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

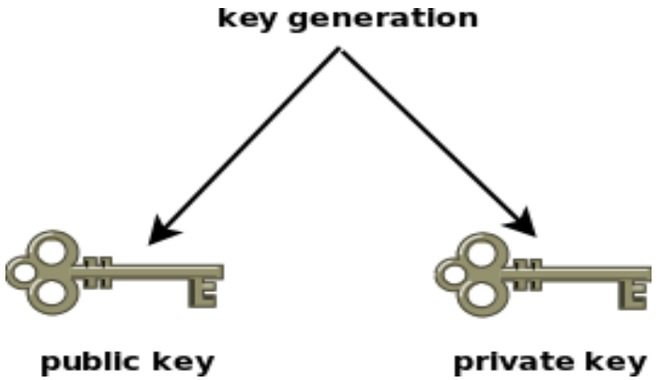
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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/

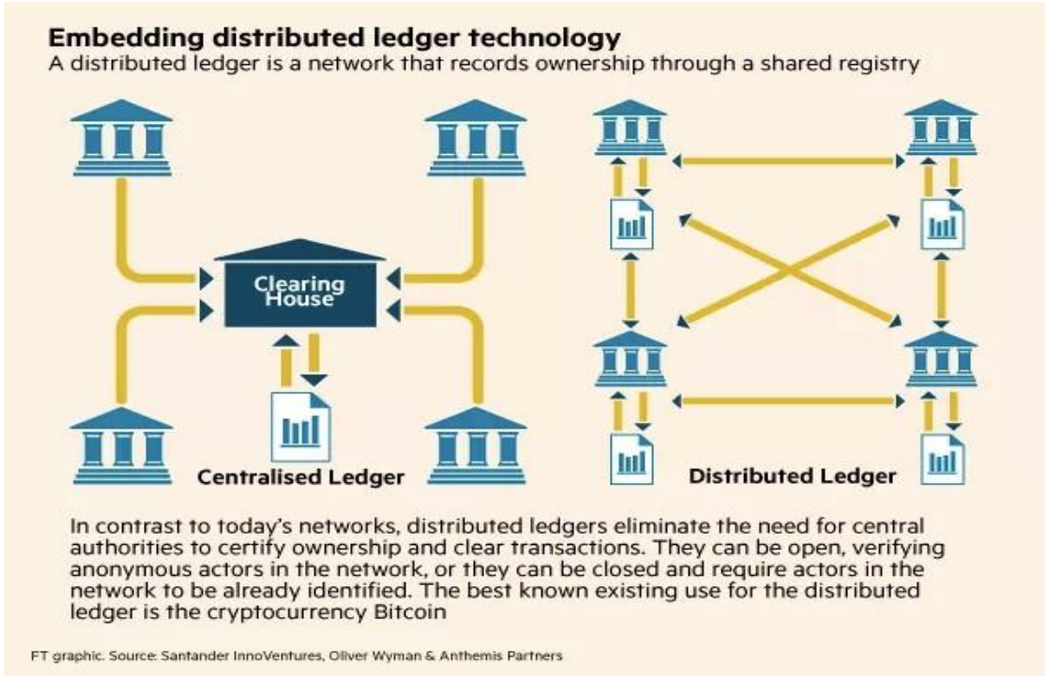
https://www.bitcoin.com/choose-your-wallet/xapo



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

"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

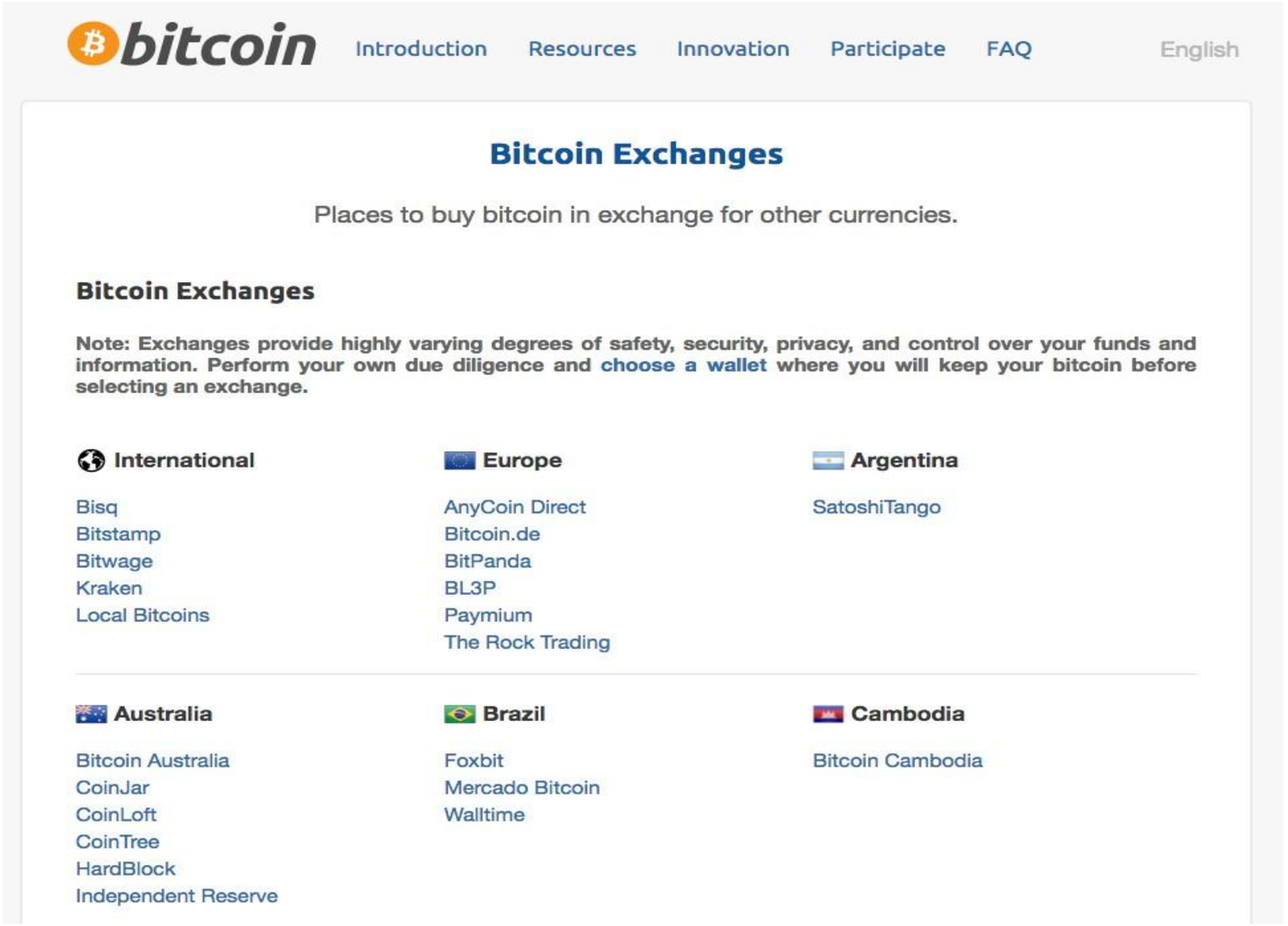
“Remember not to invest more than what you can afford to lose and to research the technology and team behind the project. Good luck!”

ethereum

- 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

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

Cryptocurrencies: Purchase Bitcoin.



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 co-operates with authorities over 'professional attack', urging users to change passwords

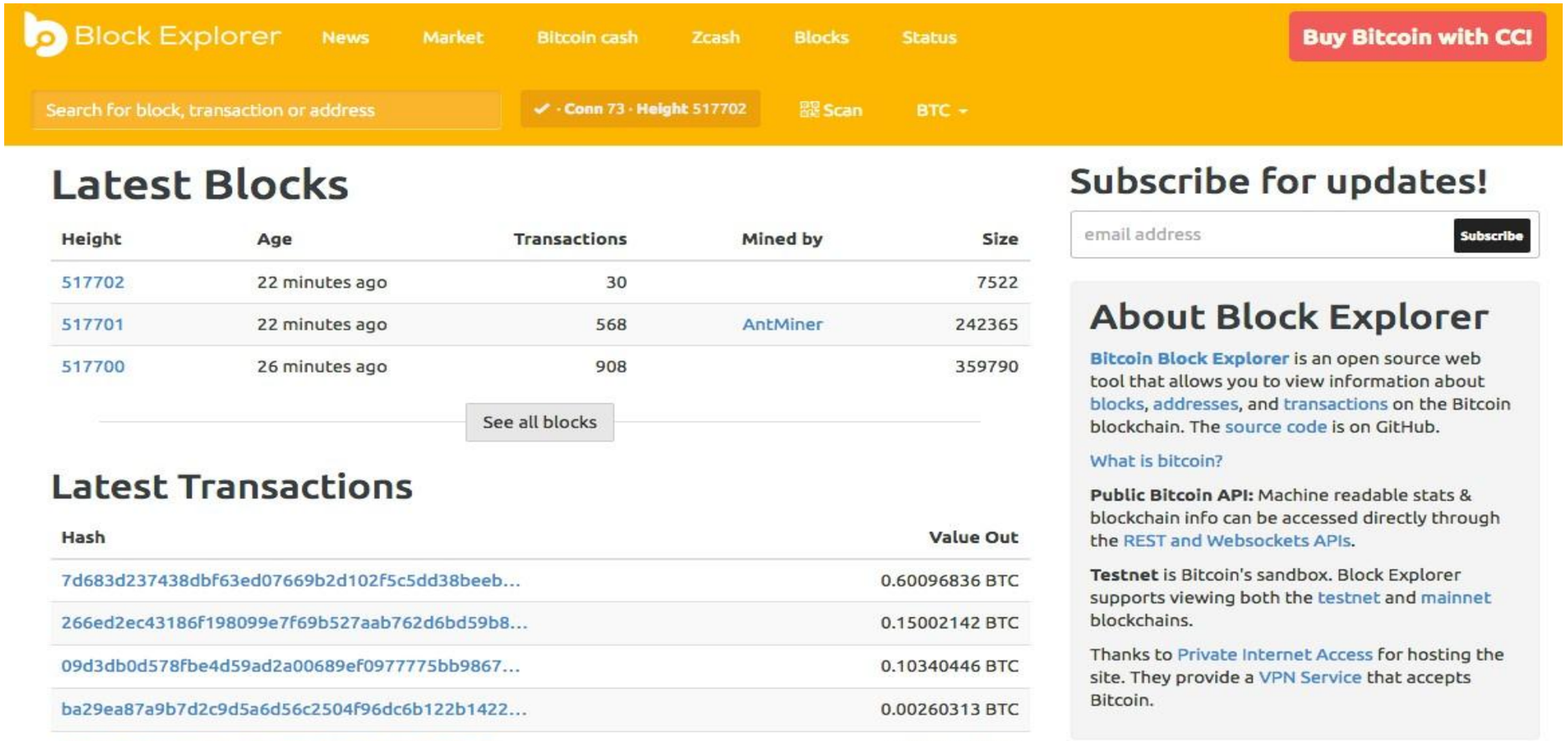
▲ NiceHash said approximately 4,700 bitcoin were stolen. Photograph: Dado Ruvic/Reuters

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

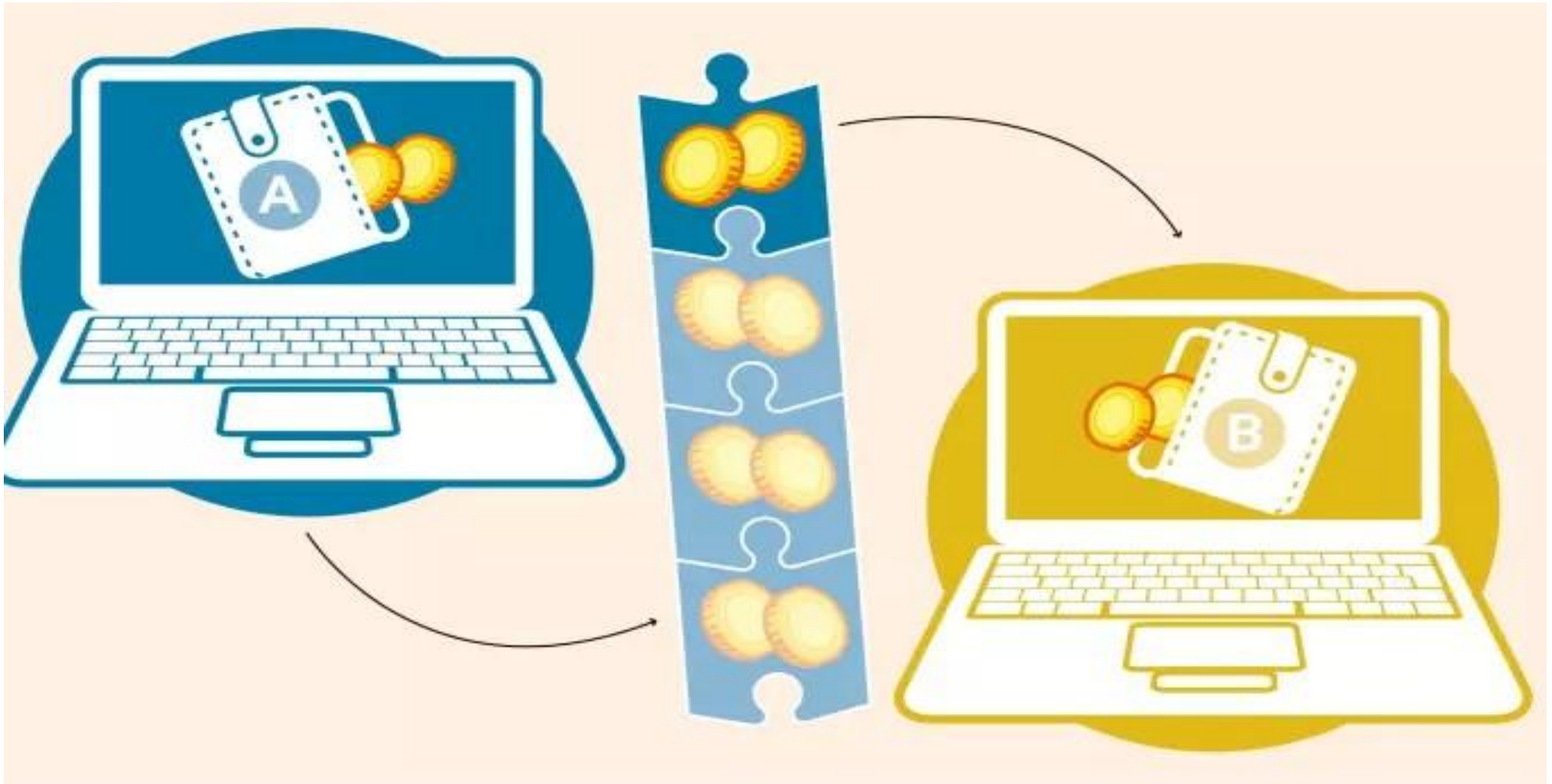
Blockchain Technologies

Blockchain Transactions



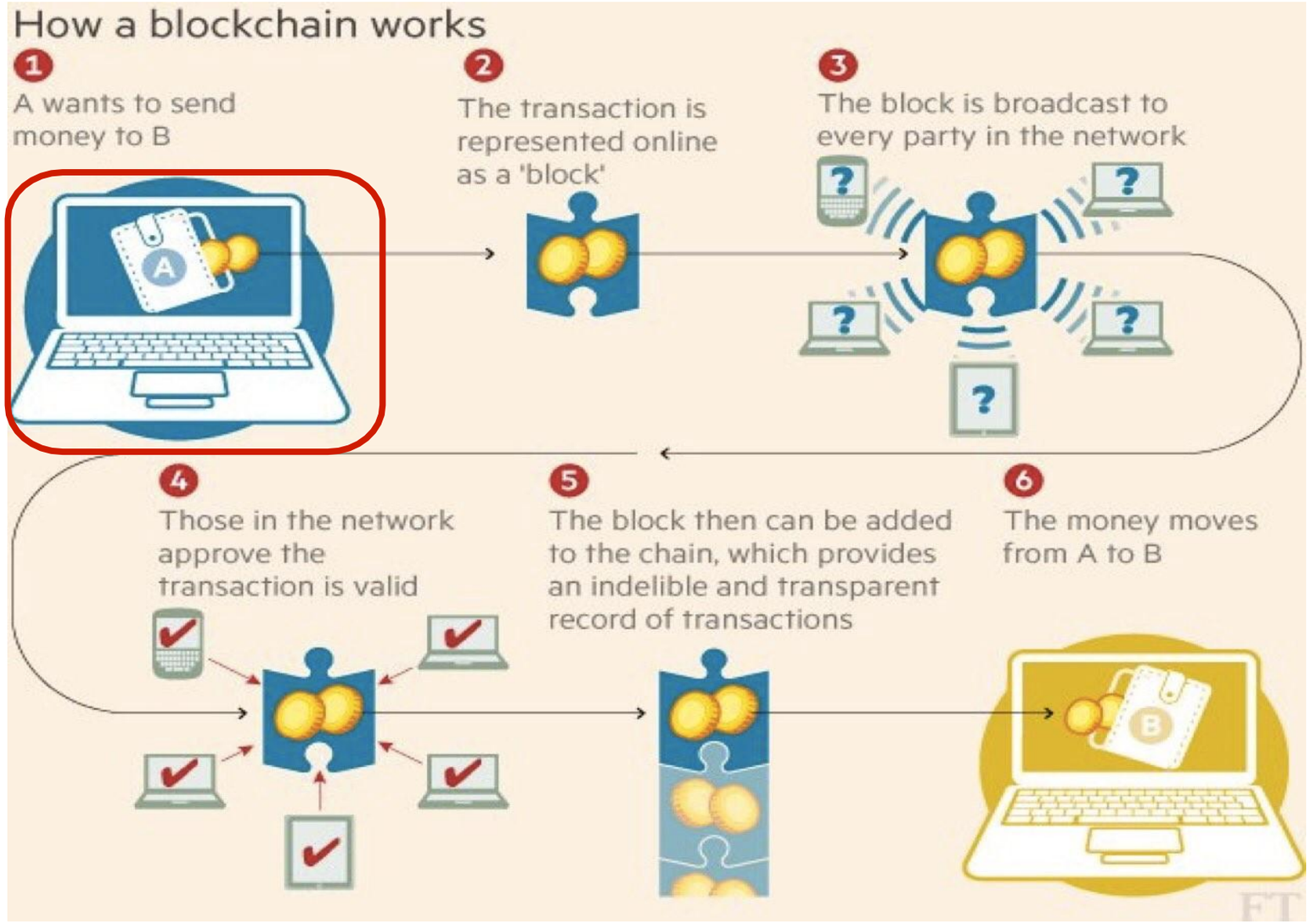
https://blockexplorer.com/

Blockchain technology



https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64

Executing Transactions - Trading



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

https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64

Processing Transactions - Mining

How a bitcoin transaction is processed

1 Payers initiate a bitcoin payment using third-party "wallet" software.

2 This and other pending transactions are broadcast on the global bitcoin network.

3 Every ten minutes or so, specialised computers on this network, known as "miners", collect a few hundred transactions and combine them in a "block".

4 Miners process the block, reaching a consensus on what the new "blockchain" should look like.

5 Miners are rewarded with newly minted bitcoin for providing vast amounts of computing power– giving them a stake in the smooth function- ing of the currency.

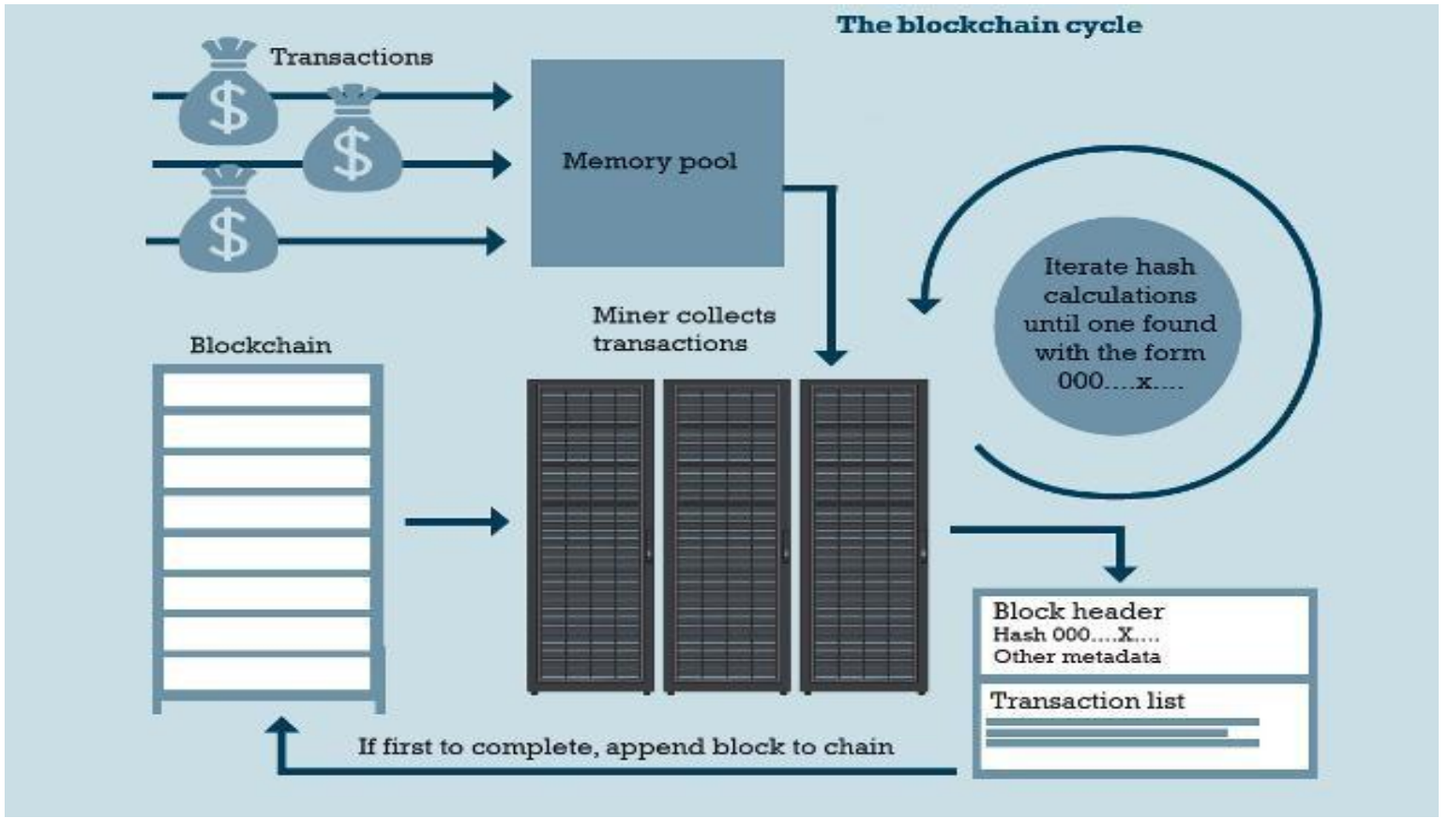
6 Miners disseminate the new blockchain to the entire network, recording the transactions in the latest block.

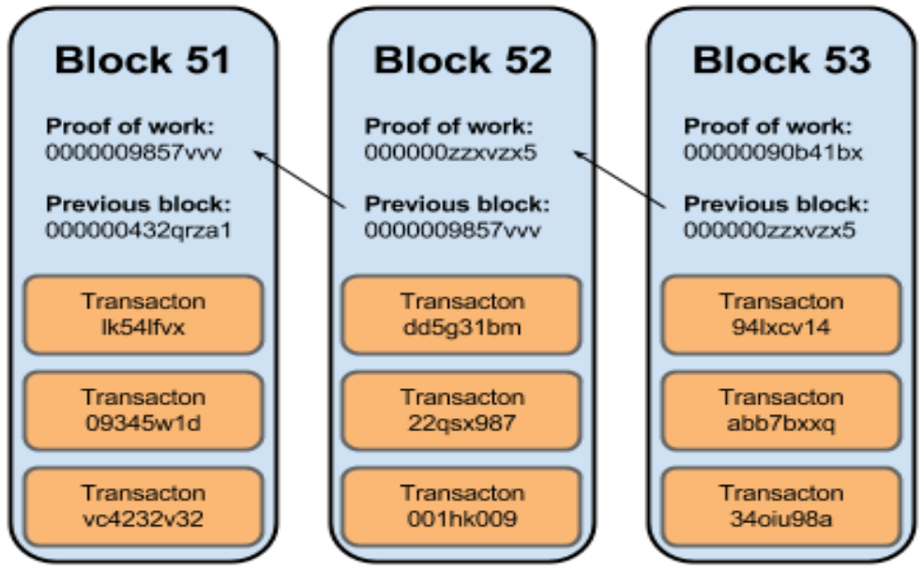
7 The payee can use his wallet software to see whether the bitcoin has arrived.

Economist.com

https://bitcoinexchangeguide.com/blockchain-distributed-ledger-technology/

Processing Transactions - Mining



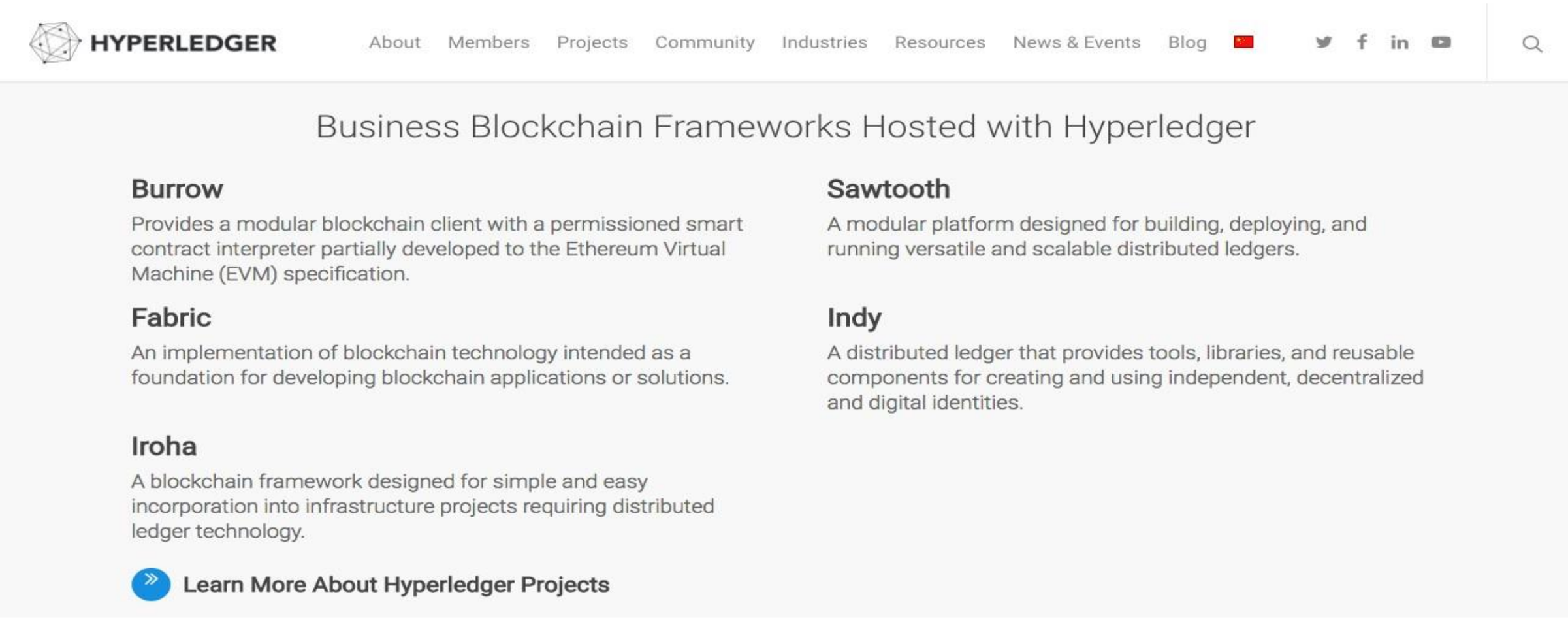


Blockchain Platforms

Ethereum Platform

https://www.ethereum.org/

Hyperledger Platforms



https://www.hyperledger.org/

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

https://due.com/blog/blockchain-payments/

Killer Apps: Registries

Notaries turn blockchain into ally for digital transactions

By Jorge Valero | EURACTIV.com

4 Oct 2017

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

Comments Print 50

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.

https://www.euractiv.com/section/digital/news/notaries-turn-blockchain-into-ally-in-digital-transactions/

Killer Apps: Internet of Things

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

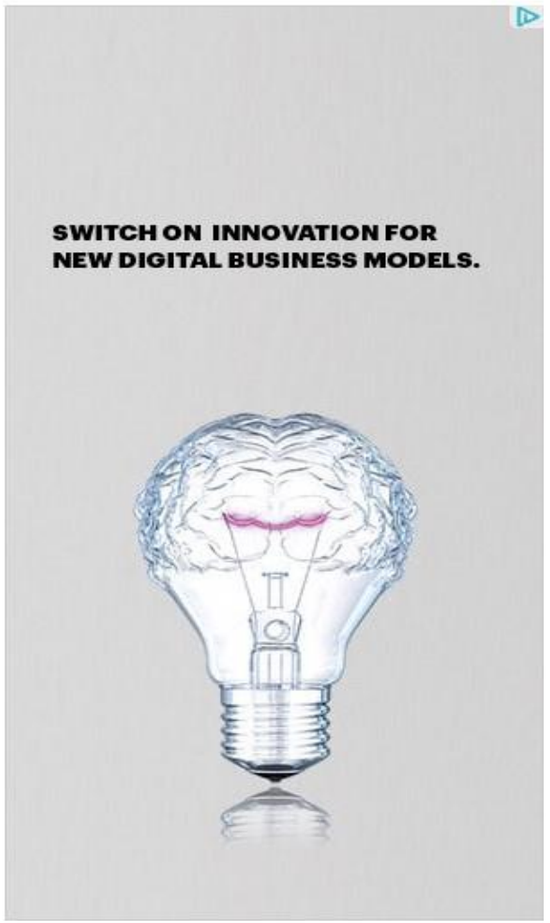
Bernard Marr, CONTRIBUTOR
FULL BIO
Opinions expressed by Forbes Contributors are their own.

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

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

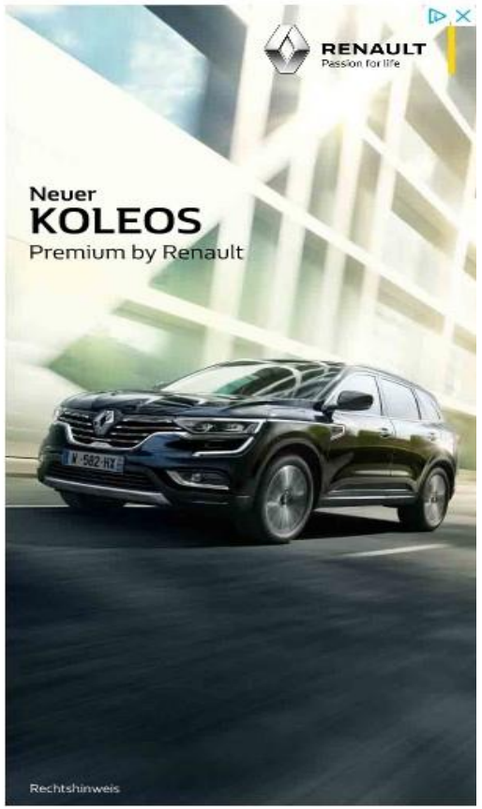
Nelson Granados, CONTRIBUTOR
I cover digital trends in travel, media and entertainment.
FULL BIO
Opinions expressed by Forbes Contributors are their own.

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

https://www.ictworks.org/blockchain-use-cases-self-sovereign-digital-identities/#.Ws4yGdNuZBw

Smart Contracts[1]

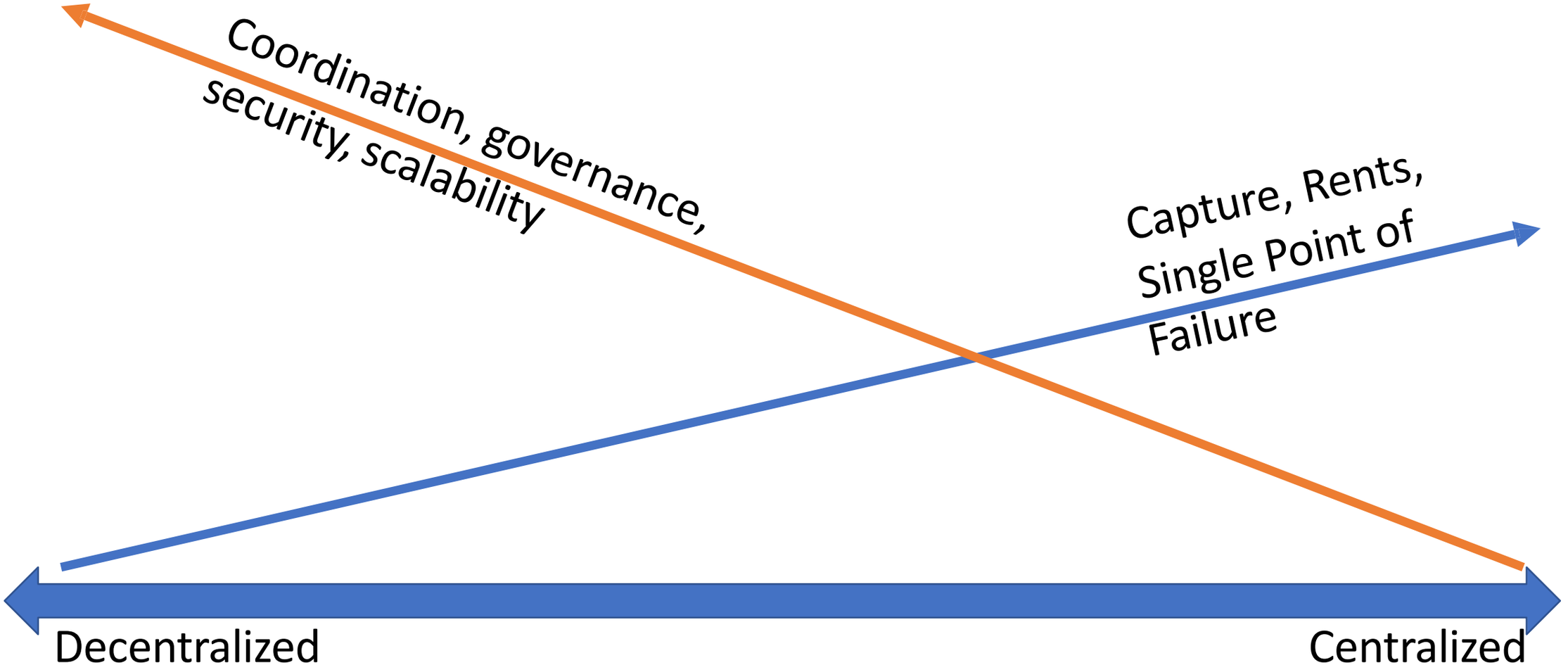
- “A set of promises,
- specified in digital form,
- including protocols
- within which the parties perform on these promises.”

  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

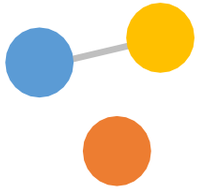
Known Participants

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