
Blockchains: Truth vs. Hype

Souradyuti Paul
IIT Bhilai

Keynote at BITCON 2019

BIT, Durg
March 1, 2019

Disclaimer

Some of the pictures used in this presentation have been taken from various sources on the Internet. If there is any omission on our part to see certain license information leading to violation of copyright or so, kindly notify the undersigned without any delay.

Souradyuti Paul

souradyuti@iitbhilai.ac.in

Blockchain: the Truth

What is Blockchain, in a word?

Answer: A Form of *Database* to store, update and access and display data.

Nomenclature

Ledger: Public/Private/Permissioned/Permissionless

How it all started? And what's so great about it?

Can we write a program to implement "Money"?

Virtual Money/Currency

World's first Virtual Currency: Bitcoin based on the Blockchain Technology (2009, Jan. 3)

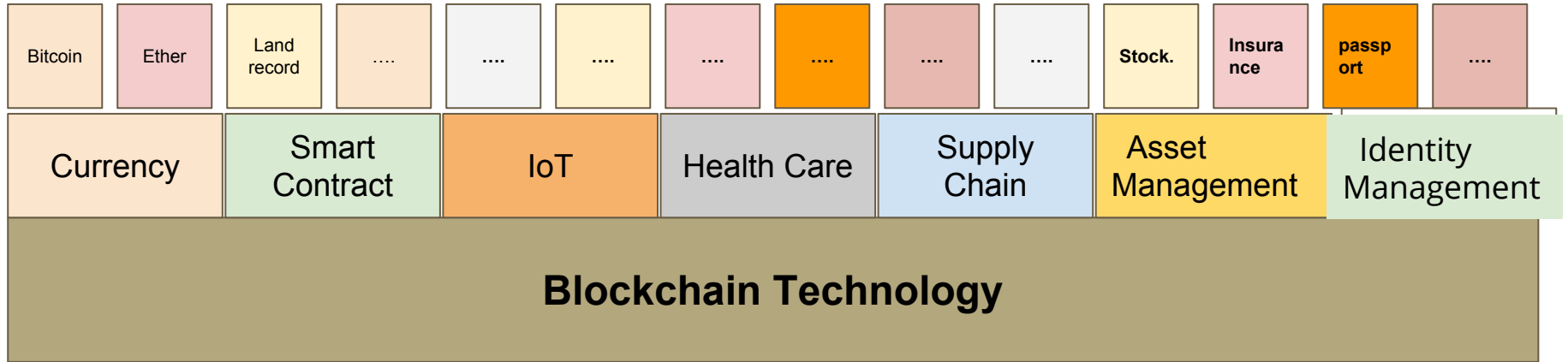


Native place of Bitcoins is the Internet. But physical forms do exist (Casascius, Ravenbit, etc.)

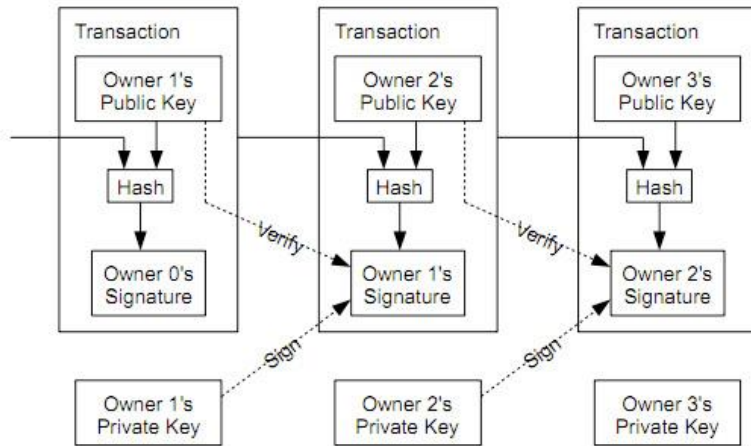
Mysterious Inventor of Bitcoin: Satoshi Nakamoto



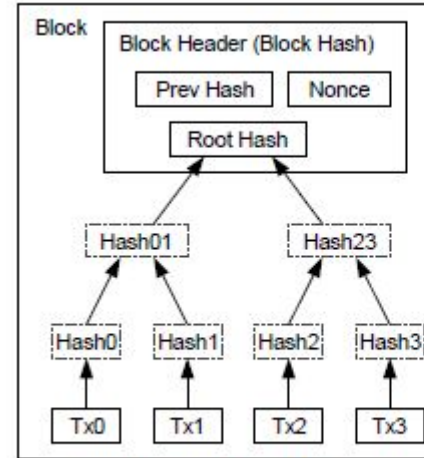
Are Bitcoin, Cryptocurrency, Blockchain same?



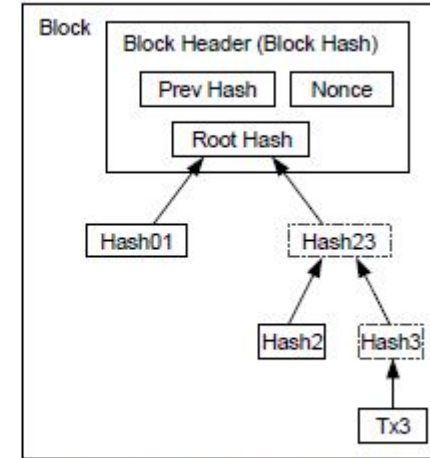
How A Blockchain looks Like



Chain of Transactions



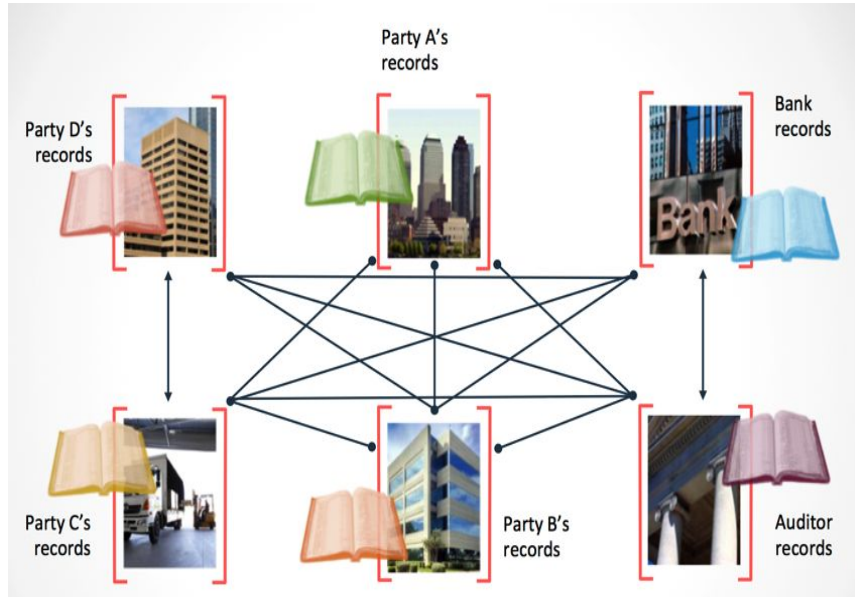
Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Chain of Blocks

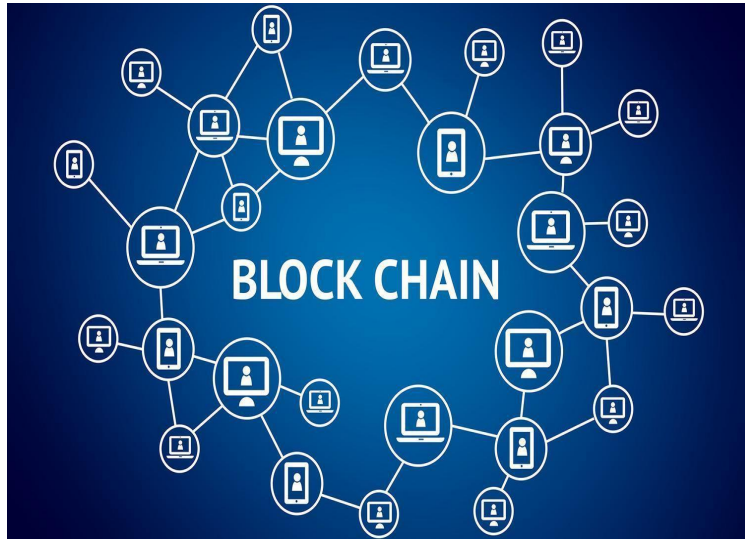
How Blockchain Works: Replicated Database Across All



Main Ingredients

1. Cryptographic Hash function
2. Cryptographic signature Scheme
3. Merkle Tree
4. Underneath TCP/IP

A Use-case of Blockchain: Cryptocurrency



Main Functionalities of Blockchain

1. Create Currency (one node)
2. Mine a currency (one or more nodes)
3. Consensus (entire network of nodes)

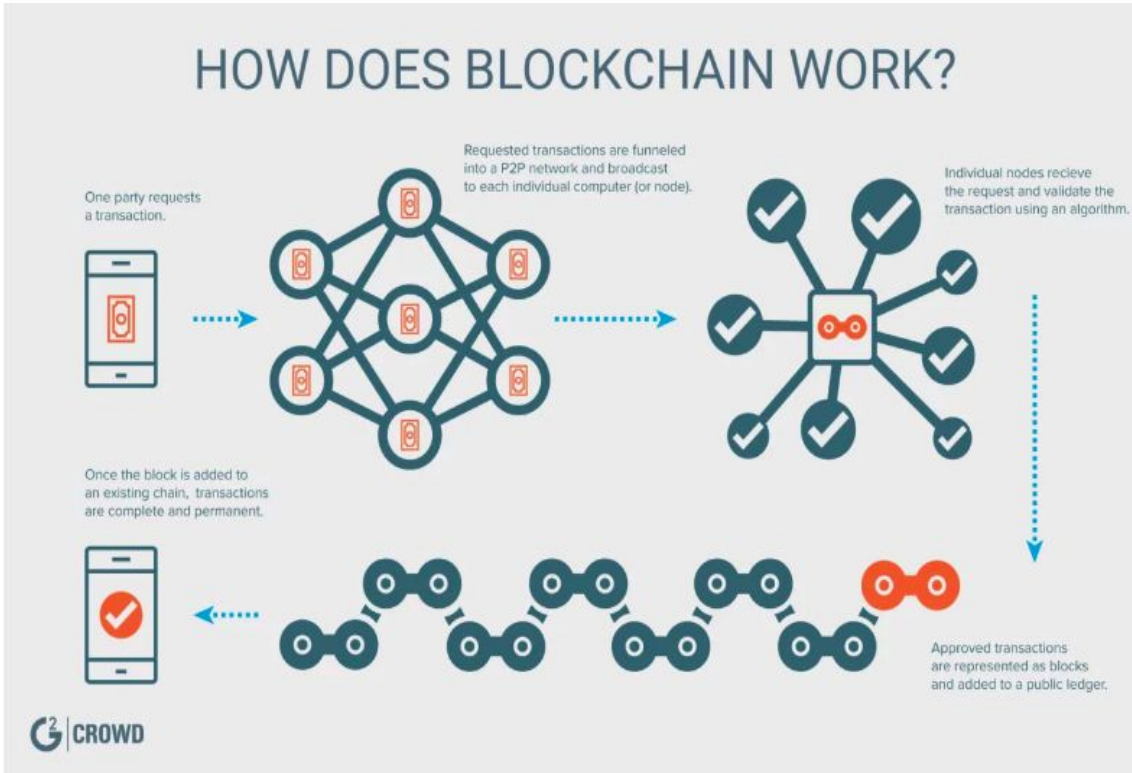
Main Components of Blockchain System

1. Bitcoin Client
2. Transaction
3. Block (collection of multiple transactions)

Reasons for Bitcoin's Success

1. Less transaction fees (cross-border money transfer)
2. No single point of failure
3. Microtransaction : Haiti erathquate
4. Business friendly: faster payment across countries (cross-border money transfer)

Blockchains: Going Beyond Cryptocurrencies



- **Moral of the story:** Transaction verification and secure syncing of multiple databases
- **Generalization:** How about using diverse databases. E.g. Govt., Hospital, Insurance, Patients
- **From Public to Private Blockchain:** Private validation is practical.

BLOCKCHAIN

REAL WORLD USES CASES


BORDER CONTROL

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




IDENTIFICATION

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



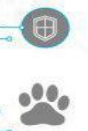
INSURANCE

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




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.



ENTERPRISE

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



GOVERNMENT

Essentia is developing an e-government pilot with Finland's Central Union of Agricultural Producers and Forest Owners that will enable urban and rural citizens to access public records.



SUPPLY CHAINS

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



HEALTHCARE

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



SHIPPING

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



REAL ESTATE

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



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.



COMPUTATION

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



ADVERTISING

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




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.



JOURNALISM

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



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.




DIAMONDS

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



FINE ART

By storing certificates of authenticity on the blockchain, it's possible to dramatically 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.




RAILWAYS

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



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.




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.



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.



What actually Blockchain Offers

- **Immutability:** Once in Blockchain always in Blockchain
- **(Decentralized) Consensus:** Among distrusting parties
- **Hackproof:** Cannot be tampered with
- **Automated Contract:** No human judiciary

Use-cases by Various Sectors

Blockchain use cases list by industry

Financial

Trading
Deal origination
POs for new securities
Equities
Fixed income
Derivatives trading
Total Return Swaps (TRS)
2nd generation derivatives
The race to a zero middle office
Collateral management
Settlements
Payments
Transferring of value
Know your client (KYC)
Anti money laundering
Client and product reference data.
Crowd Funding
Peer-to-peer lending
Compliance reporting
Trade reporting & risk visualizations
Betting & prediction markets

Insurance

Claim filings
MBS/Property payments
Claims processing & admin
Fraud prediction
Telematics & ratings

Media

Digital rights mgmt
Game monetization
Art authentication
Purchase & usage monitoring
Ticket purchases
Fan tracking
Ad click fraud reduction
Resell of authentic assets
Real time auction & ad placements

Computer Science

Micronization of work (pay for algorithms, tweets, ad clicks, etc.)
Expanse of marketplace
Disbursement of work
Direct to developer payments
API platform plays
Notarization & certification
P2P storage & compute sharing
DNS

Medical

Records sharing
Prescription sharing
Compliance
Personalized medicine
DNA sequencing

Asset Titles

Diamonds
Designer brands
Car leasing & sales
Home Mortgages & payments
Land title ownership
Digital asset records

Government

Voting
Vehicle registration
WIC, Vet, SS, benefits, distribution
Licensing & identification
Copyrights

Identity

Personal
Objects
Families of objects
Digital assets
Multifactor Auth
Refugee tracking
Education & badging
Purchase & review tracking
Employer & Employee reviews

IoT

Device to Device payments
Device directories
Operations (e.g. water flow)
Grid monitoring
Smart home & office management
Cross-company maintenance markets

Payments

Micropayments (apps, 402)
B2B international remittance
Tax filing & collection
Rethinking wallets & banks

Consumer

Digital rewards
Uber, AirBNB, Apple Pay
P2P selling, craigslist
Cross company, brand, loyalty tracking

Supply Chain

Dynamic ag commodities pricing
Real time auction for supply delivery
Pharmaceutical tracking & purity
Agricultural food authentication
Shipping & logistics management

Flexibility in Blockchain

- Public: Bitcoin, Ethereum
- Private: Hypeledger Fabric
- Permissioned: Ripple
- Permissionless: Bitcoin

Blockchain: The Hype

Can we solve any database problem using Blockchain?

When Centralized Database Is Better Than Blockchain

- Low cost of coordination (consensus)
- Privacy/Confidentiality is critical (instead of integrity)
 - *Storing private key/ciphertext in Blockchain?*
 - Zero-knowledge is expensive

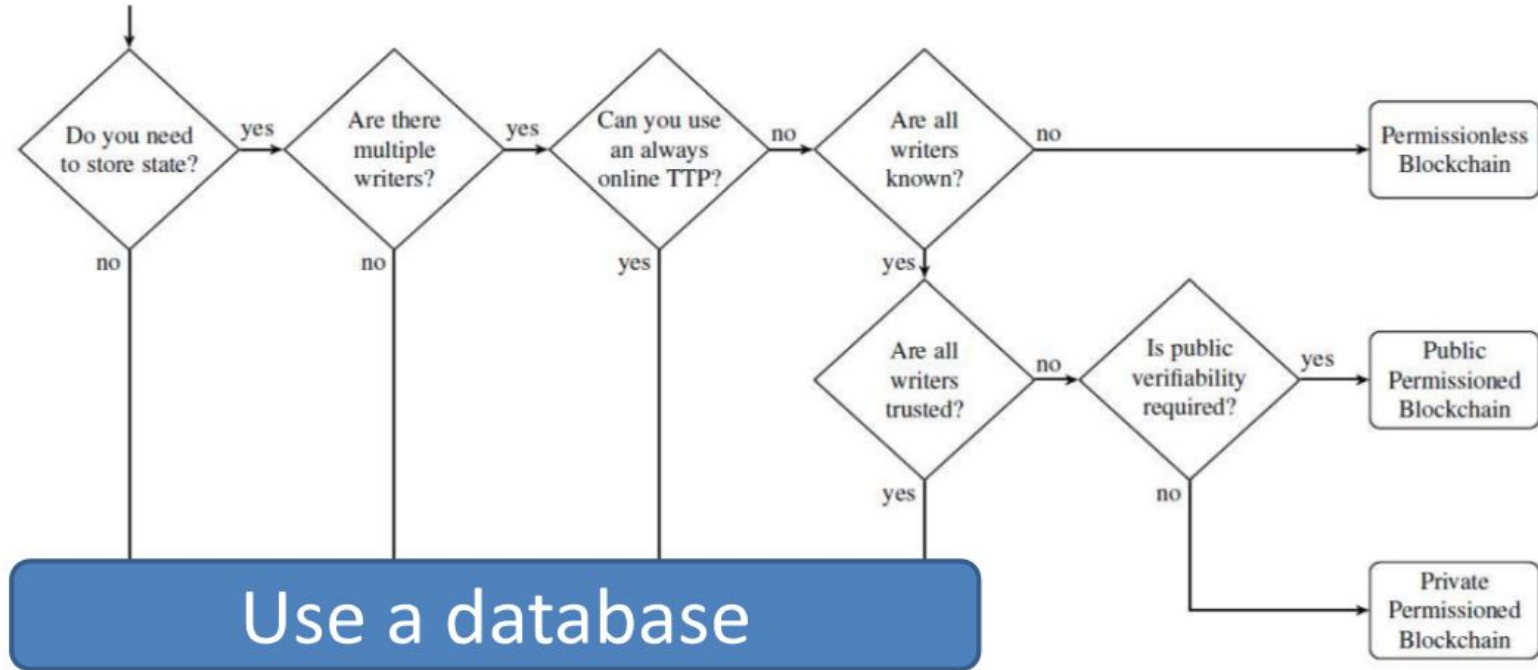
Blockchain Downsides

- High latency and low throughput
- Relatively less flexibility in access control (Permissioned Blockchain)
- Poor simulation of TTP
- Key-management is tough

When say NO to Blockchain?

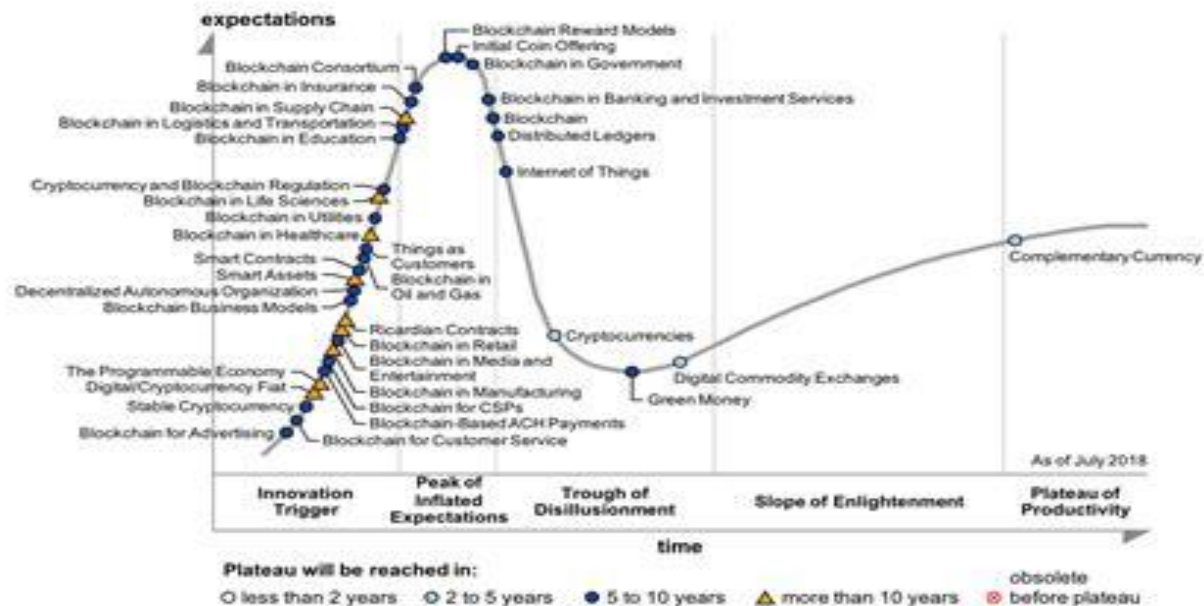
Do You Need a Blockchain?

(based on a paper by K Wüst and A Gervais)



Slide credit: Bart Preneel (presented at Blockchain 2018, ISI Kolkata)

Hype Cycle for Blockchain Business, 2018



gartner.com/SmarterWithGartner

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner.

Thanks for your attention.