CS578: Blockchain Technology: A Software Engineering Perspective

Dr. Raju Halder

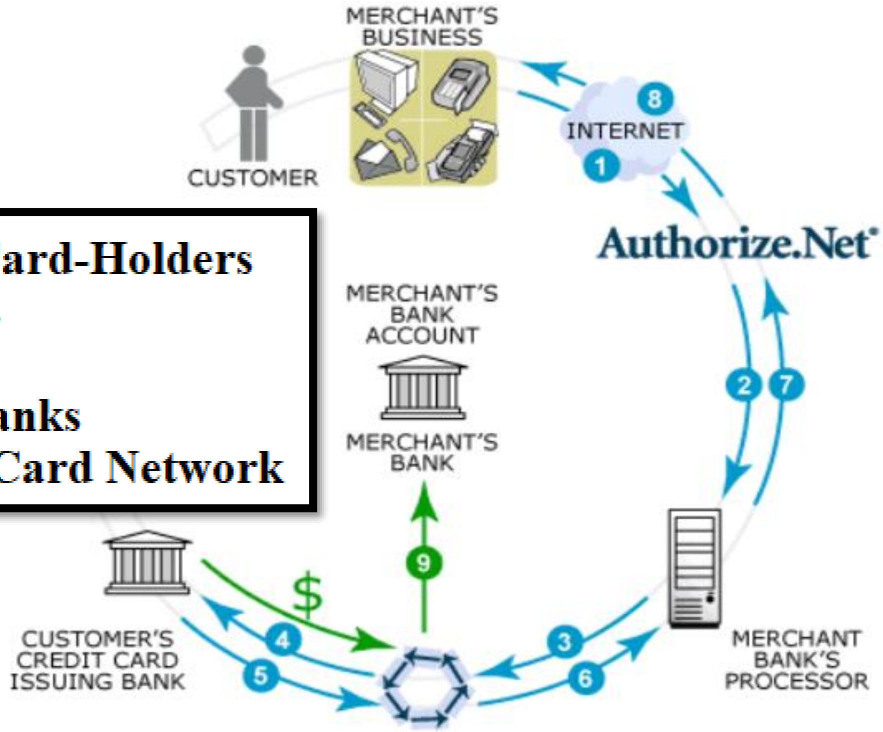
Quick Review of Blockchain Technology

- Instructors: Dr. Raju Halder
  - halder@iitp.ac.in

- Teaching Assistants
  - [Ph.D.] Akshay M. Fajge (fajge_1921cs12@iitp.ac.in)
  - [Ph.D.] Swagatike Sahoo (swagatika_1921cs03@iitp.ac.in)
  - [Ph.D.] Medhashree Ghosh (medhasree_2121cs05@iitp.ac.in)

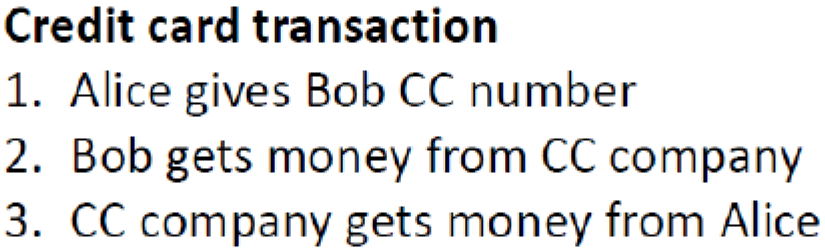
Cyber-Currencies Uses

Regulatory Agency (RBI)
Bank Employees
Customers



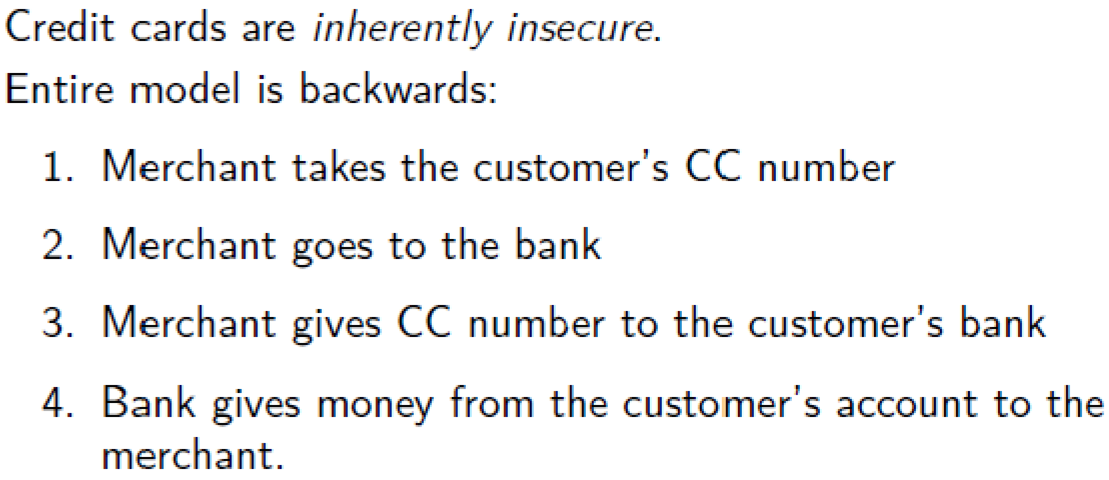
Customers/Card-Holders
Issuer-Banks
Merchants
Merchant-Banks
Visa/MasterCard Network

Cyber-Currencies Use



Credit card transaction

1. Alice gives Bob CC number
2. Bob gets money from CC company
3. CC company gets money from Alice



Credit cards are *inherently insecure*.

Entire model is backwards:

1. Merchant takes the customer's CC number
2. Merchant goes to the bank
3. Merchant gives CC number to the customer's bank
4. Bank gives money from the customer's account to the merchant.

Cyber-Currencies Use

Bank transaction

1. Alice orders bank to pay Bob
2. Bank(s) update records

Something like this would be better:

1. Customer tells bank to give money to merchant
2. That's it!

Concerns: few among many others

- Write cheque or make online-transaction
  - Someone forged your cheque/signature
  - Amount field is tampered
  - Amount deducted, but ATM has not released money.
- Check bank statement via online account/check monthly statements
  - Showing unexpected transactions
  - SIM fraud/password leak/untrusted bank employee
- Credit Card Fraud

Who is responsible?

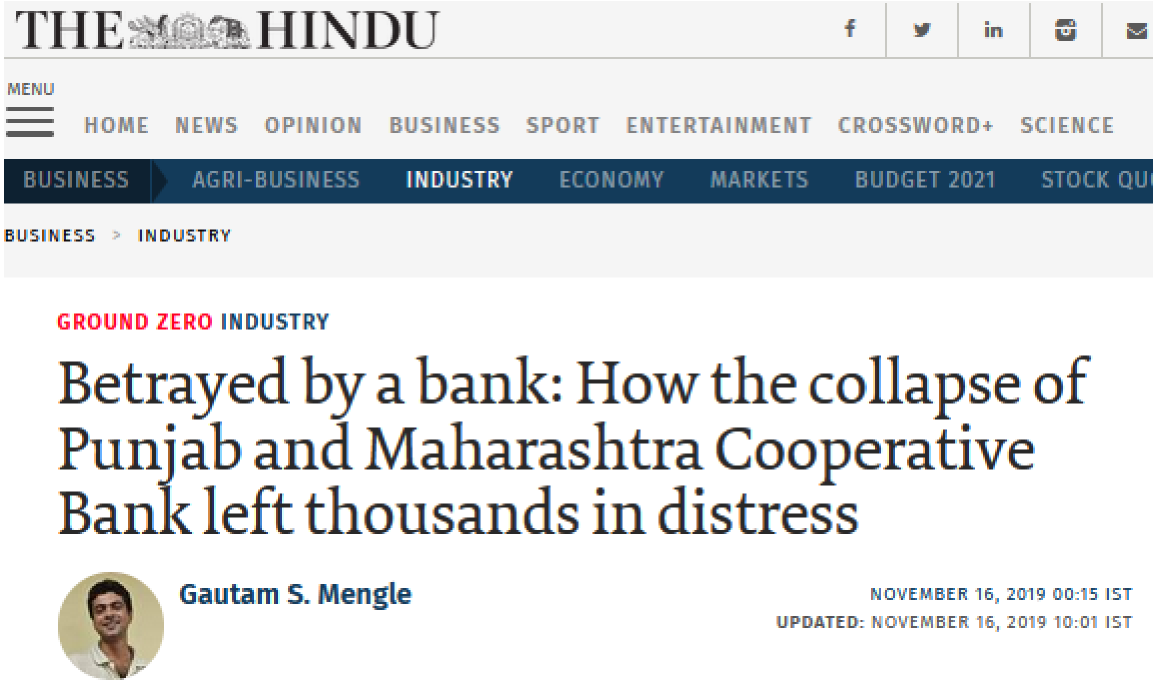
- Who maintains the ledger?
- How to argue with banks employees?
  - Non-Repudiation Issue
  - You might not have enough proof in all the cases.

Trusting Third Party Services

MoneyGram.
International Money Transfer
Trans-Fast
WORLDWIDE MONEY TRANSFER
FirstBank
Since 1894
WESTERN UNION WU
moving money for better
Ria MONEY TRANSFER

bitcoin
Send warm wishes 24/7.
FOR ONLY
TRANSFER FEE
$0.01 / $ANY
SEND UP TO
AMOUNT
FOR PICKUP ANYWHERE
moving money far better

No middleman: Micropayments, Cheap remittance

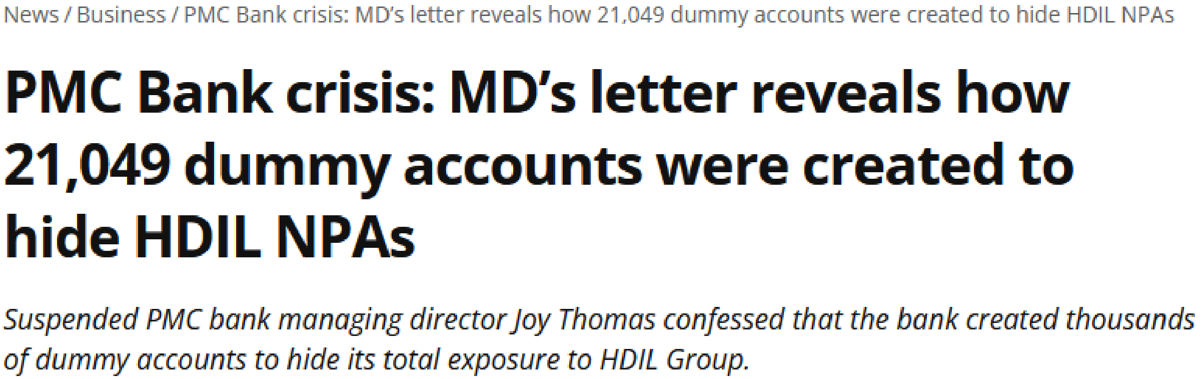

THE HINDU
MENU
HOME NEWS OPINION BUSINESS SPORT ENTERTAINMENT CROSSWORD+ SCIENCE
BUSINESS AGRI-BUSINESS INDUSTRY ECONOMY MARKETS BUDGET 2021 STOCK QU
BUSINESS > INDUSTRY

GROUND ZERO INDUSTRY

Betrayed by a bank: How the collapse of Punjab and Maharashtra Cooperative Bank left thousands in distress

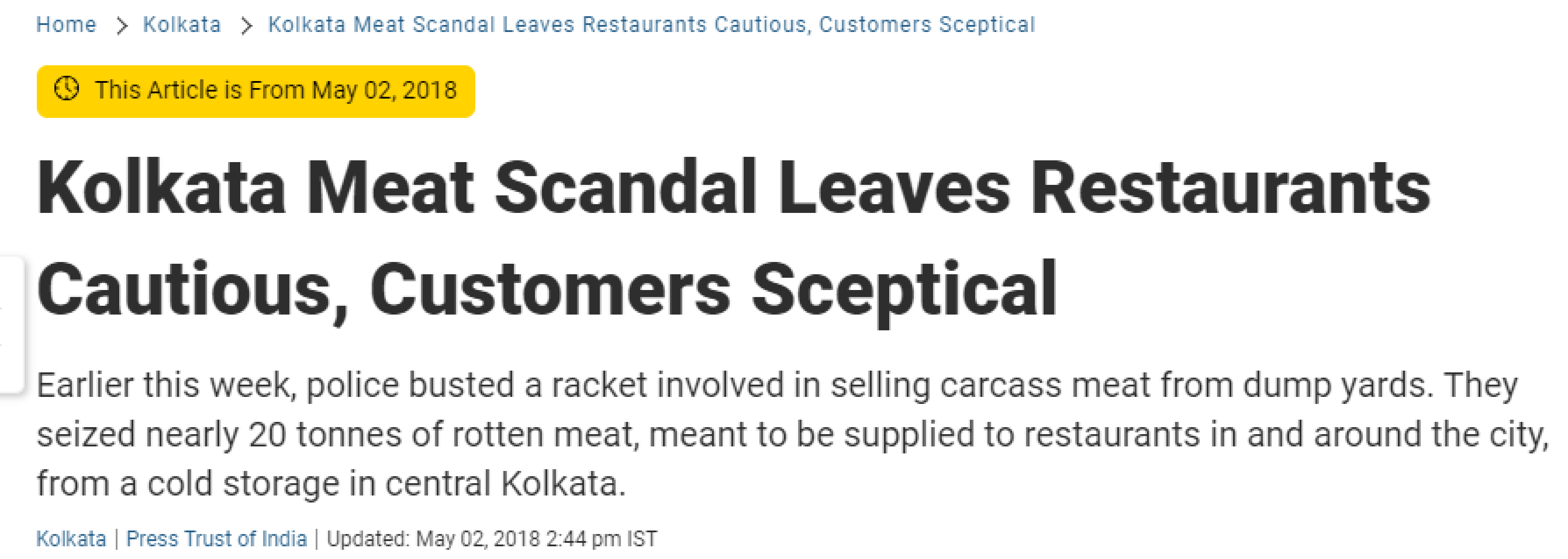
Gautam S. Mengle

NOVEMBER 16, 2019 00:15 IST
UPDATED: NOVEMBER 16, 2019 10:01 IST


News / Business / PMC Bank crisis: MD's letter reveals how 21,049 dummy accounts were created to hide HDIL NPAs

PMC Bank crisis: MD's letter reveals how 21,049 dummy accounts were created to hide HDIL NPAs

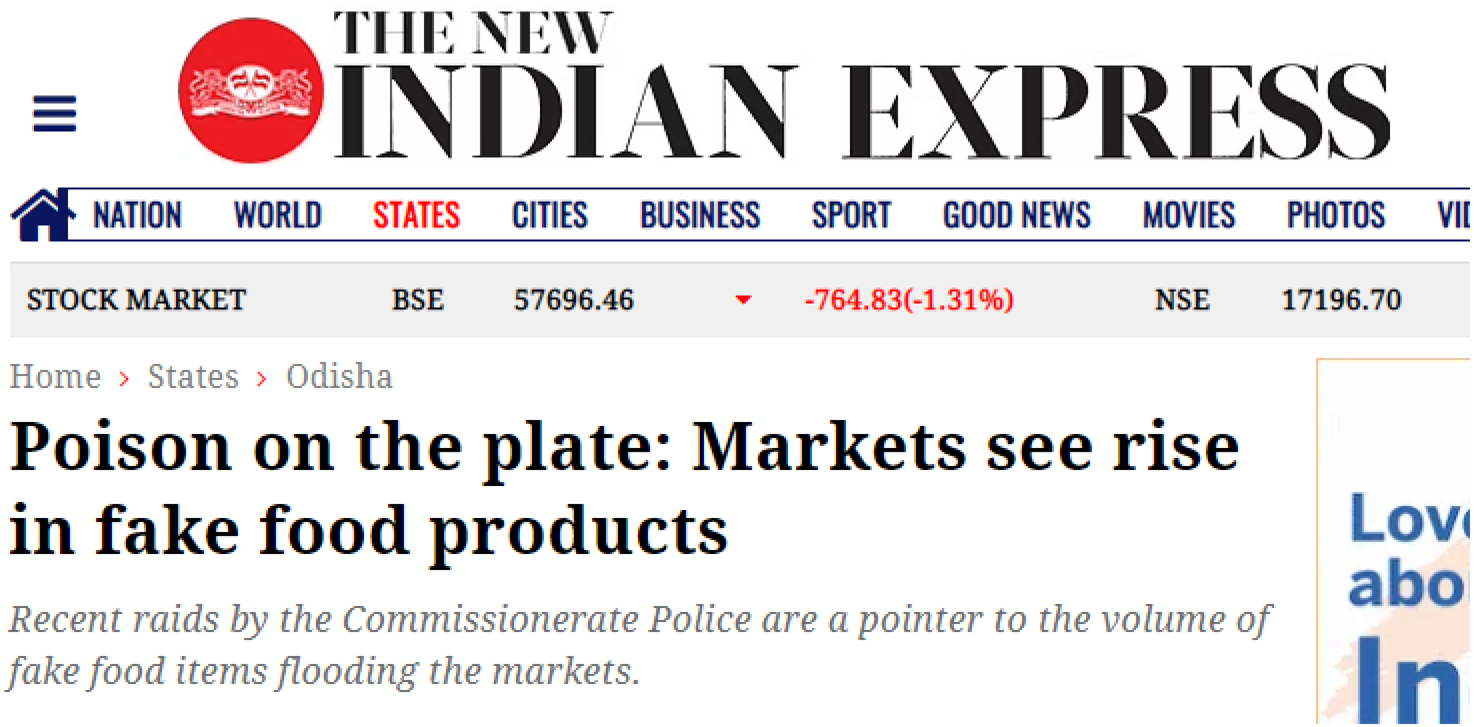
Suspended PMC bank managing director Joy Thomas confessed that the bank created thousands of dummy accounts to hide its total exposure to HDIL Group.


Home > Kolkata > Kolkata Meat Scandal Leaves Restaurants Cautious, Customers Sceptical
This Article is From May 02, 2018

Kolkata Meat Scandal Leaves Restaurants Cautious, Customers Sceptical

Earlier this week, police busted a racket involved in selling carcass meat from dump yards. They seized nearly 20 tonnes of rotten meat, meant to be supplied to restaurants in and around the city, from a cold storage in central Kolkata.

Kolkata | Press Trust of India | Updated: May 02, 2018 2:44 pm IST


THE NEW INDIAN EXPRESS
NATION WORLD STATES CITIES BUSINESS SPORT GOOD NEWS MOVIES PHOTOS VI
STOCK MARKET BSE 57696.46 -764.83(-1.31%) NSE 17196.70
Home > States > Odisha
Lov
abo
In

Poison on the plate: Markets see rise in fake food products

Recent raids by the Commissionerate Police are a pointer to the volume of fake food items flooding the markets.

An Open Question (until 2008)

Is it possible to create (digital) money without a centralized authority?

Cryptocurrency transaction

1. Alice pays Bob over Internet

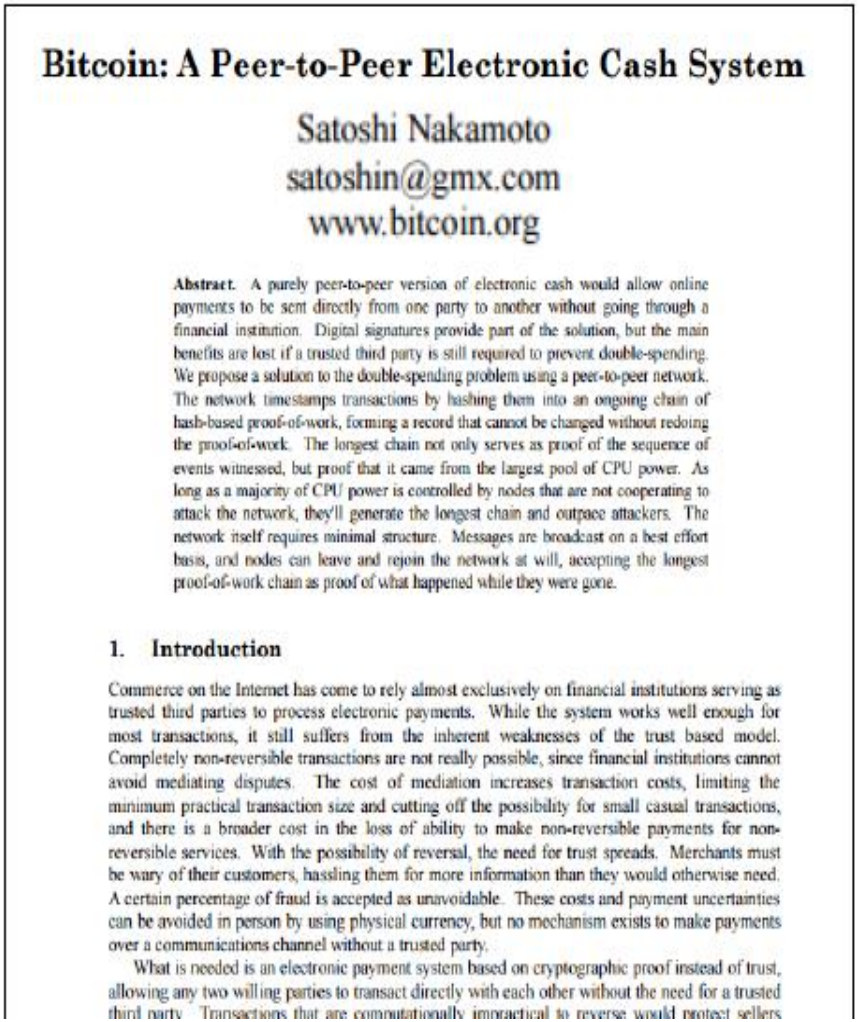
Don’t trust merchant and credit card

Bitcoin

2008: The Bitcoin white paper

2009: Reference implementation

Probably not this guy



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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is 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. Transactions that are computationally impractical to reverse would protect sellers

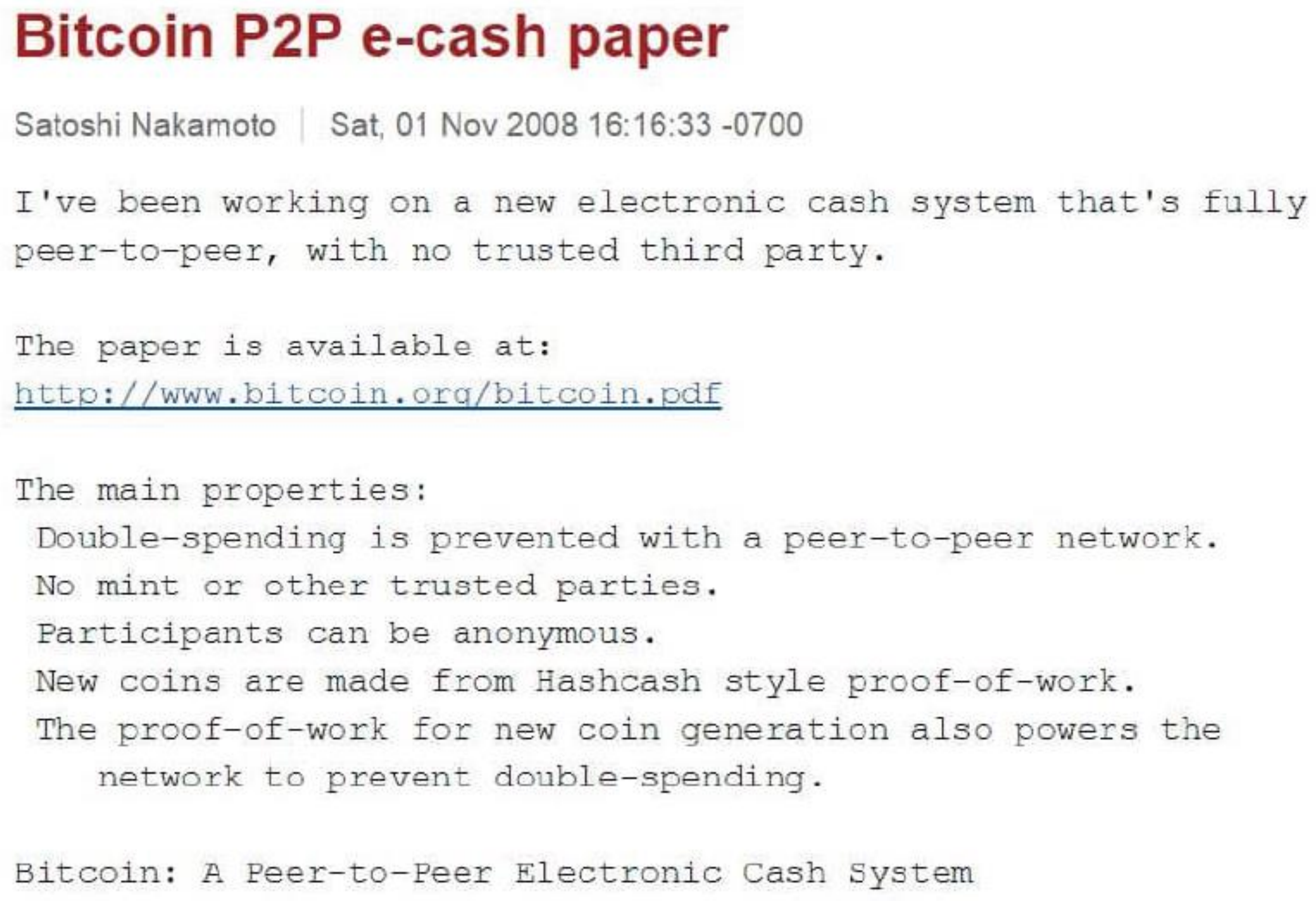
Bitcoin History

- Satoshi Nakamoto published a *whitepaper* in 2008. How to do direct transfer of money without involving a 3rd party.

- He also published complete reference code to transact, store, and mint Bitcoins. Made the software open source.

- He supported the software and answered all questions for 3 years and then disappeared (may be because he was rich or fearful)

Bitcoin History



Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

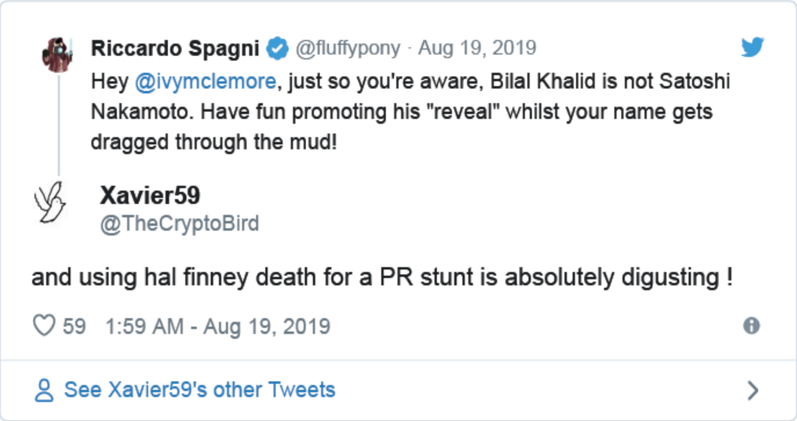
I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi's Mail



Riccardo Spagni @fluffypony · Aug 19, 2019

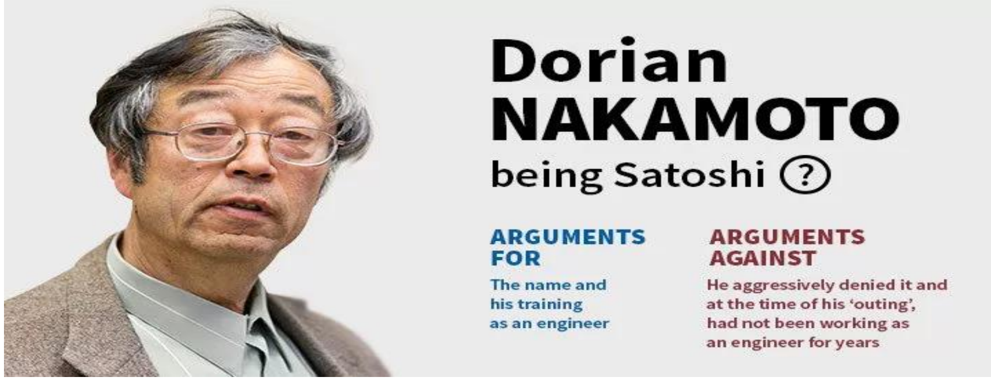
Hey @ivymclemore, just so you're aware, Bilal Khalid is not Satoshi Nakamoto. Have fun promoting his "reveal" whilst your name gets dragged through the mud!

Xavier59
@TheCryptoBird

and using hal finney death for a PR stunt is absolutely digusting !

♡ 59 1:59 AM - Aug 19, 2019

See Xavier59's other Tweets



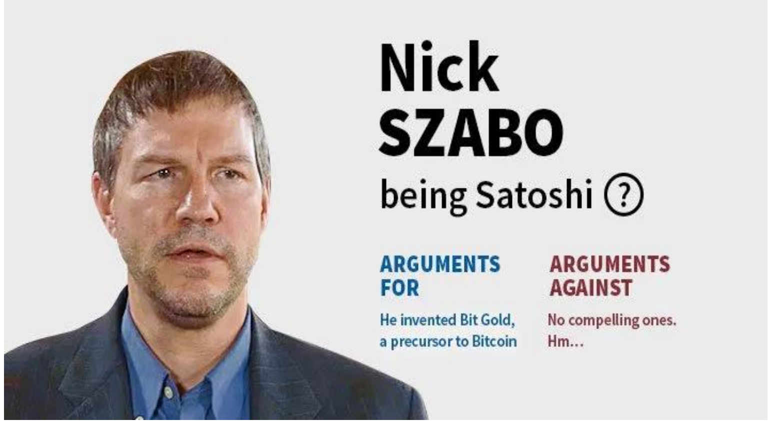
Dorian NAKAMOTO being Satoshi ?

ARGUMENTS FOR

The name and his training as an engineer

ARGUMENTS AGAINST

He aggressively denied it and at the time of his 'outing', had not been working as an engineer for years



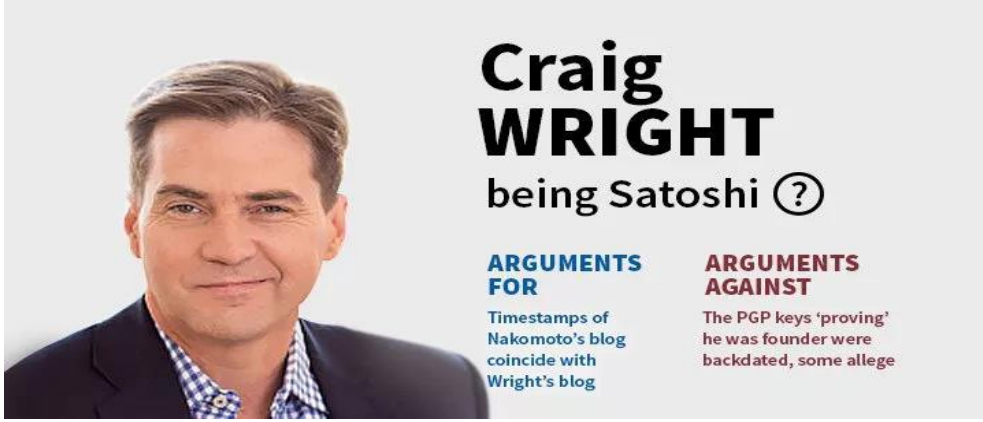
Nick SZABO being Satoshi ?

ARGUMENTS FOR

He invented Bit Gold, a precursor to Bitcoin

ARGUMENTS AGAINST

No compelling ones. Hm…



Craig WRIGHT being Satoshi ?

ARGUMENTS FOR

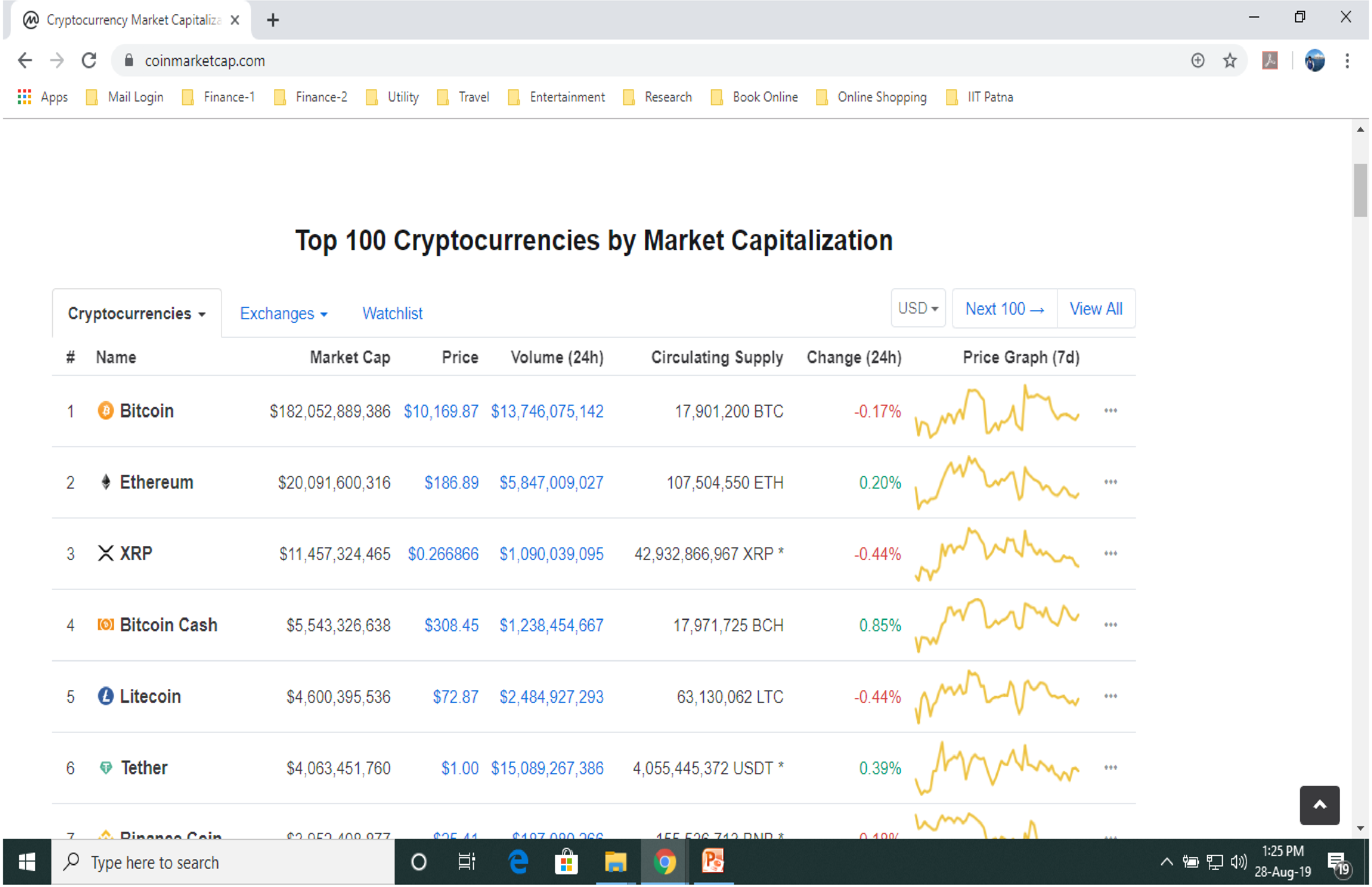
Timestamps of Nakomoto's blog coincide with Wright's blog

ARGUMENTS AGAINST

The PGP keys 'proving' he was founder were backdated, some allege

Source:
https://www.investopedia.com/

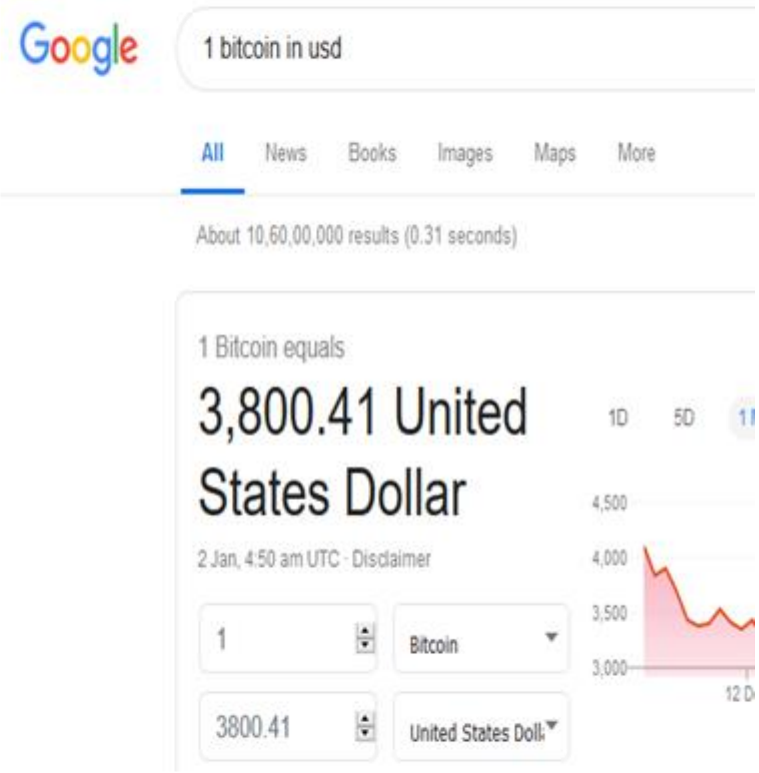
https://coinmarketcap.com/



Top 100 Cryptocurrencies by Market Capitalization

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$182,052,889,386	$10,169.87	$13,746,075,142	17,901,200 BTC	-0.17%	
2	Ethereum	$20,091,600,316	$186.89	$5,847,009,027	107,504,550 ETH	0.20%	
3	XRP	$11,457,324,465	$0.266866	$1,090,039,095	42,932,866,967 XRP *	-0.44%	
4	Bitcoin Cash	$5,543,326,638	$308.45	$1,238,454,667	17,971,725 BCH	0.85%	
5	Litecoin	$4,600,395,536	$72.87	$2,484,927,293	63,130,062 LTC	-0.44%	
6	Tether	$4,063,451,760	$1.00	$15,089,267,386	4,055,445,372 USDT *	0.39%	
7	Binance Coin	$3,952,409,977	$25.41	$197,090,266	155,536,713 BNB *	-0.19%	

Bitcoin Market Price



1 bitcoin in usd

About 10,60,00,000 results (0.31 seconds)

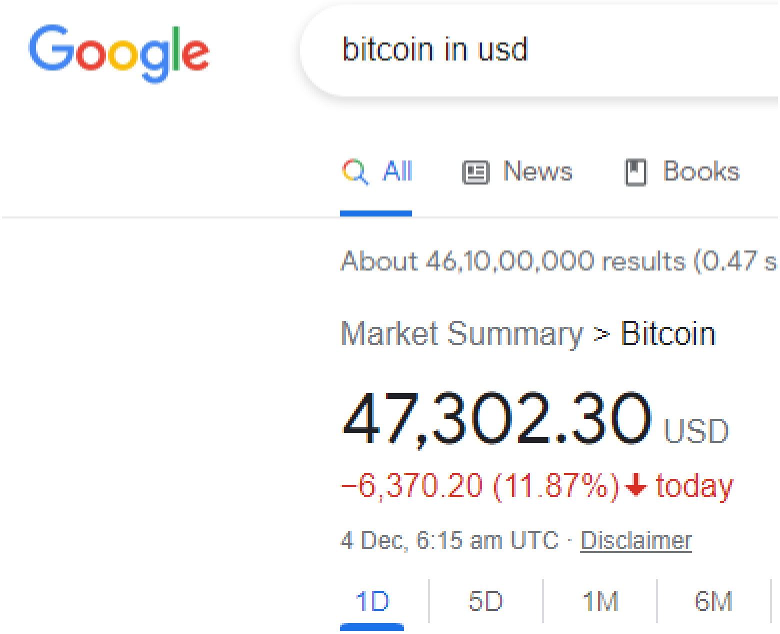
1 Bitcoin equals

3,800.41 United States Dollar

2 Jan, 4:50 am UTC · Disclaimer

1 Bitcoin

3800.41 United States Doll



bitcoin in usd

About 46,10,00,000 results (0.47 s

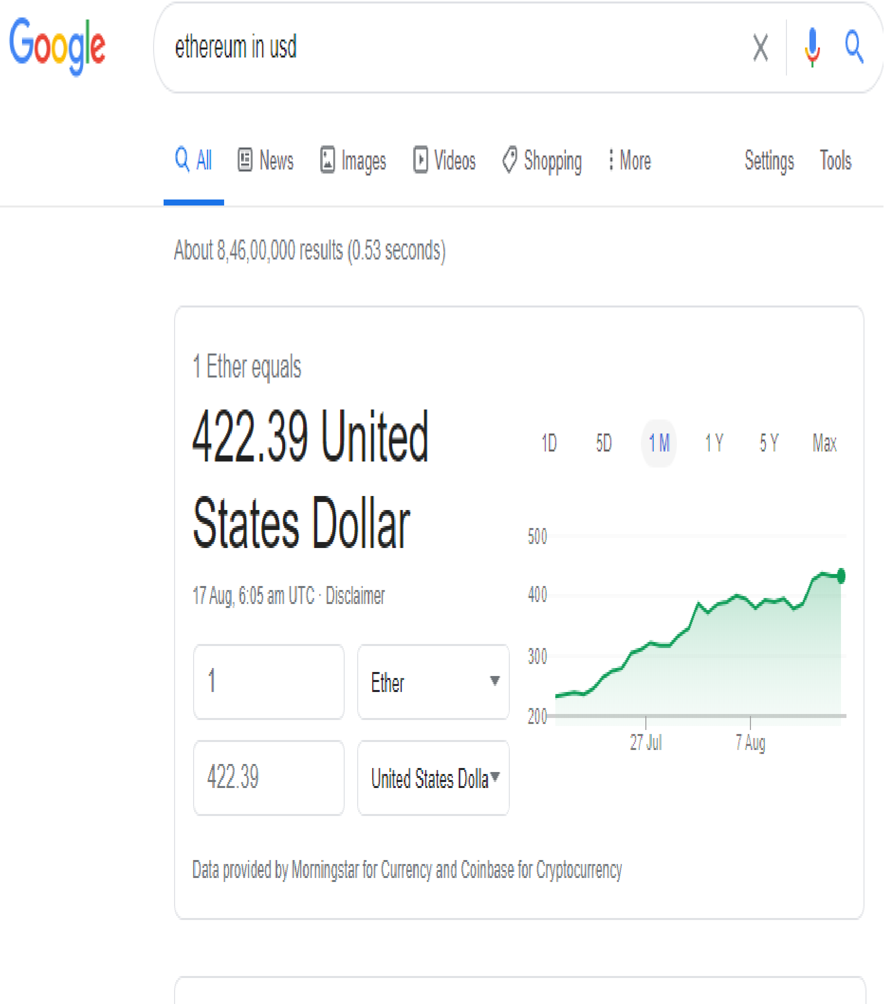
Market Summary > Bitcoin

47,302.30 USD

−6,370.20 (11.87%)↓ today

4 Dec, 6:15 am UTC · Disclaimer

Ether Market Price



ethereum in usd

About 8,46,00,000 results (0.53 seconds)

1 Ether equals

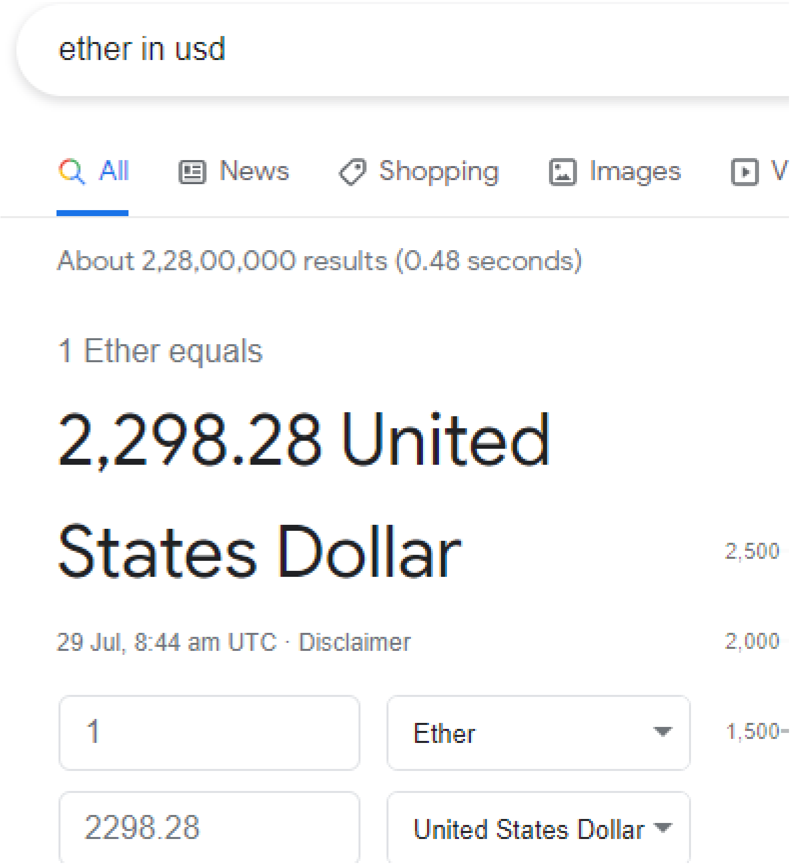
422.39 United States Dollar

17 Aug, 6:05 am UTC · Disclaimer

1 Ether

422.39 United States Dolla

Data provided by Morningstar for Currency and Coinbase for Cryptocurrency



ether in usd

About 2,28,00,000 results (0.48 seconds)

1 Ether equals

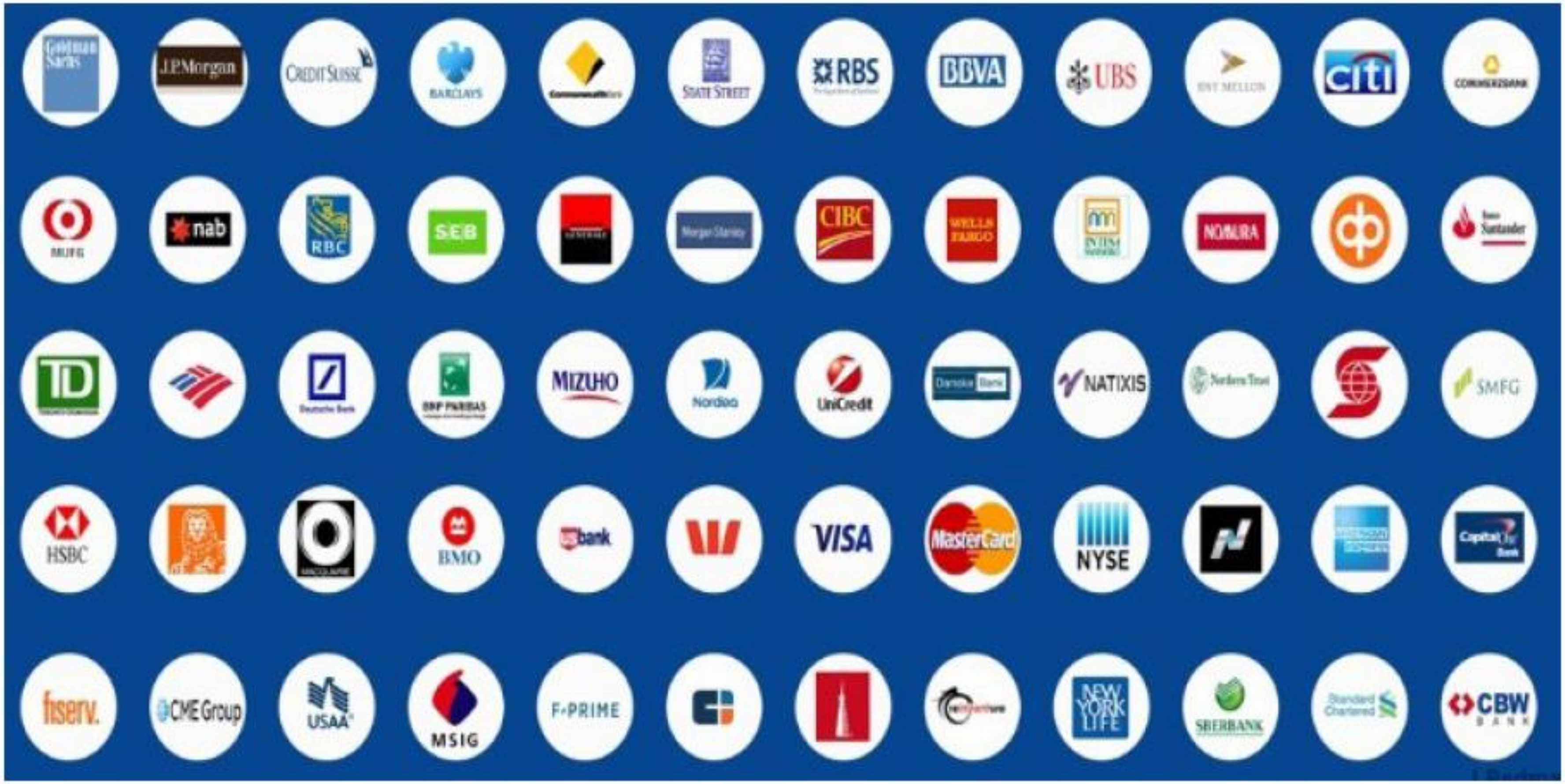
2,298.28 United States Dollar

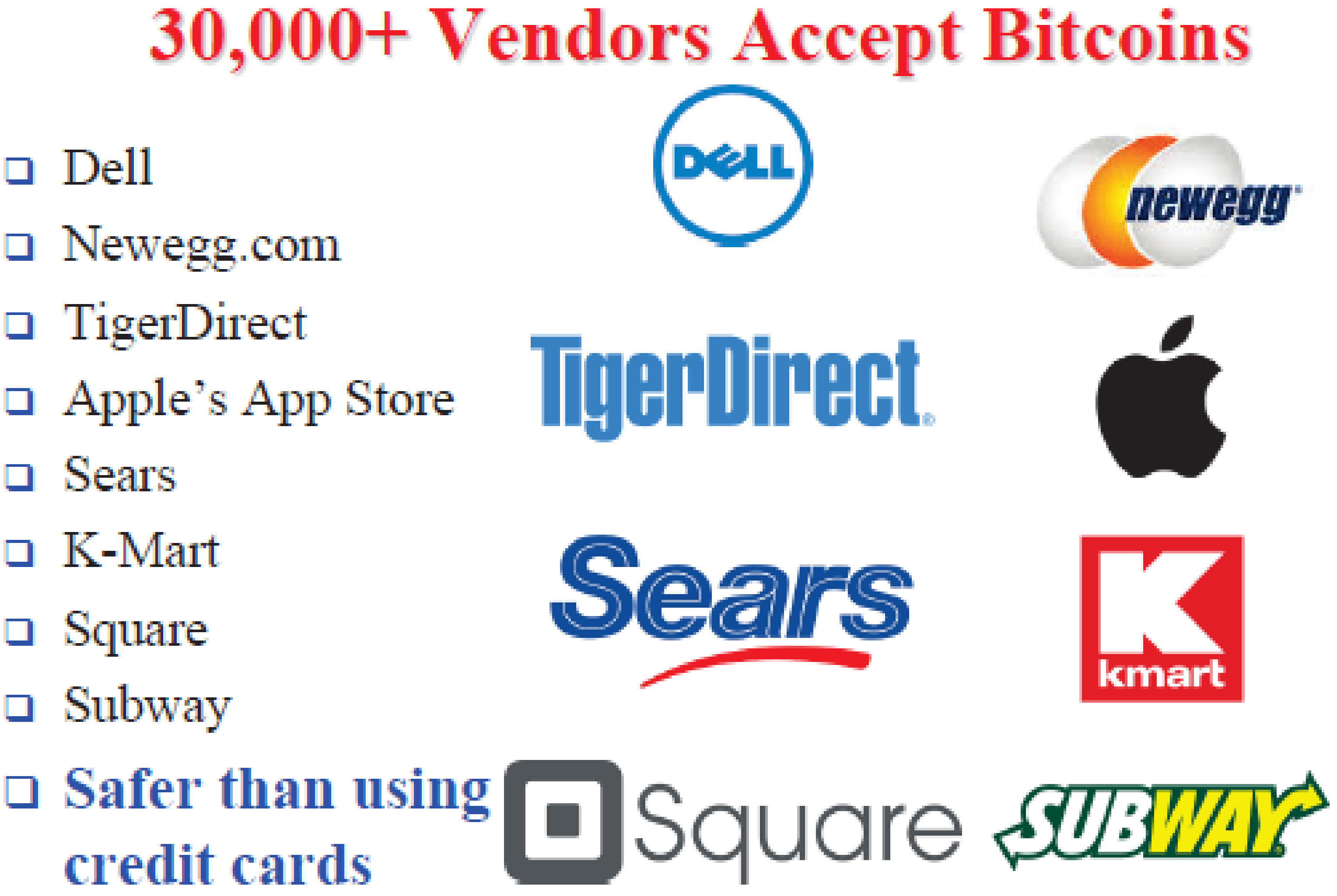
29 Jul, 8:44 am UTC · Disclaimer

1 Ether

2298.28 United States Dollar

Financial Institutions Invested in Bitcoin





30,000+ Vendors Accept Bitcoins

- □ Dell
- □ Newegg.com
- □ TigerDirect
- □ Apple’s App Store
- □ Sears
- □ K-Mart
- □ Square
- □ Subway
- □ **Safer than using credit cards**

DELL
newegg
TigerDirect
Sears
kmart
Square
SUBWAY

https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/

Bitcoin Wallet

- ❑ Program to manage your incoming/outgoing Bitcoins
- ❑ Allows generating new addresses and public/private key pairs
- ❑ Keep track of holdings of your different addresses
- ❑ Similar to Apple Wallet, Google Wallet, …
- ❑ Numerous apps on Apple's App store or Google Play Store

Coinbase Blockchain Bitcoin Free Bitcoin Billionare BitWallet Airbitz

Top 10 Bitcoin Friendly Countries

- Italy,
- United States,
- United Kingdom,
- Finland,
- Australia,
- Singapore,
- Netherlands,
- Canada,
- Slovenia, and
- Isle of Man.

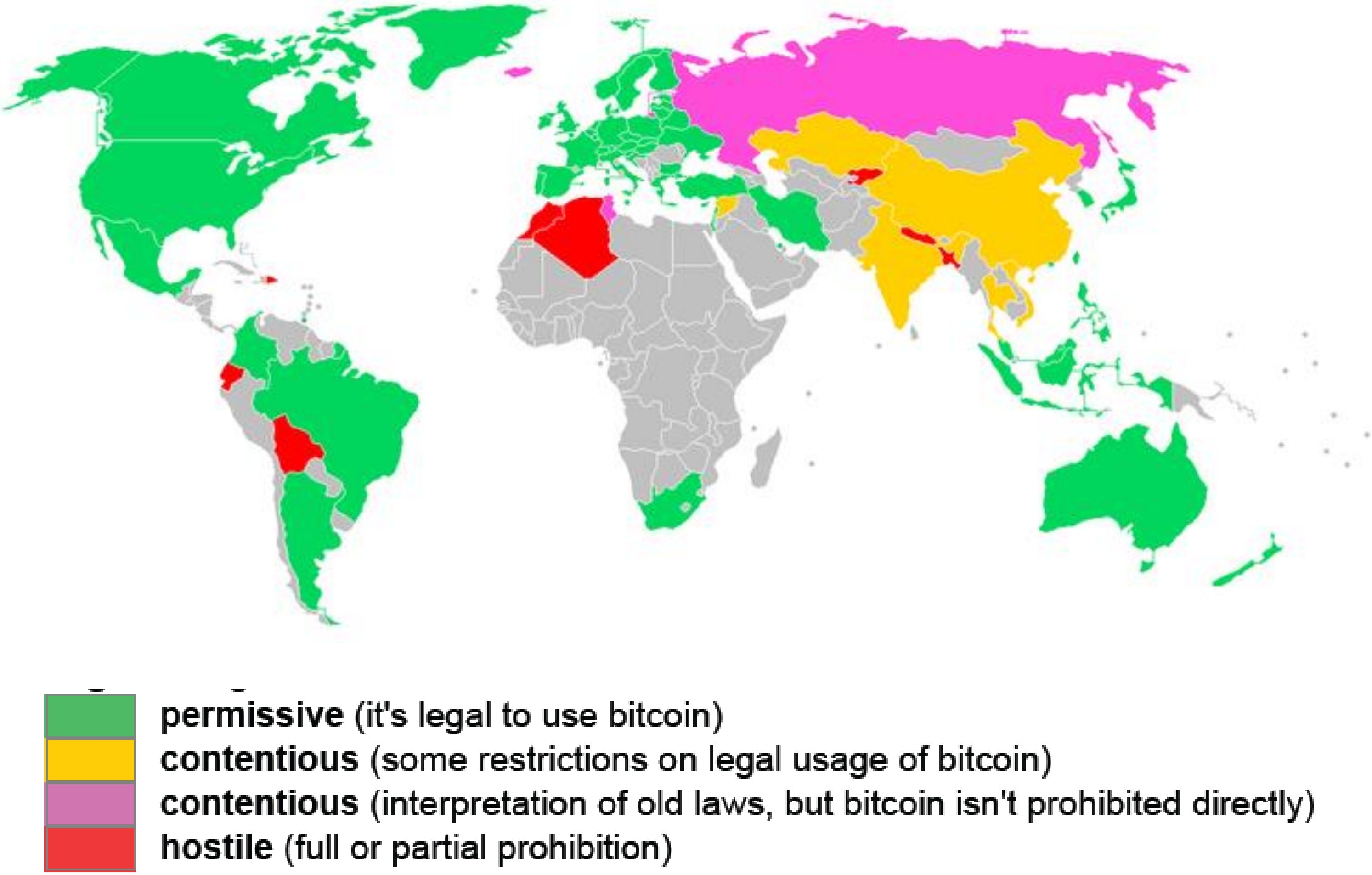
https://99bitcoins.com/bitcoin-country-top-10-nations-love-btc/

https://99bitcoins.com/bitcoin-country-top-10-nations-love-btc/

List of Countries that have Banned Bitcoin

- **Thailand –** The Thai treasure banned bitcoin outright.
- **China –** The Chinese treasure enacted policies on bitcoin that pretty much restricted the use of the virtual currency.
- **Taiwan –** The country’s Financial Supervisory Commission (FSC) blocked efforts to install Bitcoin ATMs in the country and restricted its use as an alternate currency.
- **India –** The Indian’s central bank published a lengthly document against the use of bitcoin. If the country is not accepted by the central banking system, it’s pretty much useless.
- **Germany –** The German government and central bank Bundesbank formally accepted bitcoin as a private virtual currency but not as a public currency.
- **Bolivia –** The developing country claims bitcoin was created by the United States government to wage financial warfare on other countries!
- **Russia –** The Russian Prosecutor General’s Office says “Systems for anonymous payments and cyber currencies that have gained considerable circulation — including the most well-known, Bitcoin — are money substitutes and cannot be used by individuals or legal entities.”

https://en.wikipedia.org/wiki/


🟩 permissive (it's legal to use bitcoin)
🟨 contentious (some restrictions on legal usage of bitcoin)
🟪 contentious (interpretation of old laws, but bitcoin isn't prohibited directly)
🟥 hostile (full or partial prohibition)

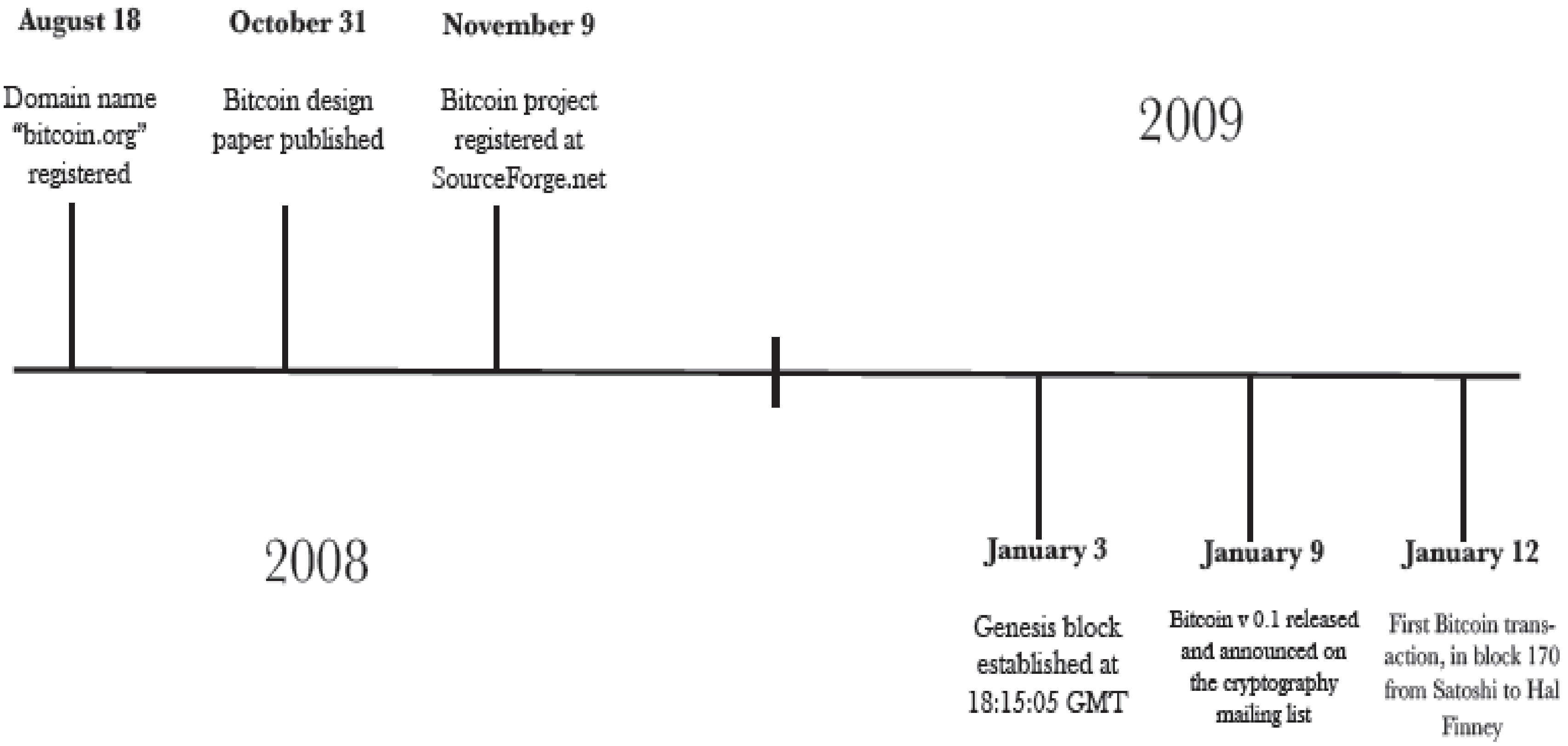
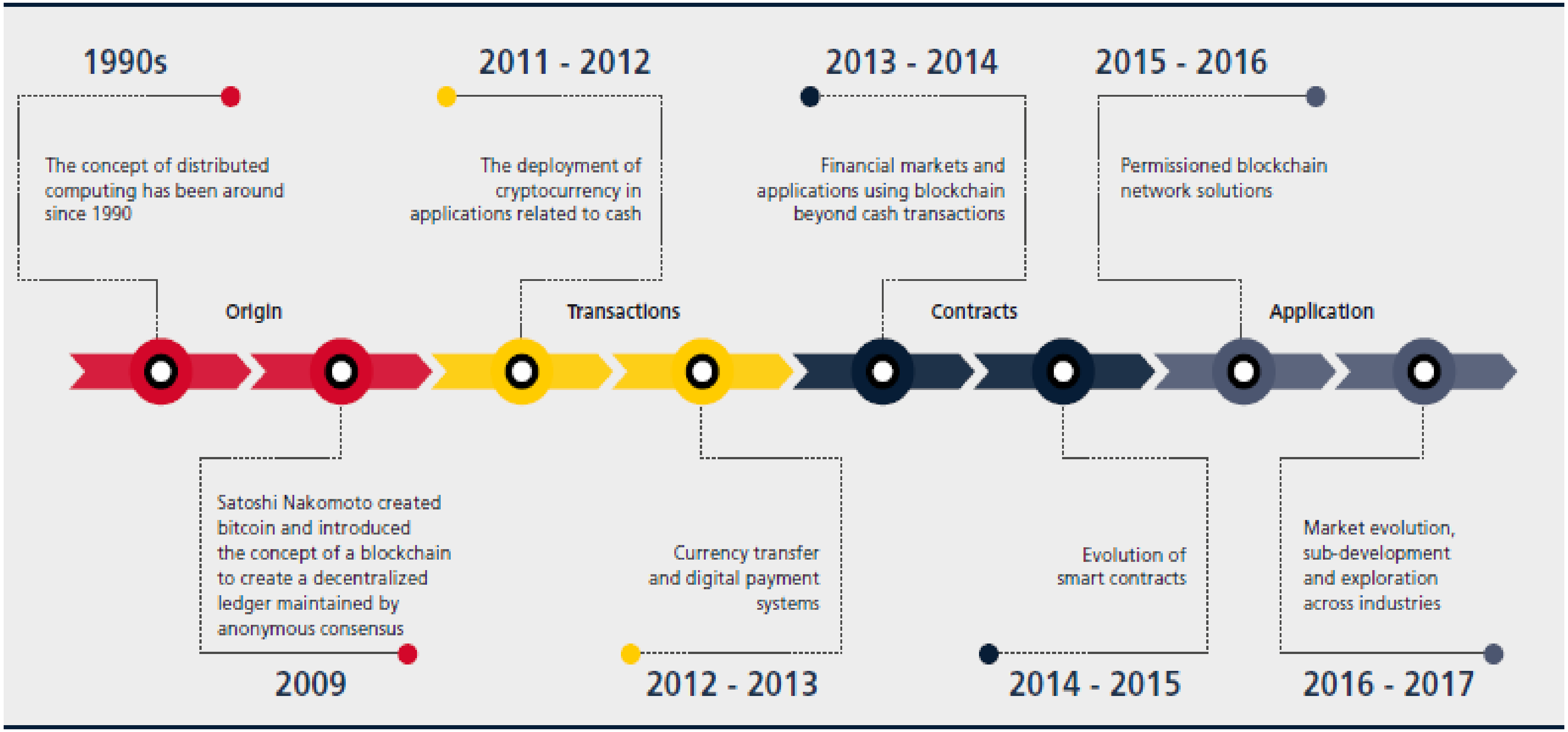

August 18
Domain name "bitcoin.org" registered
October 31
Bitcoin design paper published
November 9
Bitcoin project registered at SourceForge.net
2009
2008
January 3
Genesis block established at 18:15:05 GMT
January 9
Bitcoin v 0.1 released and announced on the cryptography mailing list
January 12
First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

Figure 1: The History of Bitcoin

BLOCKCHAIN HISTORY



1990s

The concept of distributed computing has been around since 1990

2011 - 2012

The deployment of cryptocurrency in applications related to cash

2013 - 2014

Financial markets and applications using blockchain beyond cash transactions

2015 - 2016

Permissioned blockchain network solutions

Origin

Transactions

Contracts

Application

Satoshi Nakomoto created bitcoin and introduced the concept of a blockchain to create a decentralized ledger maintained by anonymous consensus

2009

Currency transfer and digital payment systems

2012 - 2013

Evolution of smart contracts

2014 - 2015

Market evolution, sub-development and exploration across industries

2016 - 2017

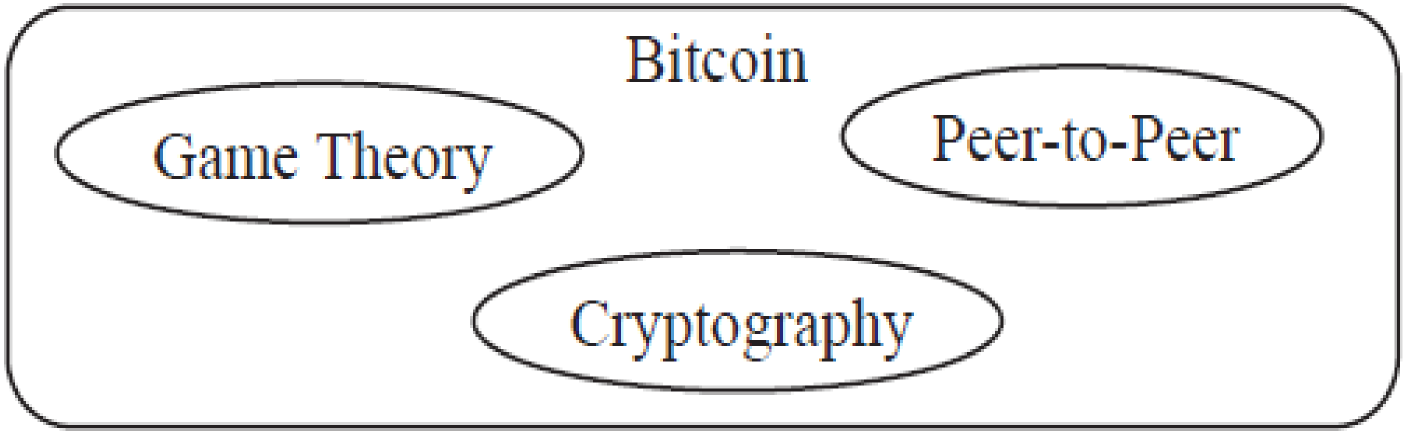
Figure 2: A history of blockchain technology; **Source:** Accenture

How many people use Bitcoin?

- This is quite a difficult question to answer accurately. One approach is to count how many bitcoin clients connected to the network in the last 24 hours. We can do this because some clients transmit their addresses to the other members of the network periodically;
- In September 2011, this method suggested that there were about 60,000 users.
- In October 2014, according to Coin desk report there were more than 7.5 million bitcoin wallets.
- In October 2016, according to blockchain.info user counts based on Blockchain wallet, there are about 8.8 mln registered Bitcoin users on its platform. Cointelegraph report
- According to blockchain.info, from October 2016 till January 2018 the Bitcoin user base has almost tripled for total of 22 million users.

https://en.bitcoin.it/wiki/Help:Introduction

Bitcoin Technology



- Bitcoin = Game Theory + Cryptography + P2P
- P2P: Information is stored throughout the global Internet
- Cryptography: Digital Signature, Message Authentication, Asymmetric Public/Private Key encryption, Hashing
- Game Theory: All activities are Win-Win.
  ⇒ People who store the chain, who mint the coin, all get paid.

Blockchain Origin: Bitcoin

- Blockchain is the technology that made Bitcoin secure.
- Blockchain was invented by the inventor of Bitcoin.
- Blockchain was born with Bitcoin and remains the largest blockchain *platform.*
- However, hundreds or **thousands of other platforms** now exist.
- After Bitcoin became successful, people started looking into the technology behind Bitcoin and found:
  - Blockchain is the key for its success
  - Blockchains can be leveraged for other applications

Blockchain Technolgy

Behind the success of Bitcoin

- IoT
- Supply Chain
- EHR
- Copyright Protection
- KYC
- Land Registry
- Data Sharing
- Cryptocurrency
- Smart Grid
- Insurance
- Smart Agriculture
- Smart Homes
- E-Commerce
- E-Governance
- Social Networking
- Education Certificate
- File Sharing
- Crowd Funding
- Postal System
- E-Voting
- Data Provenance
- E-Governance
- Asset Transfer
- Criminal Record Sharing
- Finance
- Many More….

50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS

The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE

A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM
HYPERLEDGER

ENTERPRISE

Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS

IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM
Walmart

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING

Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING

New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT

Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY

Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC.
Louis Dreyfus Company

DIAMONDS

The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

DE BEERS
Group of Companies

FINE ART

By storing **certificates** of authenticity on the blockchain, it's possible to dramati- cally reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY

For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM

In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE
COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS

Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

грузовая компания НОВОТРАНС

ENTERPRISE

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google
Alphabet

MUSIC

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

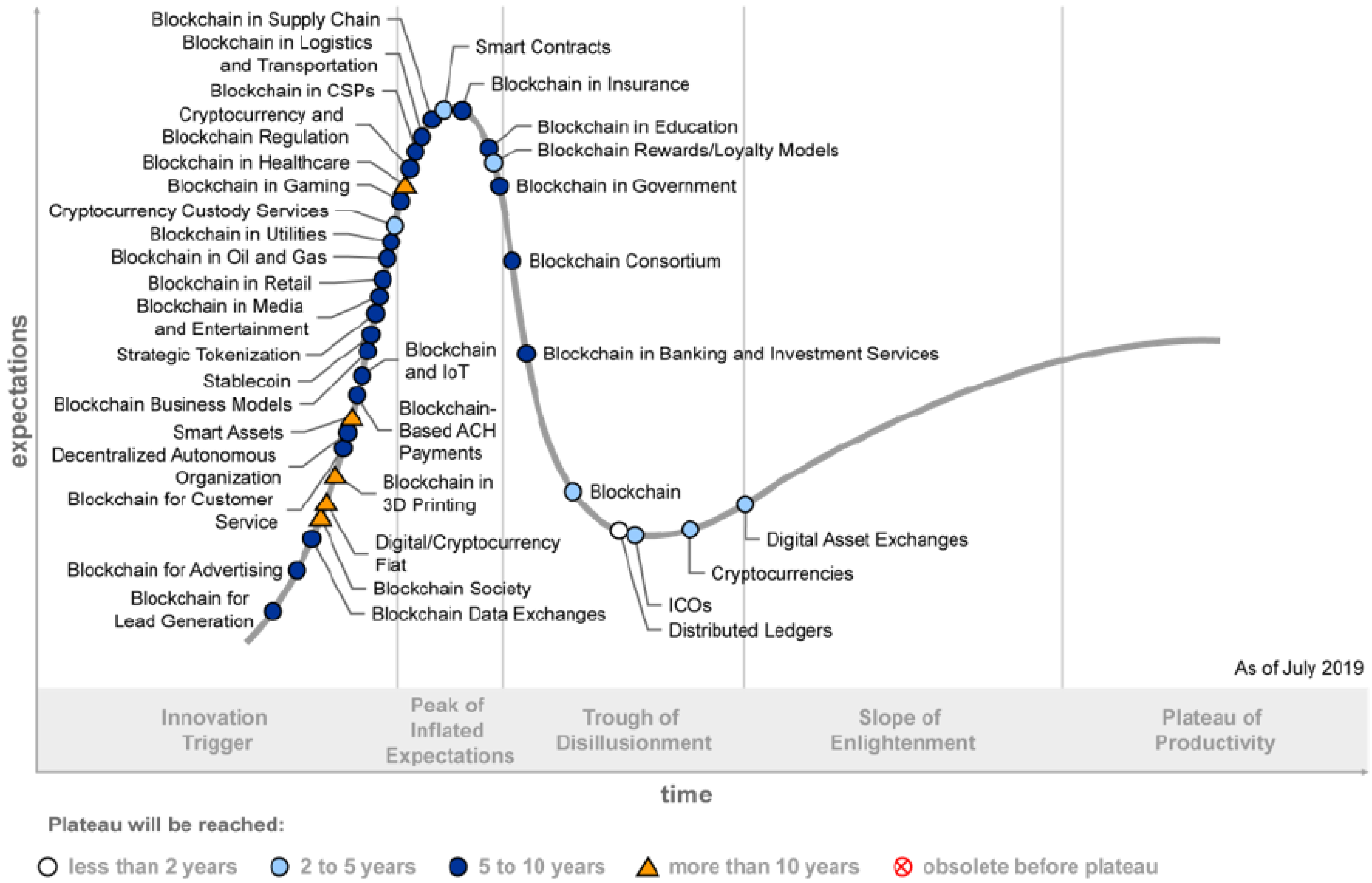
FISHING

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION

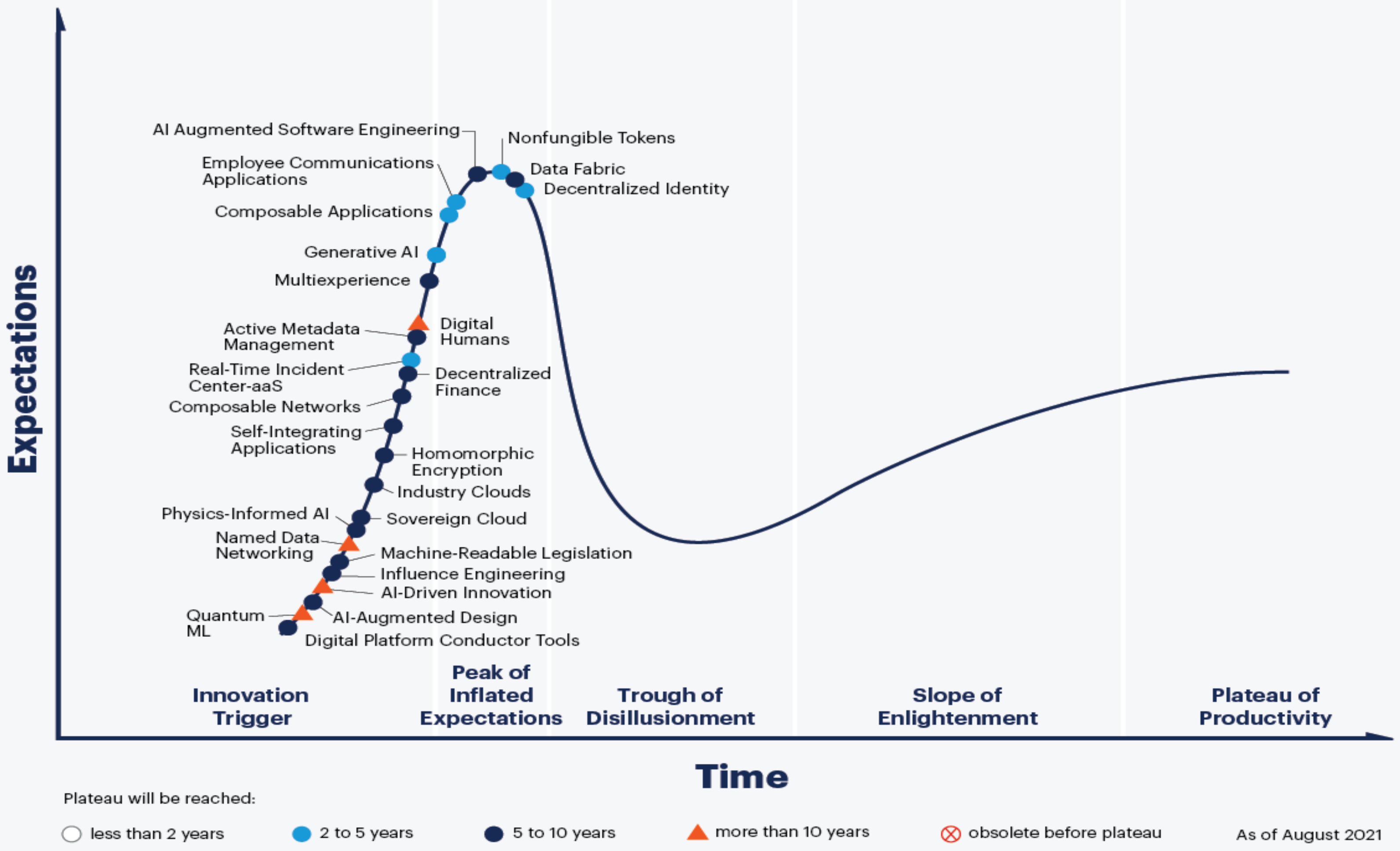
https://medium.com/@essentia1/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b

Hype Cycle for Blockchain Business, 2019



Source: Gartner
ID: 390391

Hype Cycle for Emerging Technologies, 2021



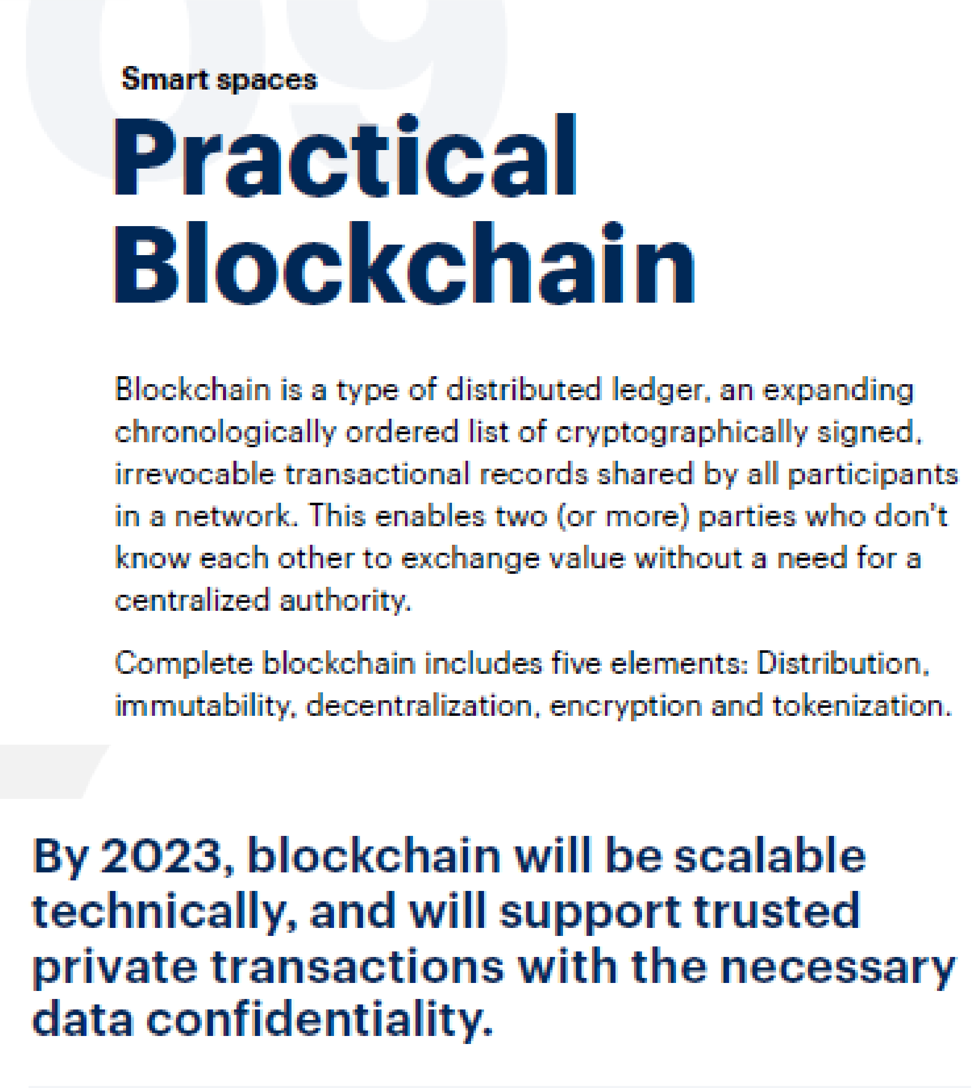
gartner.com

Source: Gartner

Gartner

Top 10 Strategic Technology Trends for 2020

Edited by
David W. Cearley, Distinguished VP Analyst, Gartner



Smart spaces

Practical Blockchain

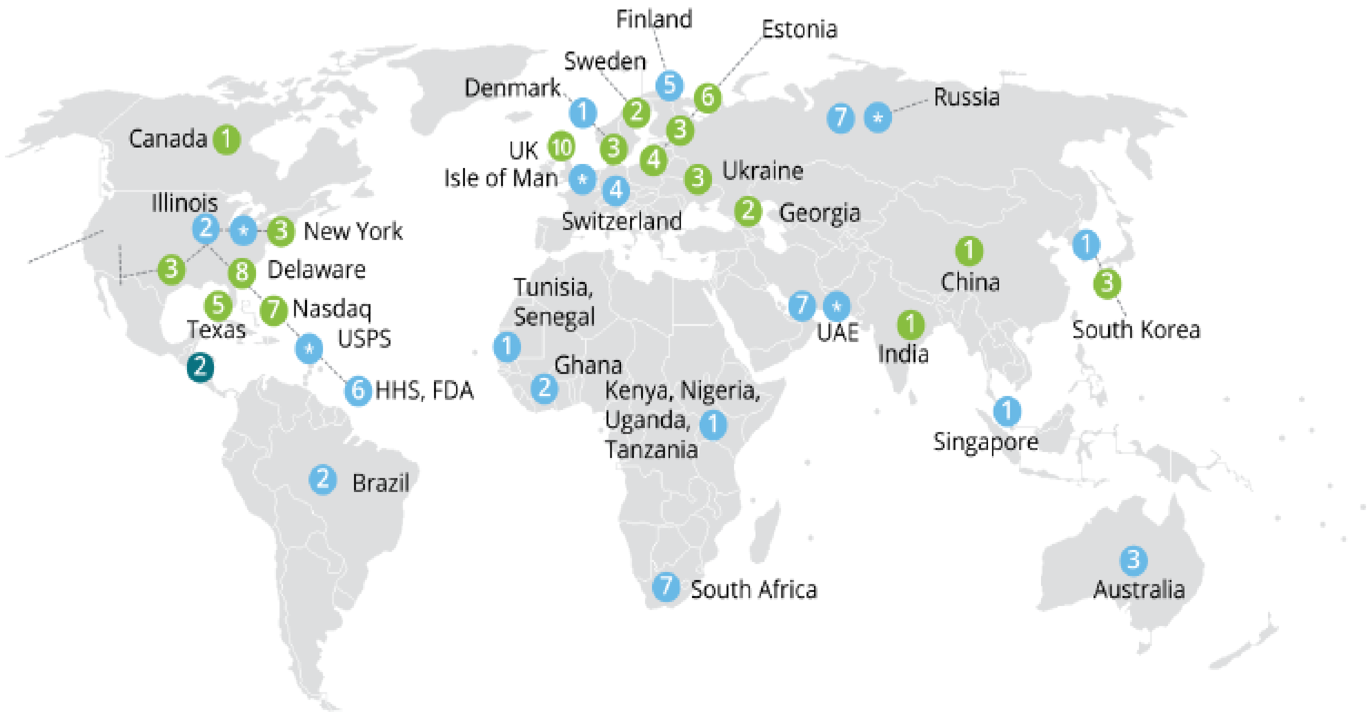
Blockchain is a type of distributed ledger, an expanding chronologically ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network. This enables two (or more) parties who don't know each other to exchange value without a need for a centralized authority.

Complete blockchain includes five elements: Distribution, immutability, decentralization, encryption and tokenization.

By 2023, blockchain will be scalable technically, and will support trusted private transactions with the necessary data confidentiality.

http://tiny.cc/opsinewsletter

One year ago: 117 Initiatives in 26 Countries



Source: Deloitte analysis in conjunction with the Fletcher School at Tufts University (March 2017)

Color coding key

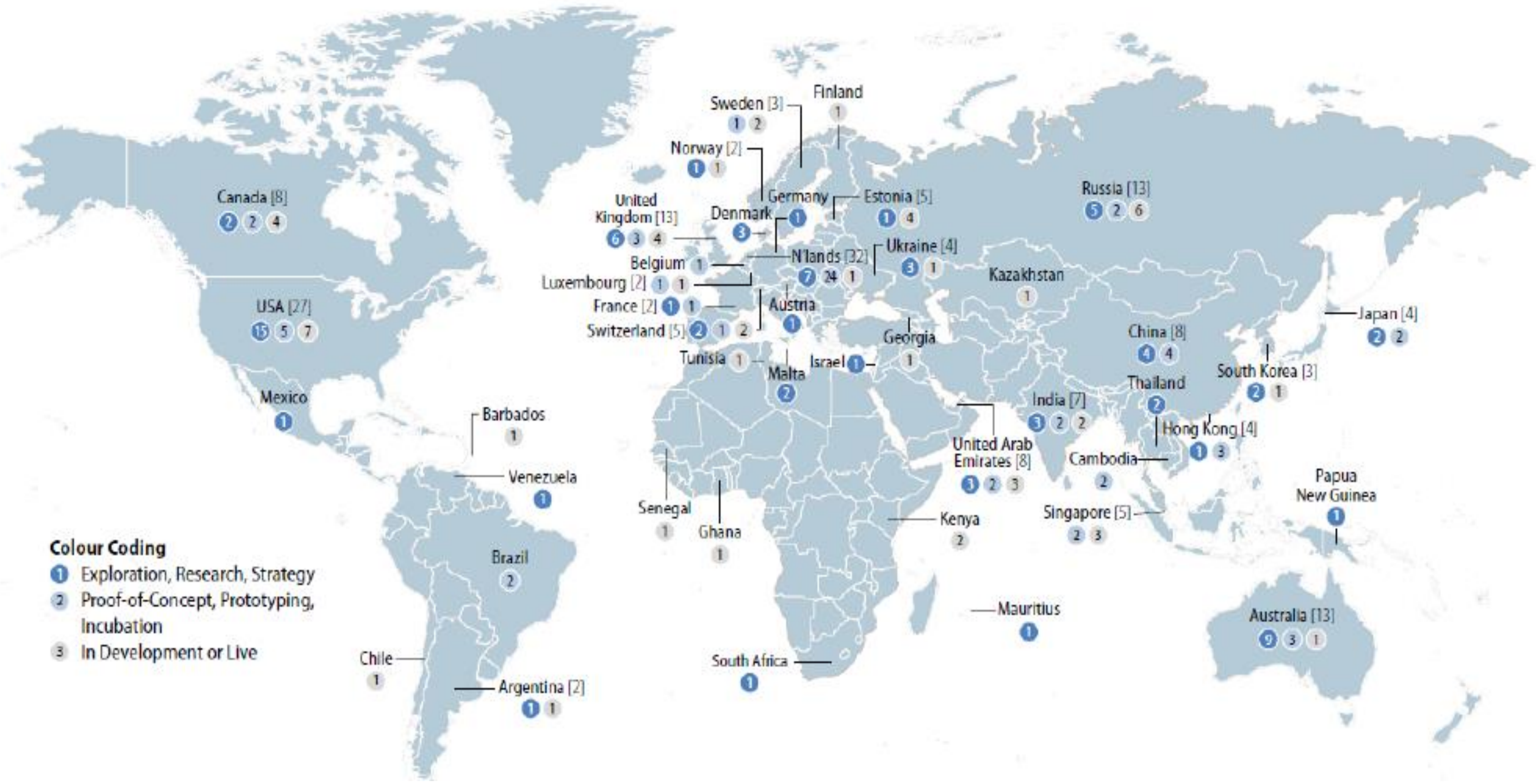
● In progress

● Planned

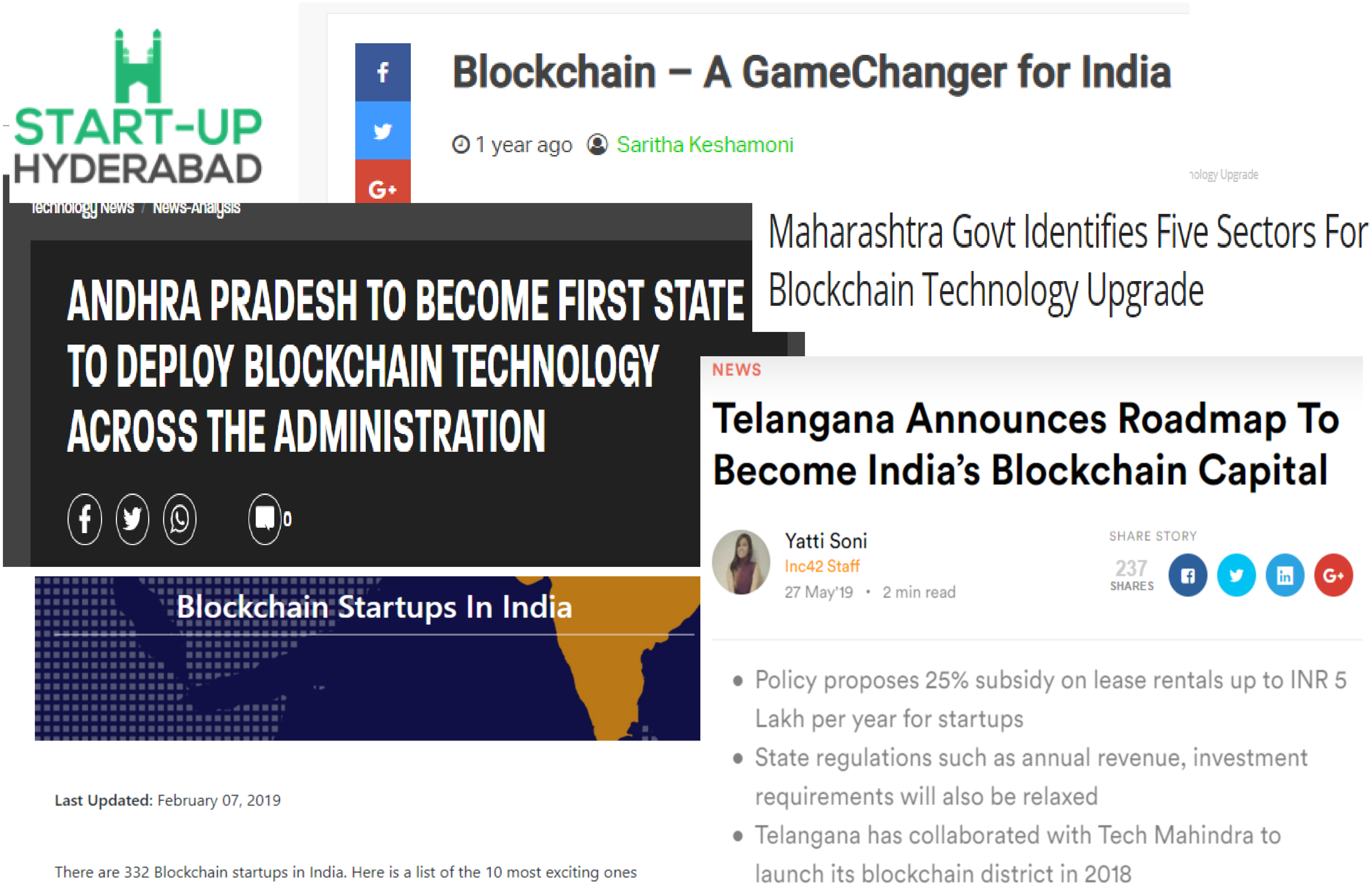
● Announced

http://tiny.cc/opsinewsletter

Now: 202 Blockchain Initiatives in 45 Countries



Source: OECD analysis of data collected by The Illinois Blockchain Initiative (March 2018)



START-UP HYDERABAD

Blockchain – A GameChanger for India

1 year ago Saritha Keshamoni

Technology News / News-Analysis

ANDHRA PRADESH TO BECOME FIRST STATE TO DEPLOY BLOCKCHAIN TECHNOLOGY ACROSS THE ADMINISTRATION

Maharashtra Govt Identifies Five Sectors For Blockchain Technology Upgrade

NEWS

Telangana Announces Roadmap To Become India's Blockchain Capital

Yatti Soni
Inc42 Staff
27 May'19 • 2 min read

SHARE STORY
237 SHARES

- Policy proposes 25% subsidy on lease rentals up to INR 5 Lakh per year for startups
- State regulations such as annual revenue, investment requirements will also be relaxed
- Telangana has collaborated with Tech Mahindra to launch its blockchain district in 2018

Blockchain Startups In India

Last Updated: February 07, 2019

There are 332 Blockchain startups in India. Here is a list of the 10 most exciting ones

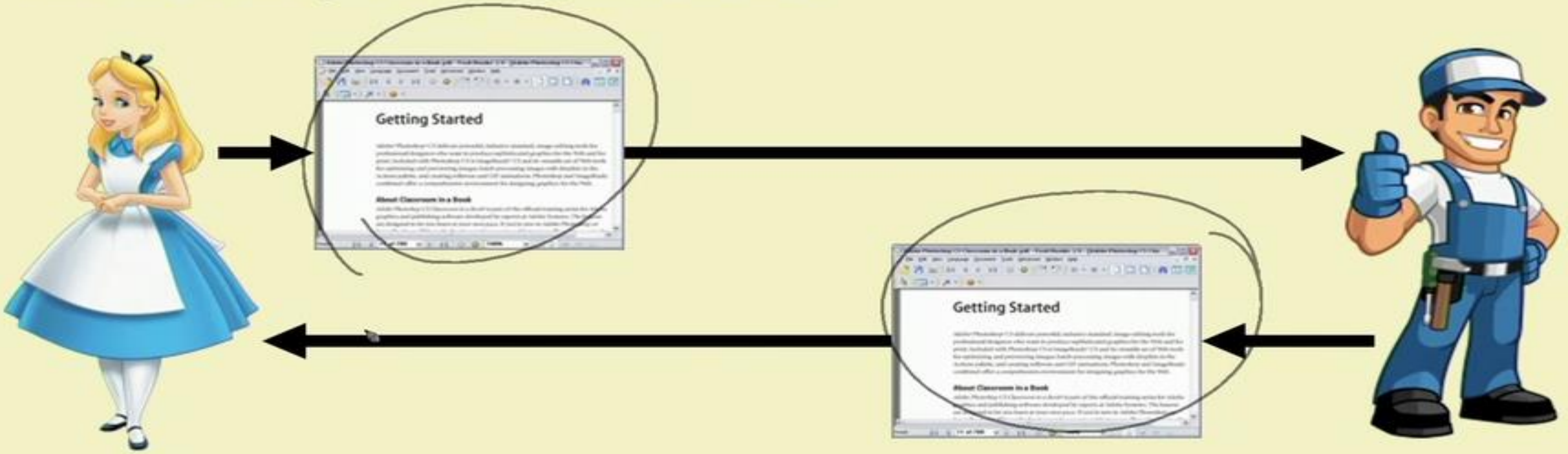
THE HINDU BusinessLine

Rajeev Chandrasekhar for Aadhaar 2.0 secured by blockchain

Vinson Kurian | Thiruvananthapuram | Updated on January 12, 2018 | Published on January 12, 2018

The launch of a virtual id for Aadhaar is, in a sense,

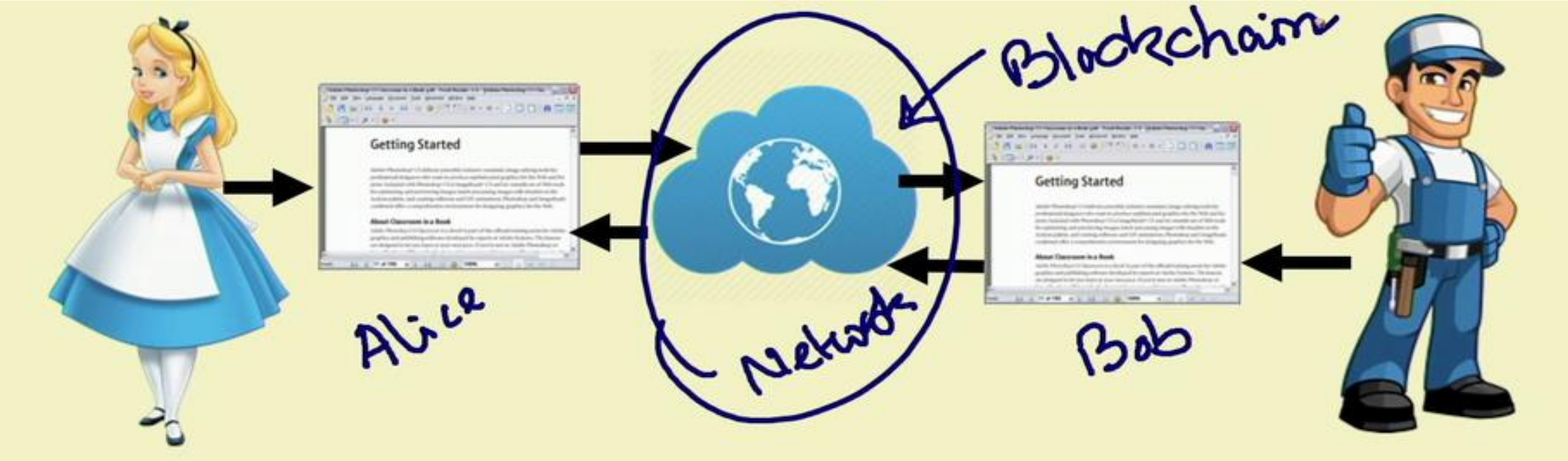
- Traditional way of sharing documents



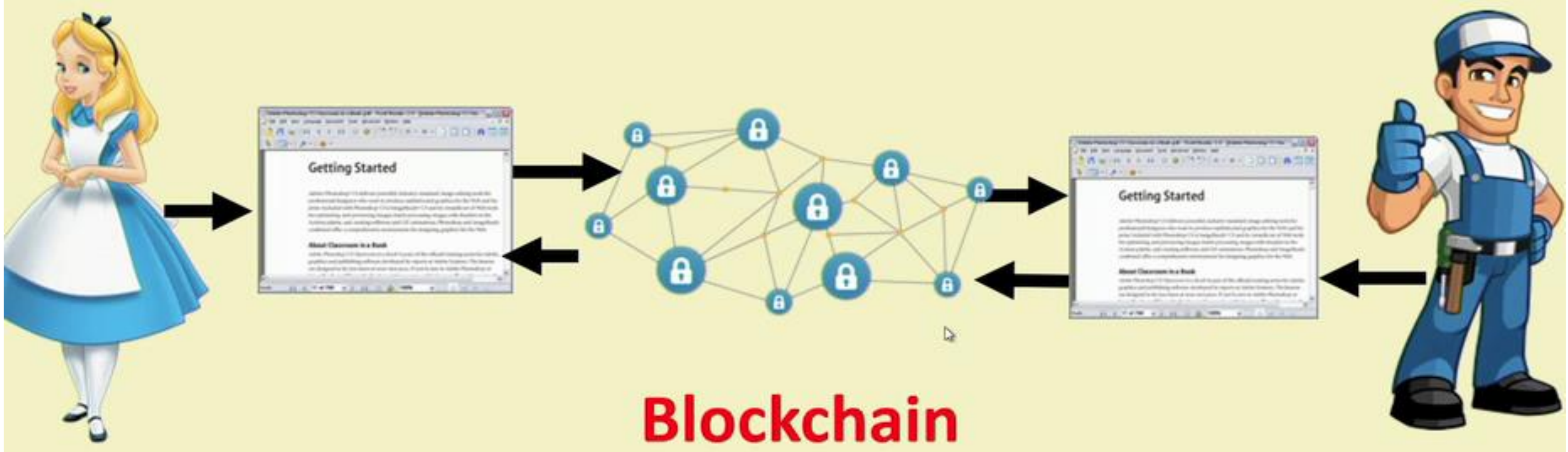
- Shared Google doc – both the users can edit simultaneously

The environment is still centralized.
Does centralized system harm?

Courtesy: Lectures by Dr. Sandip Chakraborty



Everyone edits on their local copy of the document – the Internet takes care of ensuring consistency



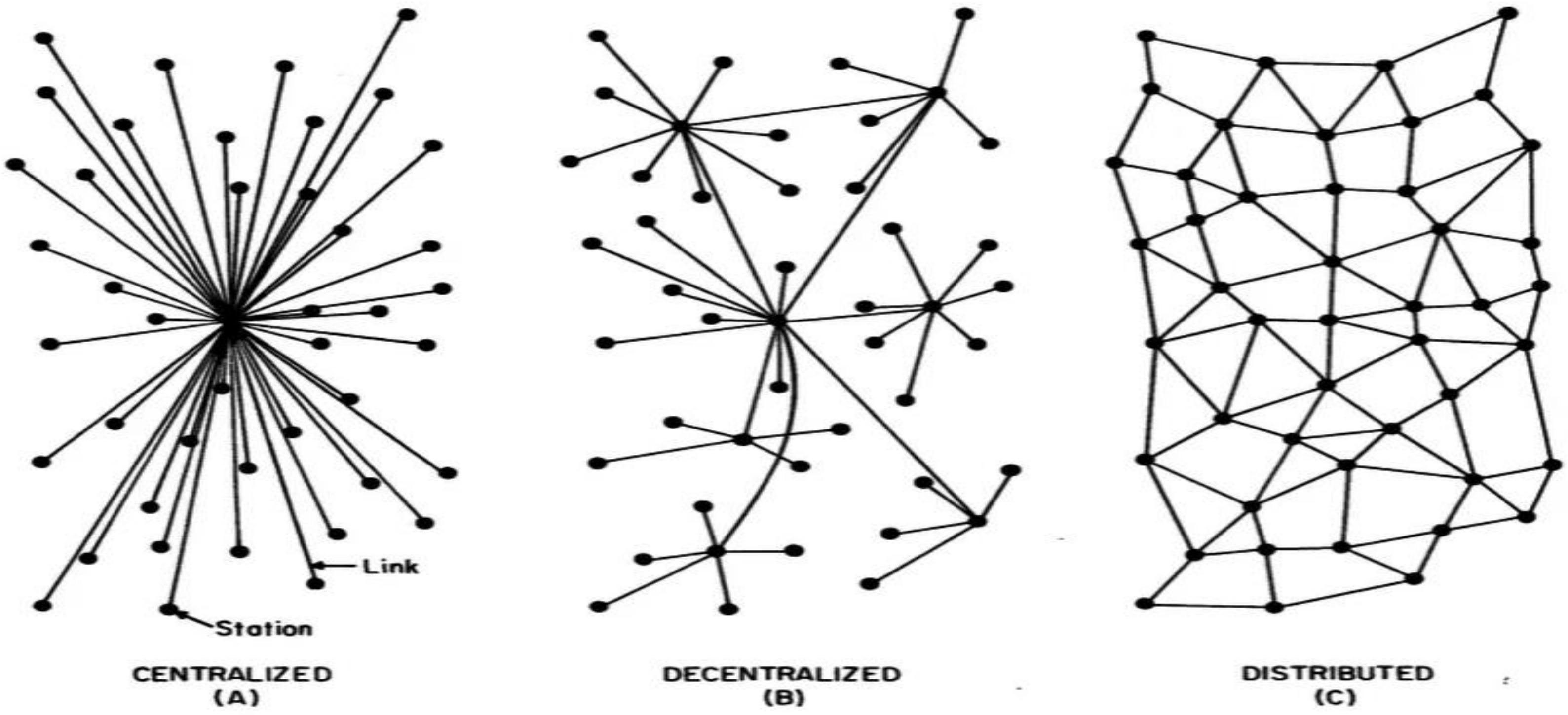
Blockchain

A decentralized database with strong consistency support

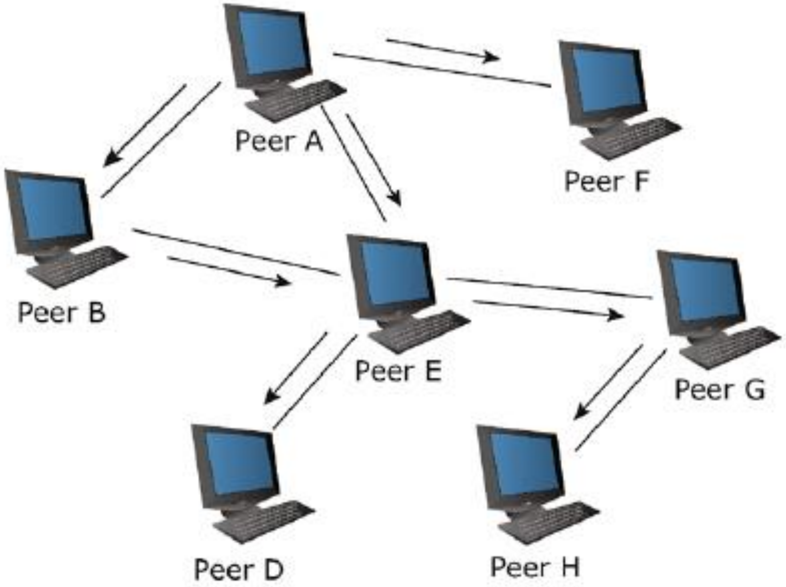
Courtesy: Lectures by Dr. Sandip Chakraborty

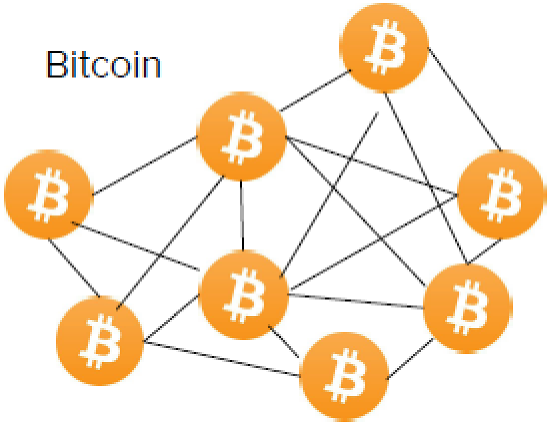
Blockchain Network
Centralization vs. decentralization

Competing paradigms that underlie many digital technologies



Peer to Peer Network



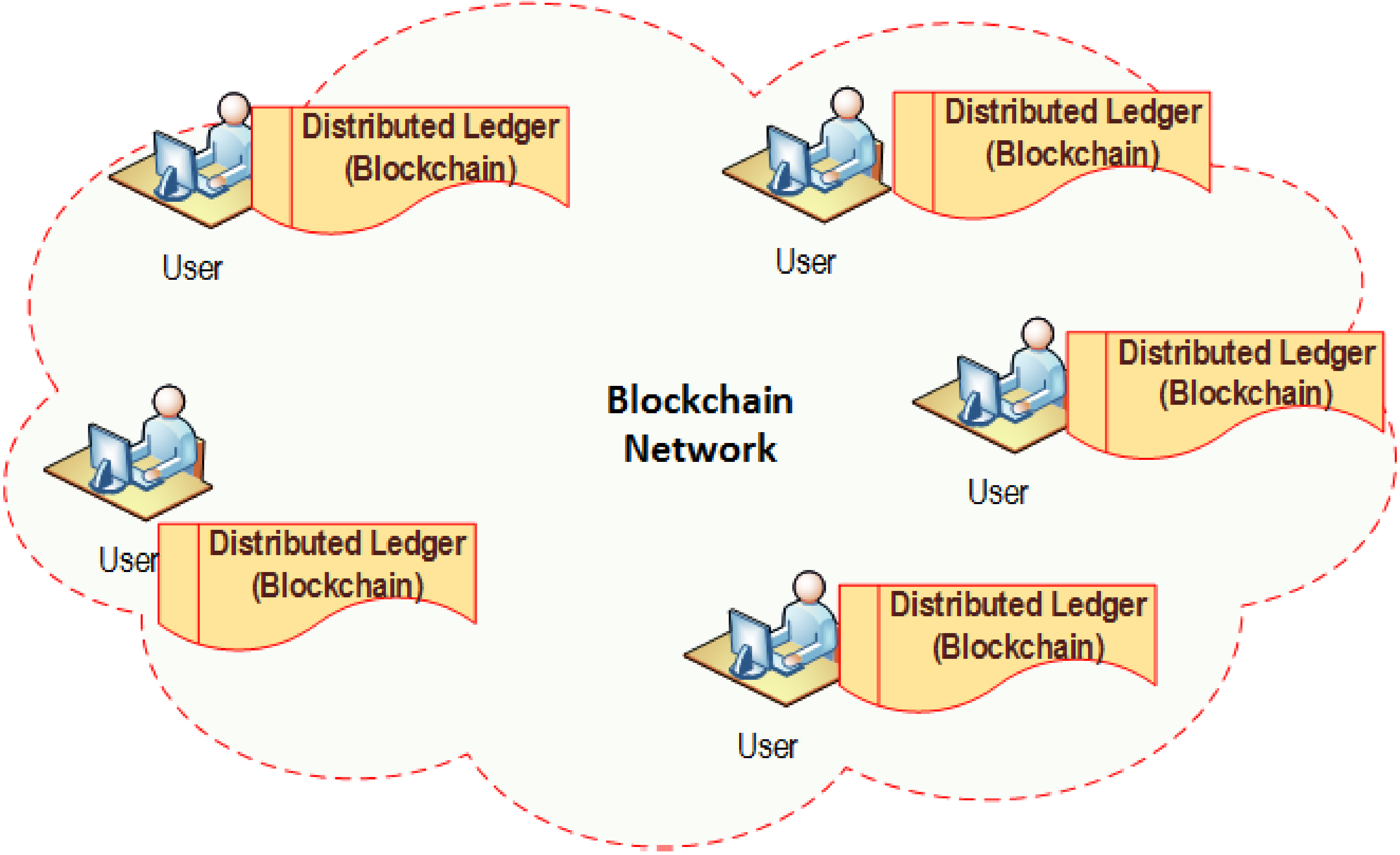


Peer to Peer Network

A distributed network architecture may be called a Peer-to-Peer (P-to-P, P2P,.) network, if the participants share a part of their own hardware resources (processing power, storage capacity, network link capacity, printers,.). These shared resources are necessary to provide the Service and content offered by the network (e.g. file sharing or shared workspaces for collaboration). They are accessible by other peers directly, without passing intermediary entities. The participants of such a network are thus resource (Service and content) providers as well as resource (Service and content) requestors (Servent-concept).

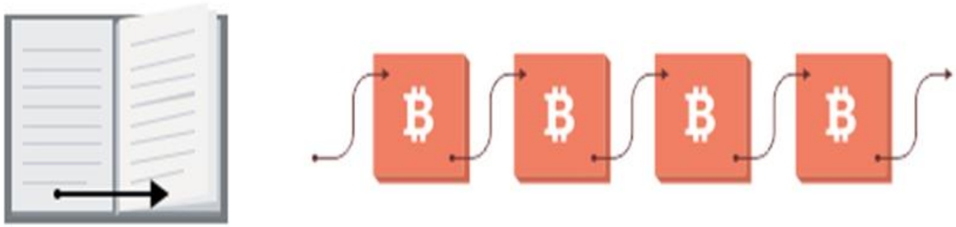
- Rüdiger Schollmeier, 2002

Blockchain Network


Distributed Ledger (Blockchain)
User
Distributed Ledger (Blockchain)
User
Blockchain Network
Distributed Ledger (Blockchain)
User
User
Distributed Ledger (Blockchain)
Distributed Ledger (Blockchain)
User

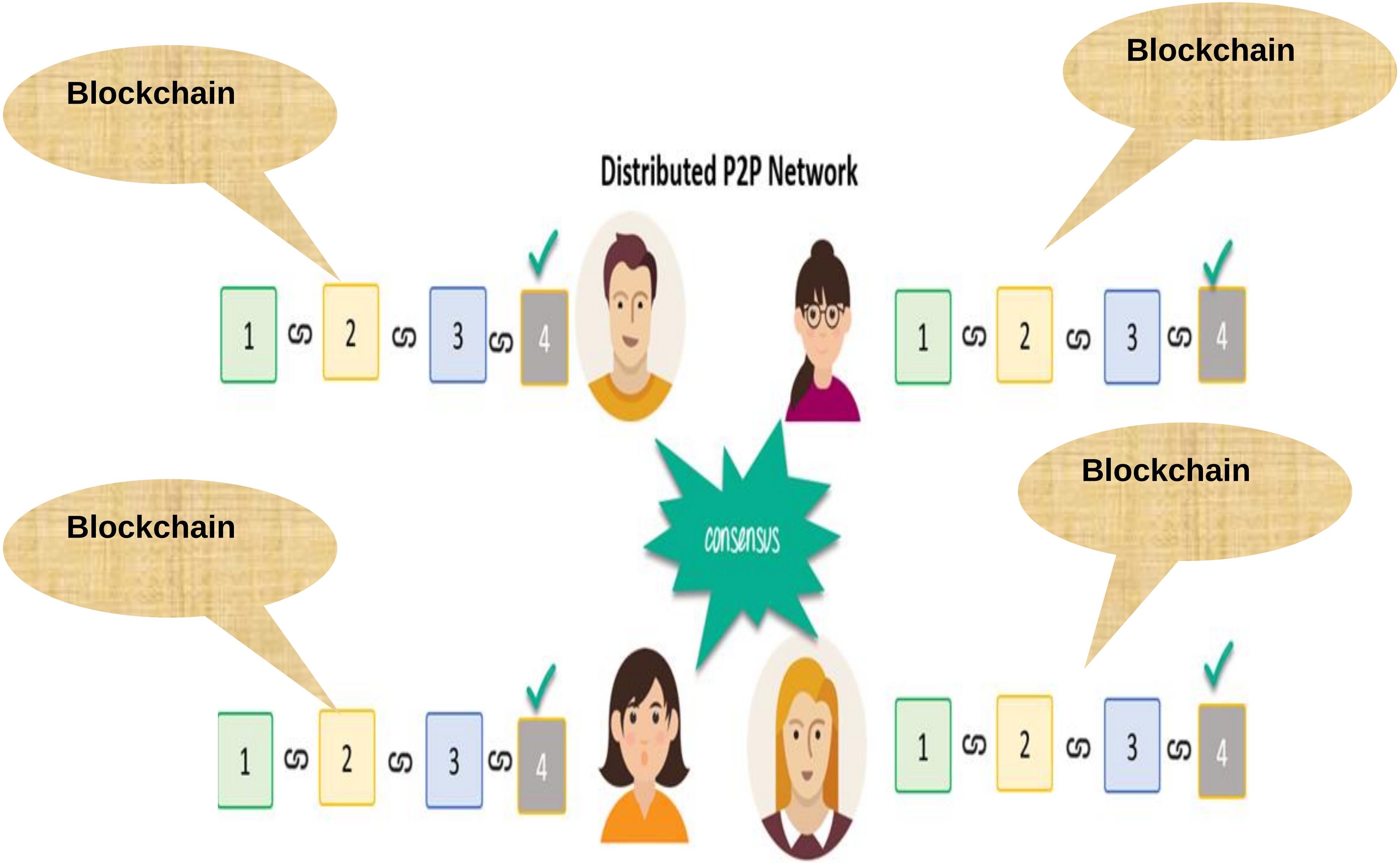
What is blockchain, and why does it matter?

- A blockchain is a historical record of transactions, much like a database
- Blocks in a chain = pages in a book.
- Each page in a book contains:
  - The text: the story
    - Equivalent to transactions in case of blockchain
  - Each page has information about itself (metadata): title of the book, chapter title, page number, etc.
    - Equivalent to transactions in case of blockchain



“Bits on Blocks”, Blog by Antony Lewis, https://bitsonblocks.net/

How to achieve consistency?

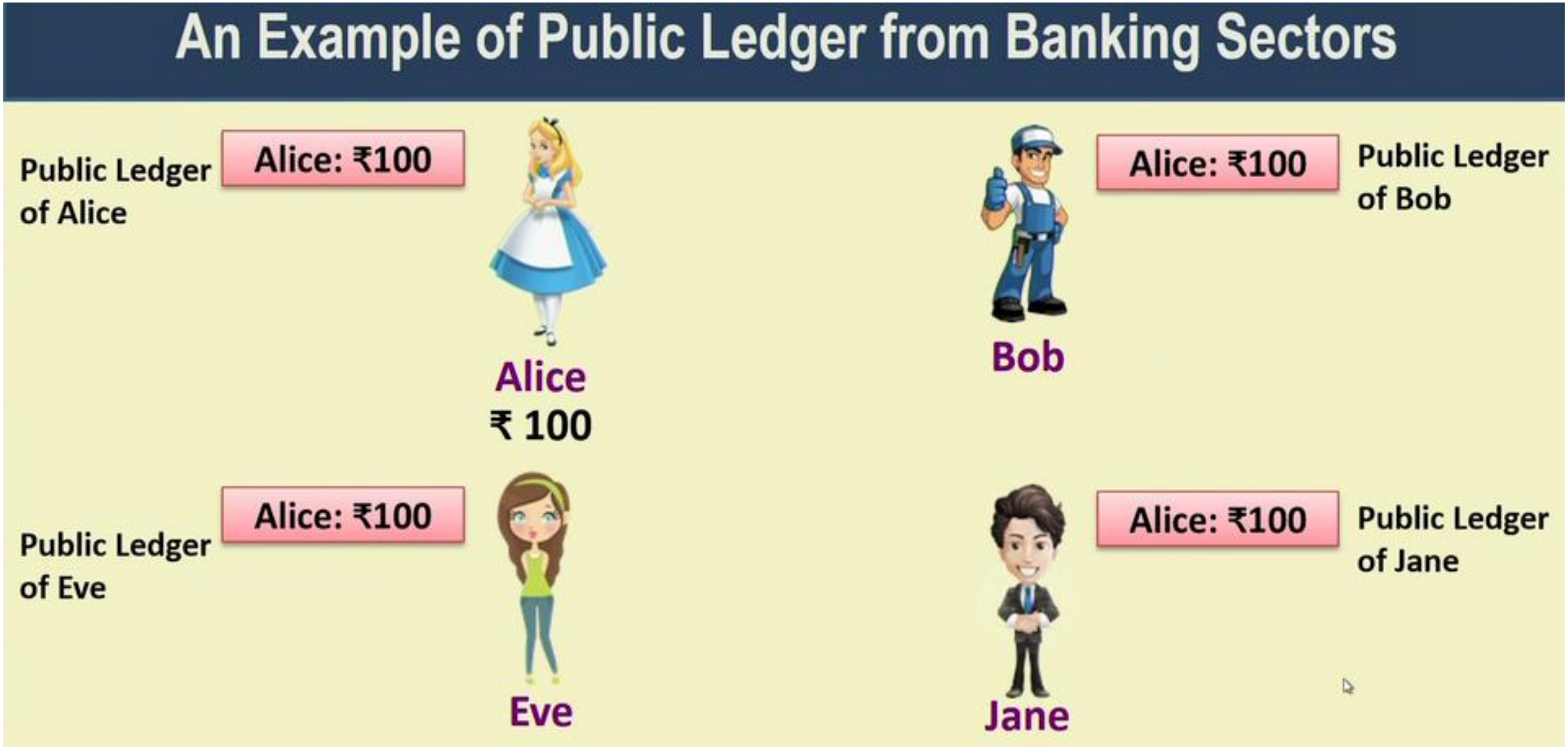


Blockchain

Blockchain

Blockchain

Blockchain



An Example of Public Ledger from Banking Sectors

Public Ledger of Alice

Alice: ₹100

Alice

₹ 100

Bob

Alice: ₹100

Public Ledger of Bob

Public Ledger of Eve

Alice: ₹100

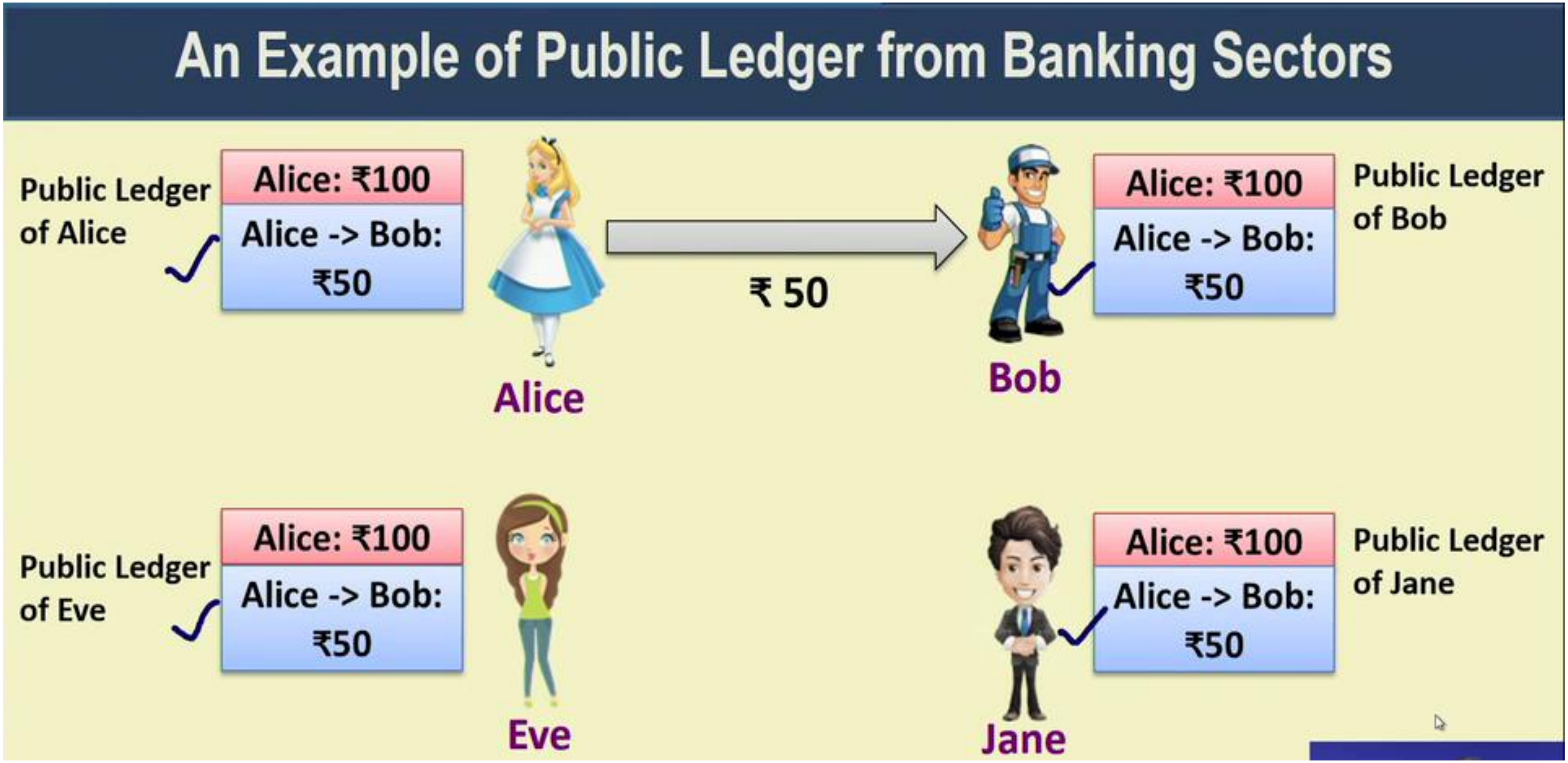
Eve

Jane

Alice: ₹100

Public Ledger of Jane

Courtesy: Lectures by Dr. Sandip Chakraborty



An Example of Public Ledger from Banking Sectors

Public Ledger of Alice ✓

Alice: ₹100

Alice -> Bob: ₹50

Alice

₹ 50

Bob

Alice: ₹100

Alice -> Bob: ₹50

Public Ledger of Bob ✓

Public Ledger of Eve ✓

Alice: ₹100

Alice -> Bob: ₹50

Eve

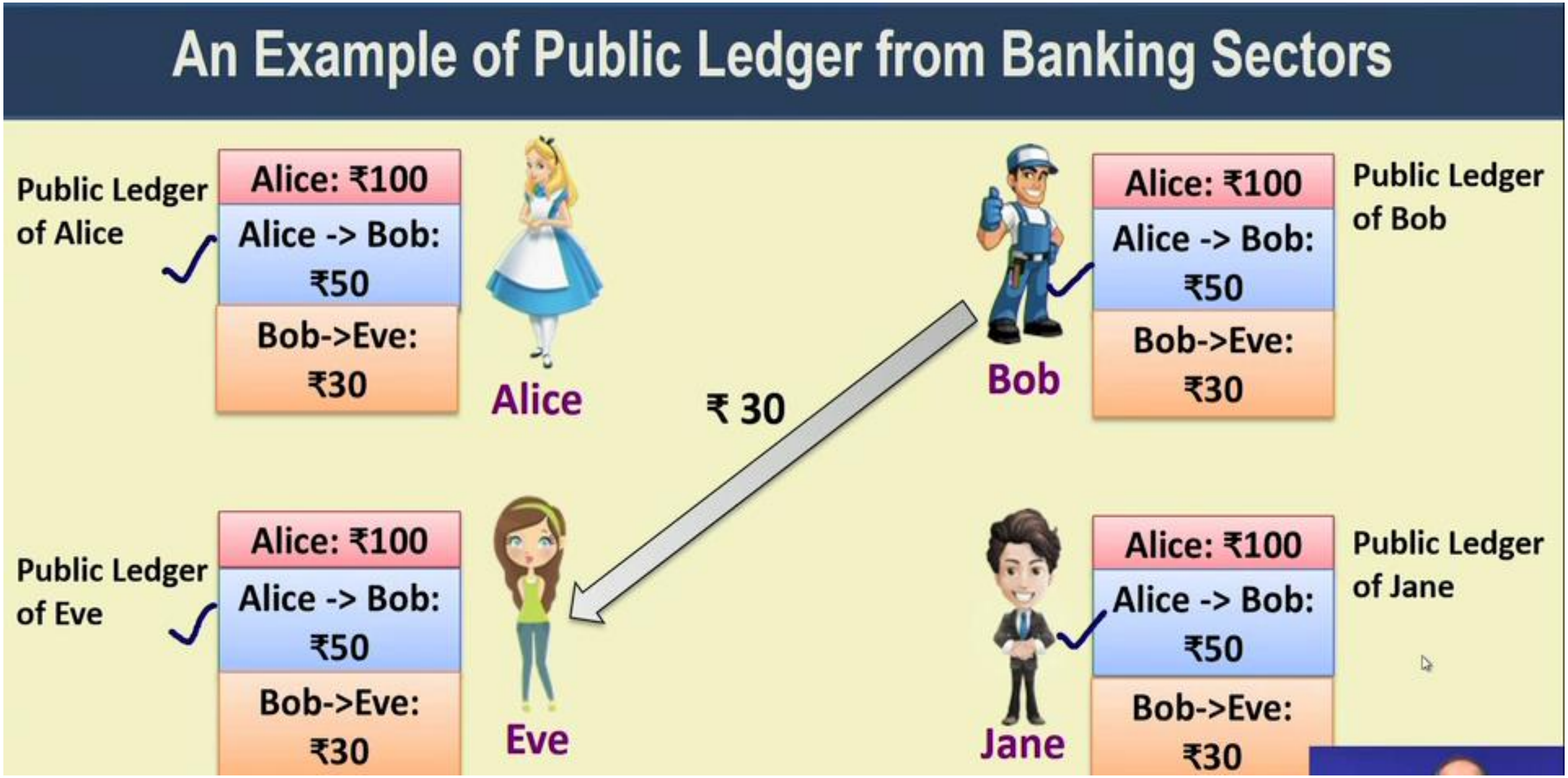
Jane

Alice: ₹100

Alice -> Bob: ₹50

Public Ledger of Jane ✓

Courtesy: Lectures by Dr. Sandip Chakraborty



An Example of Public Ledger from Banking Sectors

Public Ledger of Alice

Alice: ₹100

Alice -> Bob: ₹50

Bob->Eve: ₹30

Public Ledger of Bob

Alice: ₹100

Alice -> Bob: ₹50

Bob->Eve: ₹30

Public Ledger of Eve

Alice: ₹100

Alice -> Bob: ₹50

Bob->Eve: ₹30

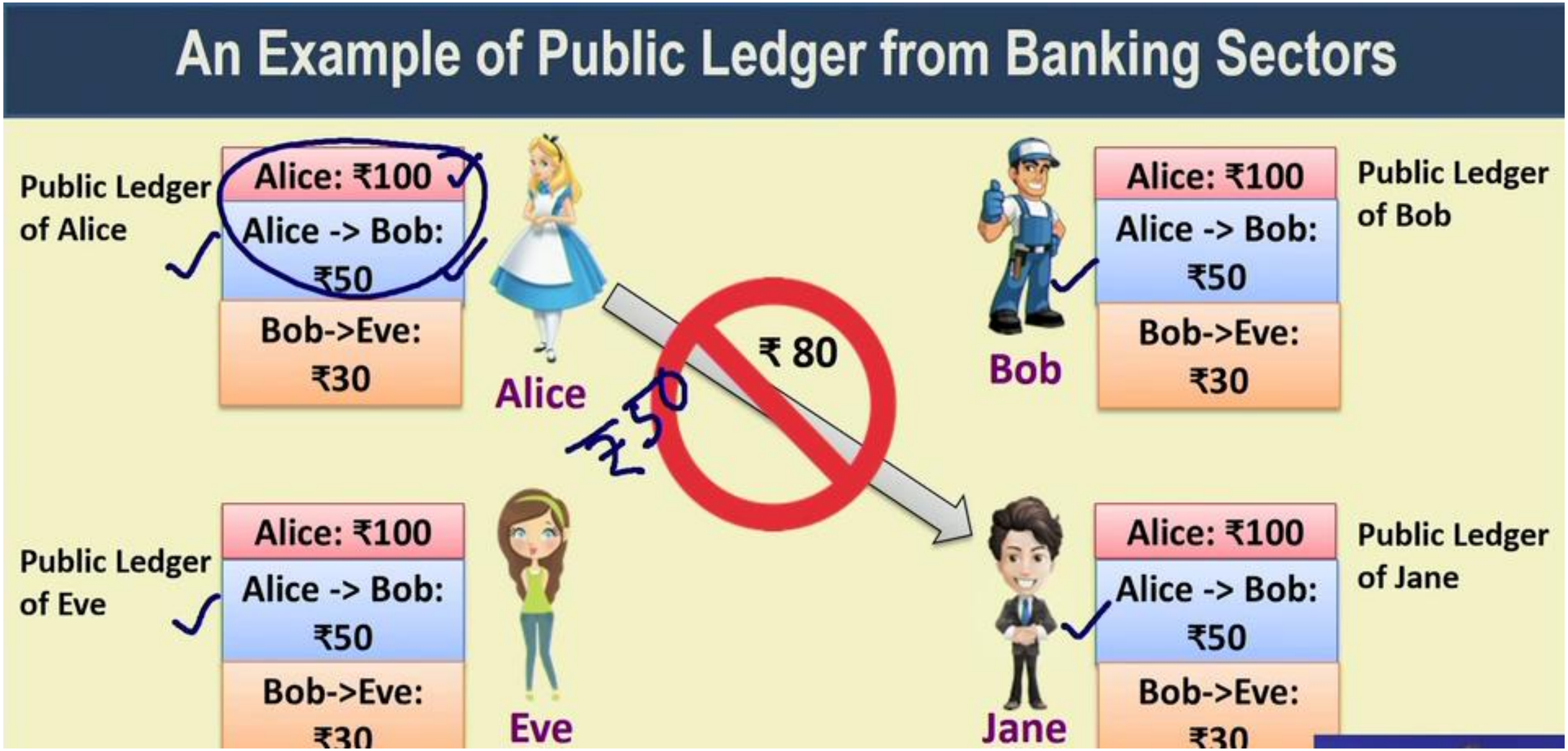
Public Ledger of Jane

Alice: ₹100

Alice -> Bob: ₹50

Bob->Eve: ₹30

Courtesy: Lectures by Dr. Sandip Chakraborty



An Example of Public Ledger from Banking Sectors

Public Ledger of Alice ✓

Alice: ₹100 ✓

Alice -> Bob: ₹50

Bob->Eve: ₹30

Alice

₹ 80

₹50

Bob

Public Ledger of Bob ✓

Alice: ₹100

Alice -> Bob: ₹50

Bob->Eve: ₹30

Public Ledger of Eve ✓

Alice: ₹100

Alice -> Bob: ₹50

Bob->Eve: ₹30

Eve

Jane

Public Ledger of Jane ✓

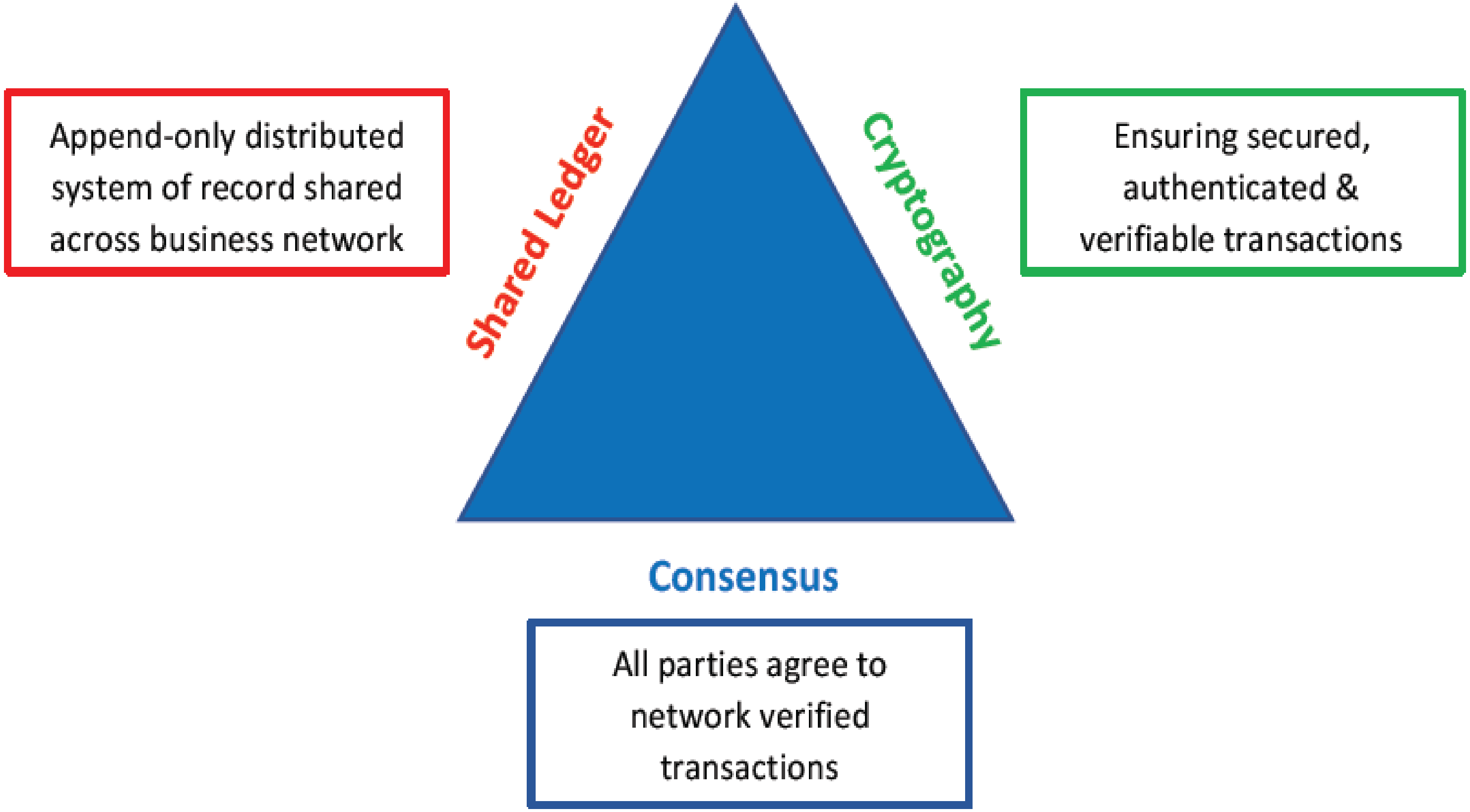
Alice: ₹100

Alice -> Bob: ₹50

Bob->Eve: ₹30

Courtesy: Lectures by Dr. Sandip Chakraborty

Underlying concepts of blockchain



Shared Ledger

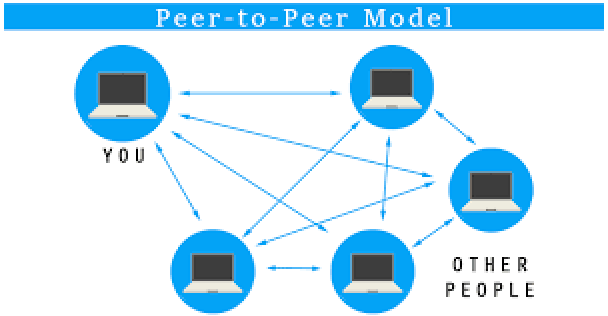
Append-only distributed system of record shared across business network

Cryptography

Ensuring secured, authenticated & verifiable transactions

Consensus

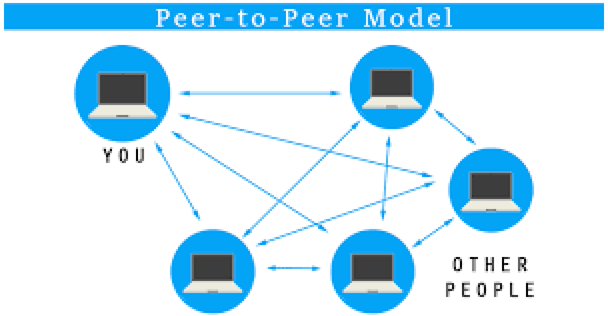
All parties agree to network verified transactions



What is Blockchain?

- **A decentralized computation and information sharing platform that enables multiple authoritative domains, who do not trust each other, to cooperate, coordinate and collaborate in a rational decision making process.**
  - Taken from Lectures by Dr. Sandip Chakraborty

- **A blockchain is "an open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way"**
  - Lansiti and Lakhani, 2017



What is Blockchain?

- **A blockchain is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable, and updatable only via consensus or agreement among peers.**
  - *www.pwc.in*

Design Goal of Cryptocurrencies

- Secure transfer in computer networks
- Cannot be copied and reused
- Anonymity
- Offline transactions
- Can be transferred to others
- Can be subdivided
- Solves Double Spending Problem

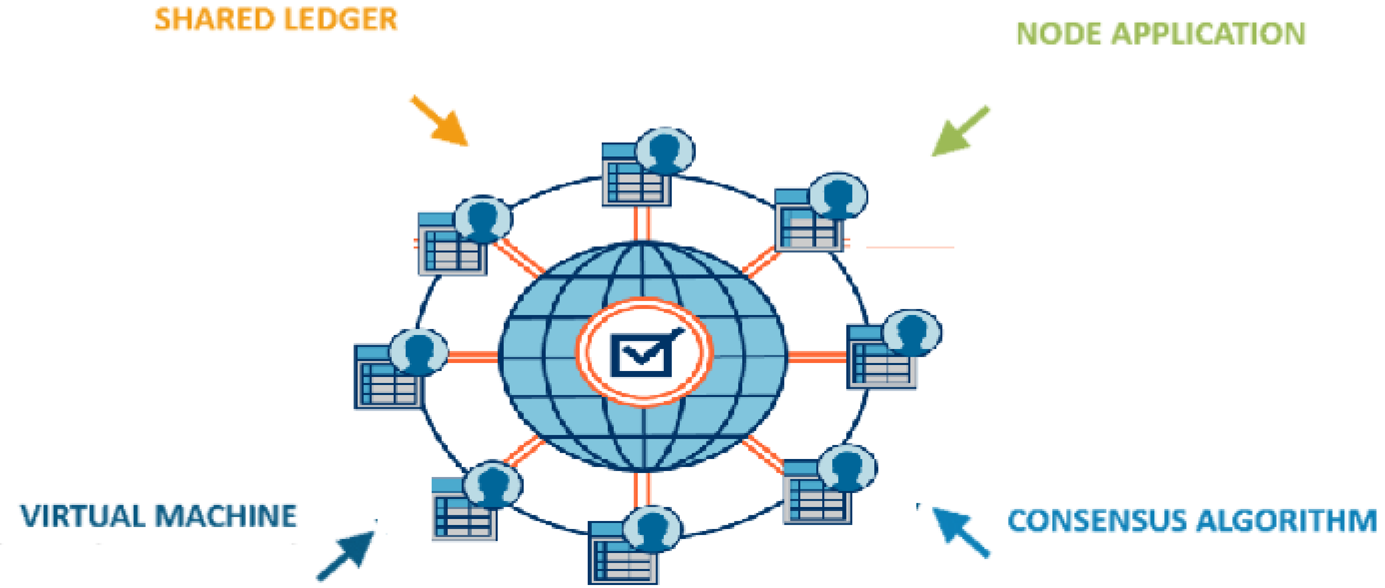
Some Key Terms

- **Distributed Ledger**
  - A List of transactions that are spread across many users (not central)
- **Node**
  - Another word for a user on a blockchain network running blockchain software and holding a copy of the ledger
- **Immutability**
  - Once data has been written to a Blockchain, no one can change it. This helps to ensure trustworthiness. Immutability is a result of how blockchain technology is designed.

Various Aspects

- **Decentralization**: There is no central entity that prints (mints) money, but rather the money is being mint by the crowd. This makes Bitcoin a decentralized system.
- **Anonymity and Authenticity**: People who use Bitcoin hope that their identity would not be revealed, in contrast to the usual way we all buy commodity over the internet using our credit card, we have to supply our personal details to be verified against the bank who treats our account. At the same time, authenticity needs to be ensured.
- **Protocols for commitments:** Ensures that every valid transaction from clients are committed and included in the blockchain within finite time.
- **Consensus:** Ensures that all local copies are consistent and up-to-date.
- **Security:** The data needs to be tamper-proof

Blockchain Logical Components



What shall I cover?

Broadly,

- Quick Review of Blockchain Technology
- Quick Introduction to Formal Methods in Critical Systems
- Defining Syntax & Semantics of Smart Contract Languages
- Various Language Paradigms
- Formal Analysis & Verification of Smart Contracts
- ML/AI & Blockchain
- Software Engineering Perspectives
- Interoperability
- Group Assignments!
- Research Directions

Thank You !