Understanding Bitcoin & Blockchain

M.Naghipourfar

Blockchain Innovation Lab

BLOCKCHAIN INNOVATION LAB

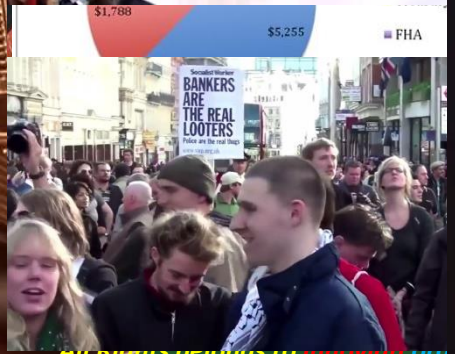
Naghipourfar

Naghipourfar

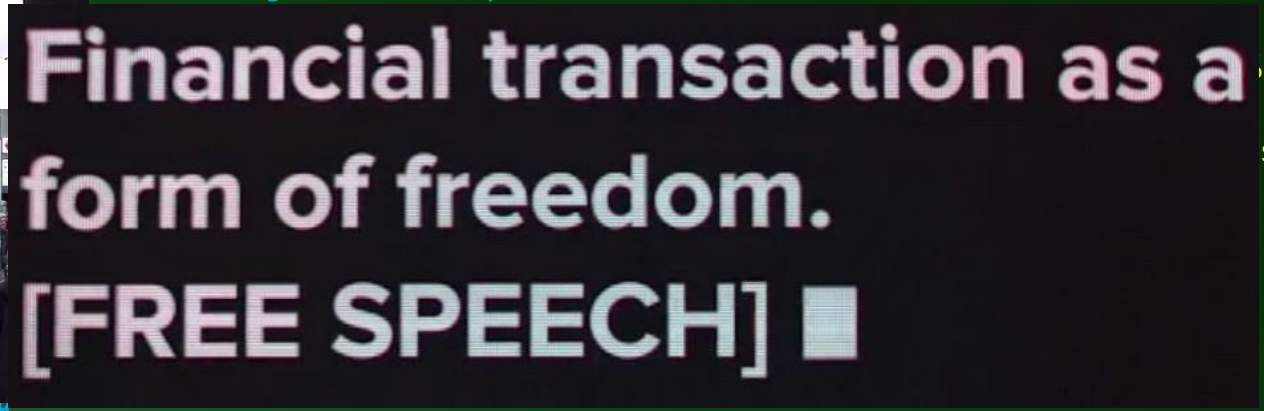
Naghipourfar

M.Naghipourfar

Preface



- Bloomberg found the Federal Reserve had, by March 2009, committed $7.77 trillion to rescuing the financial system



st 2011

How Started

bitcoin

noun (also **Bitcoin**) /ˈbɪt.kɔɪn/

A Peer-to-Peer Electronic Cash System

titled

2009

hi

esis

block

for

e day it

s first

b-

Bitcoin

bitcoin.

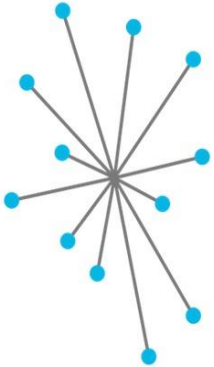
BLOCKCHAIN INNOVATION LAB

Wikileaks Story

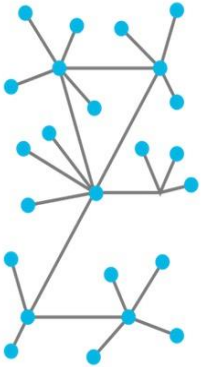
In 2014 the majority of Wikileak's public funding was bitcoin.

Ledger

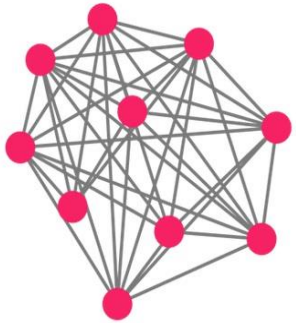
Centralized

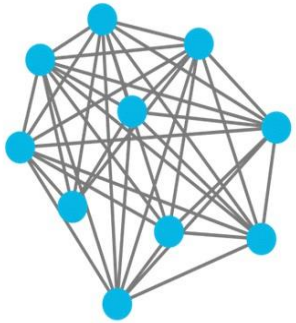


Decentralized



Distributed Ledgers





The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

Peer to Peer Networks

- Napster was envisioned as an independent Peer to Peer File Sharing service by Shawn Fanning. The service operated between June 1999 and July 2001 (26.4 Million users).
- *Unstructured peer-to-peer networks* (Gnutella, Gosip, and Kazaa)
- *structured peer-to-peer network* implement a Distributed Hash Table (DHT) which enables peers to search for resources on the network using a hash table (BitTorrent , Kad Network, Storm Botnet, YaCy, and Coral Content Distribution Network)

Overview of Bitcoin Whitepaper

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Digital currency (Centralized)

- **Digital currency** (**digital money** or **electronic money** or **electronic currency**) is a type of currency available only in digital form, not in physical
- **eCach (DigiCash)** was an electronic money corporation founded by David Chaum in 1989.
  - eCash (DigiCash) transactions were unique in that they were anonymous due to a number of cryptographic protocols
- The E-Gold system was founded by Douglas Jackson and Barry Downey and launched online in 1996 and had grown to five million accounts by 2009
- Centralized systems—such as PayPal, eCash, WebMoney, Payoneer, and cashU will sell their electronic currency directly to the end user.

Digital Currency (Decentralized)

- A cryptocurrency is a type of digital token that relies on cryptography for chaining together digital signatures of token transfers, peer-to-peer networking and decentralization.

- Bitcoin, the first cryptocurrency, a peer-to-peer electronic monetary system based on cryptography.
- Etherium, an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality.
- Bitcoin Cash, a 2017 fork of bitcoin; main differences from bitcoin are larger blocks, different difficulty adjustment algorithm, and lack of Segregated Witness.
- IOTA, an open source distributed ledger and an electronic monetary system designed for the Internet of Things. It uses a Directed Acyclic Grapgh (DAG) instead of a Blockchain.
- Ripple monetary system, a monetary system based on trust networks.
- Litecoin, originally based on the bitcoin protocol, intended to improve upon its alleged inefficiencies. Faster block times and different mining algorithm compared to bitcoin.
- Dash, originally based on the bitcoin protocol, it offers the option of instant and private transactions. It is a Decentralized Autonomous Organization.
- NEM, a peer-to-peer electronic monetary system and a blockchain platform which allows for storing digital assets.
- NEO, an open-source, public, blockchain-based distributed computing platform featuring smart assets contract functionality.
- Monero, an open source cryptocurrency created in April 2014 that focuses on privacy, decentralisation and scalability.
- Zcash, a cryptocurrency that offers privacy and selective transparency of transactions.

BLOCKCHAIN INNOVATION LAB

Crypto Functions

WikiLeaks
@wikileaks
Follow

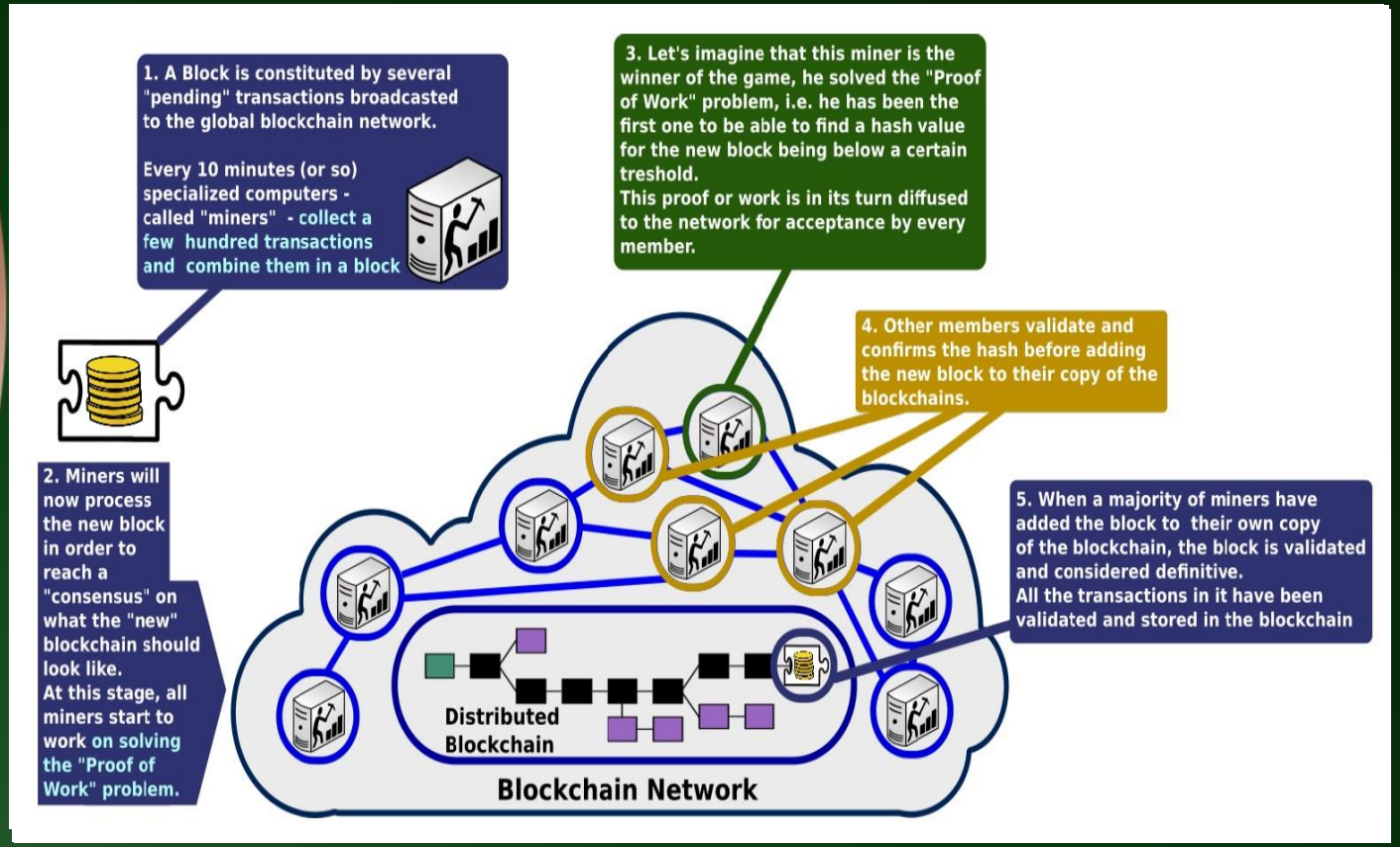
Release today of CIA 'Archimedes' malware

Digital Signatures

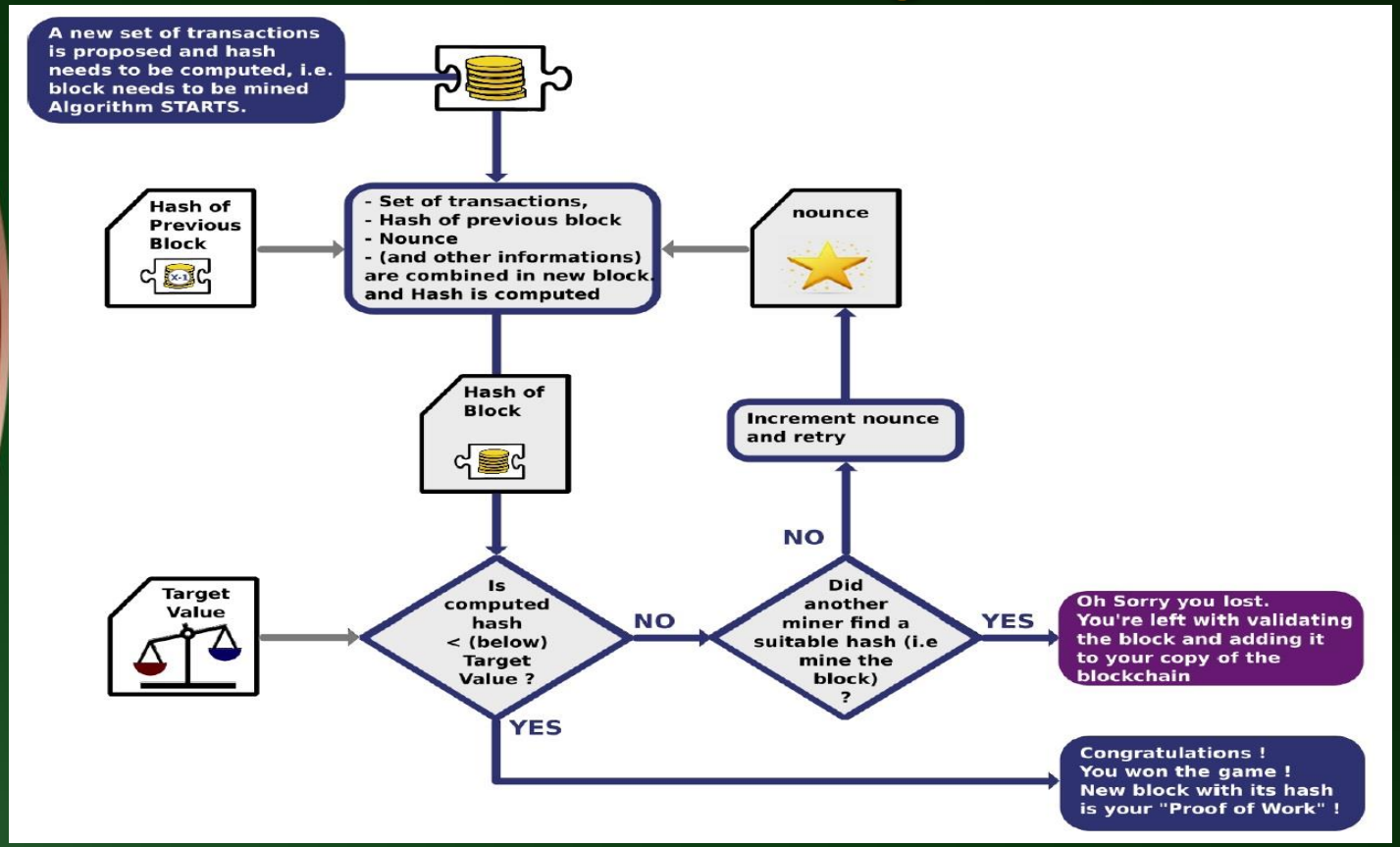
Public key
+
Private key

Blockchain of Bitcoin

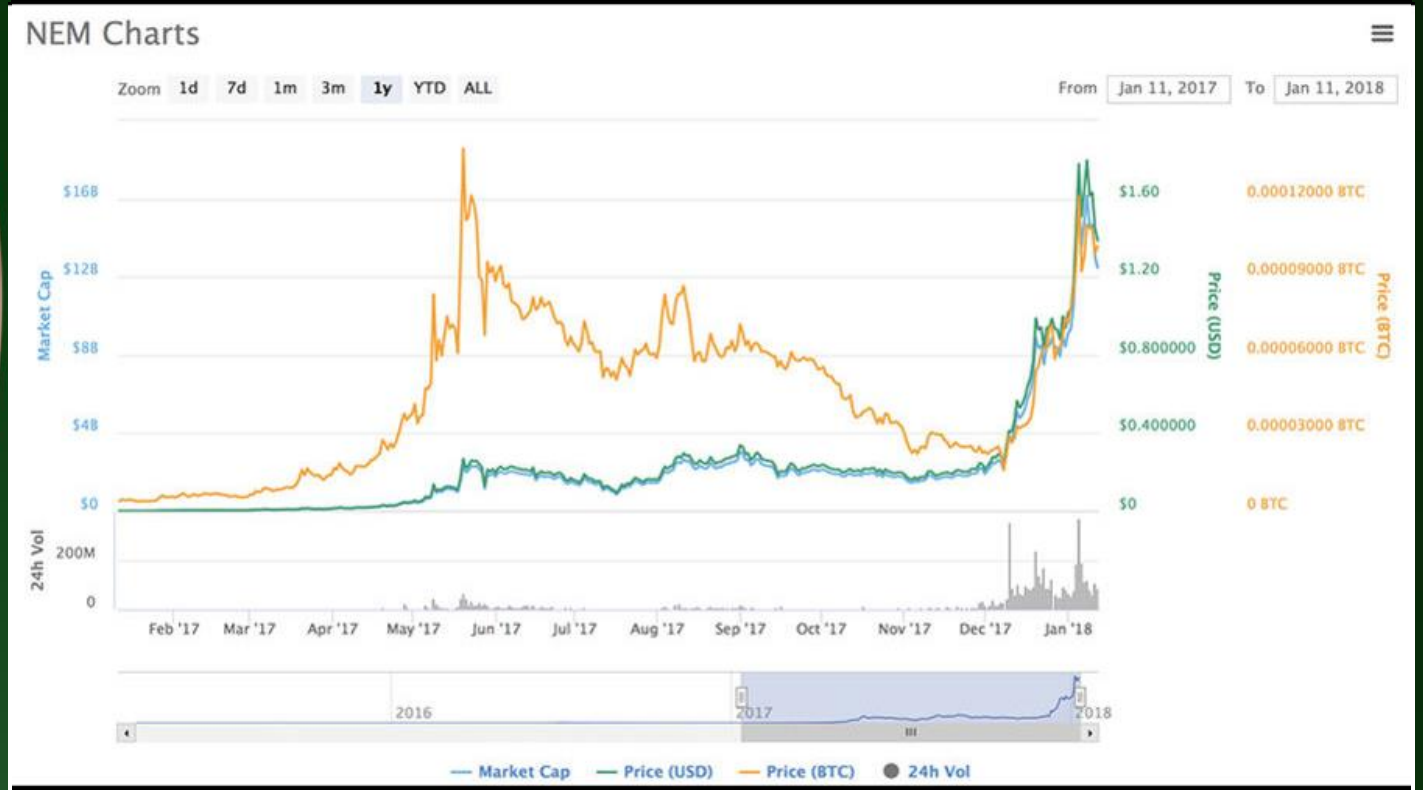
A Bitcoin Transaction



Proof of Work and Mining Reward



Some Charts



Some Recent Charts

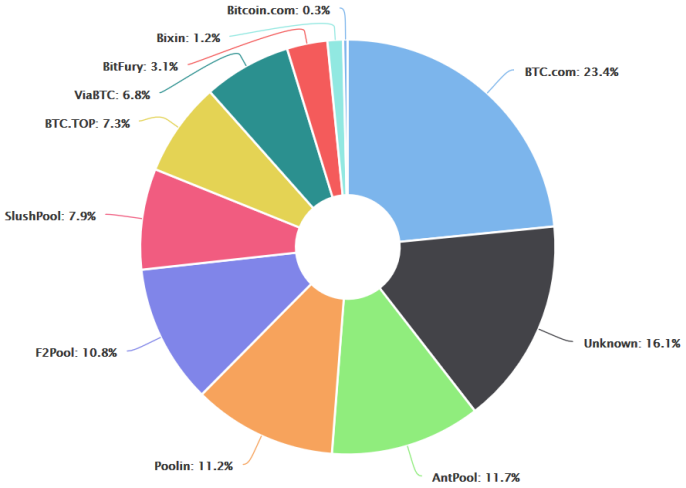
BLOCKCHAIN INNOVATION LAB

BLOCKCHAIN WALLET DATA API ABOUT BLOCK, HASH, TRANSACTION, ETC... GET A FREE WALLET

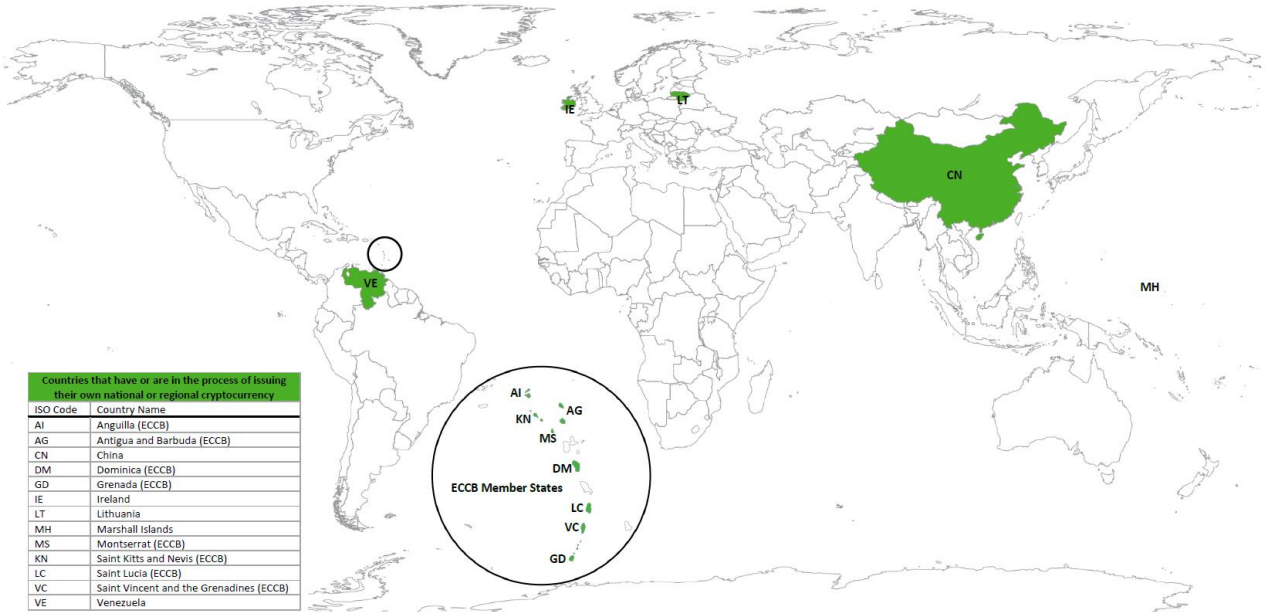
Hashrate Distribution An estimation of hashrate distribution amongst the largest mining pools

The graph below shows the market share of the most popular bitcoin mining pools. It should only be used as a rough estimate and for various reasons will not be 100% accurate. A large portion of Unknown blocks does not mean an attack on the network, it simply means we have been unable to determine the origin.

24 hours - 48 hours - 4 Days



Regulation in the World



Countries that have or are in the process of issuing their own national or regional cryptocurrency	
ISO Code	Country Name
AI	Anguilla (ECCB)
AG	Antigua and Barbuda (ECCB)
CN	China
DM	Dominica (ECCB)
GD	Grenada (ECCB)
IE	Ireland
LT	Lithuania
MH	Marshall Islands
MS	Montserrat (ECCB)
KN	Saint Kitts and Nevis (ECCB)
LC	Saint Lucia (ECCB)
VC	Saint Vincent and the Grenadines (ECCB)
VE	Venezuela

Countries that Have or Are Issuing National or Regional Cryptocurrencies

Law Library of Congress
LIBRARY OF CONGRESS

Source & Note: Created by the Law Library of Congress based on information provided in this report. As discussed in the report, the Eastern Caribbean Central Bank (ECCB), which is the monetary authority for eight island economies in the Eastern Caribbean Currency Union, has entered into an agreement for the development of a digital currency for member states.

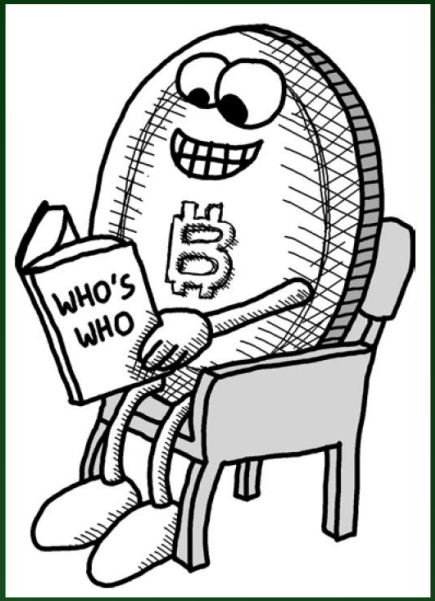
Some Useful Books

BLOCKCHAIN INNOVATION LAB

What is not?

- A currency issued by an institution
- A Ponzi scheme
- A currency backed by gold / silver
- A physical currency

- A bubble ?



What is?

- An idea / an algorithm
- An open source project
- A distributed transaction database
- A distributed peer-to-peer digital currency

Bitcoin vs Blockchain

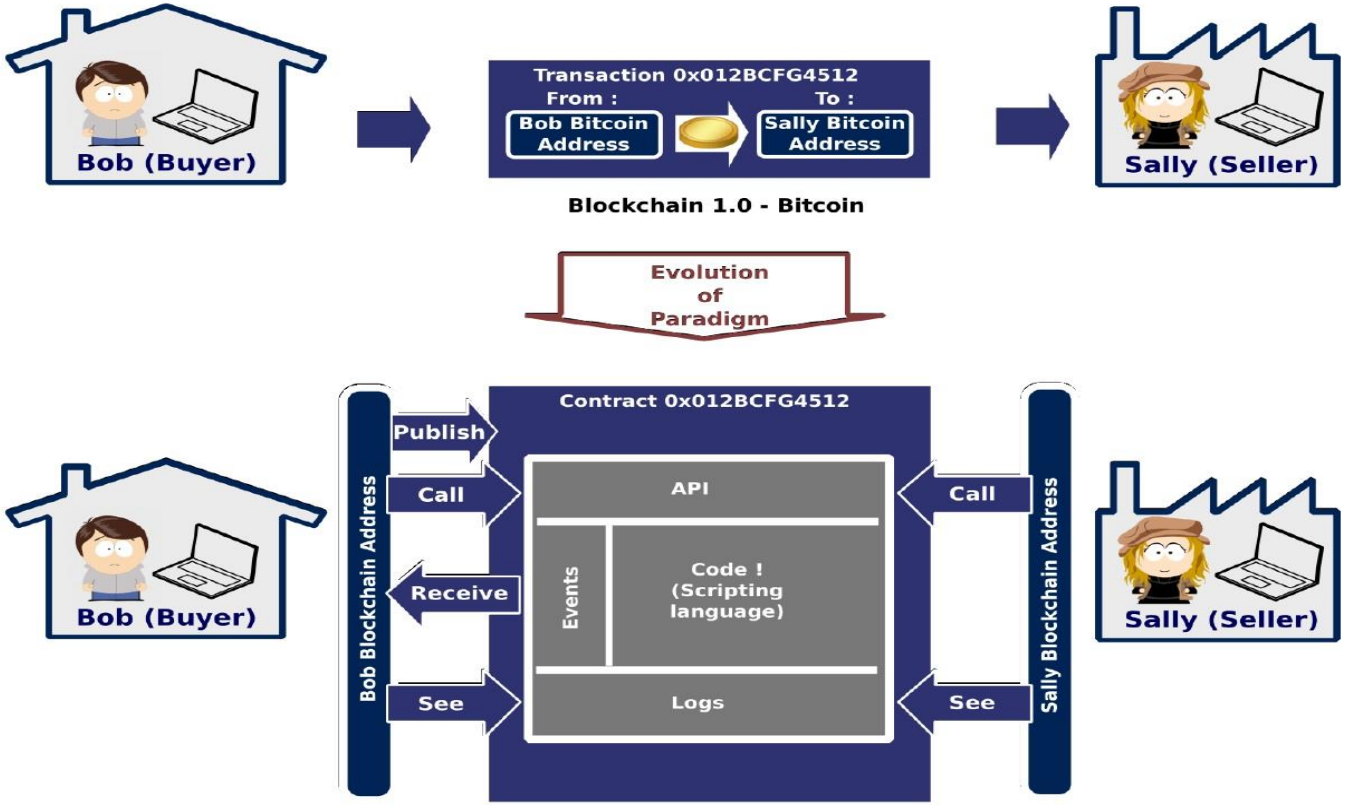
Blockchain is bigger than Bitcoin

Blockchains are platforms upon which many Fintech applications beyond cryptocurrencies can be built

BLOCKCHAIN AS A PLATFORM FOR FINANACIAL SERVICES

Use Case / Application	CROSS-BORDER PAYMENTS	ESCROW & CUSTODY SERVICES	SUPPLY CHAIN & TRADE FINANCE	CUSTOMER ACQUISTION & LOYALTY	FINANCIAL SECURITIES & TRADING	LOGISTICS & ASSET TRACKING	INTELLECTUAL PROPERTY RIGHTS	REAL ESTATE & PROPERTY	SUPPLY CHAIN MANAGEMENT	DIGITAL RIGHTS MANAGEMENT	INSURANCE	LEGAL	IDENTITY MANAGEMENT	FILE STORAGE & SHARING	ELECTRONIC MEDICAL RECORDS	AUDITING & COMPLIANCE	INTERNET OF THINGS	VOTING & GOVERNANCE SYSTEMS	COLLABORATIVE ECONOMY	OTHERS TO BE DETERMINED
Record	CURRENCY				ASSETS				CONTRACTS				DATA				P2P		
Platform	BLOCKCHAIN																		

Blockchain 2.0



BLOCKCHAIN INNOVATION LAB

Blockchain as Web 3.0

- Internet of Information
  - TCP/IP = communication protocol
  - Revolutionised the way we exchange information
  - 1st use case: e-mail
  - Evolved to: Web 2.0, streaming, push notifications…
- Internet of Value
  - Blockchain = value exchange protocol
  - Decentralised trust: shared single source of truth
  - Promises to fundamentally transform business, economy, politics, public services and more
  - 1st use case: Bitcoin
- Blockchain replaces "trusted 3rd party" concept
  - People / organisations / systems can collaborate despite having no particular confidence in each other
  - No neutral central authority required
  - Though having some may confer performance advantages
- Why distribute trust?
  - Faster (e.g. Bitcoin transactions complete in around 10 minutes vs. some days using bank clearing systems)
  - Cheaper (e.g. Bitcoin charges average around US $10 per transaction, vs. 5-10% bank commission)
  - Fewer errors / more secure (too early to tell?)

Blockchain Applications

Web 3.0

The blockchain gives internet users the ability to create value and authenticate digital information. What new business applications will result?

Smart contracts

Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met.

The sharing economy

By enabling peer-to-peer payments, the blockchain opens the door to direct interaction between parties — a truly decentralized sharing economy results.

Crowd funding

Blockchains take this interest to the next level, potentially creating crowd-sourced venture capital funds.

Governance

By making the results fully transparent and publically accessible, distributed database technology could bring full transparency to elections or any other kind of poll taking.

Supply chain auditing

Distributed ledgers provide an easy way to certify that the backstories of the things we buy are genuine. Transparency comes with blockchain-based timestamping of a date and location — on ethical diamonds, for instance — that corresponds to a product number.

Blockchain Applications

File storage

Decentralizing file storage on the internet brings clear benefits. Distributing data throughout the network protects files from getting hacked or lost.

Prediction markets

Prediction markets that pay out according to event outcomes are already active. Blockchains are a “wisdom of the crowd” technology that will no doubt find other applications in the years to come.

Protection of intellectual property

Smart contracts can protect copyright and automate the sale of creative works online, eliminating the risk of file copying and redistribution.

Internet of Things (IoT)

Smart contracts make the automation of remote systems management possible. A combination of software, sensors, and the network facilitates an exchange of data between objects and mechanisms.

NeighbourhoodMicrogrids

Blockchain technology enables the buying and selling of the renewable energy generated by neighbourhoodmicrogrids.

Blockchain Applications

Identity management

Distributed ledgers offer enhanced methods for proving who you are, along with the possibility to digitize personal documents. Having a secure identity will also be important for online interactions — for instance, in the sharing economy.

AML and KYC

Anti-money laundering (AML) and know your customer (KYC) practices have a strong potential for being adapted to the blockchain. Currently, financial institutions must perform a labour intensive multi-step process for each new customer. KYC costs could be reduced through cross-institution client verification, and at the same time increase monitoring and analysis effectiveness.

Data management

In the future, users will have the ability to manage and sell the data their online activity generates. Because it can be easily distributed in small fractional amounts, Bitcoin — or something like it.

Land title registration

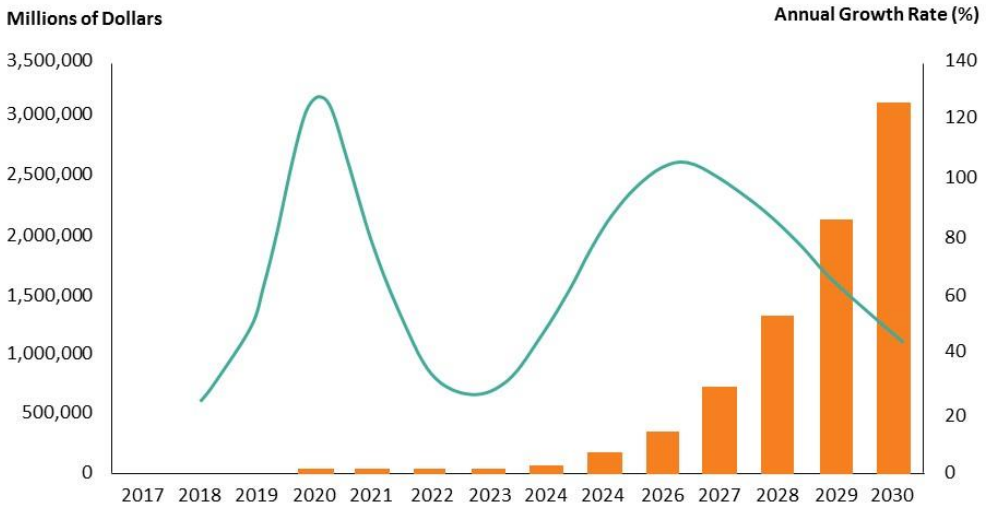
AsPublicly-accessible ledgers, blockchains can make all kinds of record-keeping more efficient. Property titles are a case in point. They tend to be susceptible to fraud, as well as costly and labour intensive to administer.

Stock trading

When executed peer-to-peer, trade confirmations become almost instantaneous. This means intermediaries — such as the clearing house, auditors and custodians — get removed from the process.

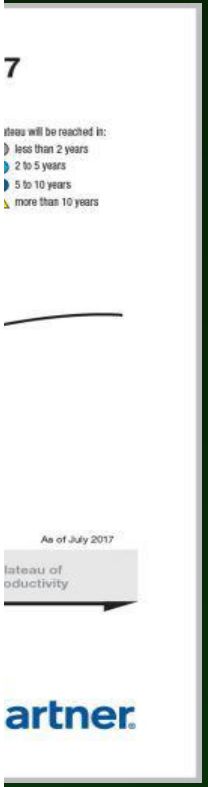
The Future

Forecast: Blockchain Business Value, Worldwide 2017-2030

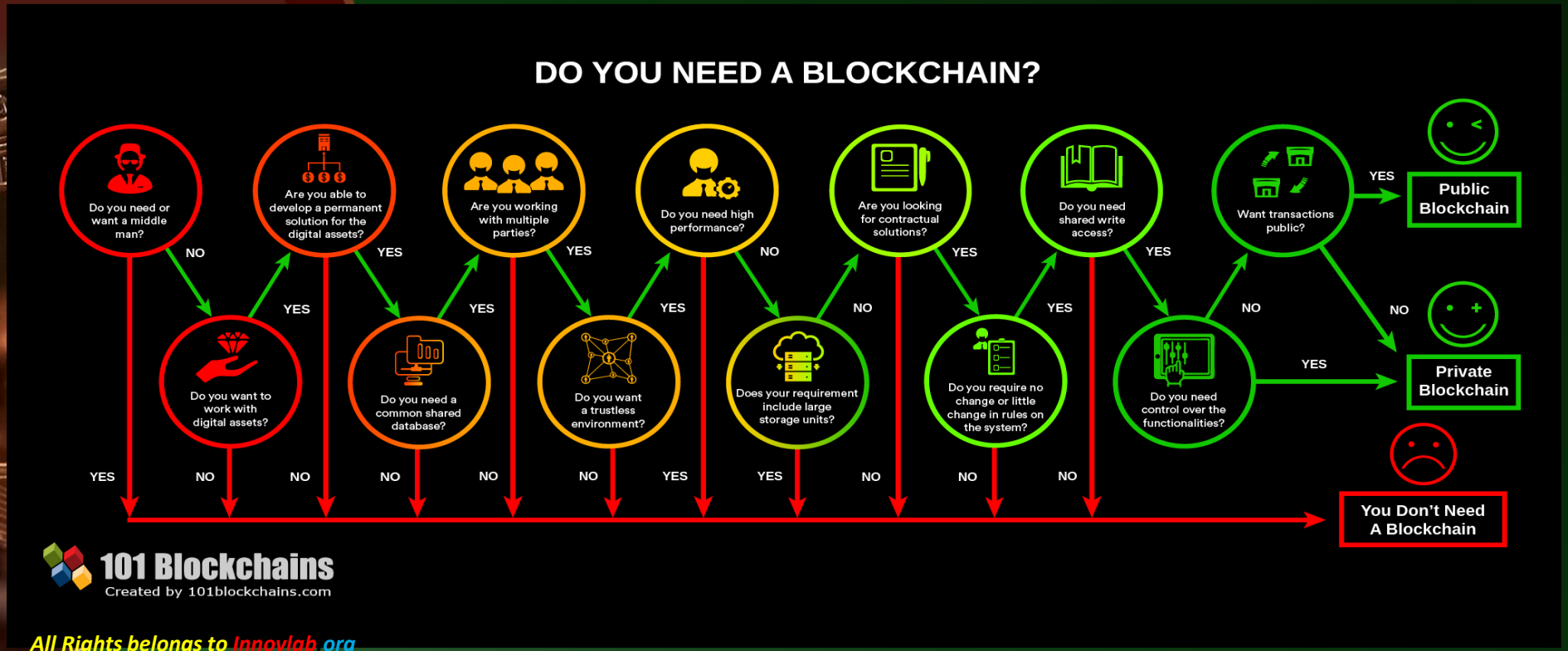


Source: GARTNER (MARCH 2017)

KRYPTO GRAPHE



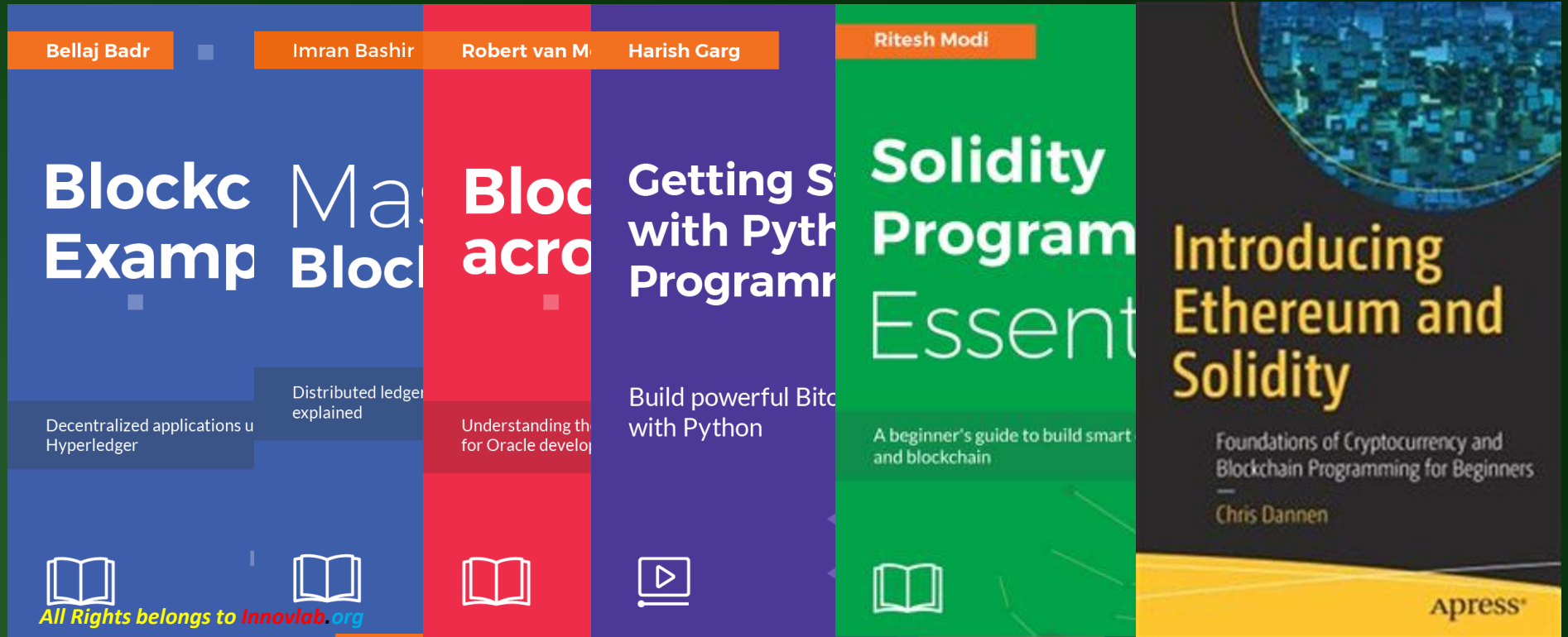
Are Your industry needs Blockchain



BLOCKCHAIN INNOVATION LAB

Some Useful Books

Some Useful Books



BLOCKCHAIN INNOVATION LAB

Some Useful Courses

PRINCETON UNIVERSITY coursera

Bitcoin and Cryptocurrency Technologies

KHANACADEMY

Free Blockchain Course

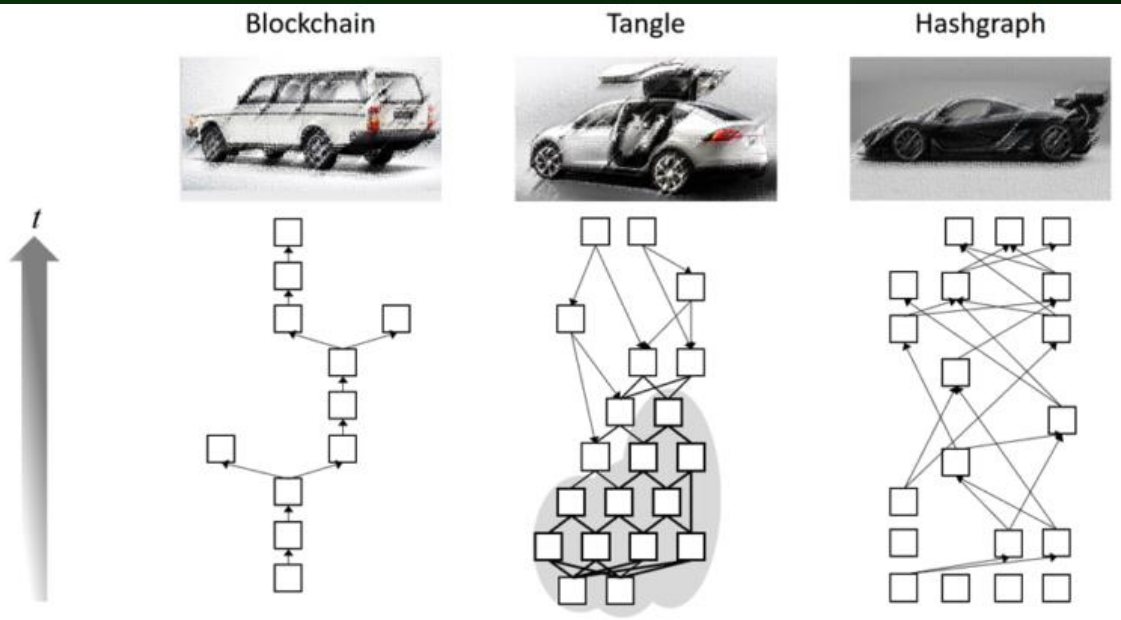
HYPERLEDGER

THE LINUX FOUNDATION

developerWorks COURSES
developer.ibm.com/courses

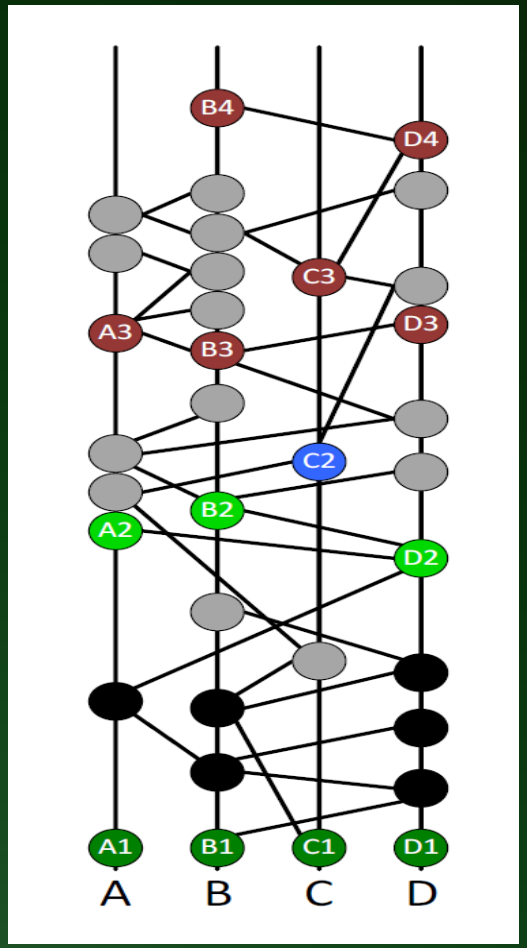
Learning path
IBM Blockchain for developers

Blockchain vs Tangle vs Hashgraph

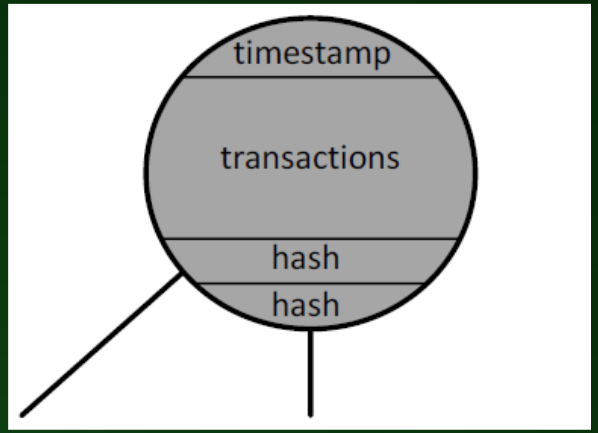


	Blockchain	Tangle	Hashgraph
Technology	Block chain	Directed acyclic graph	Directed acyclic graph
Copyright	Open source	Open source	Patented
Consensus	Proof of Work: SHA256-Hash	Proof of Work: check of Tangle tip	Virtual voting
Openness	Public ledger	Public ledger	Private ledger
Applications	Bitcoin	Iota	Swirlds
Efficiency (tps)	3-4	500-800	> 250,000

Hashgraph



- Gossip Protocol
- Event
- Witness
- Famous Witness
- Round Received



Any Question?

BLOCKCHAIN INNOVATION LAB

Naghipourfar

Naghipourfar

Naghipourfar

M.Naghipourfar