

# Blockchain Technology & Cryptocurrency



# Content

- Cryptocurrencies
- Blockchain technologies
- Blockchain platforms
- Smart contracts
- Ground Truths

# Cryptocurrencies: A Peer-to-Peer Electronic Cash System

## Bitcoin: A Peer-to-Peer Electronic Cash System

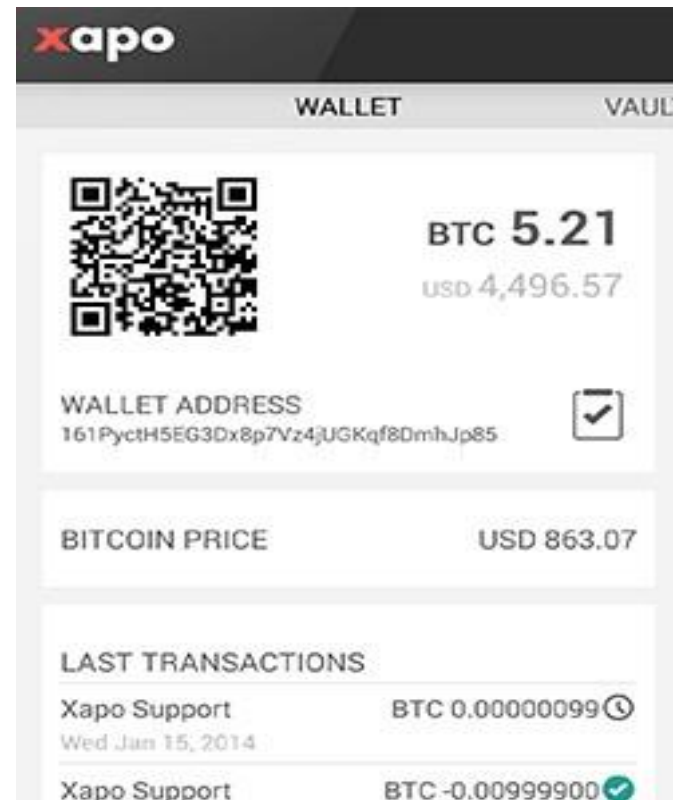
Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

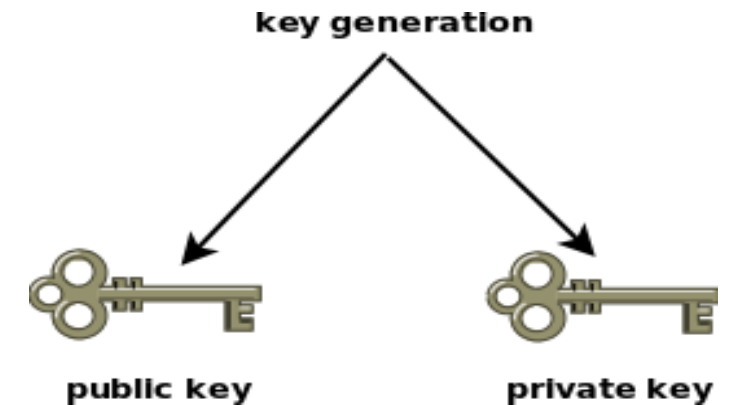
# Cryptocurrencies: Bitcoin wallets



<http://bitcoin-wiki.com/bitcoin-wallet/>



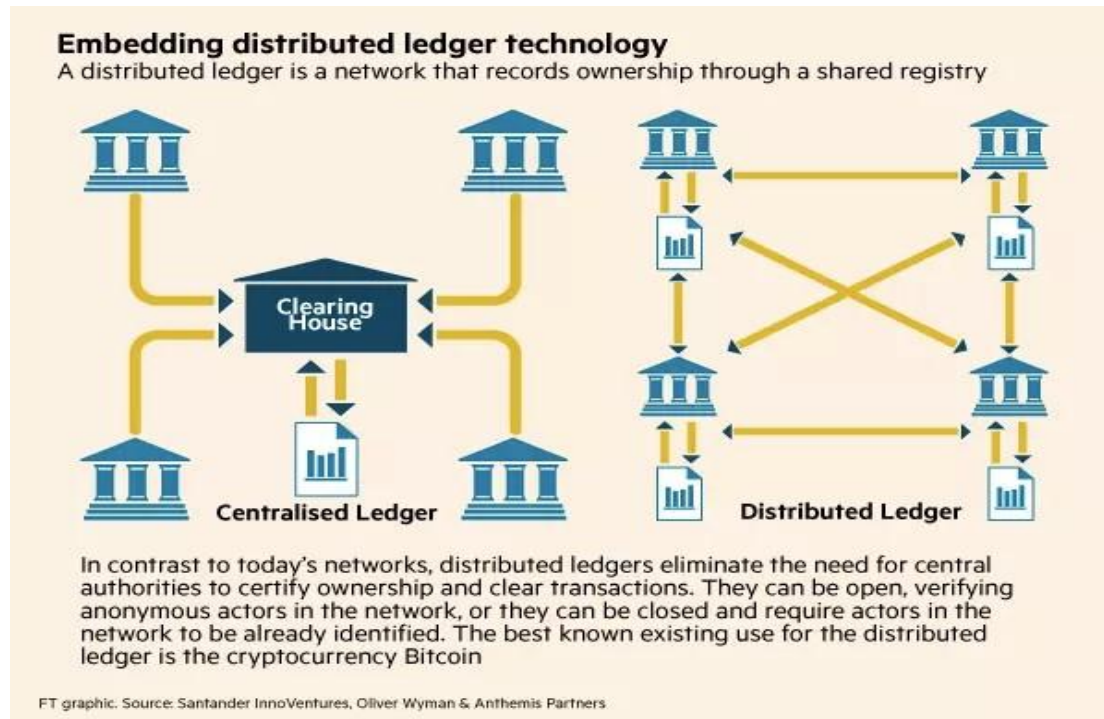
<https://www.bitcoin.com/choose-your-wallet/xapo>



<https://courses.cs.ut.ee/2015/infsec/fall/Main/PKC-PKI>

In Bitcoin, a private key is a 256-bit number, which can be represented one of several ways.

# Cryptocurrencies: The bitcoin Ledger

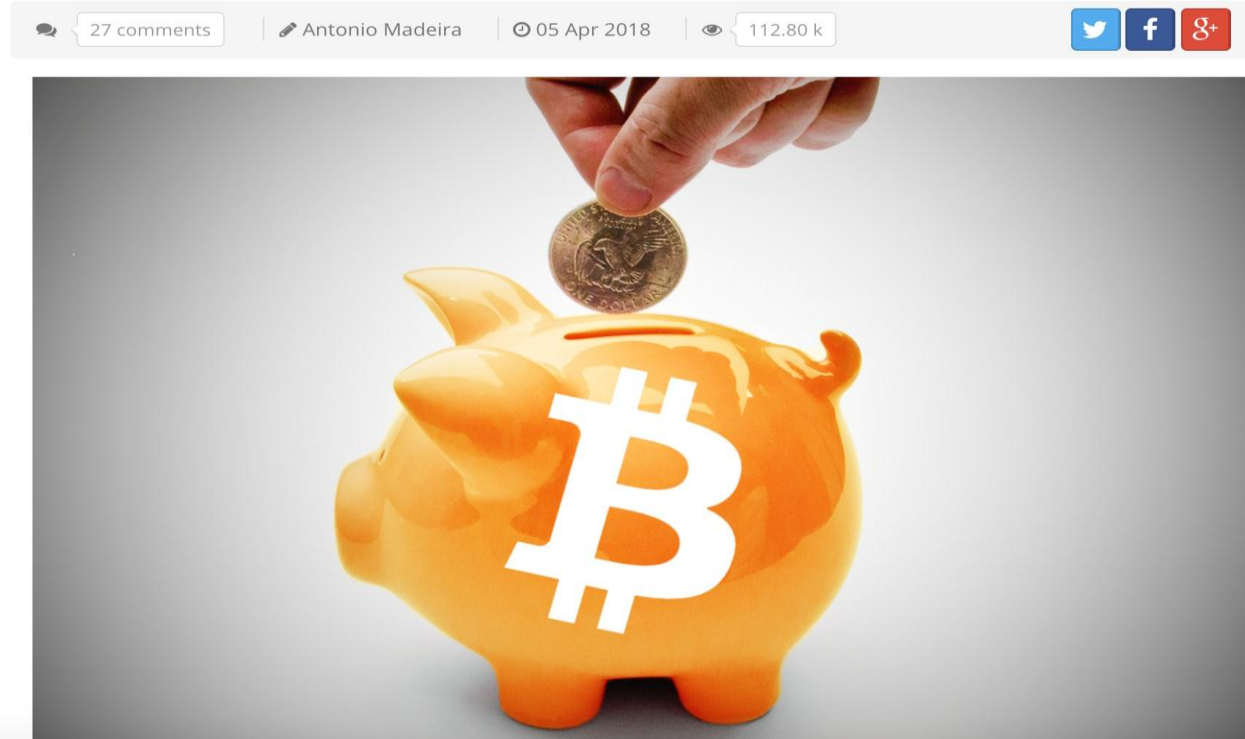


- When one bank sends money to another, no physical currency changes hands.
- Banks and settlement systems use central electronic ledgers to track assets.
- But they can be slow and inefficient, often relying on faxes or manual input.
- That not only wastes time but racks up fees.
- The system is also open to hacking and fraud.

<https://www.ft.com/content/454be1c8-2577-11e5-9c4e-a775d2b173ca>

# Cryptocurrencies: Initial Coin Offering

## How does an ICO work



**“Remember not to invest more than what you can afford to lose and to research the technology and team behind the project. Good luck!”**

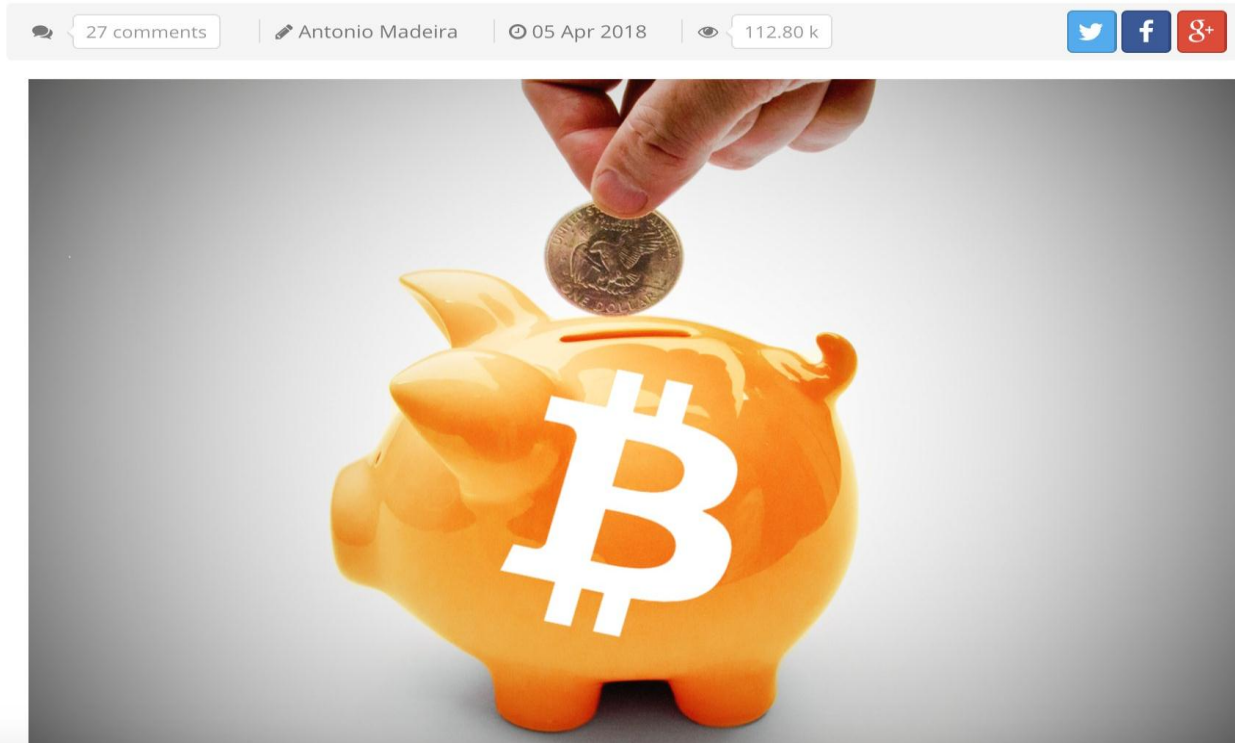
- **Initial Coin Offerings** can be considered as an alternative form of crowdfunding that has emerged outside of the traditional financial system.
- An Initial Coin Offering is an event that usually extends over a period of one week or more and in which everyone is allowed to purchase **newly issued tokens** in exchange for established cryptocurrencies like Bitcoin (BTC) or Ether (ETH).
- There are different models:
  - Static goal and static price
  - Dynamic goal and dynamic price
  - Dynamic goal and static price

<https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/>



# Cryptocurrencies: Initial Coin Offering

## How does an ICO work



- ICO Period: 20 July 2014 – 2 September 2014
- Funds gathered (USD): \$18,439,086
- Funds gathered (BTC): 31,529.49
- Tokens distributed: 60,000,000

**“Remember not to invest more than what you can afford to lose and to research the technology and team behind the project. Good luck!”**

<https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/>

# Cryptocurrencies: Purchase Bitcoin.


[Introduction](#) [Resources](#) [Innovation](#) [Participate](#) [FAQ](#) [English](#)

## Bitcoin Exchanges

Places to buy bitcoin in exchange for other currencies.

### Bitcoin Exchanges

**Note:** Exchanges provide highly varying degrees of safety, security, privacy, and control over your funds and information. Perform your own due diligence and **choose a wallet** where you will keep your bitcoin before selecting an exchange.

 <b>International</b> Bisq Bitstamp Bitwage Kraken Local Bitcoins	 <b>Europe</b> AnyCoin Direct Bitcoin.de BitPanda BL3P Paymium The Rock Trading	 <b>Argentina</b> SatoshiTango
 <b>Australia</b> Bitcoin Australia CoinJar CoinLoft CoinTree HardBlock Independent Reserve	 <b>Brazil</b> Foxbit Mercado Bitcoin Walltime	 <b>Cambodia</b> Bitcoin Cambodia



# Cryptocurrencies: Disasters (Mt. Gox Jed McCaleb, Nicehash)

## The History of the Mt Gox Hack: Bitcoin's Biggest Heist

Andrew Norry on November 29, 2017 / 1 Comment  
Post Views: 20,741

At the beginning of 2014, Mt Gox, a bitcoin exchange based in Japan, was the largest bitcoin exchange in the world, handling over 70% of all bitcoin transactions worldwide. By the end of February of that year, it was bankrupt.

The victim of a massive hack, Mt. Gox lost about 740,000 bitcoins (6% of all bitcoin in existence at the time), valued at the equivalent of €460 million at the time and over \$3 billion at October 2017 prices. An additional \$27 million was missing from the company's bank accounts. Although 200,000 bitcoins were eventually recovered, the remaining 650,000 have never been recovered.



<https://blockonomi.com/mt-gox-hack/>

## Bitcoin: \$64m in cryptocurrency stolen in 'sophisticated' hack, exchange says

**Mining marketplace NiceHash suspends operations while it cooperates with authorities over 'professional attack', urging users to change passwords**



▲ NiceHash said approximately 4,700 bitcoin were stolen. Photograph: Dado Ruvic/Reuters

Nearly \$64m in bitcoin has been stolen by hackers who broke into Slovenian-based bitcoin mining marketplace NiceHash.

<https://www.theguardian.com/technology/2017/dec/07/bitcoin-64m-cryptocurrency-stolen-hack-attack-marketplace-nicehash-passwords>

# **Blockchain Technologies**

# Blockchain Transactions

Block Explorer News Market Bitcoin cash Zcash Blocks Status Buy Bitcoin with CCI

Search for block, transaction or address - Conn 73 - Height 517702 Scan BTC -

## Latest Blocks

Height	Age	Transactions	Mined by	Size
517702	22 minutes ago	30		7522
517701	22 minutes ago	568	AntMiner	242365
517700	26 minutes ago	908		359790

See all blocks

## Latest Transactions

Hash	Value Out
7d683d237438dbf63ed07669b2d102f5c5dd38beeb...	0.60096836 BTC
266ed2ec43186f198099e7f69b527aab762d6bd59b8...	0.15002142 BTC
09d3db0d578f8e4d59ad2a00689ef0977775bb9867...	0.10340446 BTC
ba29ea87a9b7d2c9d5a6d56c2504f96dc6b122b1422...	0.00260313 BTC
76c1575f1909f6eaa660cb460b495ba964c591bf081...	1.9762774 BTC
ada8d2052dfcf4c2e46120306e2c562bf9acfb0b5ed4...	0.3545435 BTC
819fc08acdf03b7966d5498019da2f58d38ff8b0d119...	0.03374796 BTC

## Subscribe for updates!

email address

Subscribe

## About Block Explorer

**Bitcoin Block Explorer** is an open source web tool that allows you to view information about [blocks](#), [addresses](#), and [transactions](#) on the Bitcoin blockchain. The [source code](#) is on GitHub.

[What is bitcoin?](#)

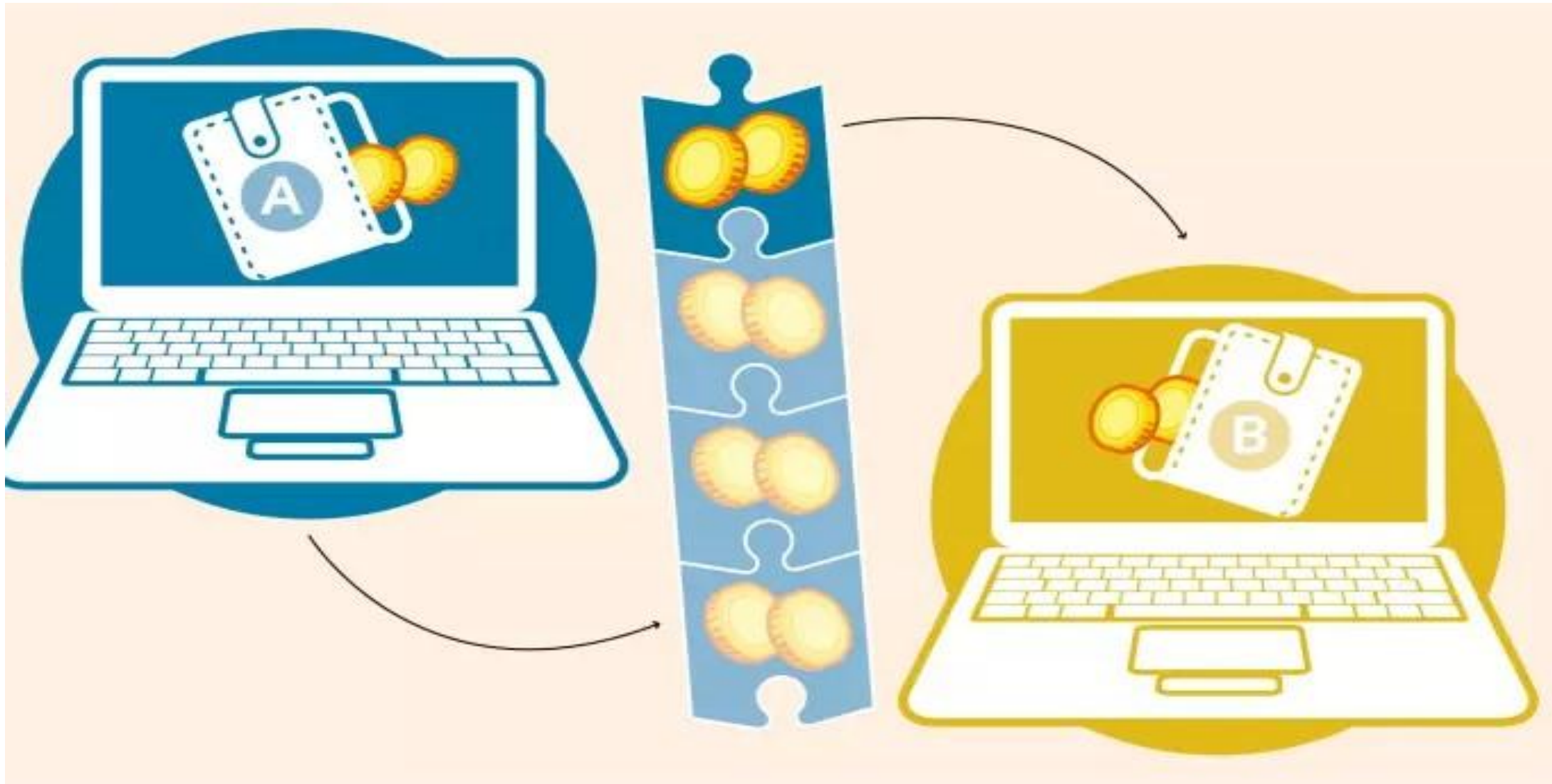
**Public Bitcoin API:** Machine readable stats & blockchain info can be accessed directly through the [REST](#) and [Websockets APIs](#).

**Testnet** is Bitcoin's sandbox. Block Explorer supports viewing both the [testnet](#) and [mainnet](#) blockchains.

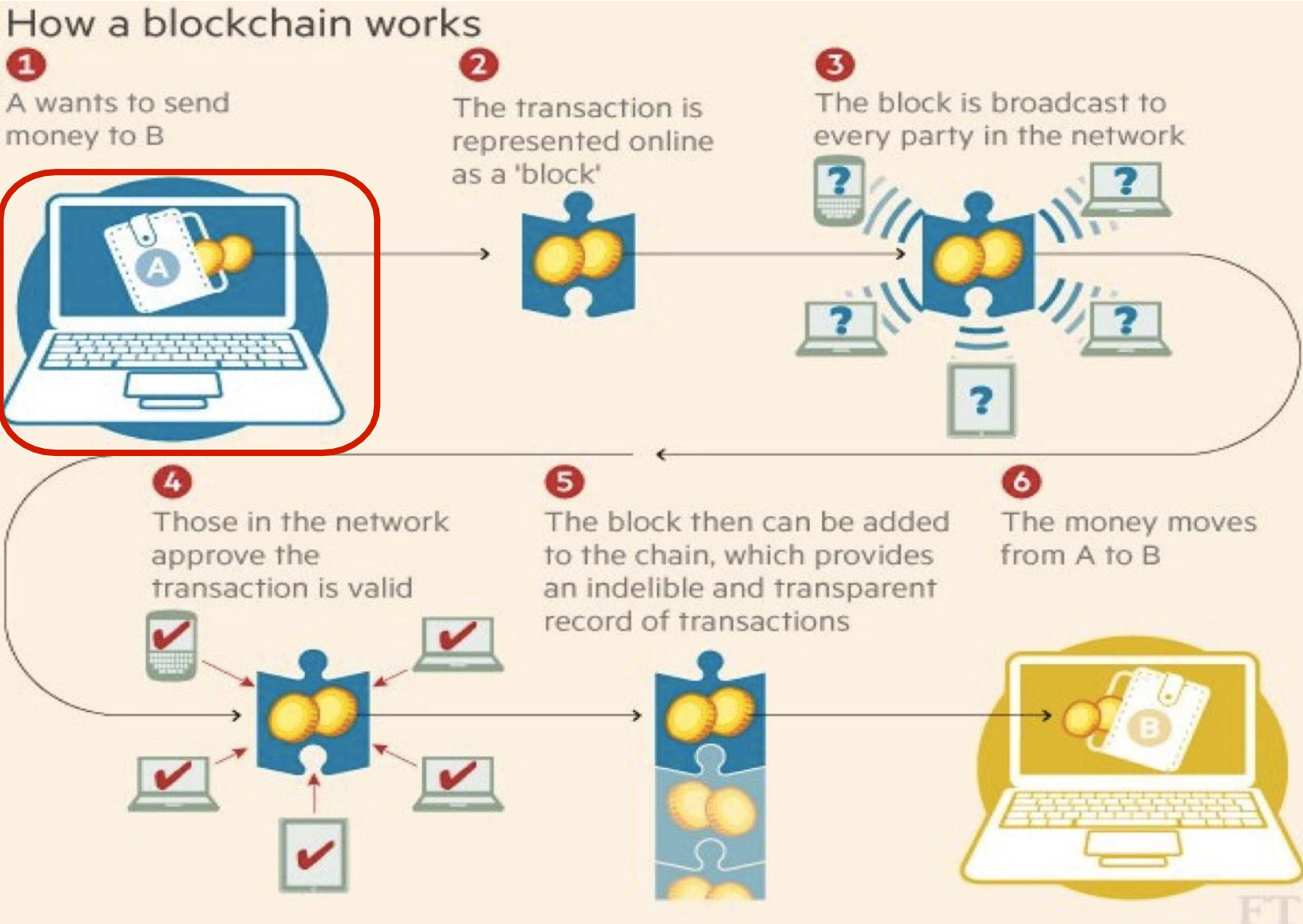
Thanks to [Private Internet Access](#) for hosting the site. They provide a [VPN Service](#) that accepts Bitcoin.



# Blockchain technology



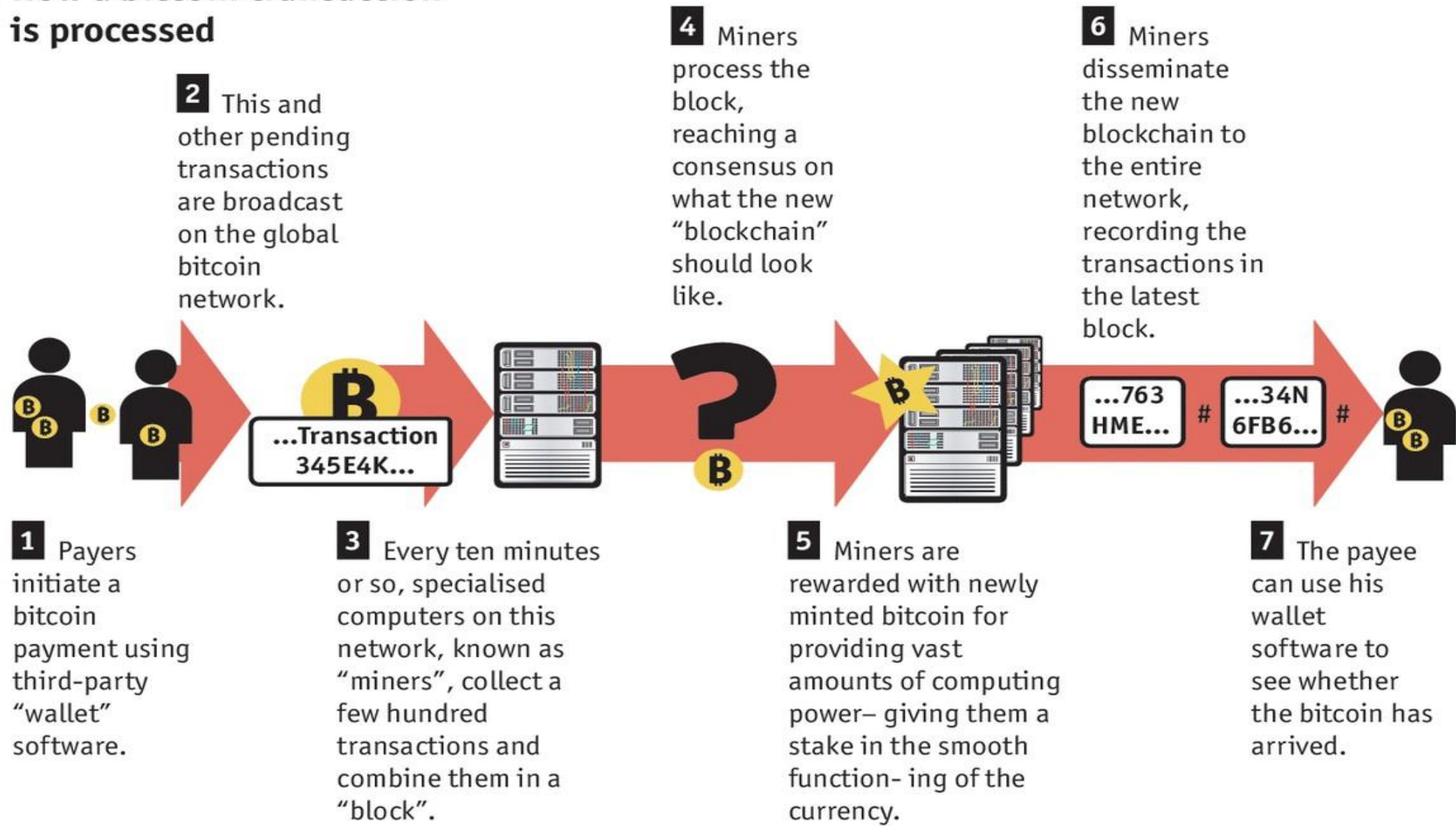
# Executing Transactions - Trading



- Major technologies that make Bitcoin include:
- Hashes
- Digital signatures
- Public key cryptography
- P2P
- Proof of Work

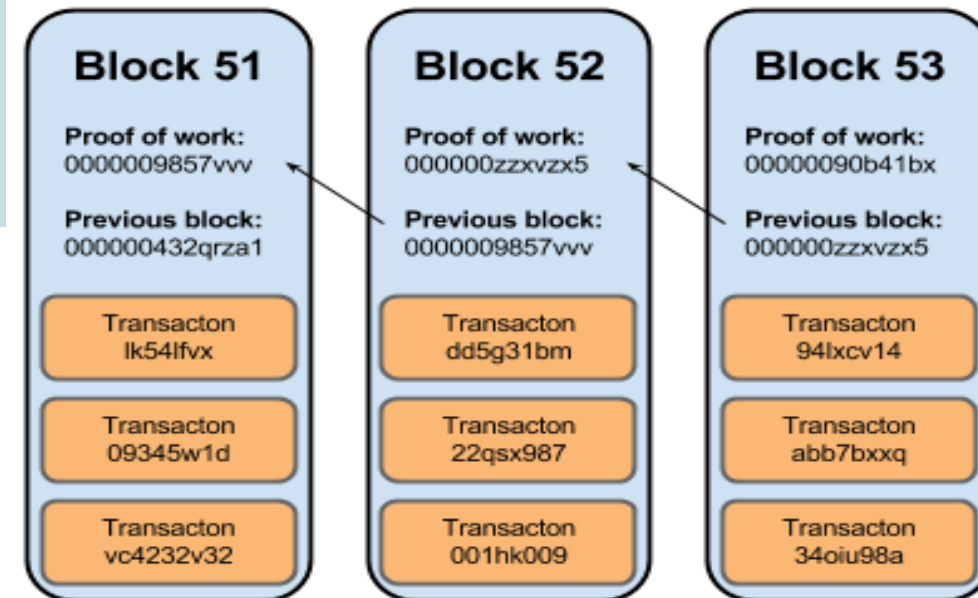
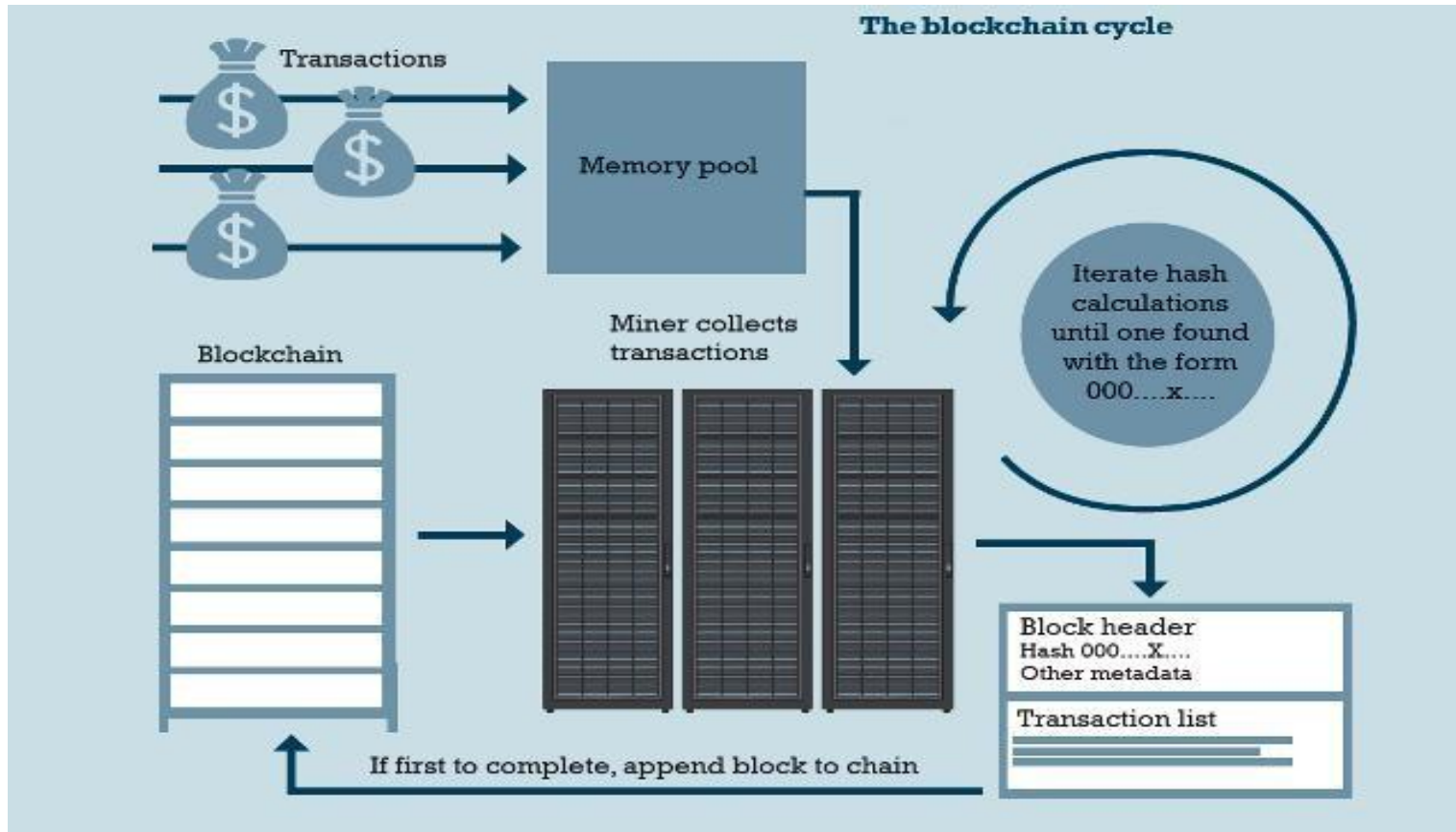
# Processing Transactions - Mining

## How a bitcoin transaction is processed





# Processing Transactions - Mining



# **Blockchain Platforms**

# Ethereum Platform

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



The image features the Ethereum logo, a blue diamond shape with a white 'E' inside, positioned at the top center. Below the logo, the word 'ethereum' is written in a lowercase, sans-serif font. Underneath 'ethereum', the words 'BLOCKCHAIN APP PLATFORM' are written in a smaller, uppercase, sans-serif font, enclosed in a dark blue rectangular box. The background is a perspective view of a modern building's interior, showing a series of parallel lines that create a sense of depth and architectural structure.

## Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts:** applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

These apps run on a custom built **blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.**



A network diagram consisting of five interconnected nodes. The nodes are labeled: 'YOUR KARMA' (pink), 'YOUR FRIENDS' (blue), 'YOUR DATA' (green), 'YOUR VIDEOS' (orange), and 'YOUR REPUTATION' (yellow). The nodes are connected by a series of lines, forming a network structure.

# Hyperledger Platforms

[About](#)[Members](#)[Projects](#)[Community](#)[Industries](#)[Resources](#)[News & Events](#)[Blog](#)

## Business Blockchain Frameworks Hosted with Hyperledger

### Burrow

Provides a modular blockchain client with a permissioned smart contract interpreter partially developed to the Ethereum Virtual Machine (EVM) specification.

### Fabric

An implementation of blockchain technology intended as a foundation for developing blockchain applications or solutions.

### Iroha

A blockchain framework designed for simple and easy incorporation into infrastructure projects requiring distributed ledger technology.

### Sawtooth

A modular platform designed for building, deploying, and running versatile and scalable distributed ledgers.

### Indy

A distributed ledger that provides tools, libraries, and reusable components for creating and using independent, decentralized and digital identities.

[» Learn More About Hyperledger Projects](#)

# Killer Apps: Payments

WHAT'S NEXT FOR BLOCKCHAIN PAYMENTS IN 2018?

👤 Miranda Marquit © January 2, 2018



The year closed out with a wild ride for Bitcoin. The cryptocurrency surged to \$20,000 and then fell by about 40% before rebounding to some degree.

But Bitcoin *isn't the be all and end all of blockchain technology*. Indeed, blockchain payments are seeing more interest. So, as a new year gets underway, what can we expect from blockchain payments?

**Bitcoin Unlikely to Remain the Main Platform for Blockchain Payments**



# Killer Apps: Registries

## Notaries turn blockchain into ally for digital transactions

By Jorge Valero | EURACTIV.com

4 Oct 2017

Supporters



Haiti is still struggling to get back on its feet after the 2010 earthquake. All their records were on paper and most of them disappeared. Notaries could build new land registries based on blockchain technology to increase efficiency. [DG ECHO/Flickr]

Comments Print 50 in g+ Twitter Email

*This article is part of our special report EU law goes digital.*

**Once feared as a technology that would make legal practitioners redundant, blockchain has now actually strengthened the role of notaries as interpreters of complex transactions, best illustrated by the convoluted issue of land registries.**



Advertisement



# Killer Apps: Internet of Things

## Blockchain And The Internet Of Things: 4 Important Benefits Of Combining These Two Mega Trends



**Bernard Marr**, CONTRIBUTOR  
FULL BIO ▾

Opinions expressed by Forbes Contributors are their own.

The **Internet of Things (IoT)** and **blockchain** are two topics which are causing a great deal of hype and excitement, not just in the technology circle but in the wider business world, too.



Adobe Stock  
Adobe Stock

Many say they are set to revolutionize all aspects of our lives, while others point out that there is a lot of hot air around both ideas, and a lot is yet to be proved.

However, the idea that putting them together could result in something even greater than the sum of its (not insignificant) parts, is something which is starting to gain traction.



<https://www.forbes.com/sites/bernardmarr/2018/01/28/blockchain-and-the-internet-of-things-4-important-benefits-of-combining-these-two-mega-trends/#635c031c19e7>

# Killer Apps: Media and Entertainment

## How Blockchain Could Start To Make Waves In Media And Entertainment In 2018



**Nelson Granados**, CONTRIBUTOR

*I cover digital trends in travel, media and entertainment.*

[FULL BIO](#) ▾

Opinions expressed by Forbes Contributors are their own.

### TWEET THIS



If you are in media and entertainment, 2018 will be a year to closely monitor and possibly experiment or invest in blockchain innovation, if you haven't done so yet. Otherwise, you could be left behind.



A woman touches an ATM machine for digital currency Bitcoin in Hong [ + ]

Blockchain technology made big news in December thanks to the bitcoin cryptocurrency surging past \$10,000 to a \$20,000 peak, the launch of bitcoin futures in major exchanges, and the announcement that the Australian Stock Exchange will use blockchain technology for trade settlement. Blockchain could also start to be implemented in media and entertainment in 2018.



<https://www.forbes.com/sites/nelsongranados/2018/01/04/what-blockchain-has-in-store-for-media-and-entertainment-in-2018/#3045f0b771f4>

# Killer Apps: Supply Chain Management

## Perspectives

### Using blockchain to drive supply chain transparency

#### Future trends in supply chain

New technologies are presenting promising opportunities for improvement across the supply chain. Using blockchain in the supply chain has the potential to improve supply chain transparency and traceability as well as reduce administrative costs.



## Monitor advancements

A blockchain supply chain can help participants record price, date, location, quality, certification, and other relevant information to more effectively manage the supply chain. The availability of this information within blockchain can increase traceability of material supply chain, lower losses from counterfeit and gray market, improve visibility and compliance over outsourced contract manufacturing, and potentially enhance an organization's position as a leader in responsible manufacturing.

**Deloitte recommends:** Using blockchain in the supply chain can help participants record price, date, location, quality, certification, and other relevant information to more effectively manage the supply chain.



Using blockchain to drive  
supply chain innovation

**Download the PDF**

<https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html>



# Killer Apps: Digital Identities

**ICTworks**

## Two Blockchain Use Cases for Self-Sovereign Digital Identities

By Wayan Vota on January 31, 2018



Source: Gravity

# Smart Contracts[1]

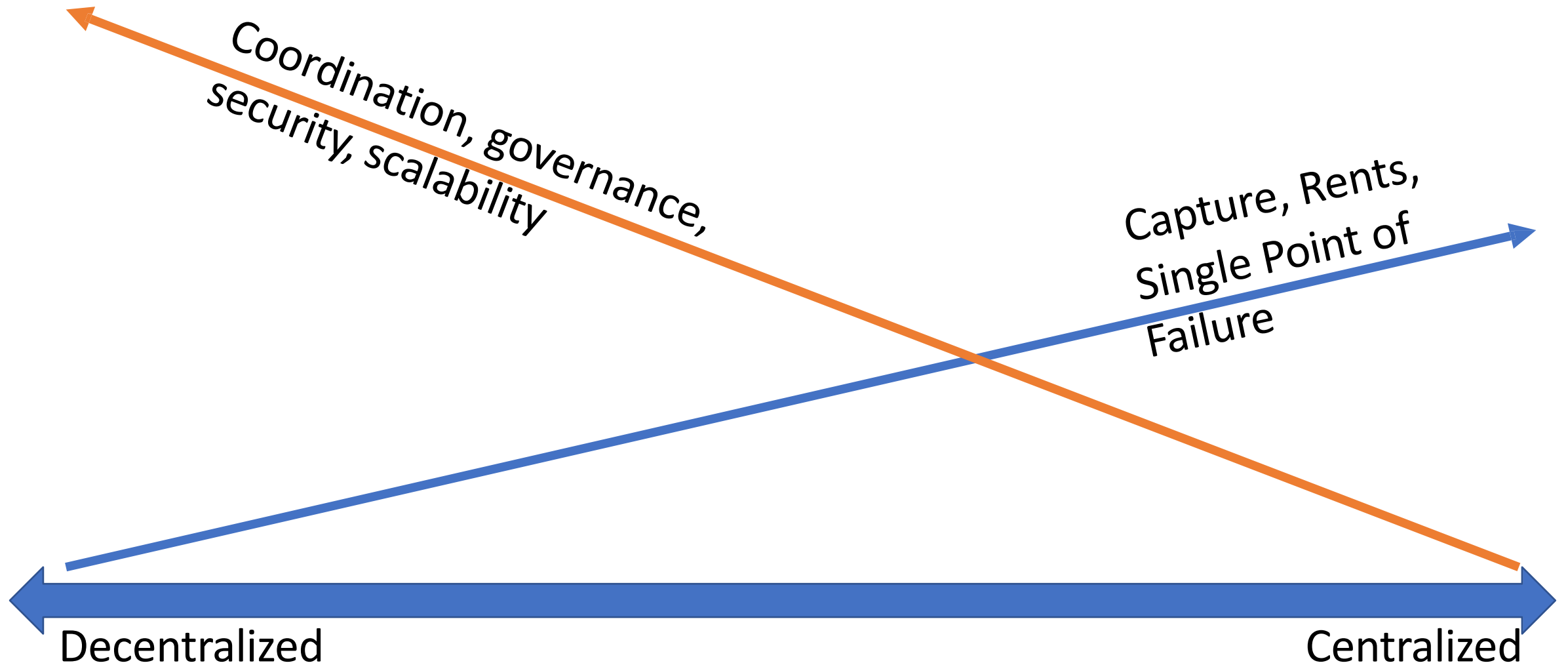
- “A set of promises,
- specified in digital form,
- including protocols
- within which the parties perform on these promises.”

Nick Szabo, 1996

However ....

- Smart Contracts may not be **‘Smart’**
- Smart Contracts may not be **‘Contracts’**

# Framework for Comparing Costs & Trade-offs (Coase)[1]





# Incumbents' Choices of Databases[2]

Access



Client Server

Permissioned

Permissionless

## Traditional Databases

Trusted Party Hosts Data

Trusted Party can Create, Read, Update, & Delete (CRUD)

Client Server Architecture

## Private Blockchain

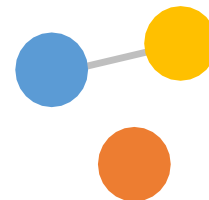
Known Participants

Private Write Capability

Append Only Timestamped Log

Publicly Verifiable

No Native Currency Needed



## Public Blockchain

Unknown Participants

No Central Intermediaries

Public Write Capability

Peer to Peer Transactions

Native Tokens & Incentives



# Initiatives[2]

## Real Time Gross Settlement

- Brazil, Canada (Project Jasper), Europe and Japan (Project Stella), Singapore (Project Ubin), South Africa (Project Khokha)

## Digital Currency

- Central Bank Claim: Bahamas (Sand Dollar), Ecuador (Dinero Electrónico), Iran (Payman), Sweden (E-Krona)
- Commercial Bank Claim: Philippines (ePiso), Senegal (eCFA), Tunisia (e-Dinar)
- Possible Hybrid: China (Digital Currency Electronic Payment)
- Commodity Backed: U.K. (Royal Mint Gold), Venezuela (Petro)
- Other: Dubai – emCash, Saudi & UAE (cross-border pilot), Uruguay (Digital Peso)

# Truths[2]

- Nakamoto solved the payments riddle - avoiding double spending
- Money is but a social & economic construct
- We already live in an age of digital money
- Append-only logs & multiparty consensus provides a peer-2-peer alternative
- Blockchain technology can address verification and networking costs
- Adoption rests on addressing comparative viability & value proposition

# Truths[2]

- Crypto markets are rife with scams, fraud, hacks & manipulation
- Cryptocurrencies have evolved into a speculative asset class
- Crowdfunding built on smart contracts & ICOs raised nearly \$30 billion
- Lightly & non regulated markets provide retail investors direct way to trade
- The potential, though, to be a catalyst for change is real

# References

1. 'Even if a Thousand Projects Don't Make It, Blockchain Is Still a Change Catalyst' Gensler, CoinDesk
2. 'Economics of Money & Blockchain Technology and Evaluating Projects' MIT Cryptocurrency Online Course