advisor

Blockchain

Blockchain

Milestones



Bitcoin whitepaper published
@ 31 Oct 2008

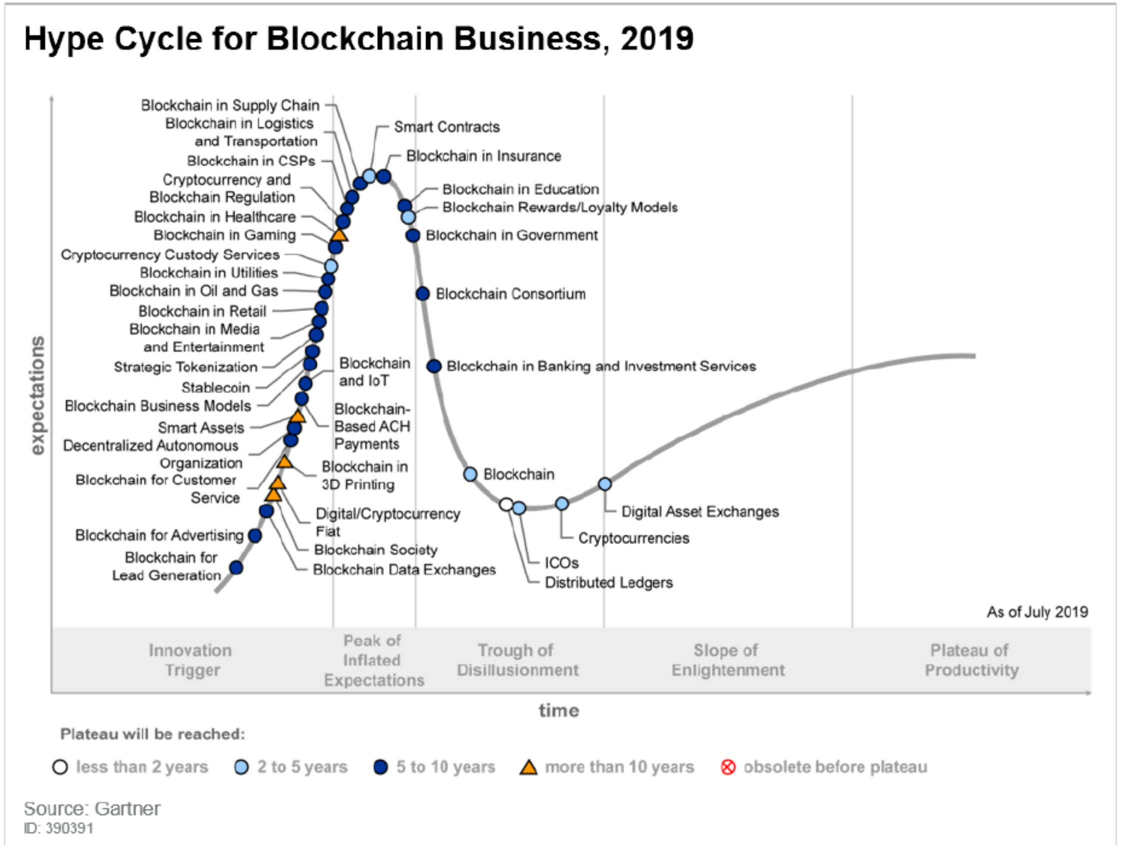
Bitcoin primordial block #0
@ 3 Jan 2009

Ripple initial released
@ 2012

Bitcoin fork - Bitcoin XT
@ 27 Dec 2014

UBS creates the first blockchain lab
@ L39, 2 April 2015

Blockchain is ‘widely’ used in
the financial institutions now

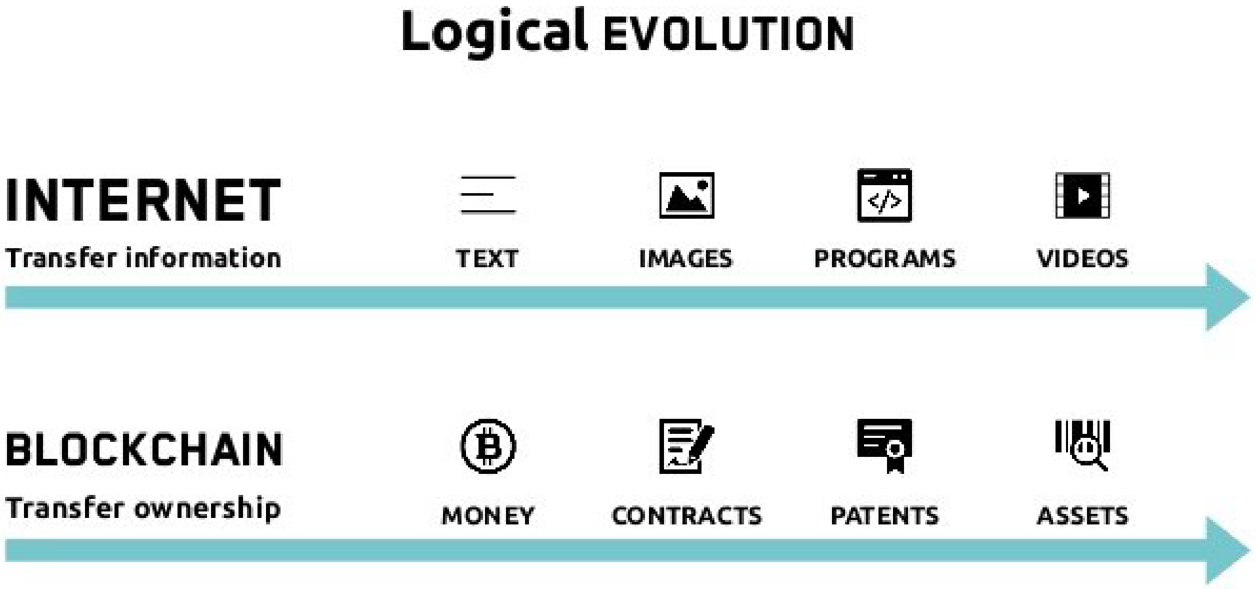


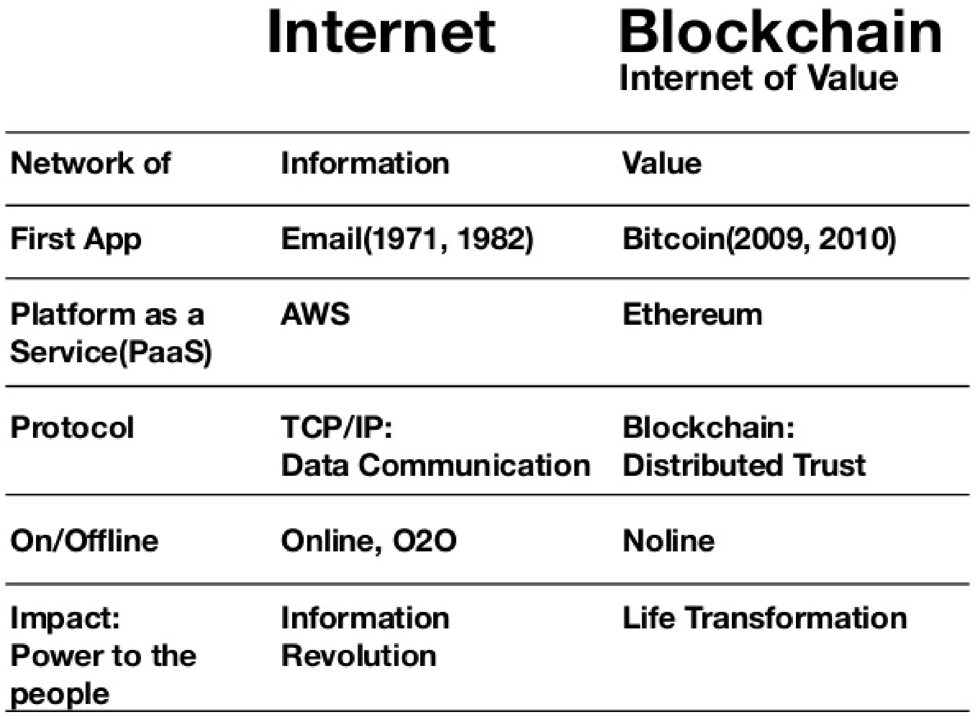
Hype Cycle for Blockchain Business, 2019

Source: Gartner
ID: 390391

Blockchain

Internet vs Blockchain

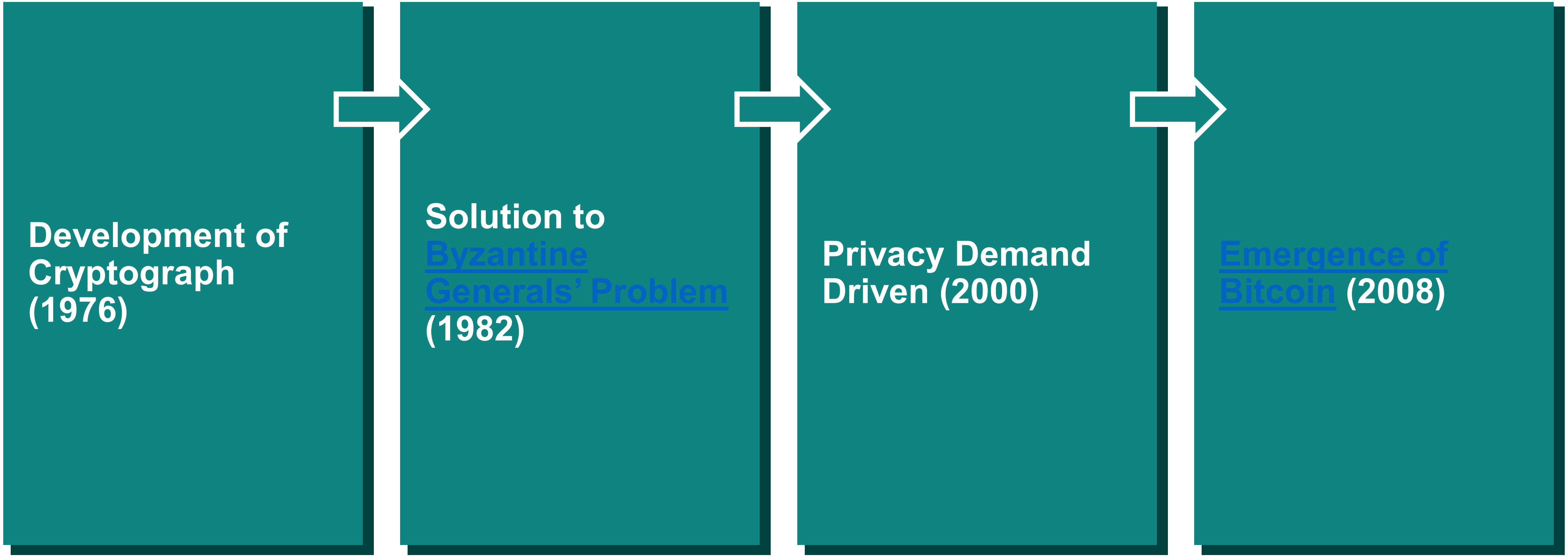




	Internet	Blockchain Internet of Value
Network of	Information	Value
First App	Email(1971, 1982)	Bitcoin(2009, 2010)
Platform as a Service(PaaS)	AWS	Ethereum
Protocol	TCP/IP: Data Communication	Blockchain: Distributed Trust
On/Offline	Online, O2O	Noline
Impact: Power to the people	Information Revolution	Life Transformation

Blockchain

Timeline



Development of Cryptograph (1976)

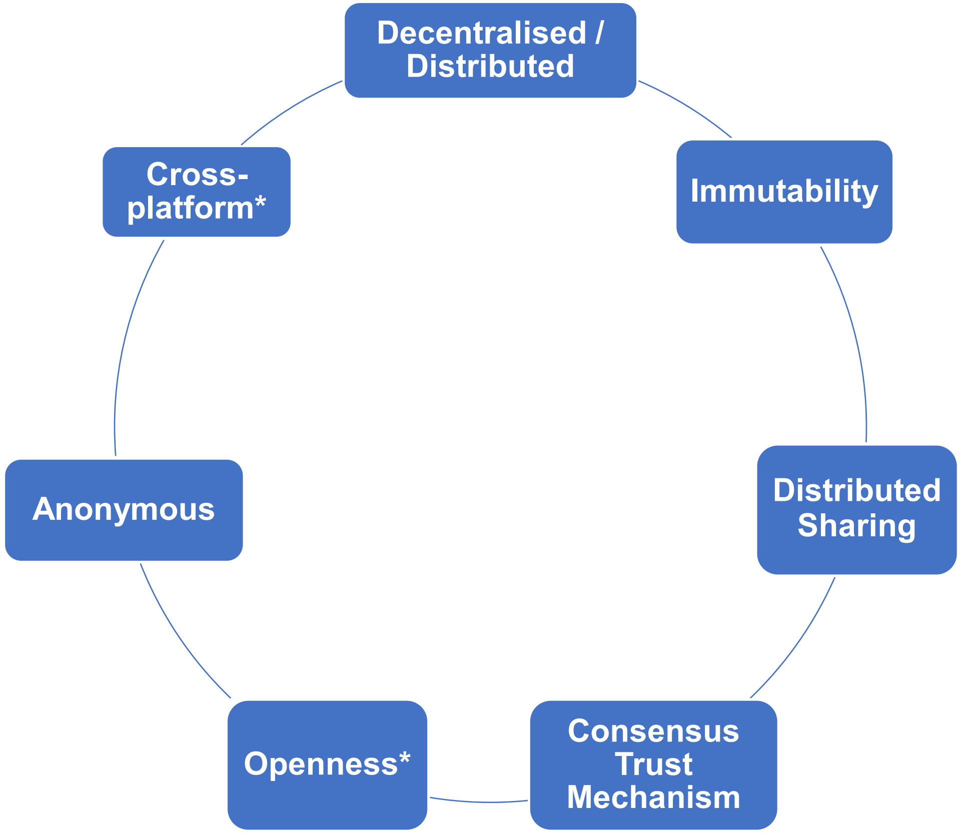
Solution to Byzantine Generals’ Problem (1982)

Privacy Demand Driven (2000)

Emergence of Bitcoin (2008)

Blockchain

Features



Decentralised / Distributed

Immutability

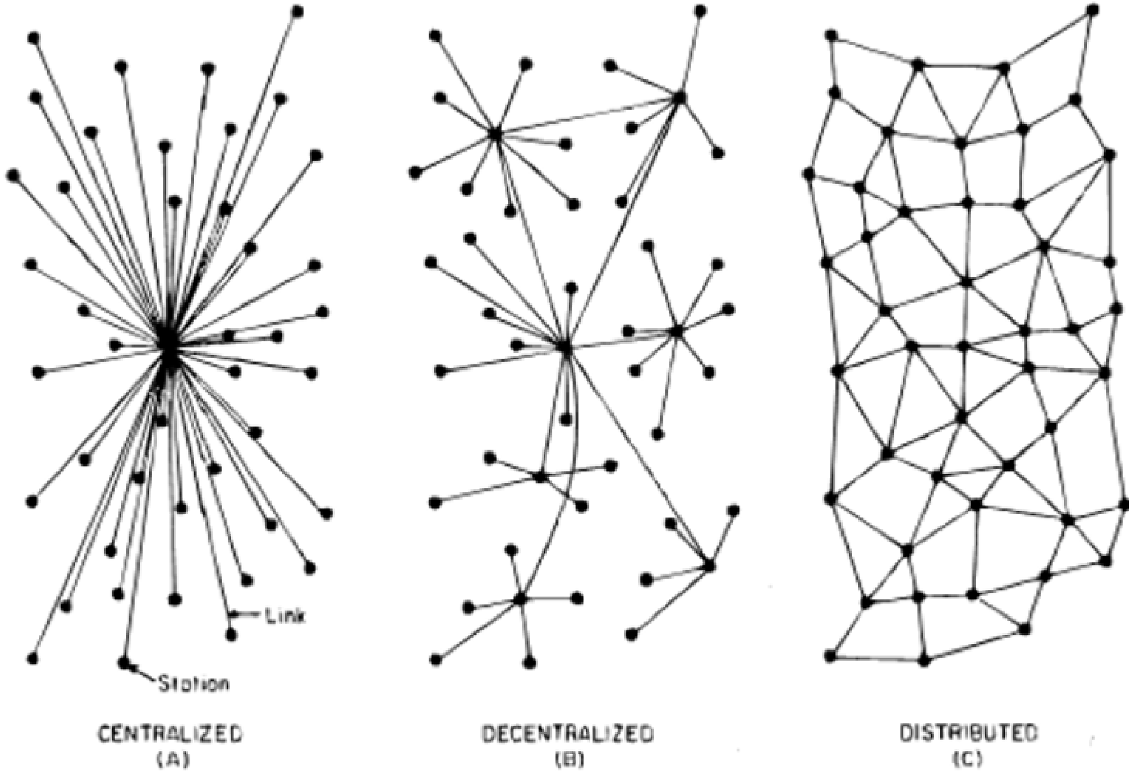
Distributed Sharing

Consensus Trust Mechanism

Openness*

Anonymous

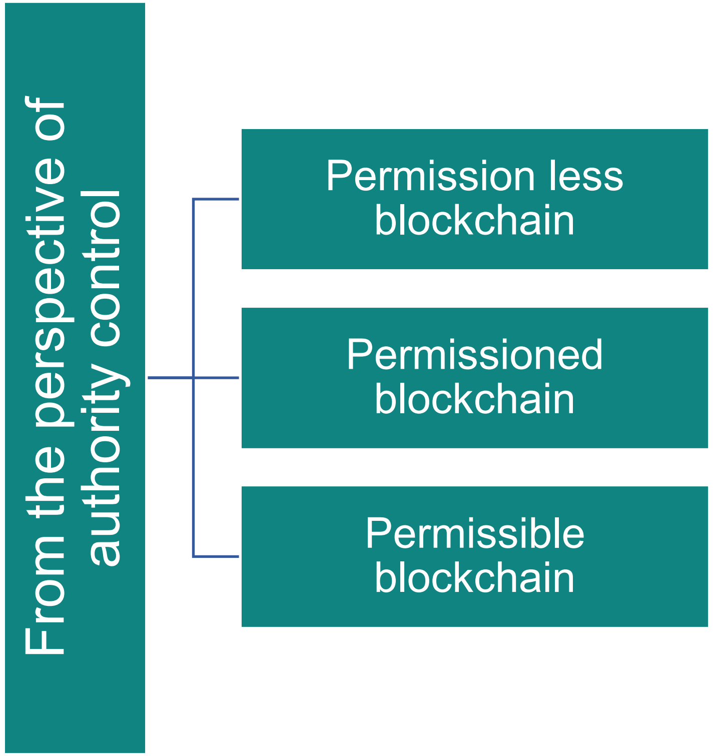
Cross-platform*



Blockchain

Different types

	Public blockchain	Private blockchain	Consortium blockchain
Participate in decision-making	Any node can participate in decision-making	Only internal nodes can participate in decision-making	Only nodes that are specially allowed can participate in decision-making
Those participating in decision-making	A large number	A small number	A medium number
Decision-making speed	Slow	Fast	Medium
Network	P2P network (Peer-to-Peer network)	High-speed network	High-speed network
Transaction data	Public	Non-public	Non-public
Attribute	Changeless data storage, encryption and timestamp technology	Changeless data storage, encryption and timestamp technology	Changeless data storage, encryption and timestamp technology


From the perspective of authority control

Permission less blockchain

Permissioned blockchain

Permissible blockchain

Blockchain 1.0

Double Spending Problem

The emergence of bitcoin and blockchain has solved a long-standing problem in the industry of encrypted digital currency: 'Double spending' refers to how to prevent a deal of digital cash from being used twice. Blockchain solves the problem of 'double spending' by means of peer-to-peer file sharing and public key encryption technologies. The ownership of a currency is recorded by the public general ledger and confirmed by the encryption protocol and mining community. Blockchain is 'trustless', because the user does not need to trust the other party in the transaction or any centralised agency, who only needs to trust this system. Each block in blockchain involves sets of transactions, which are released to the general ledger one after another, that is, added to the 'chain'. These blocks can be checked publicly, and everyone can see records of each transaction.

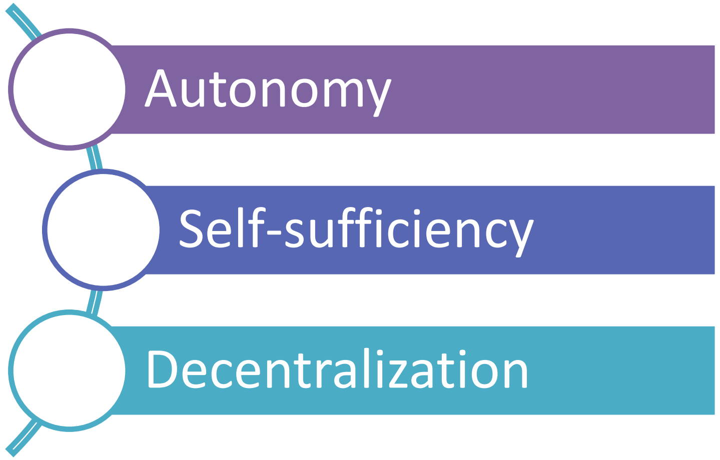
Byzantine Generals' Problem

While in the Bitcoin blockchain designed by Satoshi Nakamoto, a very ingenious method is applied to reach a consensus among all the nodes, which has also solved the Byzantine generals' problem under certain conditions to a certain extent, namely, PoW (Proof of Work) mechanism. Specifically speaking, the PoW mechanism applied in Bitcoin blockchain is to adopt SHA-256 algorithm to calculate a hash according to the ledger data, timestamp and other information and a random number recorded in one blockchain, wherein the random number will not be public, and participants involved in accounting, namely the so-called miners are required to calculate the random number with their computer based on the hash and those calculate correctly are qualified for accounting.

Blockchain 2.0

Blockchain 1.0 is designed to realise decentralization of currency and payment instrument, while Blockchain 2.0 is designed to decentralize the entire market in a more macroscopic way, which makes it possible to register, confirm and transfer assets and contracts of various types with the function of decentralized trading ledgers of blockchain. Actually, Satoshi Nakamoto designed solutions on blockchain for third-party entrusting transaction, bond contract, third-party arbitration, multi-signature transaction and other problems when the blockchain was presented. Actually, all the financial transactions can be completed on blockchain, including stock, private equity, crowd funding, bonds, hedge fund, annuity, pension and futures, options, credit default swap and other financial derivatives. Public records, certificates, all notarial documents and tangible or intangible assets can be migrated to blockchain, with corresponding certificates.

Smart contract can redeploy assets of all the above types, and will become increasingly complex and autonomous as the time goes on. Contents of smart contract will be far more than simple asset transaction, but will include a wide range of contents. Besides, it stipulates the parties involved mutually agree to do or not do something as same as traditional contracts, and smart contract is featured that the two parties being not required to trust each other. **This is because smart contract is defined and executed by codes, which is completely automatic and cannot be intervened.** Smart contract can operate in such manner mainly because it contains 3 elements: autonomy, self-sufficiency and decentralisation.

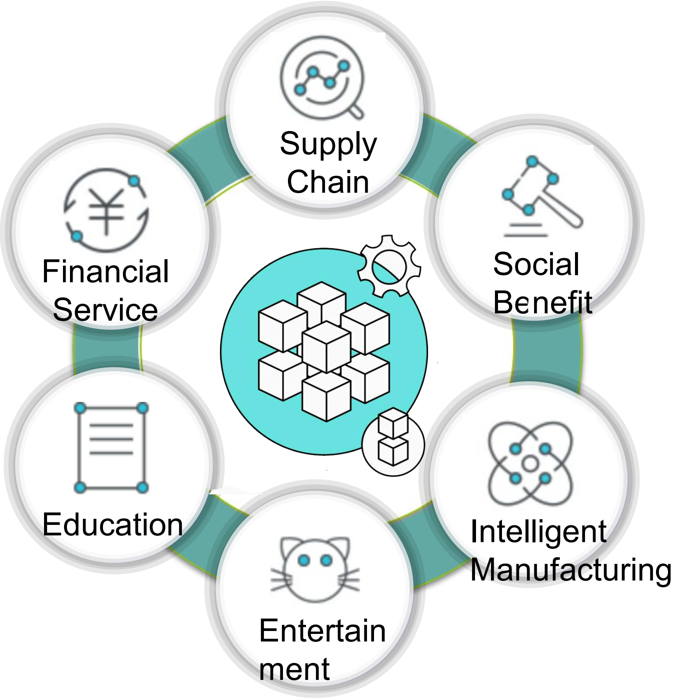


Blockchain 3.0

With the development of blockchain technology and promotion of distributed coordination mode, blockchain will definitely change people's lifestyle in a wide and deep way. Therefore, scholars have made expectations for the future prospective of blockchain, the Blockchain 3.0.

Blockchain can not only reshape various aspects of economic form, but also provide possibilities to change similarities for other industries and even touch various aspects of social life. Its main contribution lies in providing a set of effective decentralized data structure, interaction mechanism and computing mode for distributed society system and distributed artificial intelligence, and providing solid data basis and credit base to realise a parallel society. Blockchain can become a new pattern which reduces friction and improve efficiency for activity organization forms, and can also extend the existing pattern.

Finally, smart society will greatly promote the transfer from the traditional society management structure featured in centralisation, information asymmetry, interaction non-equivalence, etc. to an innovative society management structure featured in decentralization, rights equality, information symmetry and position equivalence, and realize flexible, focused and convergent intelligent society management target by effectively avoiding uncertainty, complexity and diversity in the traditional society management.



Blockchain

2nd Internet – e.g. OpenBazaar

What is OpenBazaar?

OpenBazaar is a different way to do online commerce. It’s a peer to peer application that doesn’t require middlemen, which means no fees & no restrictions.

How does OpenBazaar work?

OpenBazaar connects people directly via a peer to peer network. Data is distributed across the network instead of storing it in a central database.

How are there no fees and restrictions?

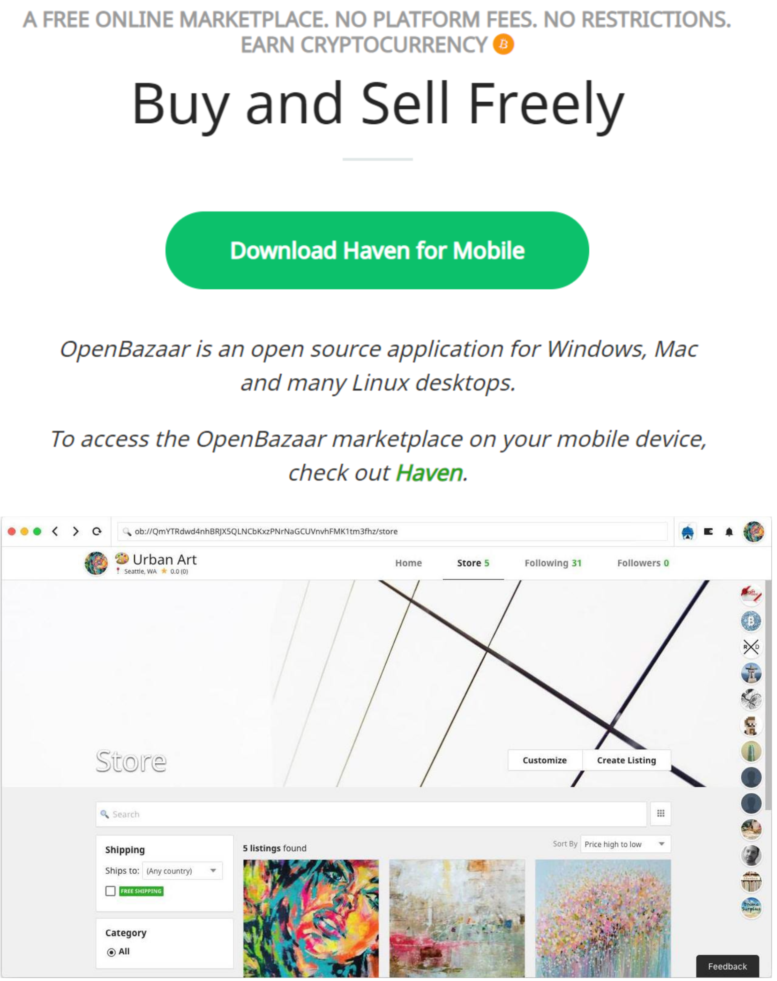
OpenBazaar isn’t a company nor an organization; it’s free open source software. It was built to provide everyone with the ability to buy and sell freely ✌

Who controls the OpenBazaar network?

Nobody has control over OpenBazaar. Each user contributes to the network equally and is in control of their own store and private data world.

Is Bitcoin the only supported payment method?

Pay with multiple cryptocurrencies on OpenBazaar: Bitcoin, Bitcoin Cash, Litecoin, and Zcash. More cryptocurrencies to come.



A FREE ONLINE MARKETPLACE. NO PLATFORM FEES. NO RESTRICTIONS.
EARN CRYPTOCURRENCY

Buy and Sell Freely

Download Haven for Mobile

OpenBazaar is an open source application for Windows, Mac and many Linux desktops.

To access the OpenBazaar marketplace on your mobile device, check out Haven.

ob://QmYTRdwd4nhBRJX5QLNCbKxzPNrNaGCUVnvhFMK1tm3fhz/store

Blockchain

Risks

- 51% Attack
- Lost Private key
- Privacy/Virus
- Efficiency

References to read

[1] Walport, M.G.C.S.A., 2016. Distributed ledger technology: Beyond blockchain. UK Government Office for Science, 1, pp. 1-88.

[2] Diffie, W. and Hellman, M., 1976. New directions in cryptography. IEEE transactions on Information Theory, 22(6), pp. 644-654.

[3] Lamport, L., Shostak, R. and Pease, M., 2019. The Byzantine generals problem. In Concurrency: the Works of Leslie Lamport, pp. 203-226.