TOPICS

- Bitcoin
- Blockchain
- Technical Aspects
- Altcoins and Monetary Aspects
- Non Monetary Applications
- Blockchain and Edge Computing in Industrial Automation

PARTICIPANT EXPOSURE

How many of you:

- Have heard of Bitcoins & Blockchain
- Own cryptocurrency? Or mine cryptocurrencies ?
- Feel you understand the underlying blockchain technology?
- Feel you know the difference between "regulated" & "trust economy"?
- Are involved in projects that involve blockchain technology implementation or related activities?

LET'S DISCUSS MONEY FIRST

1) Why don't you trust an e-mail with a scanned paper bill ?

Because you need a validating entity of the transaction

2) What is a ledger in Accounting?

Just a table of numbers

3) Why is an inanimate number important?

Because of exchange value

4) Why can't you fake your bank account or print your own money?

Government backed, legally backed Monetary system.

5) How can you claim that you have "money"?

Because a bank (or organization) says that you do!

LET'S DISCUSS MONEY FIRST

* **Money (Definition)** is any item or **verifiable** record that is **generally accepted** as payment for goods and services and repayment of debts **in a particular country** or **socio-economic context**

* **What is 'Fiat Money'** (fiat = latin for "let it be")

Historically, most currencies were based on physical commodities such as gold or silver, but fiat money is based solely on the faith and credit of the economy. (collapse of the Bretton Woods system in 1971, when the United States ceased to allow the conversion of the dollar into gold). Fiat money is currency that a government has declared to be legal tender, but it is **not backed by a physical commodity**. The value of fiat money is derived from the relationship between supply and demand rather than the value of the material that the money is made of.

PORTABLE-DURABLE-DIVISIBLE-SCARCE-LIMITED SUPPLY

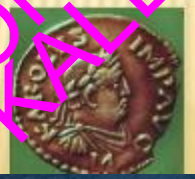
DEFINITION OF MONEY

- Money is any commodity that satisfies the following:
  - Medium of exchange (item accepted for exchange)
  - Store of value (value stored over time)
  - Unit of account (common measure of goods/services)



INTRODUCTION OF COINS

- Croesus, king of Lydia, created the first gold and silver coins in 561 B.C.
- Charlemagne standardized Medieval coins when he conquered most of Europe in 800 A.D.
- In 806 A.D., the Chinese started issuing paper currency, but it led to inflation.


PAPER MONEY

- In Europe during the 1600's, goldsmiths's notes can be used as evidence of ability to pay. It mark the first use of banknotes in England.

US DOLLAR

- The colony of Massachusetts was the first colony to issue paper currency in the US.
- When George Washington was president, the Spanish peso was used. He assigned Benjamin Franklin and Alexander Hamilton to establish a money supply for the new country.
- During the Revolutionary War, congress issued "Continentals". Due to oversupply, they were worthless.

MONEY IN COLONIAL AMERICA

- Gunpowder, musket balls, corn, and hemp served s commodity money. It was used to settle debts and make purchases.
- Some colonies established fiat monies such as wampum (shells used by Narragansett Native Americans)

WHERE IT ALL STARTED

Blockchain technology was first introduced in a whitepaper entitled: "Bitcoin: A Peer-to-Peer Electronic Cash System," by Satoshi Nakamoto in 2008.

- No reliance on trust
- The system works without a central bank or single administrator
- First solution to "double spending problem"
- First implementation of a Blockchain
- Digital signatures / Peer-to-peer network/ Proof-of-work
- Public history of transactions
- Honest, independent nodes control majority of CPU computing power
- Nodes vote with CPU computing power
- Rules and incentives enforced through consensus mechanism

https://bitcoin.org/bitcoin.pdf

BLOCKCHAIN = THEORY

BITCOIN = FIRST APPLICATION

PRECURSORS TO BITCOIN (DIGITAL CASH)

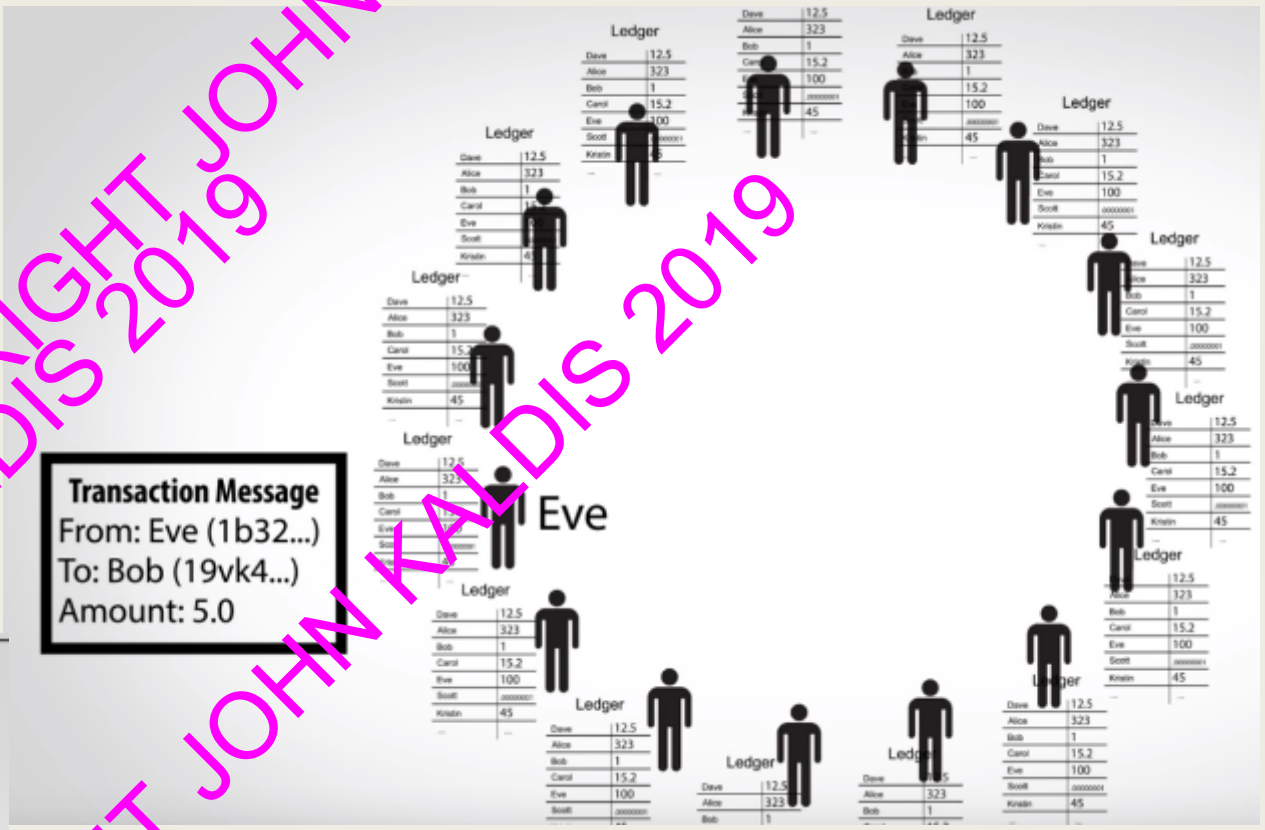
- Hashcash (1997) Adam Back
  - Proof-of-work system to limit email spam
  - SHA-1 hash of the header
- B-money (1998) Wei Dai
  - Public keys identify pseudonyms
  - Broadcast solution to computational problem
  - Arbitrator and fine schedule
  - Broadcasted subset account servers with bail
- BitGold (2001-2005) Nick Szabo
  - Public challenge string of bits
  - Client puzzle functions
  - Securely timestamped

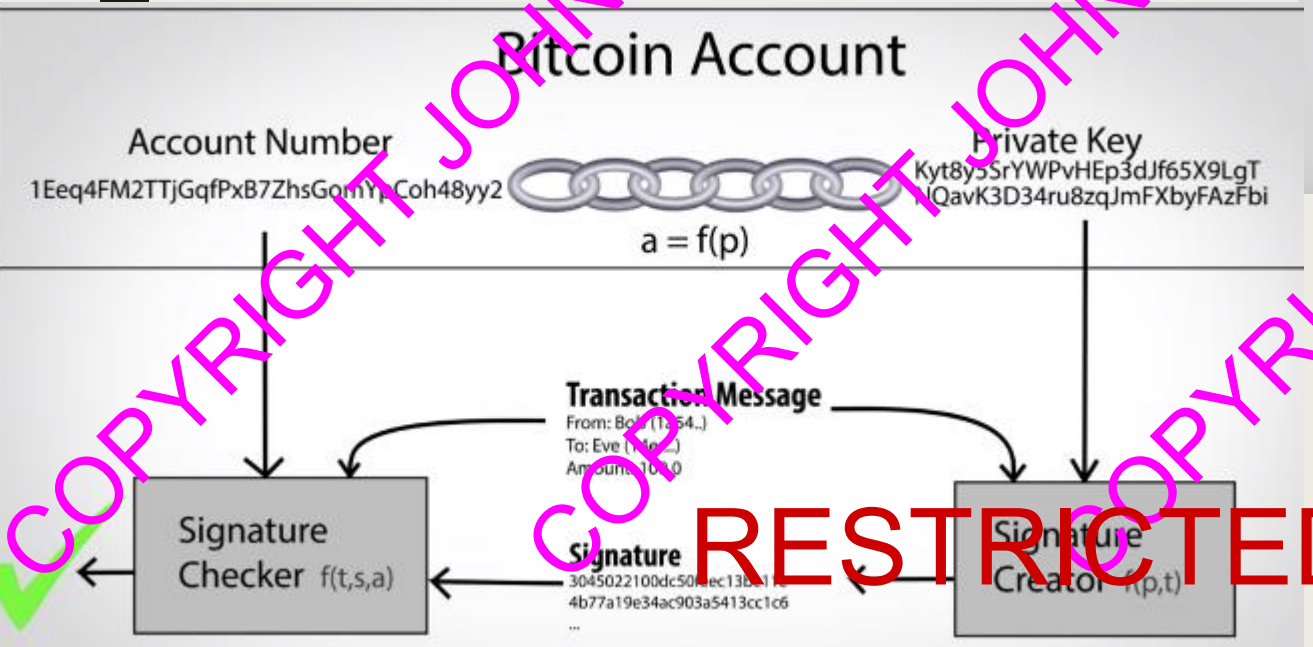
INTRO

- How Bitcoin Works in 5 Minutes (Simple Technical)
- https://www.youtube.com/watch?v=l9jOJk30eQs

Build your own Blockchain

All keep a synced version of a ledger

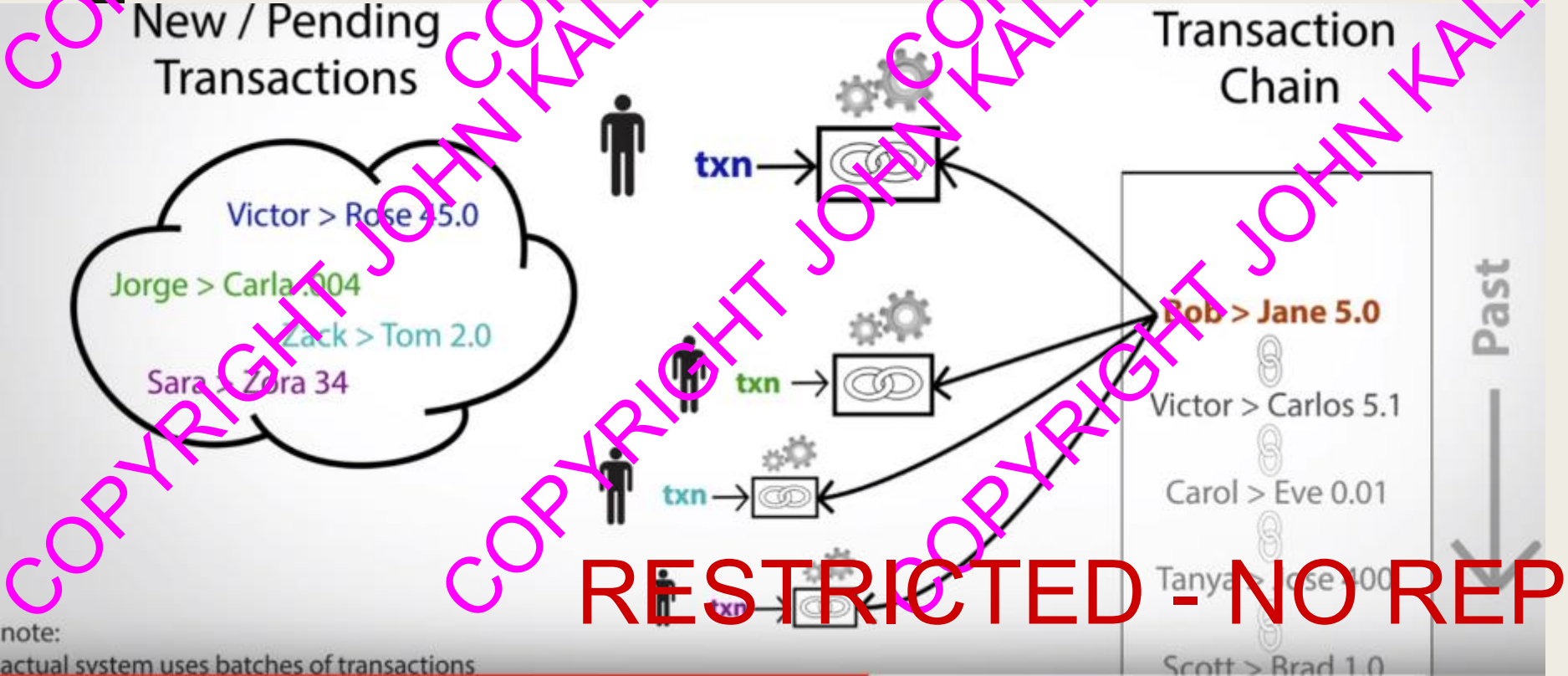




- No central coordinating and validating authority (Central Bank)
- Prevent other people spending your money through cryptography / signature

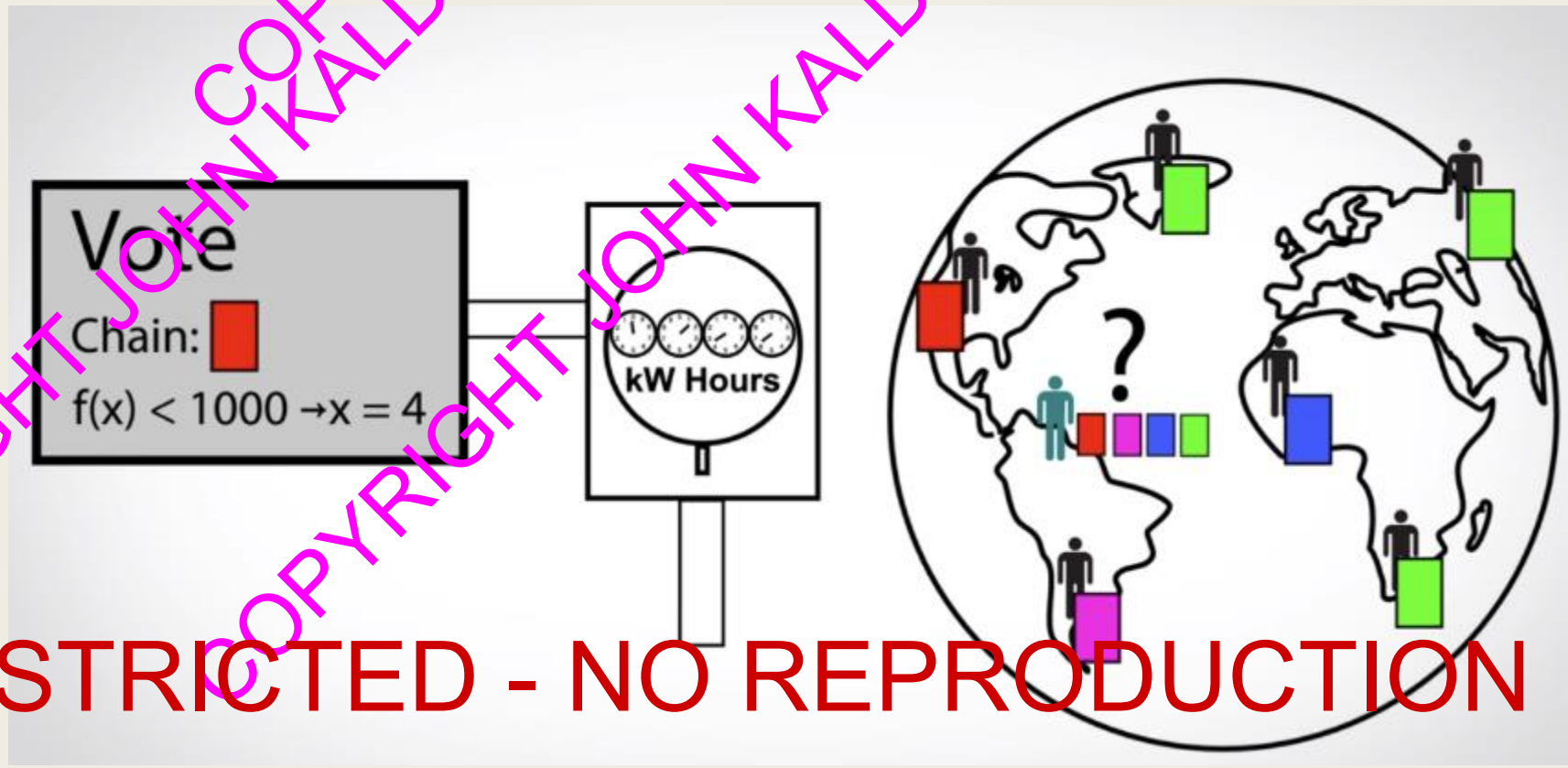
Transaction Order to avoid Double Spending

- A “digital / Mathematical lottery is held among “participants” to choose which transaction is added next
- The “puzzle” is an **irreversible** cryptographic function (HASH), which also gets input from “previous transactions” (linking to the chain) and tries to reach a “threshold”
- Finding solutions is **hard**. Checking solutions is **easy**.



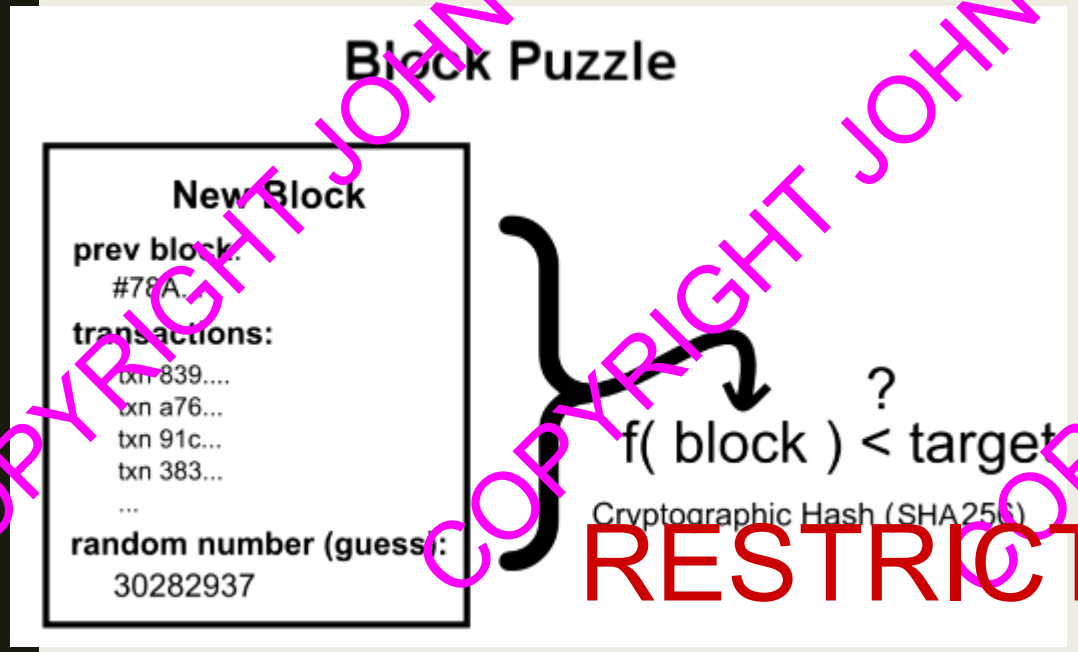
Consensus – Trust the Majority

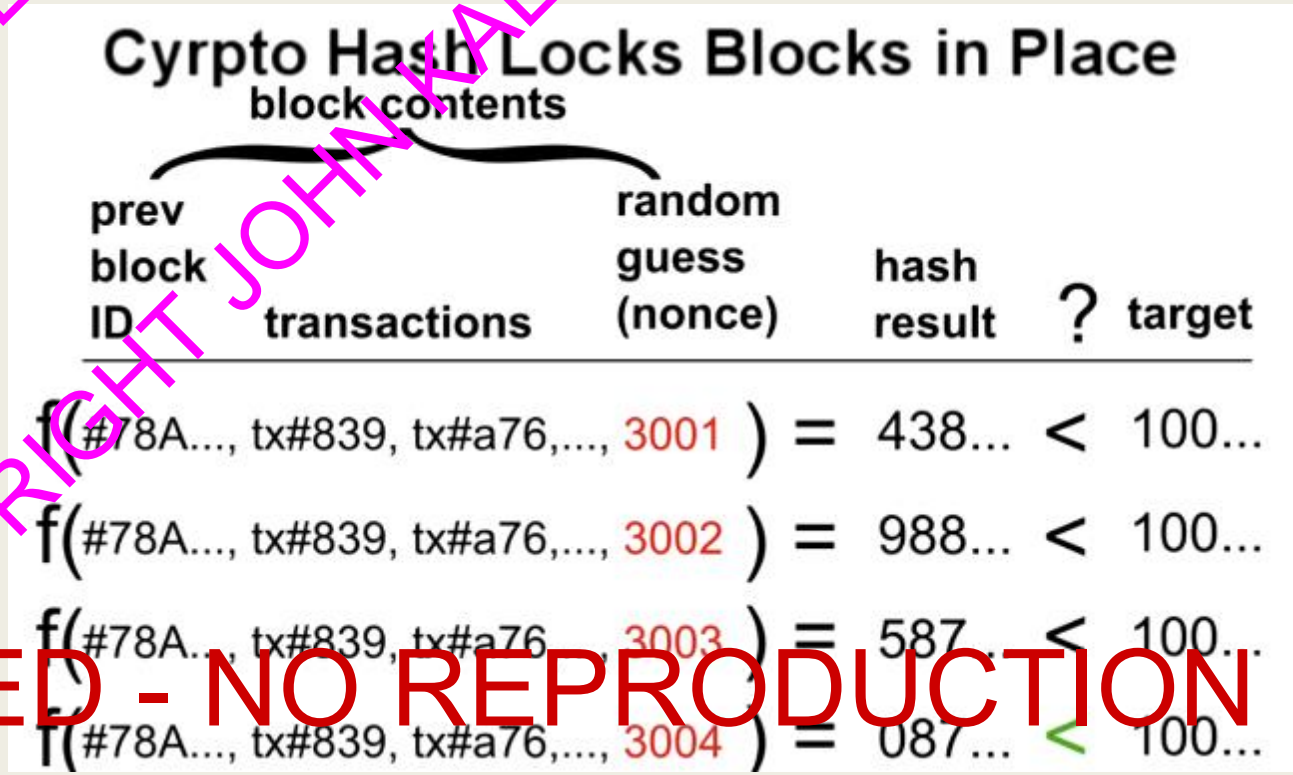
- Which version of the ledger from all “participants” should you trust? The most common
- How do you ensure someone does not disseminate millions of copies of a false ledger? Cost to “vote” through immense computing power required to outvote others (not worth it costwise)
- No need for “trust”. Currently 1 block requires 100 Billion Giga-Hashes to be solved!



The Hashing “Puzzle”

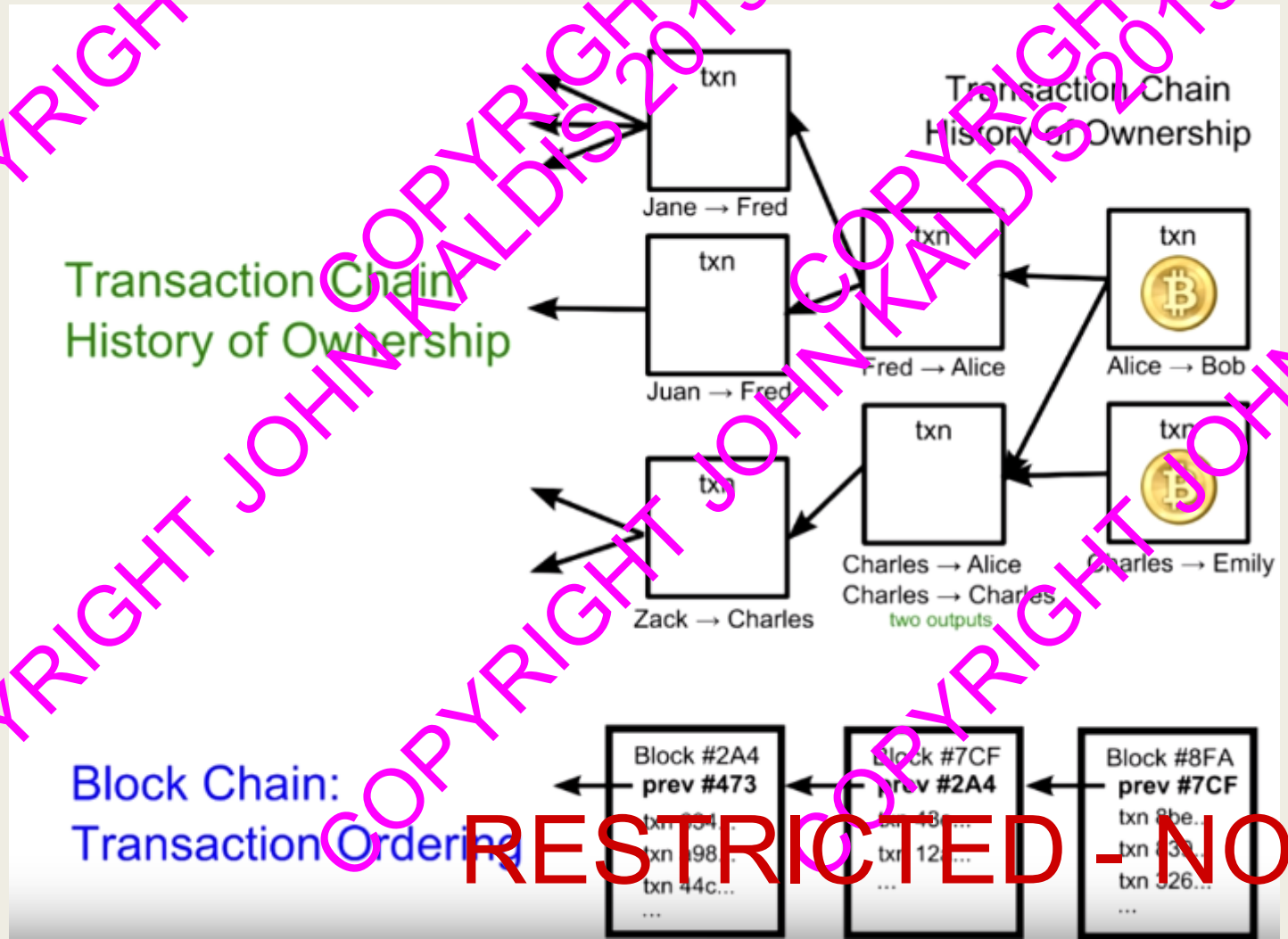
- Bitcoin uses SHA256 as hashing function. Only random guesses work.
- It takes years for one computer to find a solution but all together globally take approximately **10 minutes.**
- When computers get “stronger” through the years, we make the problem “harder” to keep the 10 minutes constant! (Lower the threshold)
- The previous block reference is part of the input of the next “puzzle” hence no blocks can be substituted by “thieves”





Block + Chain

- We process transactions in “blocks” and link them together in a “chain” (Hence it is called **blockchain**)



How does crypto money get “created”

- Every time someone wins the “lottery” to pick the next transaction in the chain, they are awarded money (out of thin air)
- The main purpose of “mining” though is to ensure that all ledger “agree”
- In the year 2140 no more money will be created and participants will be paid on fees added on to transactions
- Predefined supply of money at a “constant rate” lead to deflation!

Blockchain / Transaction Recap

- **A blockchain is a globally shared, transactional database.**
- A distributed database that maintains a list of records. (Simple).
- This means that everyone can read entries in the database just by participating in the network.
- If you want to change something in the database, you have to create a so-called transaction which has to be accepted by all others.

Peer to Peer Network

Every single person on the network has a copy of the ledger
There is no single centralized original copy

Useful Notions

- Double Spending problem
- Order of Transactions
- Signature
- Block
- Trustless – Distributed trust consensus
- proof of work effort
- Everybody can see the transaction (actually a code not a name)
- Voting tally for the Blockchain
- Hashing functions
- Reference Inputs before you spend outputs

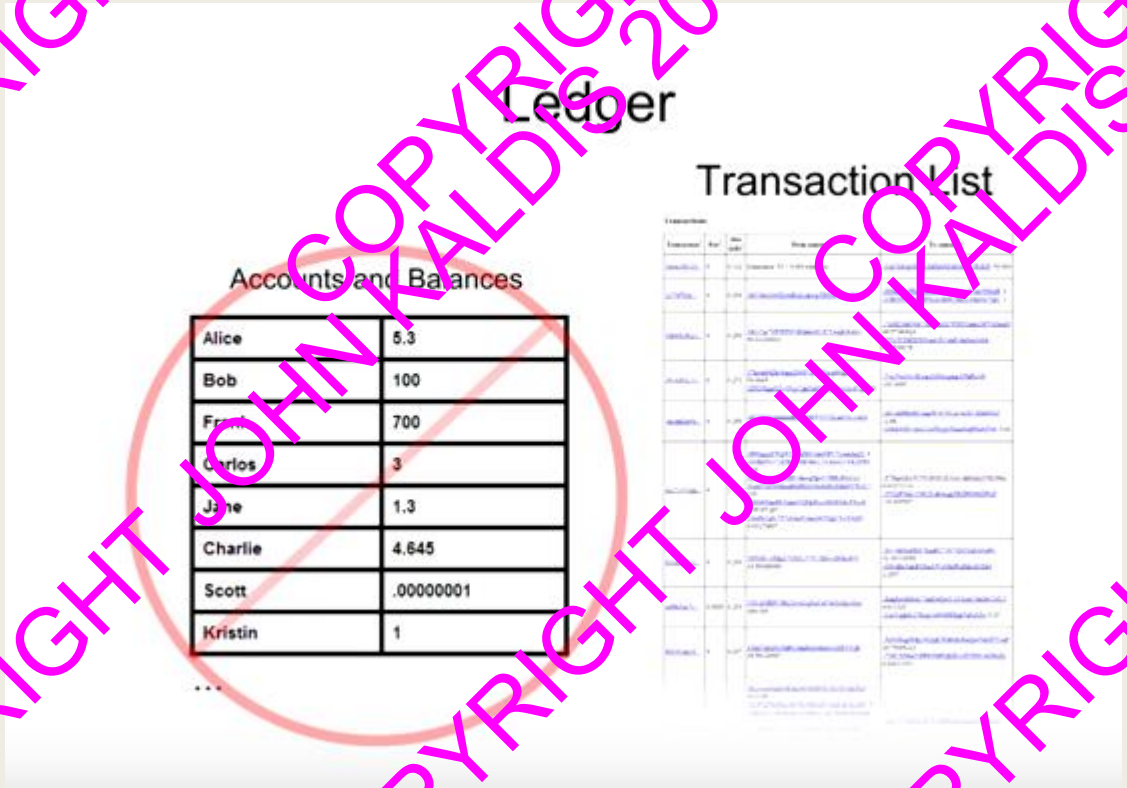
Blockchain / Transaction Recap

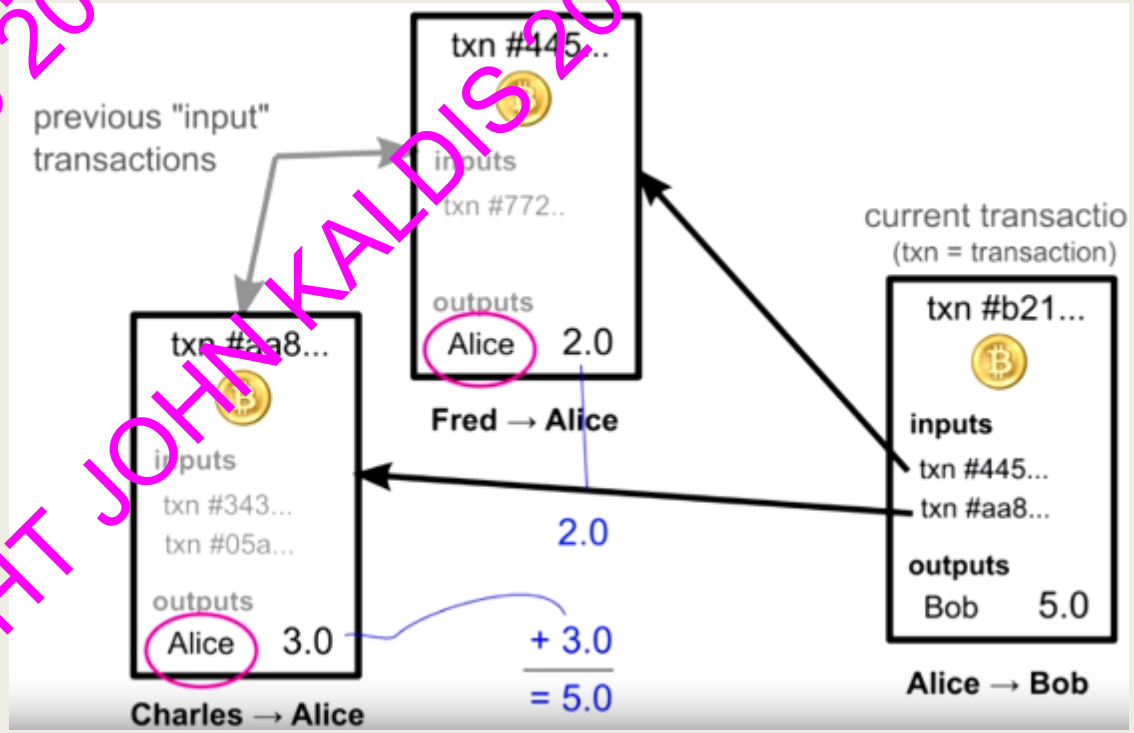
- The word transaction implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied.
- Furthermore, while your transaction is applied to the database, no other transaction can alter it.
- Each Block contains history of every block before it

Blockchain / Transaction Recap

- Furthermore, a transaction is always cryptographically signed by the sender (creator).
- This makes it straightforward to guard access to specific modifications of the database.
- In the example of the electronic currency, a simple check ensures that only the person holding the keys to the account can transfer money from it.
- Every transaction is linked to a unique cryptographic signature.
- Easy to verify and nearly impossible to falsify.

Unlike Traditional Banks
No Balances
Full Transaction History





to send Money (output) you need to reference previous transactions where you acquired it (inputs)

How to send money

- Inputs are consumed completely
- You get “change” back

How to send money

- You send money to the “public key” (the address) of someone
- You need a digital signature to unlock and spend funds

What is a Cryptocurrency Wallet?

- a software program that stores private and public keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance
- Unlike traditional 'pocket' wallets, digital wallets don't store currency. They are essentially signing off ownership of the coins to your wallet's address
  - *Desktop/Mobile: They are only accessible from the single computer in which they are downloaded. Private but vulnerable to hacks and virus (All money lost)*
  - *Online: wallets run on the cloud and are accessible from any computing device in any location. Vulnerable to hacking.*
  - *Hardware: They store a user's private keys on a hardware device like a USB.*
  - *Paper wallets: are an offline cold storage method of saving cryptocurrency. It includes printing out your public and private keys on a piece of paper which you then store and save in a secure place. The keys are printed in the form of QR codes which you can scan in the future for all your transactions.*

The GENESIS Block – 03 Jan 2009

The first 50 BTC block reward cannot be spent

```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
000000F0  79 62 [illegible]                                  yb[illegible]
00000100  F3 55 04 E5 1[illegible]                          óU.å.[illegible]
00000110  8A 4C [illegible]                                 ŠL[illegible]
```

TECH STUFF

Possible Bitcoin addresses:

1461501637330902918203684832716283019655932542976

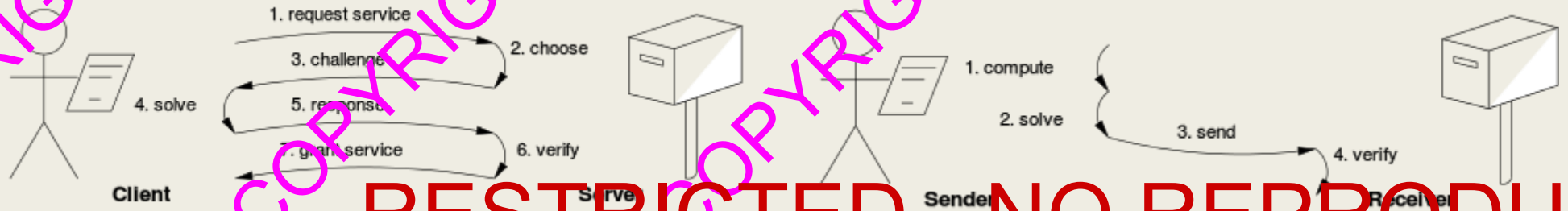
(1.46 x 10^48 or 2^160)

Proof of work

- A key feature of these schemes is their **asymmetry:** the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle or CPU pricing function

- A proof-of-work (PoW) system (or protocol, or function) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer.

- Exists since 1992 (Pricing via Processing or Combatting Junk Mail) , revived as used by Bitcoin “Hashcash” (exists since 1997). Bitcoin based on SHA-256 hash



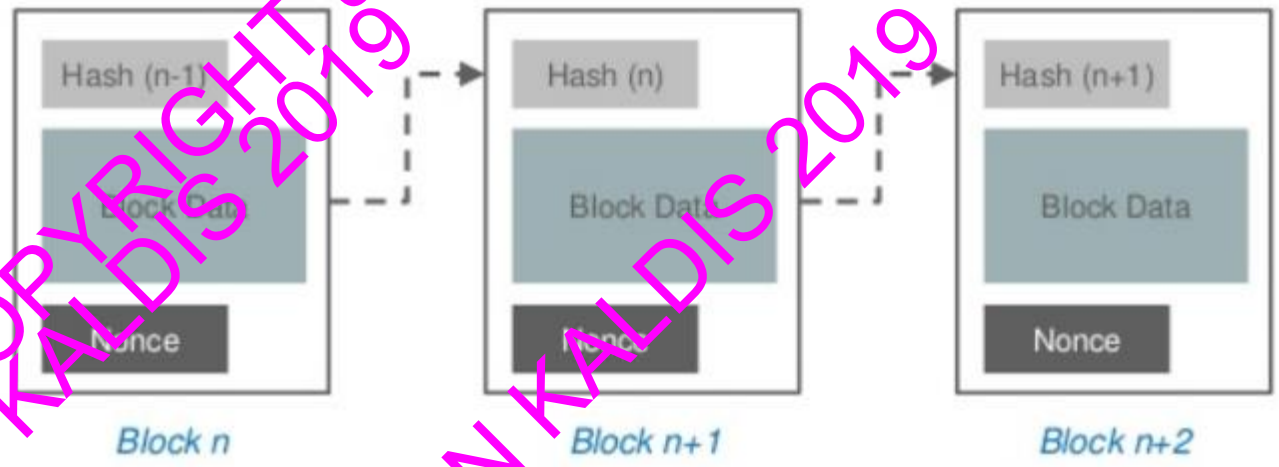
Proof of work

- in Bitcoin double-spend protection is provided by a decentralized P2P protocol for tracking transfers of coins, rather than the hardware trusted computing function used by RPOW.
- Bitcoin has better trustworthiness because it is protected by computation. Bitcoins are "mined" using the **Hashcash proof-of-work** function by individual miners and verified by the decentralized nodes in the P2P bitcoin network.

- Many POW systems require the clients to do useless work, such as inverting a hash function.
- This means that a lot of resources (mainly the electricity that powers the clients' computers) is used only for providing trust in the currency.
- To be more efficient with that resource expenditure, some alternative coins use a POW system where the performed work is **actually useful**. For example, Primecoin requires clients to find unknown prime numbers of certain types, which can have useful side-applications

Proof Of Work

Proof Of Work involves solving a computationally expensive puzzle to add blocks to the Blockchain



Bitcoin has *miners* who validate have to solve a *complex mathematical puzzle* to add a block to the blockchain

Miners search for a specific *nonce* which gives the desired *hash* which is predetermined

* Proof of Work is not needed in Trusted networks

Proof-of-Work: Solution to Byzantine General's Problem

Vote

Attack	Retreat
Attack	Retreat
Attack	

Majority want to attack, so everyone attacks

attack

Crypto & Hash Intro

Hash function:

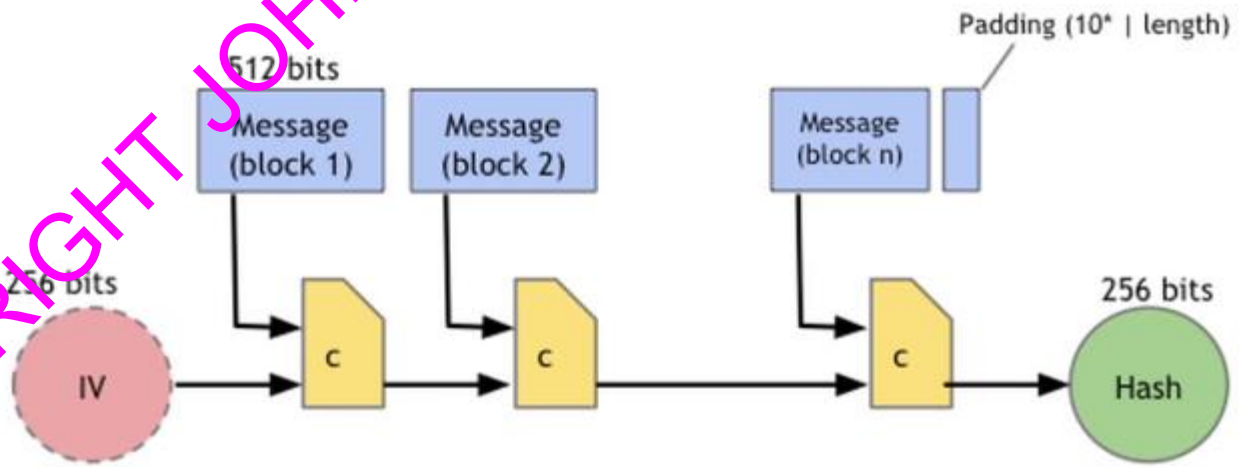
- takes any string as input
- fixed-size output (we'll use 256 bits)
- efficiently computable

Security properties:

- collision-free
- hiding
- puzzle-friendly

a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value

SHA-256 hash function



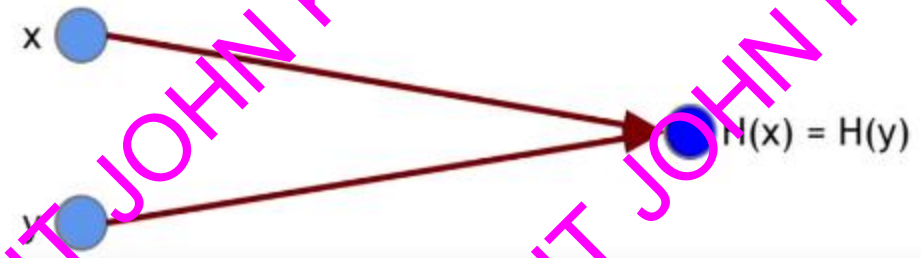
Theorem: If c is collision-free, then SHA-256 is collision-free.

Crypto & Hash Intro

Hash property 1: Collision-free

Nobody can find x and y such that

x != y and H(x)=H(y)



try 2^{130} randomly chosen inputs

99.8% chance that two of them will collide

Hash property 2: Hiding

We want something like this:

Given H(x), it is infeasible to find x.

Hiding property:

If r is chosen from a probability distribution that has *high min-entropy*, then given H(r | x), it is infeasible to find x.

Crypto & Hash Intro

Hash property 3: Puzzle-friendly

Puzzle-friendly:

For every possible output value y,
if k is chosen from a distribution with high min-entropy,
then it is infeasible to find x such that H(k | x) = y.

Puzzle-friendly property implies that no solving strategy is much better than trying random values of *x*.

Intuitively, what this means is that if someone wants to target the hash function to come out to some particular output value *y*, that if there's part of the input that is chosen in a suitably randomized way, it's very difficult to find another value that hits exactly that target.

Hash Pointers & Data Structures

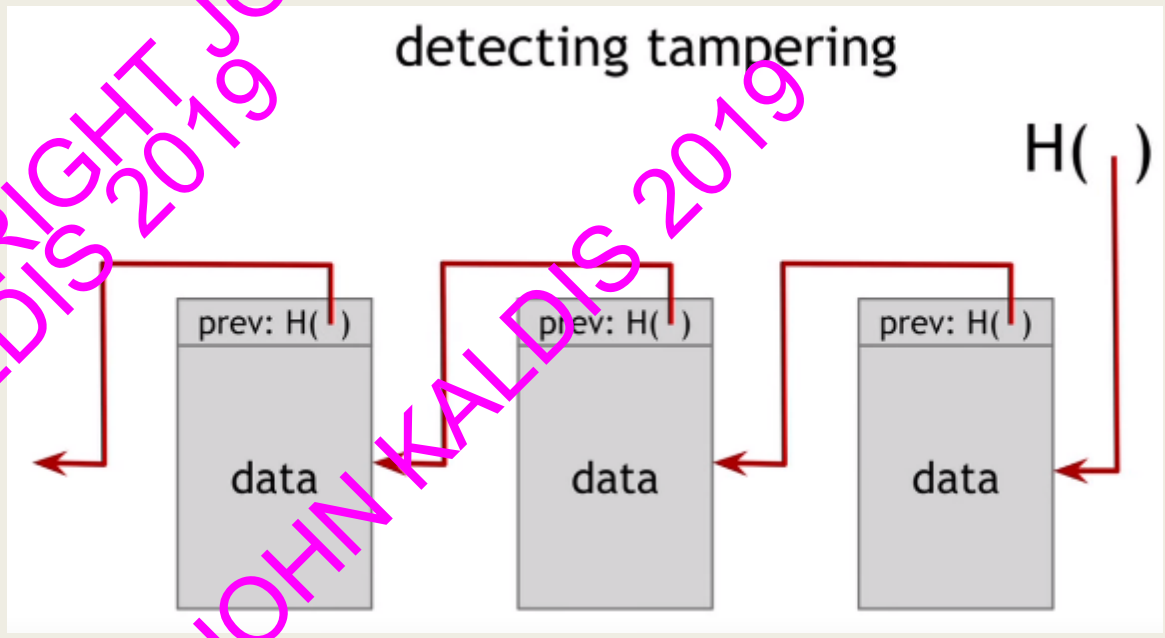
hash pointer is:

* pointer to where some info is stored, and
* (cryptographic) hash of the info

if we have a hash pointer, we can

* ask to get the info back, and
* verify that it hasn't changed

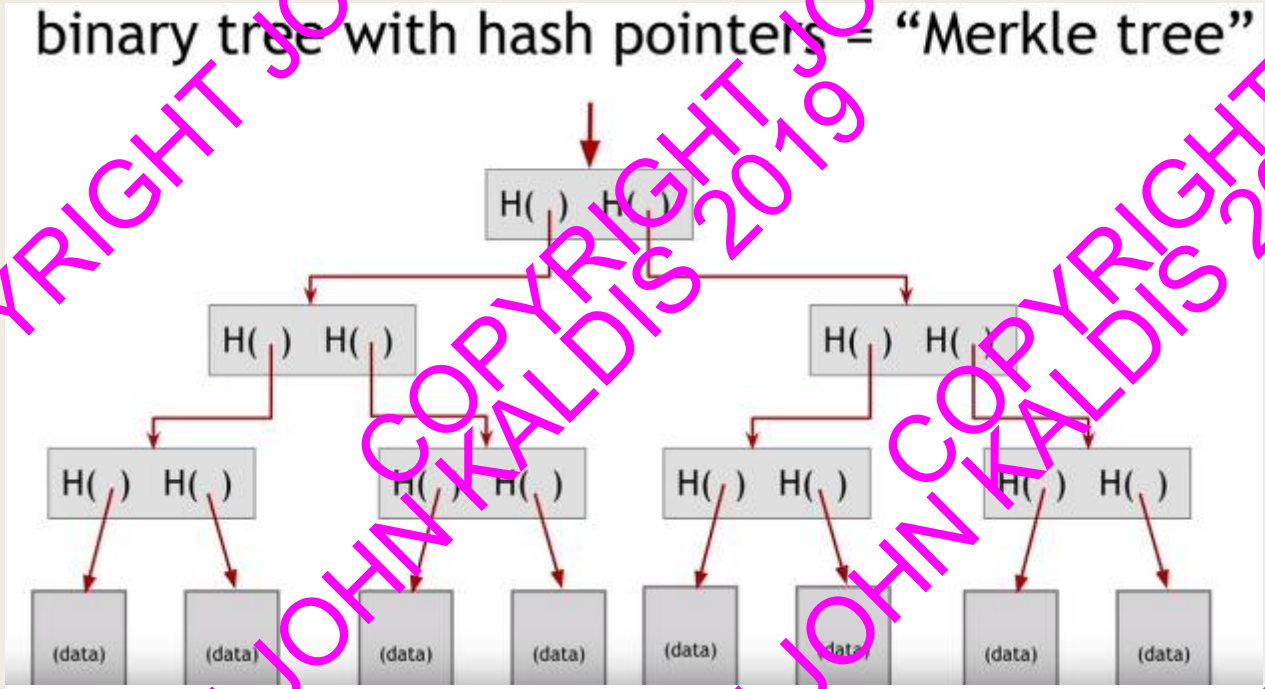
Where is it stored ?
What value did it have the last time we saw it ?

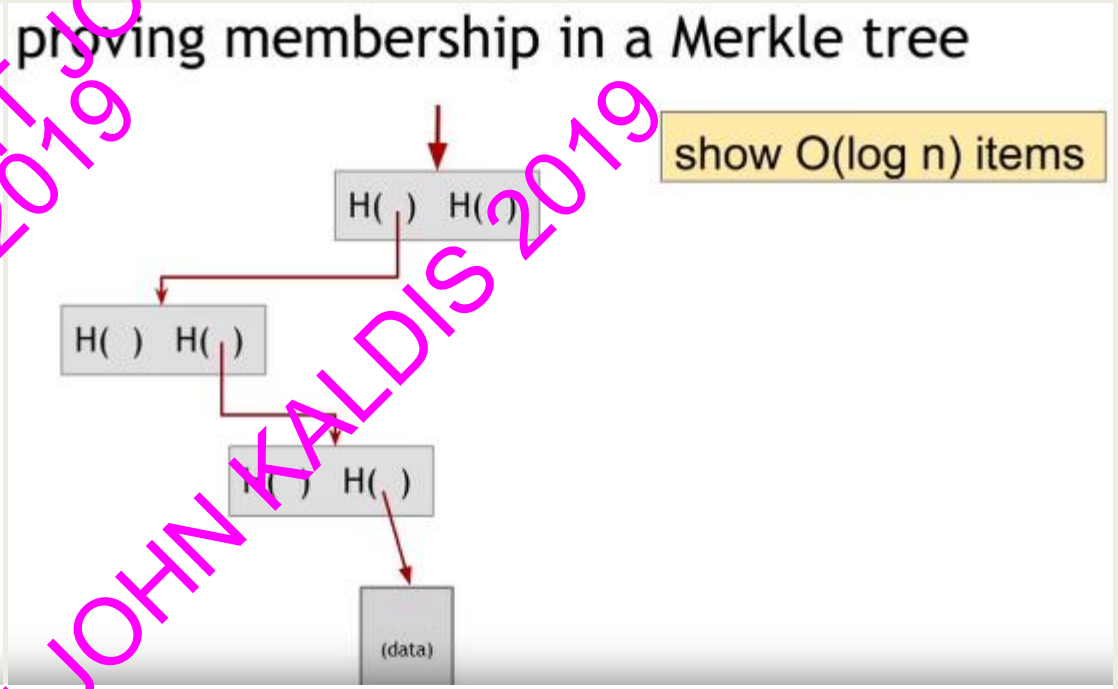


Keep adding data in blocks
Prohibit alteration of previous data !

*Because of “Collision Free Property”

Hash Pointers & Data Structures





If you want to prove that you are a “member”, you only have to show few data.

So a Merkel tree is a binary search tree built with hash pointers, and we can do “logarithmic time “membership proofs

Hash Pointers & Data Structures

Digital Signatures

```
(sk, pk) := generatekeys(keysize)
        sk: secret signing key
        pk: public verification key

sig := sign(sk, message)

isValid := verify(pk, message, sig)
```

Bitcoin uses ECDSA standard

Elliptic Curve Digital Signature Algorithm

Sum Up

- To bring it all together, blockchain could not exist without hashing and digital signatures.
- Hashing provides a way for everyone on the blockchain to agree on the current world state.
- digital signatures provide a way to ensure that all transactions are only made by the rightful owners.
- We rely on these two properties to ensure that the blockchain has not been corrupted or compromised

Bitcoin consensus gives us:

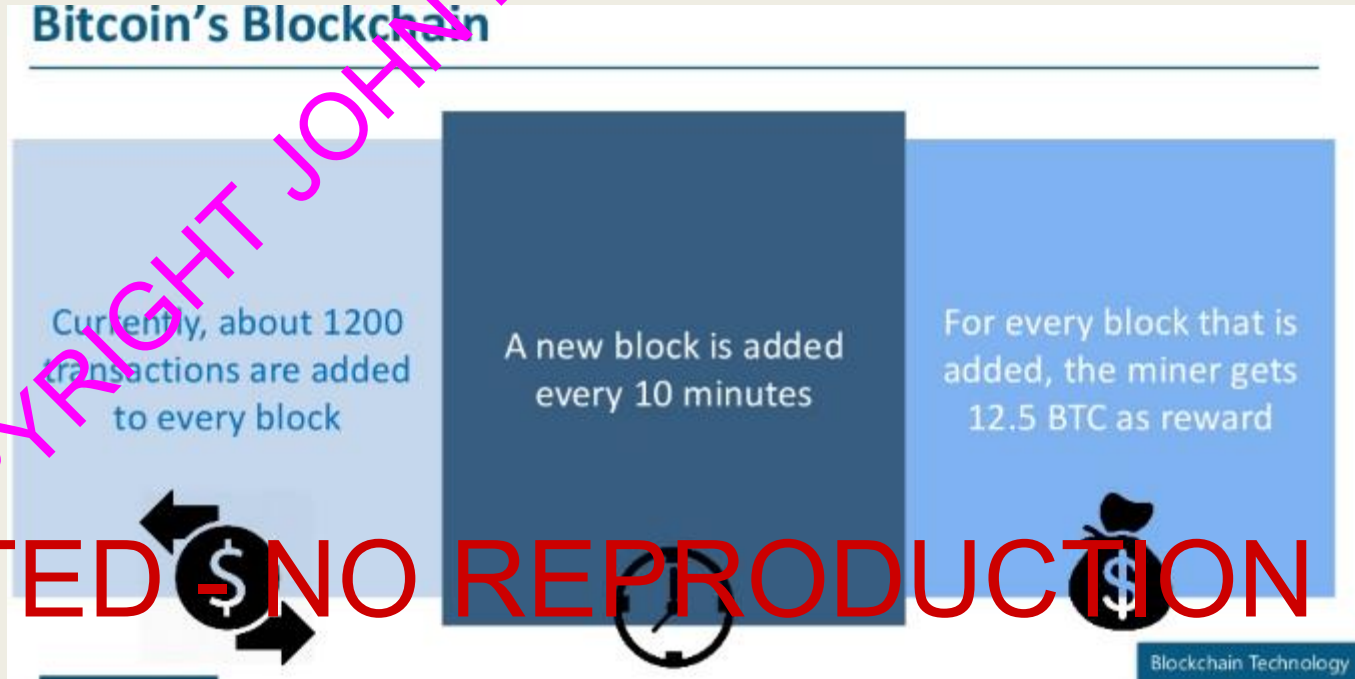
- Append-only ledger
- Decentralized consensus
- Miners to validate transactions

NEXT VIDEO

- Bitcoin Ordering & Mining 10 minutes
- https://www.youtube.com/watch?v=Lx9zgZCMqXE&t=650s

What is 'Bitcoin Mining'

- Bitcoin mining is the process by which transactions are verified and added to the public ledger/ block chain
- Also the means through which new bitcoin are released.
- The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle.
- The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards.
- The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released bitcoin
- The amount of new bitcoin released with each mined block is called the block reward.



Mining – Solving the Hard Problem

Difficulty factor is recalculated every ***2,016 blocks*** *~ every* ***2 weeks***

Difficulty is a measure of how hard it is to find a hash below the target value, a 256-bit number, during PoW

Every two weeks the bitcoin network *difficulty factor* is recalculated to make sure that blocks are found on average *every 10 minutes* despite increasing *hash rates* over time.

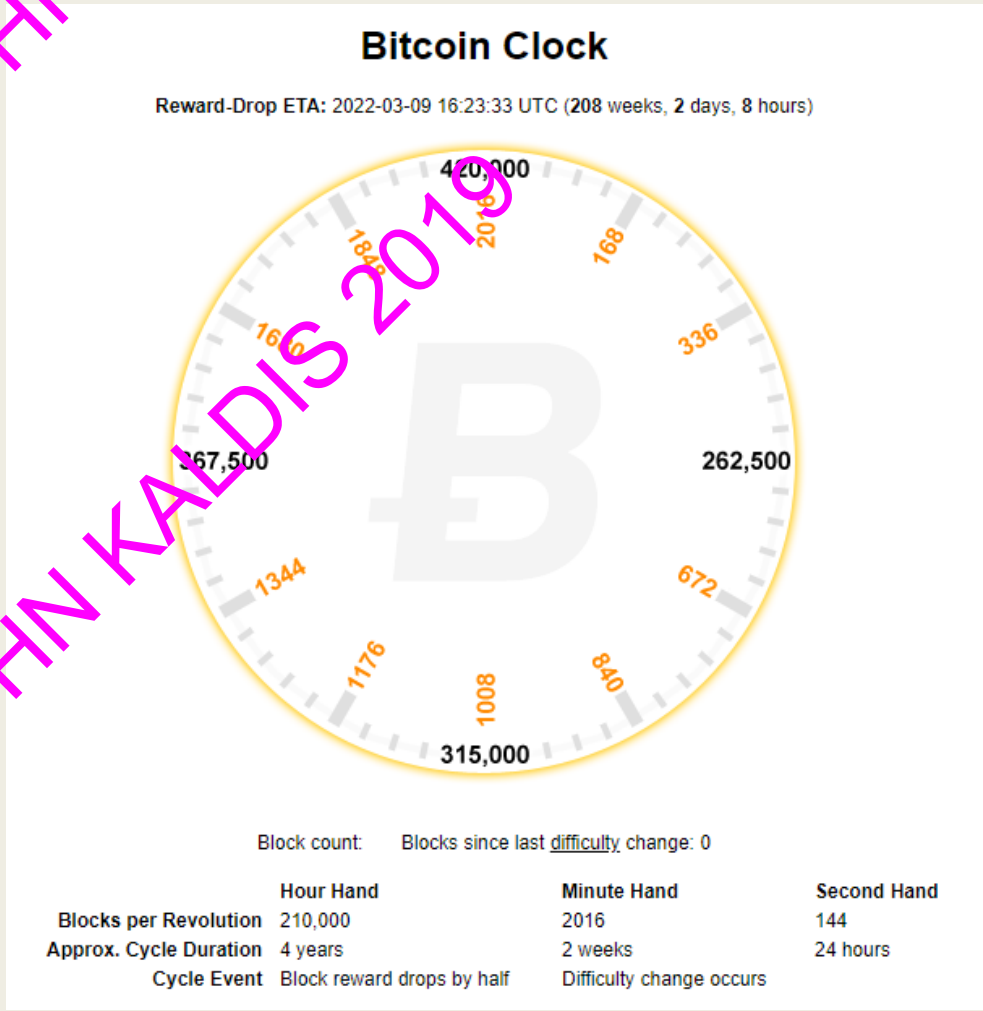
Anyone mining bitcoins has a 'Hash Rate', a measurement of how many math calculations your computer is doing per second

The difficulty almost always goes up which means it becomes progressively harder to mine bitcoins. Bitcoin has become so difficult to mine that the vast majority of miners join a bitcoin *mining pool*.

A mining pool is a way for bitcoin miners to work together for a better chance at finding a bitcoin block

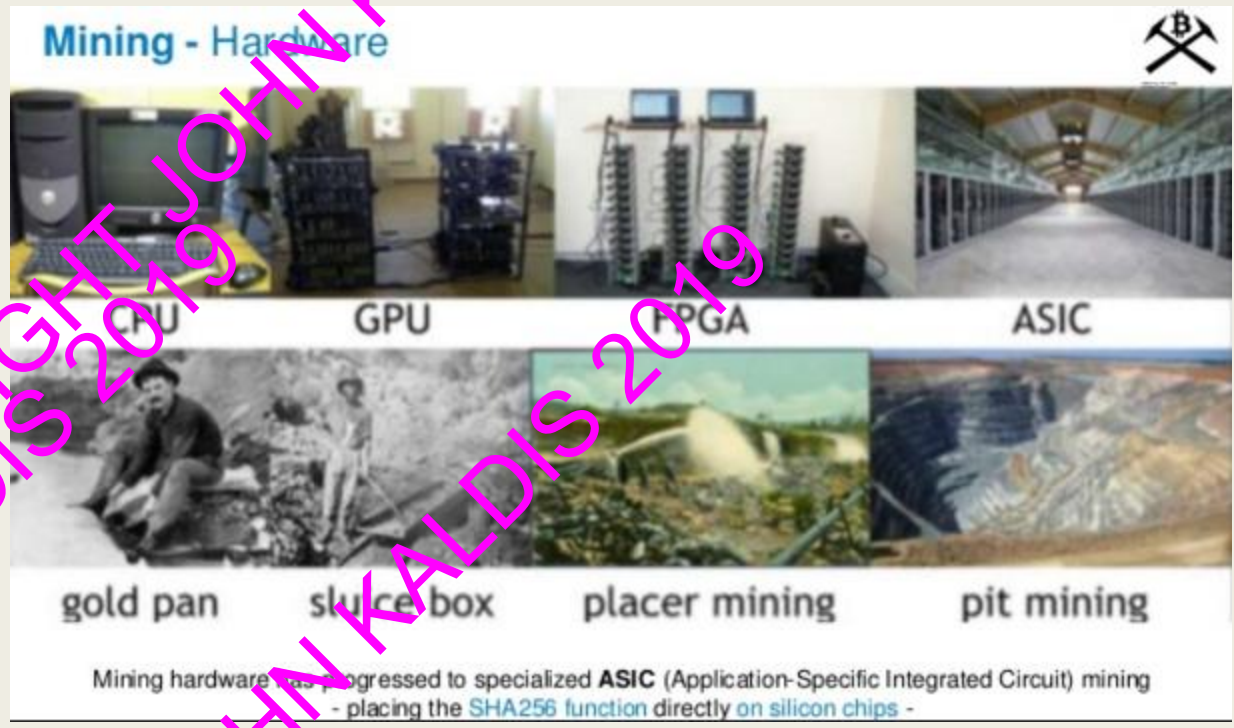
What is 'Bitcoin Mining'

- The block reward is halved every 210,000 blocks, or roughly every 4 years.
- The block reward started at 50 in 2009, is now 12.5, and on 24 May 2020 it will become 6.25
- and will continue to decrease.
- See http://bitcoinclock.com/
- This diminishing block reward will result in a total release of bitcoin that approaches 21 million in 2140

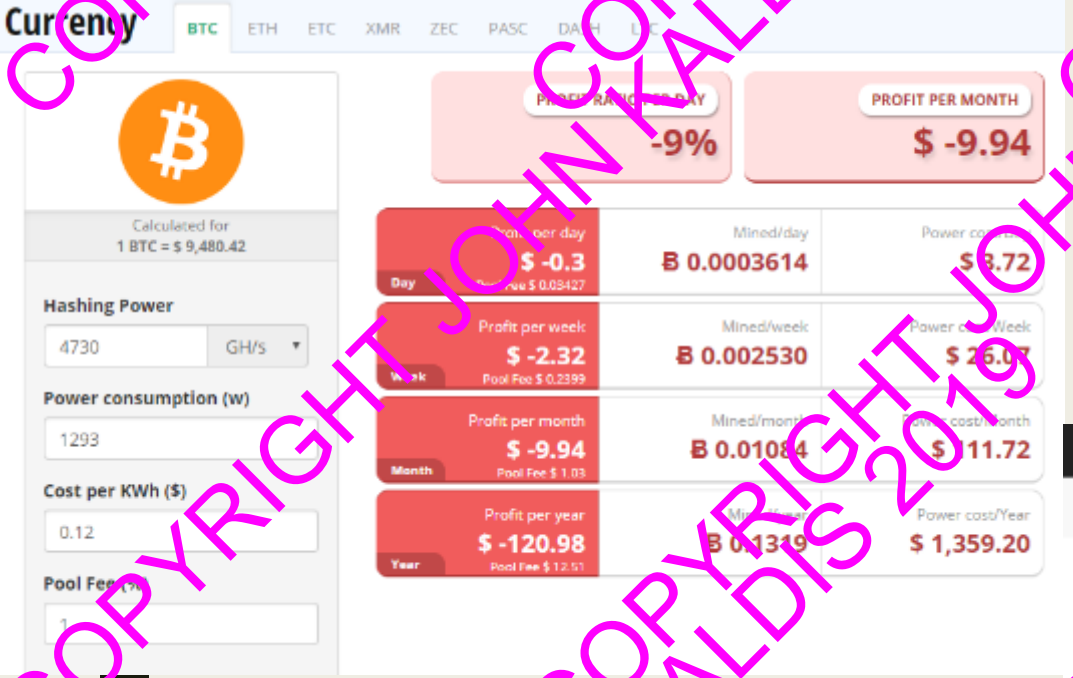


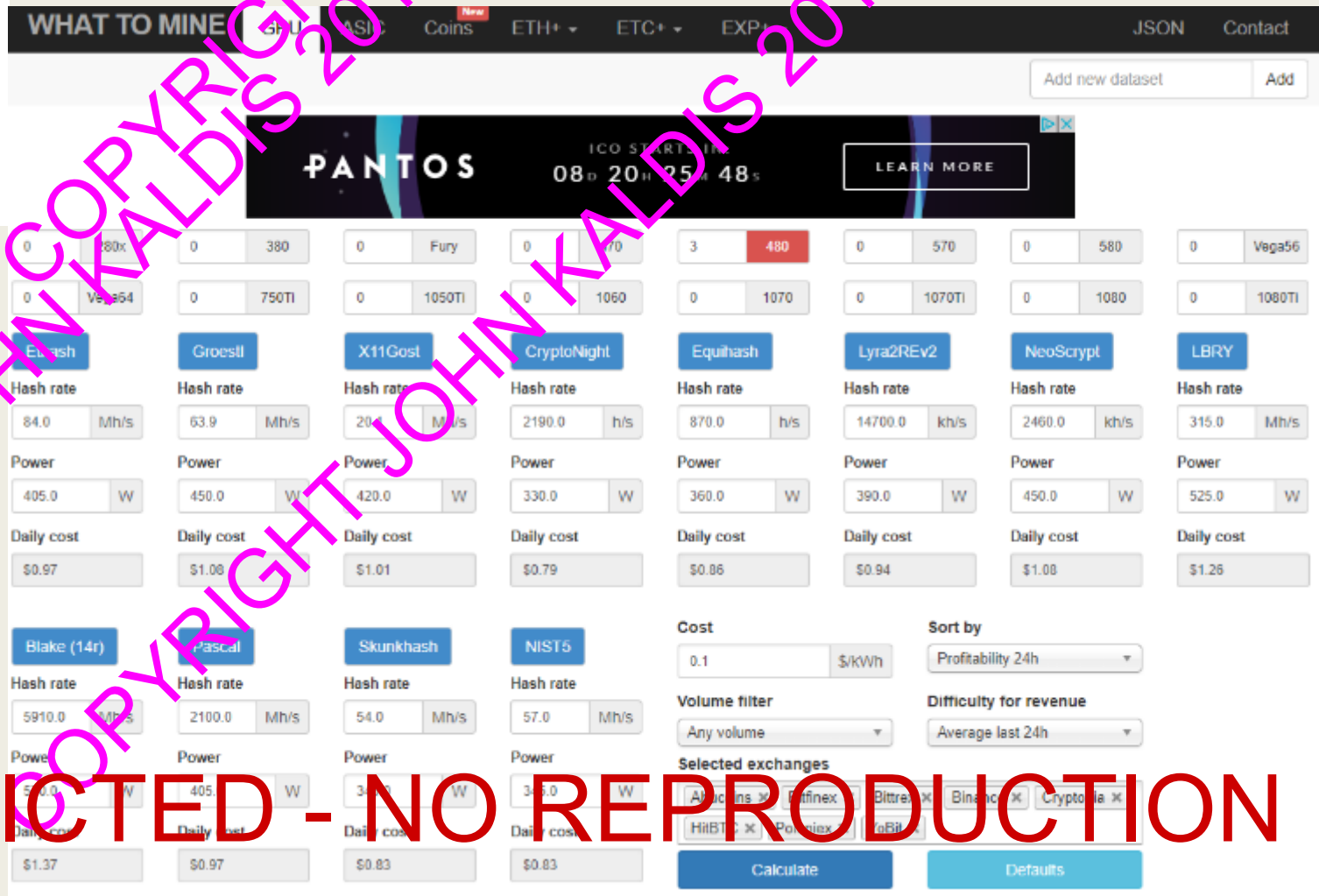
Difficulty increase

- In the earliest days of Bitcoin, mining was done with CPUs from normal desktop computers.
- Graphics cards, or graphics processing units (GPUs), are more effective at mining than CPUs and as Bitcoin gained popularity, GPUs became dominant.
- Eventually, hardware known as an ASIC, which stands for Application-Specific Integrated Circuit, was designed specifically for mining bitcoin. The first ones were released in 2013 and have been improved upon since, with more efficient designs coming to market.
- Mining is competitive and today can only be done profitably with the latest ASICs. When using CPUs, GPUs, or even the older ASICs, the cost of energy consumption is greater than the revenue generated.



Miners switched to alternative crypto-coins

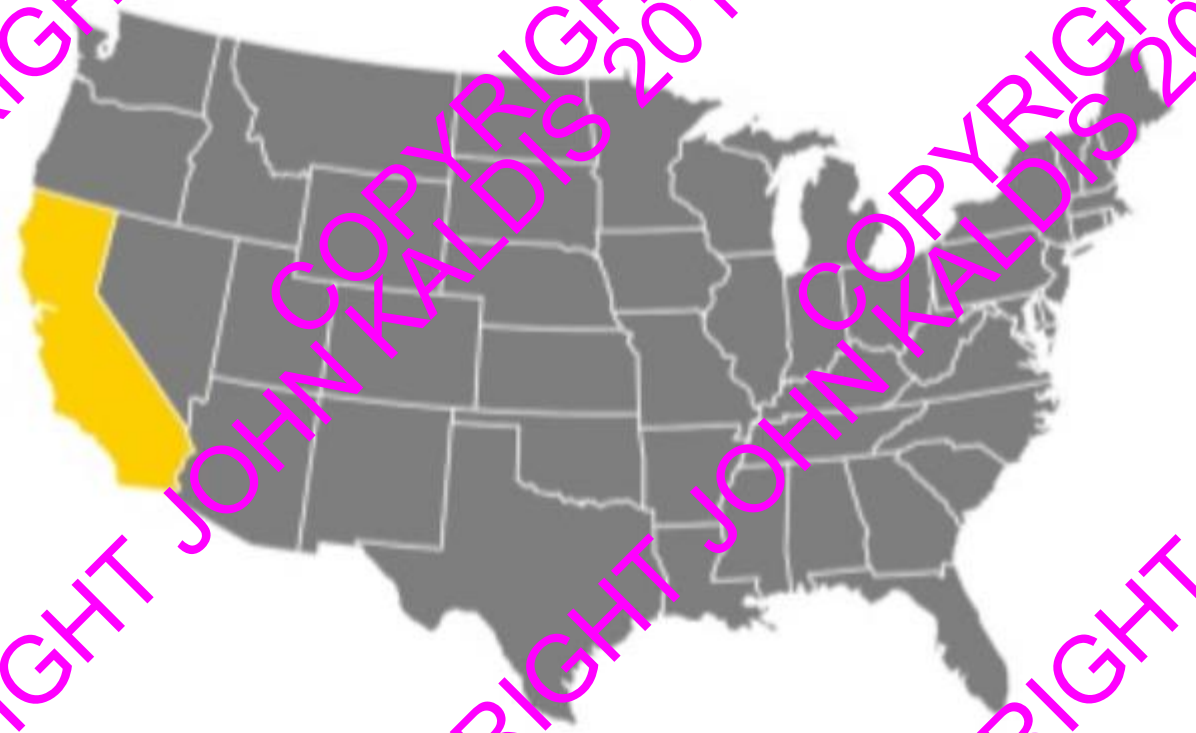




- https://www.cryptocoincharts.info/coins/info claims to be indexing 4,220 cryptocurrencies

Profitability in cryptocurrencies ?

STARTUP FUNDING



More than $1B invested worldwide
in 138 Venture-Capital-backed
bitcoin & blockchain startups

51%

of those are based in Silicon Valley

Altcoins - Tokens

Ethereum

- Cryptocurrency 2.0
- vs namecoin DNS (2013)

Ethereum is a Turing complete blockchain that lets developers create peer to peer applications on top of it easily

Ethereum is an open-source & public blockchain based distributed computing platform

FEATURES

- Currency Issuance
- Decentralized Autonomous Organizations (DAO)
- Smart Contracts
- Smart Property

Smart Contracts are the basic building blocks of Ethereum

Ethereum also provides a cryptocurrency token called "ether"

Vitalik Buterin: Ethereum network will handle 1 million transactions per second

- Solidity for ETHEREUM

- Solidity is a contract-oriented, high-level language for implementing smart contracts.
- It was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM).

- Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.
- A contract in the sense of Solidity is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.

Ethereum Alliance

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.

The Ethereum project was bootstrapped via an ether pre-sale during August 2014 by fans all around the world. It is developed by the Ethereum Foundation, a Swiss nonprofit, with contributions from individuals and organizations across the globe.

www.ethereum.org

Ethereum Tools

Several Ethereum offerings include:

- The Ethereum Wallet, which is a gateway to decentralized applications on the Ethereum blockchain, allowing users to hold and secure ether and other crypto-assets built on Ethereum, as well as write, deploy and use smart contracts
- Design and issue your own cryptocurrency/traceable token
- Kickstart a project with Crowdsale

www.ethereum.org

What is Ether?

- Ether is the crypto-fuel for the Ethereum network.
- Ether is a necessary element – a fuel – for operating the distributed application platform Ethereum. It is a form of payment made by the clients of the platform to the machines executing the requested operations, functioning as the incentive that ensures that developers will write quality applications, and that the network remains healthy.
- The total supply of ether and its rate of issuance was decided by the donations gathered on the 2014 presale.
- Developers who intend to build apps that will use the Ethereum blockchain need ether.
- Users who want to access and interact with smart contracts on the Ethereum blockchain also need ether.

www.ethereum.org

PoS vs PoW

- As a hybrid proof-of-stake (PoS)/proof-of-work (PoW) algorithm, Casper v1 is going to decrease (and eventually end) the profitability for Ethereum miners.
- The release date is estimated to be sometime in ~~2018~~ 2019, 2020 ? Constantinople

With the upcoming hard fork, there could potentially be three forks of Ethereum:

- Ethereum PoS
- Ethereum PoW
- Ethereum Classic

But Ethereum developers have stated that they'll be releasing what they call the "difficulty time bomb"

(increases the mining difficulty exponentially until the chain becomes impossible to mine)

DEFINITION of 'Proof of Stake (PoS)'

- Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to how many coins he or she holds. This means that the more Bitcoin or altcoin owned by a miner, the more mining power he or she has.
- The proof of stake was created as an alternative to the proof of work (PoW), to tackle inherent issues in the latter
- The proof of stake (PoS) seeks to address the issue of computing power and energy needed, by attributing mining power to the proportion of coins held by a miner. This way, instead of utilizing energy to answer PoW puzzles, a PoS miner is limited to mining a percentage of transactions that is reflective of his or her ownership stake. For instance, a miner who owns 3% of the Bitcoin available can theoretically mine only 3% of the blocks

Three "Levels" of Blockchain

1. Storage for digital records
2. Exchanging digital assets (called tokens)
3. Executing smart contracts
   - *Ground rules – Terms & conditions recorded in code*
   - *Distributed network executes contract & monitors compliance*
   - *Outcomes are automatically validated without third party*

Tech Trends 2017, The Kenetic Enterprise, "Blockchain: Trust economy", Deloitte University Press, 2017

- Zcash uses a special proof to secure the network called zk-snark - or proof of construction
- This happens through the use of **zero knowledge proofs**
- Has caused a lot of controversy for its method of distributing the crypto currency. The organisation is not set up as an opensource community but as a Company
- they plan to reward investors and workers in the Company which is by a tax on mining rewards called "Founders reward"

Monero is private

- Monero uses ring signatures, ring confidential transactions, and stealth addresses to obfuscate the origins, amounts, and destinations of all transactions

Monero is untraceable

- Sending and receiving addresses as well as transacted amounts are obfuscated by default. Transactions on the Monero blockchain cannot be linked to a particular user or real-world identity.

QUESTION: Do we want privacy or transparency ?

ripple

The Bank Coin

- Global system of mutual settlements
- Designed primarily for financial institutions
- 34000% increase in 2017

ripple

Fast

Payments settle in 4 seconds.

XRP

4 Sec

ETH

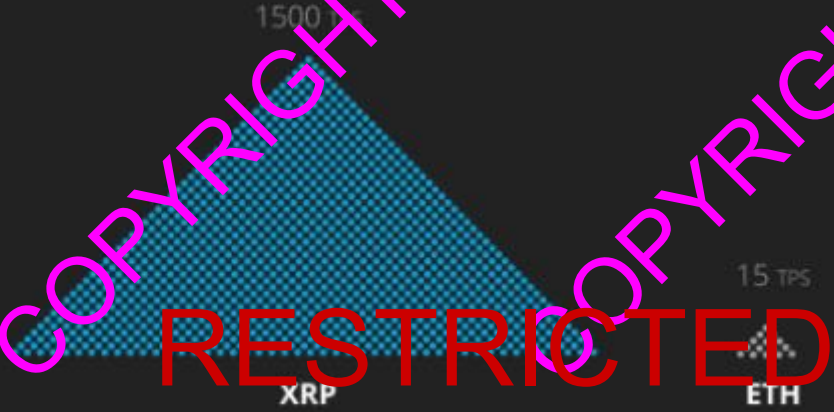
2+ Min

BTC

4+ Hours

TRADITIONAL SYSTEMS

3-5 Days



Scalable

XRP consistently handles 1,500 transactions per second, 24x7, and can scale to handle the same throughput as Visa.*

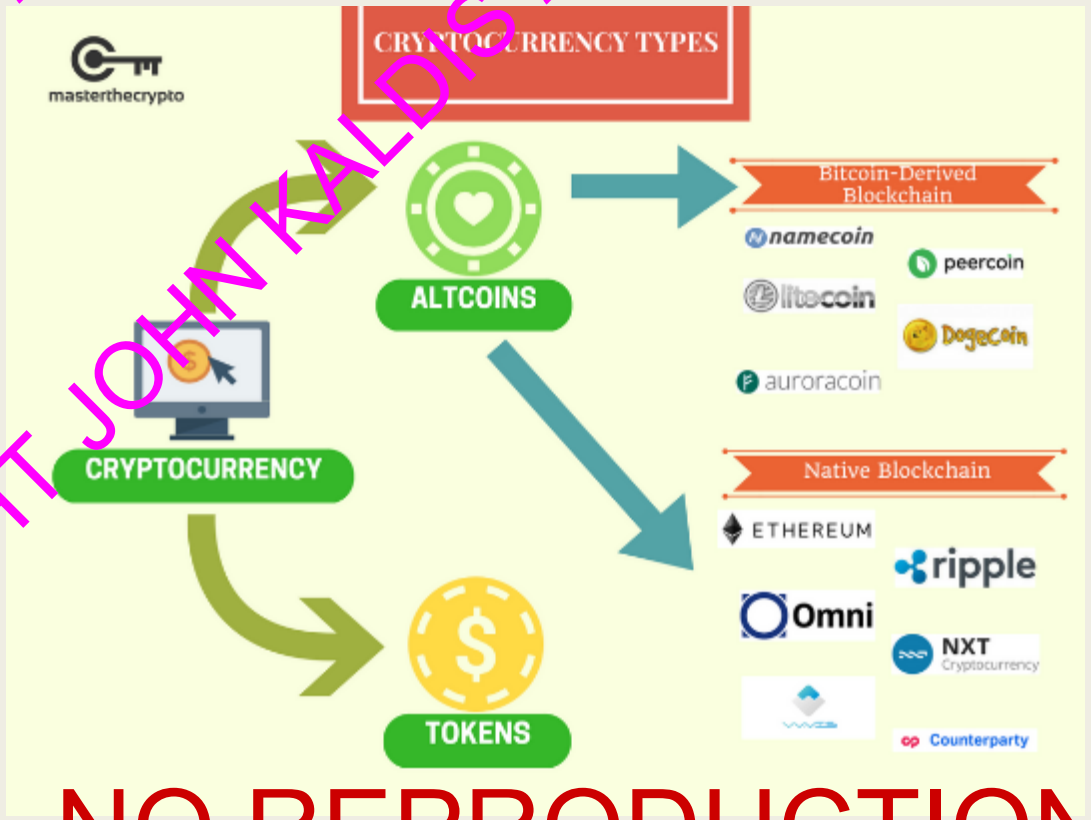
*Source: 50,000 transactions per second, as of July 15, 2017

Coins vs Tokens: Categorization of Cryptocurrencies

The most common categorization of cryptocurrencies are:

- Alternative Cryptocurrency Coins (Altcoins)
- Tokens

It is important to note that all coins or tokens are regarded as cryptocurrencies, even if most of the coins do not function as a currency or medium of exchange. The term **cryptocurrency is a misnomer** since a currency technically represents a unit of account, a store of value and a medium of exchange



Altcoins and Forks

- Alternative cryptocurrency coins are also called altcoins or simply “coins”. They’re often used interchangeably. Altcoins simply refers to coins that are an alternative to Bitcoin. The majority of altcoins are a variant (fork) of Bitcoin, built using Bitcoin’s open-sourced, original protocol with changes to its underlying codes, therefore conceiving an entirely new coin with a different set of features
- A software fork occurs when there is a change in the underlying programming protocol, resulting in the “forking” or split of the original blockchain. This usually results in the creation of a new coin. There are different types of forks such as **hard fork, soft fork or accidental fork**.

A fork occurs when the single blockchain splits into two, either due to:

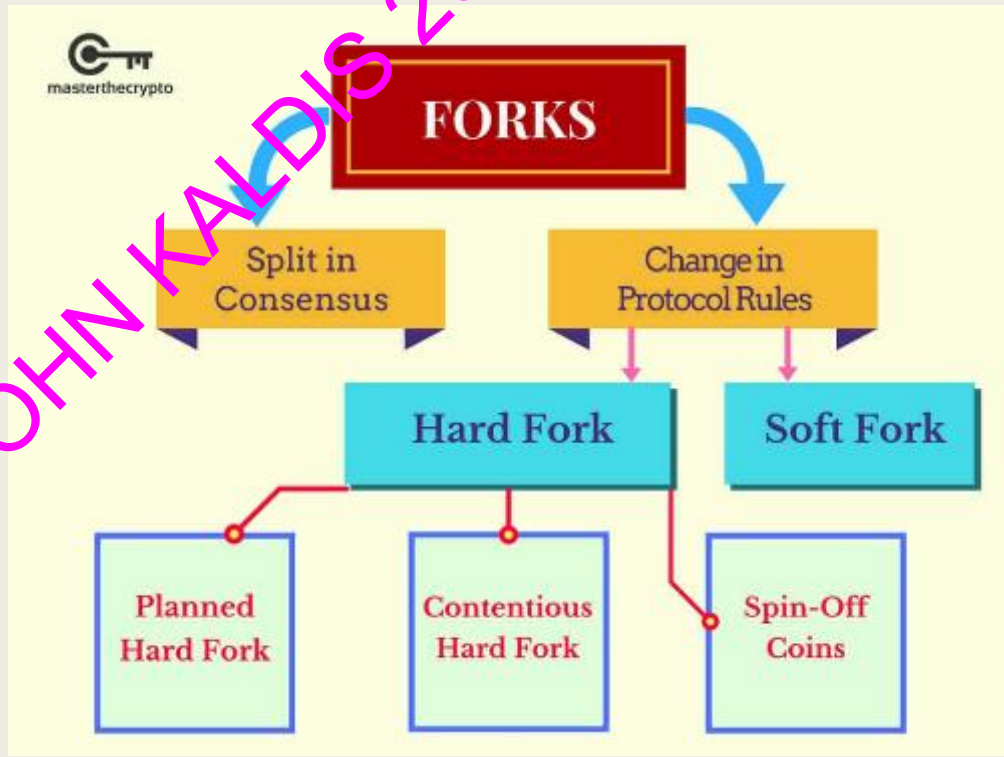
1) A Split in Consensus

As Bitcoin is a distributed and decentralized network, a fork occurs when miners discover a block at the same time, resulting in two split chains. However, this is a temporary fork as the chain that finds the next block first becomes the longest chain and automatically becomes the truth. Therefore, the shorter chain will be abandoned by the network.

2) A Change in the Underlying Rules of the Protocol

This represents a conscious change of the underlying codes by developers, and are **permanent**. The reason for changing the codebase can be due to:

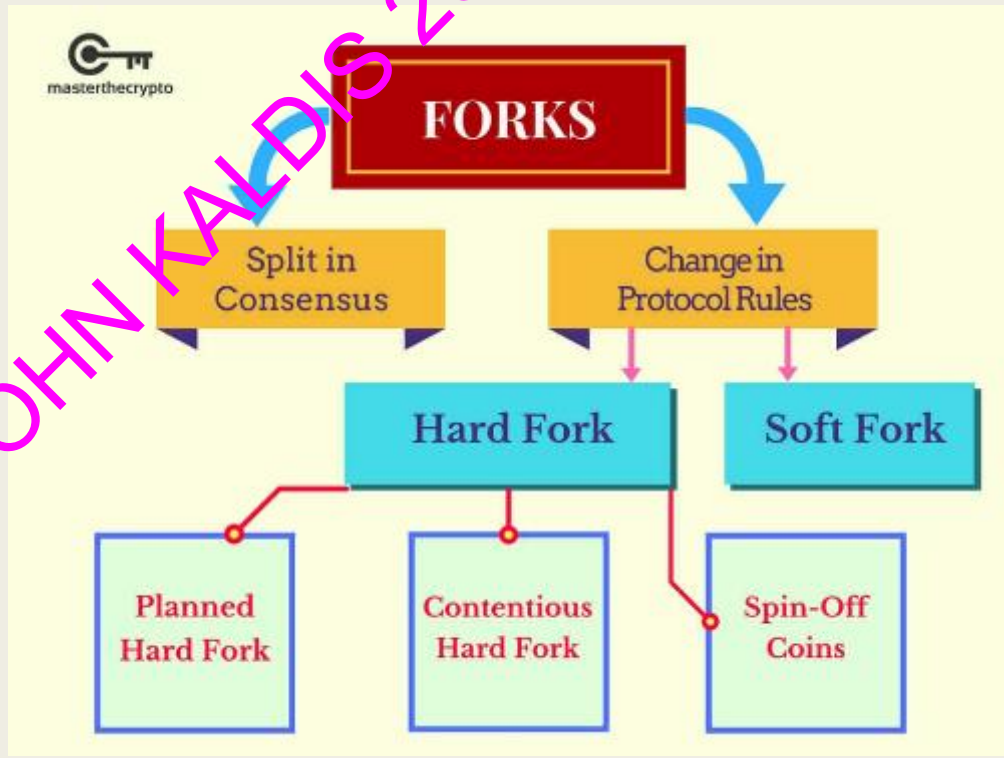
- Adding new features to enhance the network's functionalities
- Changing a core rule (such as increasing the block size)



A change in the underlying rules of the protocol is generally classified into :

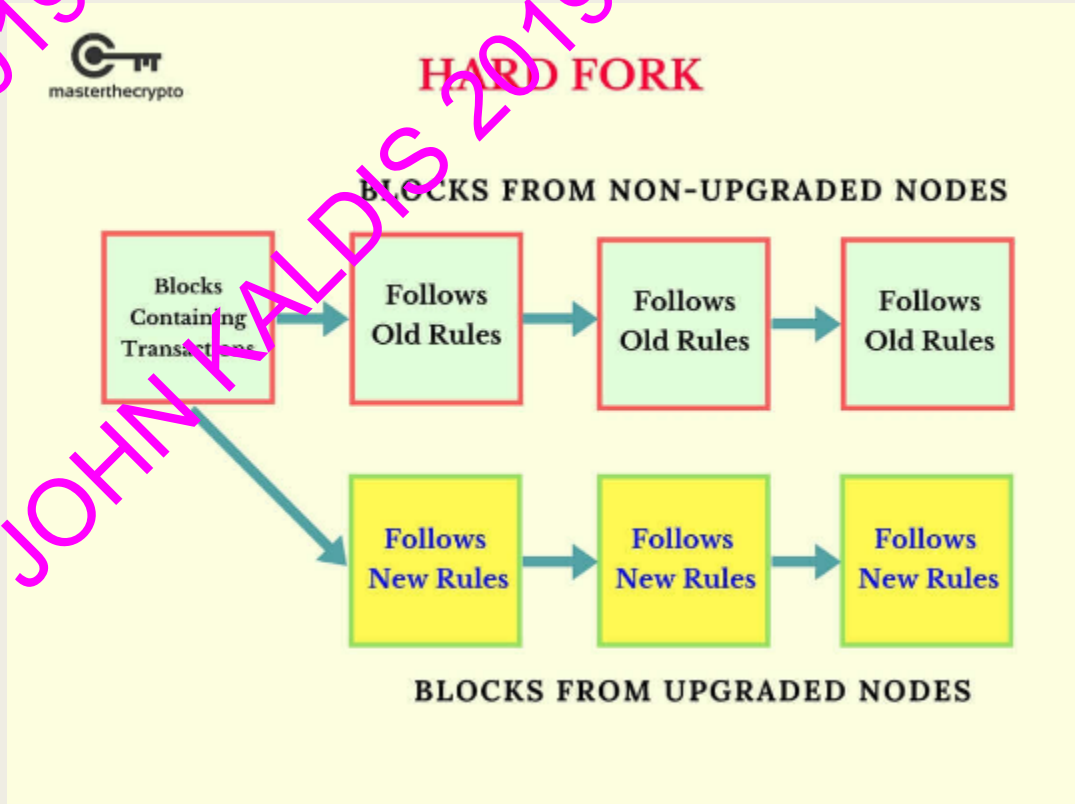
1) **Soft Forks**

- A soft fork is a software upgrade that is backwards compatible with older versions
- This means that participants that did not upgrade to the new software will still be able to participate in validating and verifying transactions.
- It is much easier to implement a soft fork as only a majority of participants need to upgrade the software



2) Hard Forks

- Hard forks refer to a software upgrade that isn't compatible with older versions. All participants must upgrade to the new software to continue participating and validating new transactions.
- Those who didn't upgrade would be separated from the network and cannot validate the new transactions.
- This separation results in a permanent divergence of the blockchain.
- As long as there is support in the minority chain – in the form of participants mining in the chain – the two chains will concurrently exist



There are:

- **Planned Hard Forks** (ex. Monero, Byzantium etc)
- **Contentious Hard Forks** (due to disagreement ex. Ethereum Classic and Bitcoin Cash)
- **Spin-off Coins:** Since Bitcoin's protocol is open source, anyone can view the code base and make changes to it in the pursuit of creating a new coin with new features (ex. Namecoin, Peercoin, Litecoin etc)

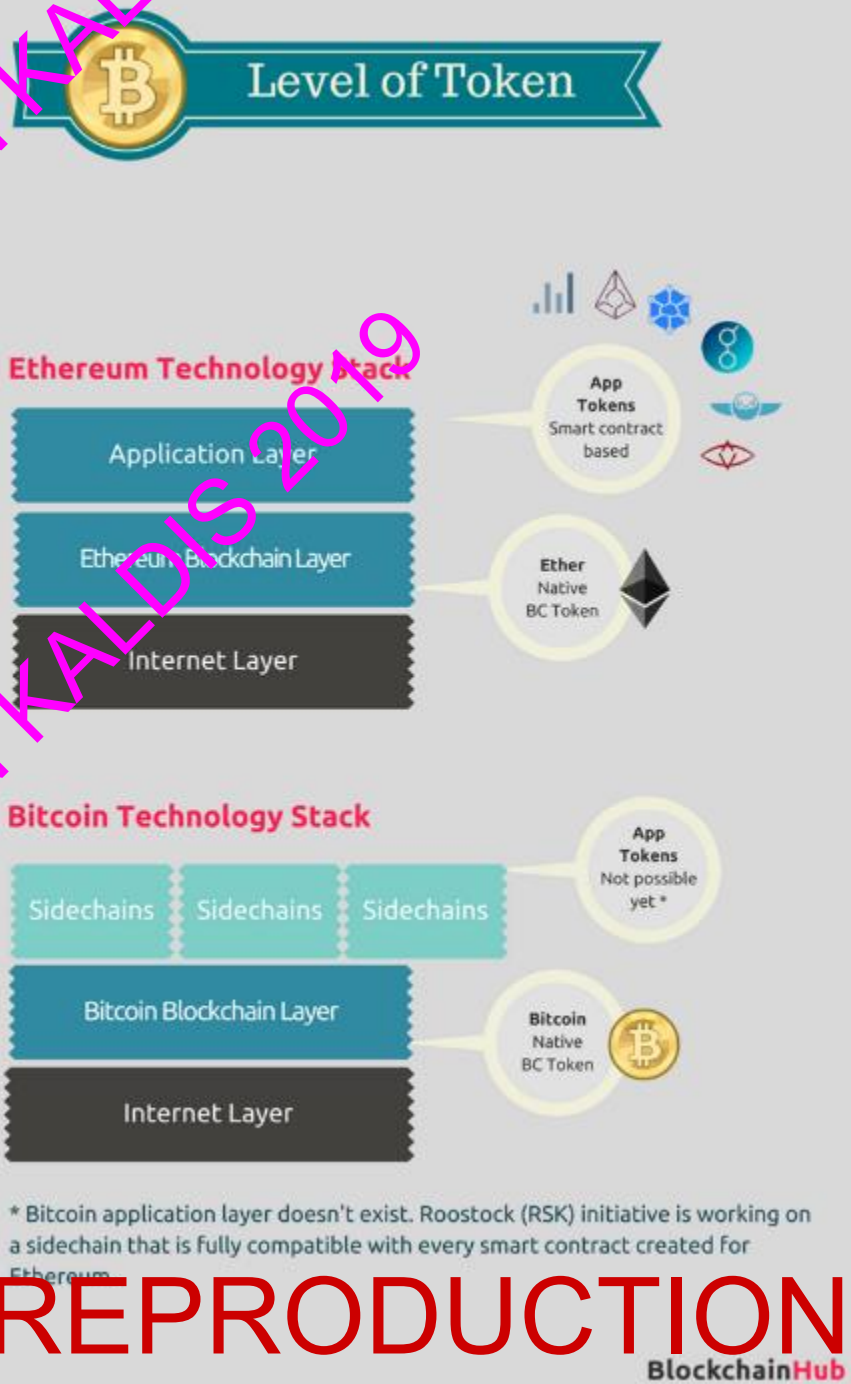
Tokens

- Tokens are a representation of a particular asset or utility, that usually resides on top of another blockchain.
- Tokens can represent basically any assets that are fungible and tradeable, from commodities to loyalty points to even other cryptocurrencies
- Creating tokens is a much easier process as you do not have to modify the codes from a particular protocol or create a blockchain from scratch. All you have to do is follow a standard template on the blockchain – such as on the Ethereum or Waves platform – that allows you to create your own tokens.
- This functionality of creating your own tokens is made possible through the use of smart contracts
- Tokens are created and distributed to the public through an Initial Coin Offering (ICO), which is a means of crowdfunding, through the release of a new cryptocurrency or token to fund project development

Tokens vs Altcoins

The main difference between altcoins and tokens is in their structure;

altcoins are separate currencies with their own separate blockchain while tokens operate on top of a blockchain that facilitates the creation of decentralized applications



CRYPTOCURRENCY GLOSSARY

Virtual currency	A type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community."
Digital currency	A form of virtual currency that is electronically created and stored. Some types of digital currencies are cryptocurrencies, but not all of them are.
Crypto-currency	A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transactions, preventing counterfeit and operating independently of a central bank.
Alt-coin	An abbreviation of "Bitcoin alternative," and thus describes every single cryptocurrency except for Bitcoin.
Coins	Coins really only have one utility—to act as simple stores of value with limited-to-no other functionality. Usually referred to Bitcoin
Tokens	Are programmable, representing digital assets that can have a variety of values attached. They can represent assets as diverse as vouchers, IOUs, or even objects in the real world. Usually referred to Ether

ICO Initial Coin Offerings

- A form of Smart Contract
- Fund Projects in return for Tokens
- Form of Fundraising - Roots with Crowdfunding
- Asset Backed (feel more “secure”)
- Utility Tokens (medium of exchange in some microeconomy)
- Access a scarce resource of the project
  - *Filecoin: Decentralized Storage Space*
  - *Openmined: Data Sets*

- About 30 launched per day
- 3B$ invested until January 2018
- Example EOS raised 700M USD in Bitcoin and Ether

Filecoin

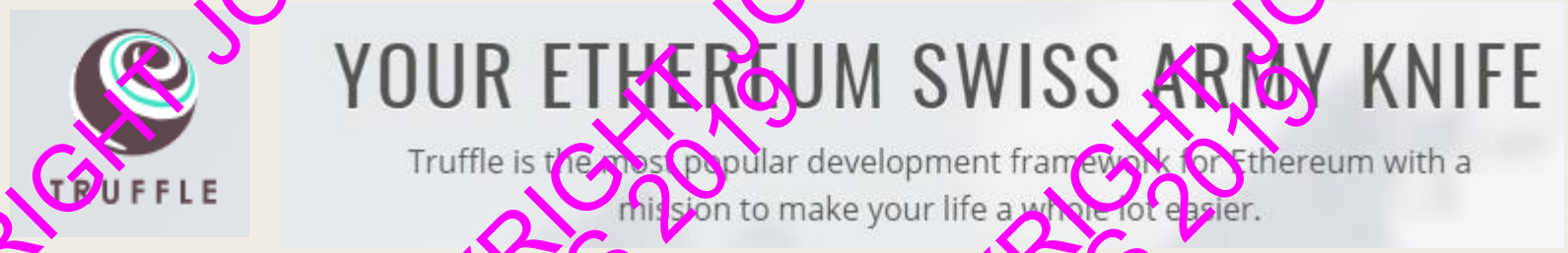
OpenMined

ICO vs IPO

	ICO	IPO
1. Initiate	Write a summary; announce to crypto community to gather interest and feedback	Hire an investment bank to underwrite the IPO
2. Documentation	- White paper - Website	Filings with SEC - Registration statement - Prospectus
3. Marketing	PR-campaign - Crypto forums - Slack	Roadshow - Pre-sale IPO to institutional investors - Set pricing
4. Sales process	Buyers send cryptocurrencies to a digital address, smart contracts issue tokens according to exchange ratio	Allocate shares according to book building
5. Listing	Tokens listed on a crypto exchange	Shares listed on an exchange

- No comprehensive regulatory oversight (IPO needs minimum 6 months)
- Weak Track Record and Credibility
- Adoption of Utility vs Dividends
- Raising capital ≠ Creating Value
  - *Consider Ocean Pollution by Oil companies vs Linux*
- Short Duration of Offering
- Open to all vs Exclusive access

Build an ICO



- Solidity as the programming language,
- OpenZeppelin Solidity contracts as the base of the contract,
- Truffle Framework as a testing and building tool,
- Testrpc for simulating local Ethereum blockchain node,
- JavaScript as the programming for unit tests,
- MyEtherWallet.com for testing and deploying contract on Ethereum blockchain.

Company	Use of funds
OmiseGo	Proprietary blockchain for interoperable digital wallets
Tezos	Proprietary blockchain that is decentralized and self-governing
EOS.io	Proprietary blockchain that targets higher transaction speeds and scalability than Ethereum
Bancor	Protocol with built-in price discovery and a liquidity mechanism, allowing users to issue tokens or exchange them automatically
Status	Protocol that has a messaging platform and mobile browser to interact with decentralized applications
TenX	Protocol for crypto debit cards
BAT	Protocol for digital advertising
Civic	Protocol for on-demand, secure and low-cost access to identity verification services

COMPARISON OF FUNDRAISING METHODS

	ICO	Equity Crowdfunding	Reward Crowdfunding	VC	IPO
Startup stage	Prototype	Prototype	Prototype	Prototype→late stage	Late stage
Equity	No	Yes	No	Yes	Yes
Requirement	White paper (optional) - Desired amount - Project milestones - Team - Types of tokens - Exchange ratio	Educational materials - Investment description - Types of securities - Investment limits	Educational materials - Project description - Marketing deck - Types of rewards	Pitch deck - Management - Use of funds - Business model	Prospectus - Company description - Types of securities - Management - Financial info
Investors	Blockchain enthusiasts	Angel investors	Early adopters	Limited partners	Public
Period	3-6 months	1-3 months	1-2 months	3-12 months	>1 year
Fundraising cost	Low	Medium	Low	High	High
Channel	Online	Online	Online	Offline	Offline
Liquidity	Medium	Low	Low	Low	High
Downside risks	Project fails, fraud	Bankrupt	Project fails	Devalue, bankrupt	Price drops

ICO FUNDRAISING DWARFS VC FUNDING

Initial coin offerings (ICOs) have become the preferred avenue for blockchain startups to raise funds. Even non-blockchain and non-fintech startups are starting to look at ICOs

Top ICOs (to Aug '17)

Filecoin $250M
Decentralized storage network

Tezos $232M
Self-amending cryptographic ledger

EOS $185M
Open source platform for scalable decentralized apps

Bancor $153M
Price discovery and liquidity mechanism for tokens

Source: CB Insights, Fortune

CASE STUDY: THE DAO

The DAO was the largest ICO in history. The key to its success is its ideology of a self-governing organization.

	The DAO
Issuing company	Slock.it
Mission	The first implementation of Decentralized Autonomous Organization (DAO) code to automate organizational governance and decision-making. It aims to codify the rules and decision-making apparatus of an organization, eliminating the need for documents and people in governing, creating a structure with decentralized control.
Token	DAO
Platform	Ethereum
Amount intended	50,000 ETH / $500,000
Amount raised	$160M
Date	30 April 2016
Motivation	DAO allows users to direct the DAO's operations. Users use tokens to vote.
Fund allocation	100% to the DAO
Coin distribution	100%
Token usage	• The tokens represent ownership over the DAO, which includes being able to nominate and vote on DAO activities, nominate and vote on DAO curators. • Any profits the DAO makes on its investments will be given back to token holders as dividends.

SLOC it a door lock that is connected to a smart contract on the Blockchain which controls when and who can open the lock this enables anyone to rent sell or share their property without need of a middleman.
(on demand Air BnB)

CASE STUDY: RIPPLE VS. OMISE

Ripple has not raised funds through ICOs. Although it has similar mission to Omise, it's less likely to raise funds via ICO because it's success is less reliant on network effects and its associated externality.

	Ripple	Omise
Mission	Ripple's distributed financial technology enables banks to send real-time international payments across networks.	The complete set of powerful payment features that allows fast, flexible and seamless experiences all ready built-in.
Value proposition	• **Access:** Direct bank to bank settlement • **Speed:** Instant (4 sec vs ETH 2-mins) • **Certainty:** real-time traceability of funds • **Cost:** lowest total cost	• **White label, no redirect:** invisible to users/not • **Secure** • **Automate payouts:** to stakeholders with API • **Ease:** one-click, no card (only bank a/c)
Target customer	Banks (remittances, corporate disbursement)	E-commerce/Enterprise (payment, transfers)
Blockchain platform	Private	Public
Validators	Participating institutions (banks)	Anyone with Omise server
Funding	$93.6M in 7 Rounds from 27 Investors (Series B)	$20.4M in 4 Rounds from 9 Investors (Series B)

REGULATORY TREATMENT AROUND THE WORLD

Regulators have started weighing in on ICOs, some declaring or contemplating outright bans. But many are taking more cautious approaches. Cryptocurrency markets remain volatile, but highly resilient.

U.S. Securities and Exchange Commission

- Application of the Howey Test (investment of money in a common enterprise with an expectation of profits predominantly from the efforts of others) to ICOs to determine if a particular token should be classified as a security falling under securities law

Monetary Authority of Singapore

- No definitive regulation, but have viewed cryptocurrencies with a light touch
- MAS has launched a tokenized version of the SGD via Project Ubin

finma

- No regulation at current time; cryptocurrencies viewed as assets.

中国人民银行 THE PEOPLE'S BANK OF CHINA

- Issued a ban on ICOs on Sept 4. Top 30+ cryptocurrencies saw significant, double-digit percentage price drops, but most have begun recovery
- Concerns over fraud and pyramid schemes

SFC

- Issued a statement on Sept 5 that certain ICO structures would classify the token issuance as a security, which would be a regulated activity that requires license
- Following similar approach to U.S. SEC

THE BANK OF KOREA

- Like Japan, Korea has legalized bitcoin (July 2017) as a remittance method
- However, a digital currency task force led by the central bank intends to crackdown on ICO issuances and intends to introduce regulations

SECTION 3

- Monetary & Non-monetary Applications

GOVERNMENTAL INTERVENTION VS PUBLIC SUPPORT

The decentralization of money offered by virtual currencies like bitcoin has its theoretical roots in the Austrian school of economics,

especially with Friedrich von Hayek in his book Denationalisation of Money: The Argument Refined,

in which he advocates a complete free market in the production, distribution and management of money to end the monopoly of central banks

WHY DOES BITCOIN HAVE VALUE AND HOW IS THE PRICE DETERMINED?

- The answer to this question is rather simple and it lies in basic economics:
  - scarcity,
  - utility,
  - supply and demand
  - VALUE vs PRICE
- Determinants of Exchange Rates (BTC/USD) note exactly applicable as in (USD/EUR)
  - Differentials in Inflation
  - Differentials in Interest Rates
  - Current-Account Deficits
  - Public Debt
  - Political Stability and Economic Performance

MONETARY ISSUES

- Interest? Bitcoin Interest ("BCI") is a competitive staking cryptocurrency (a "fork")
- Deflationary (opposite of inflation). Predefined Supply – Increasing Difficulty
- Volatile and "thin market" Low number of buyers and sellers, unresponsive trading Platforms
- Non value producing asset
- Oligopoly (China-Russia)
- Ponzi Scheme Concerns
- High Herfindahl-Hirschman index (HHI) (a commonly accepted measure of market concentration)
- "I can say almost with certainty that cryptocurrencies will come to a bad end," Warren Buffet
- Governmental intervention vs Public Support

DEFLATION (AND BITCOIN)

- Deflation is a contraction in the supply of circulated money within an economy, and therefore the opposite of inflation
- In effect, deflation causes the nominal costs of capital, labor, goods and services to be lower than if the money supply did not shrink
- Inflation reduces the value of currency over time, but deflation increases it. This allows one to buy more goods and services than before with the same amount of currency
- **People save instead of spending. (Yet those few who invest are very strong)**
- Generally "bad" for economy (with exceptions but this is out of scope)
- Deflationary spiral is an economic argument that proposes that runaway deflation can eventually lead to the collapse of the currency given certain conditions and constraints

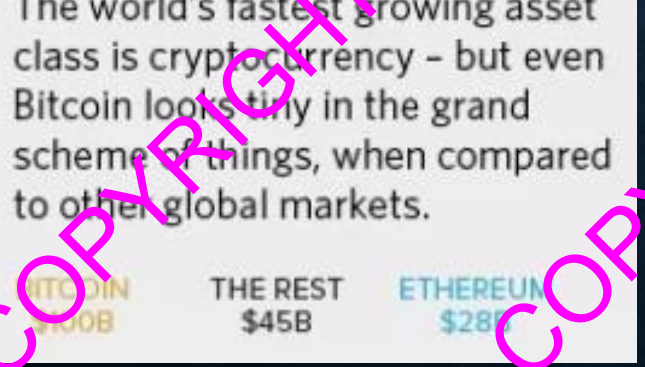
MONEY REPLACEMENT ?

Current paper-based systems drive **$18 trillion** in transactions per year.

Approximately **1-2%** is Banking fees, commissions etc.

Cryptocurrency

The world's fastest growing asset class is cryptocurrency – but even Bitcoin looks tiny in the grand scheme of things, when compared to other global markets.



Global Stock Markets

The market capitalization of all of the world's stock markets is equal to **$73 trillion**.

The Derivative Market

The low end estimate of the size and scope of global derivative markets is **$544 trillion** on a notional contract basis.

The high end estimate for the value of all derivative contracts is as high as **$1.2 quadrillion**.

The truth is that no one really knows the exact size of the market.

Coins & Bank Notes

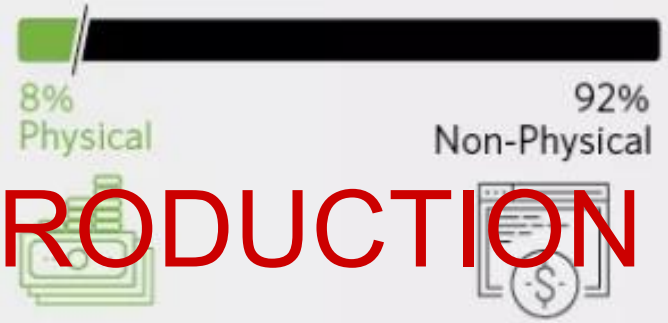
The total value of all of the world's coins and banknotes is roughly **$7.6 trillion**.

Narrow Money

The total value of the world's easily accessible money is **$36.8 trillion**. This includes the world's coins, banknotes, and checking deposits.

Broad Money

The total value of the world's money is **$90.4 trillion**. This includes coins, banknotes, money market accounts, as well as saving, checking, and time deposits.



BUT IS IT AN ASSET ?

An asset is a resource with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit

Anything that is capable of being owned or controlled to produce value, is an asset

Two fundamental types of asset

- Tangible, e.g. a house
- Intangible, e.g. a mortgage

Intangible assets subdivide

- Financial, e.g. bond
- Intellectual, e.g. patents
- Digital, e.g. music

Cash is also an asset

- Has property of anonymity

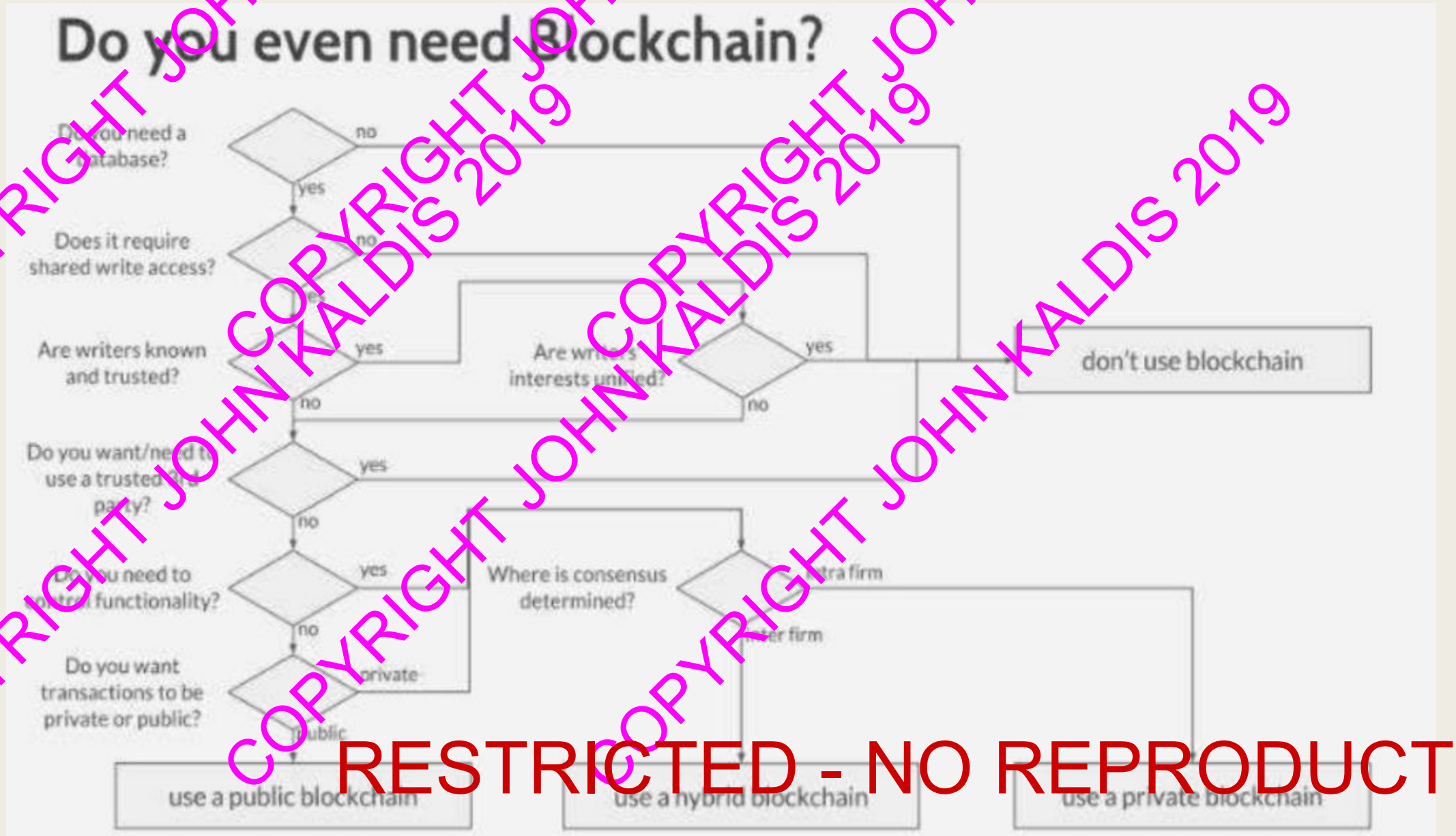
LINEAR VS LOG !!!

Non Monetary Applications

Imagine

Ledgers can be used for the recording tracking monitoring and transacting of all forms of assets all asset registries inventories and exchanges including every area of economy. physical assets such as cars, products, machines and houses and intangible assets such as votes, ideas, health, reputation, music etc

Blockchain non monetary Applications



Blockchains

- Bad at real-time interactions
- Bad at storing large amounts of data
- Bad at executing long-running business logic

- Good at ensuring system continuity and integrity
- Good at securing data from tampering and loss
- Good at reducing infrastructure cost

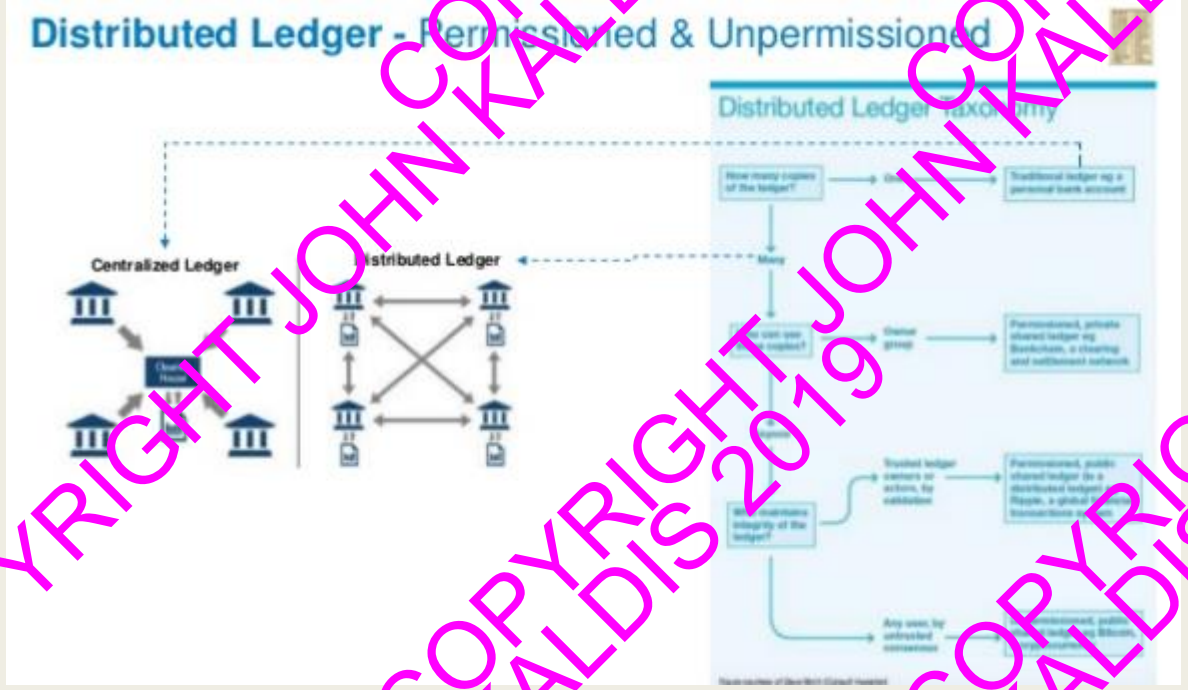
Miiko Matsumura, co-founder of the Evercoin Cryptocurrency Exchange :
BLOCKCHAIN IS AN EXTREMELY SLOW DATABASE FIT ONLY FOR NO TRUST SITUATIONS

Public Blockchains are good at...

- Setting up a system with minimal initial investment
- Enabling trustworthy interactions between parties that do not normally trust each other, because:
  - their identity cannot be safely assessed, or
  - they are not subject to a commonly trusted authority
- Certifying the ownership and creation date of public data records

Public Blockchains are bad at...

- Processing low-value transactions: each transaction costs a good deal of money
- Processing frequent transactions: systems have low throughput
- Processing time-critical transactions: systems have high latency
- Processing process-critical transactions: there is no concept of “final”, as committed (and legitimate) transactions can be discarded later on
- Ensuring business continuity: no control over the system, which in the future may evolve in unwanted directions or even terminate with short notice



Permissionless

- The great advantage to an open, permissionless, or public, blockchain network is that guarding against bad actors is not required and no access control is needed
- This means that applications can be added to the network without the approval or trust of others, using the blockchain as a transport layer

Permissioned (private) blockchain

- Permissioned blockchains use an access control layer to govern who has access to the network.
- Validators on private blockchain networks are vetted by the network owner. They do not rely on anonymous nodes to validate transactions nor do they benefit from the network effect.

Smart Contracts

Consensus protocols are key to determining the sequence of actions resulting from the contract's code. This enables peer-to-peer trading of everything from renewable energy to automated hotel room bookings.

"Contracts Get Smarter with Blockchain", CIO Journal, The Wall Street Journal, World Trade Organization, International Trade Statistics 2015, 2015, p. 41.

No government or supranational organization can manipulate the “contract”

Everyday transactions

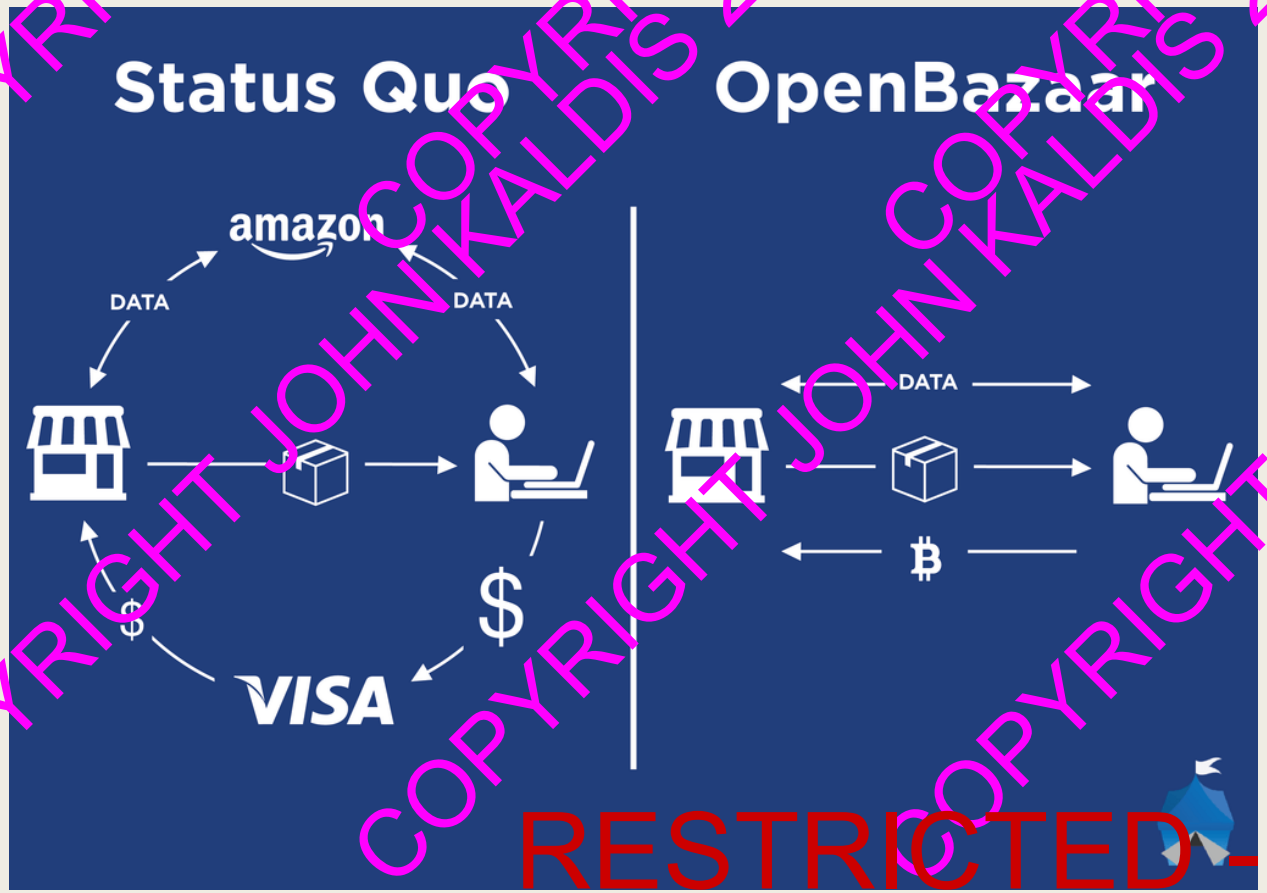
- Contracts between employees and employers
- Mutual investments with predefined sharing
- Bank Interest changes automatically according to amount invested without negotiations
- Renting / Leasing / Buying
- Monitoring / Maintenance
- Anything practically that has rules

Imagine

In this system all property could become smart property this is the notion of encoding every assets of the Blockchain with the unique identifier such that the asset can be tracked controlled and exchanged on the blockchain

Industry/Application	Function
 Financial Services	Cryptocurrency, stock market, micropayments
 Technology Media & Communications	Intellectual Property, IoT Deployments
 Consumer Applications	Car buying/leasing contracts, loyalty points and rewards
 Healthcare	Patient records, claims
 Public Sector	Land registry, voting, vehicle registration, digital identities, benefits disbursements
 Horizontal Applications	Smart Contracts, Cyber Security, Audits

OpenBazaar



Financial Services

BARCLAYS

In September 2016, Barclays carried out the world's first trade transaction using blockchain

NASDAQ will soon run Blockchain trading

Nasdaq

Voting

Estonia, a small Baltic nation is the first to implement Blockchain based E-Voting System

Followmyvote is world's first open-source online voting solution based on blockchain

followmyvote.com

Real Estate

UBITQUITY

Solves issues of huge paperwork and high agent fees

Using Ubitquity, anyone can manage, track, and transfer land titles and property deeds

Music Streaming

Artists lose up to 86% of the proceeds from their music because of illegal downloading

MYCELIA

Mycelia is a Blockchain based platform for artists to sell their work directly to customers

Supply Chain Management

Middlemen in supply chains take time, add costs, and make mistakes often

PROVENANCE

Provenance facilitates "transparent and traceable" trade on the Blockchain

Decentralized Internet Vision

- Imagine a “decentralized” internet
- Where all the essential services you use today (Amazon, Facebook, Uber, etc) are **protocols!**
- Dropbox is storing p2p
- Open source frameworks instead of operated by a corporate entity, operated by nodes! (No margin cuts!)

	Web 2.0	Web 3.0 (dApps)
Scalable computation	Amazon EC2	Ethereum, Truebit
File storage	Amazon S3	IPFS/Filecoin, Storj
External data	3rd party APIs	Oracles (Augur)
Monetization	Ads, selling goods	Token model
Payments	Credit Cards, Paypal	Ethereum, Bitcoin, state channels, 0x

Notable non-cryptocurrency designs include:

- Steemit – a blogging/social networking website and a cryptocurrency
- Hyperledger – a cross-industry collaborative effort from the Linux Foundation to support blockchain-based distributed ledgers, with projects under this initiative including Hyperledger Burrow (by Monax) and Hyperledger Fabric (spearheaded by IBM)
- Counterparty – an open source financial platform for creating peer-to-peer financial applications on the bitcoin blockchain
- Quorum – a permissionable private blockchain by JPMorgan Chase with private storage, used for contract applications
- Bitnation – a decentralized borderless "voluntary nation" establishing a jurisdiction of contracts and rules, based on Ethereum
- Factom, a distributed registry
- Tezos, decentralized voting.
- Microsoft Visual Studio is making the Ethereum Solidity language available to application developers.
- IBM offers a cloud blockchain service based on the open source Hyperledger Fabric project

SLOC it a door lock that is connected to a smart contract on the Blockchain which controls when and who can open the lock this enables anyone to rent sell or share their property without need of a middleman.
(on demand Air BnB)

Edge Computing & Blockchains for Industrial Automation

Flexible Decentralized Factory Automation

FAR-EDGE

- Joint effort of global leaders in manufacturing and IoT towards adoption of *virtualized* Factory Automation

Focuses on

- Cloud and Edge Computing for Manufacturing
- Decentralization of control
- RAMI 4.0 & Industrial Internet standards

Expected Outcomes

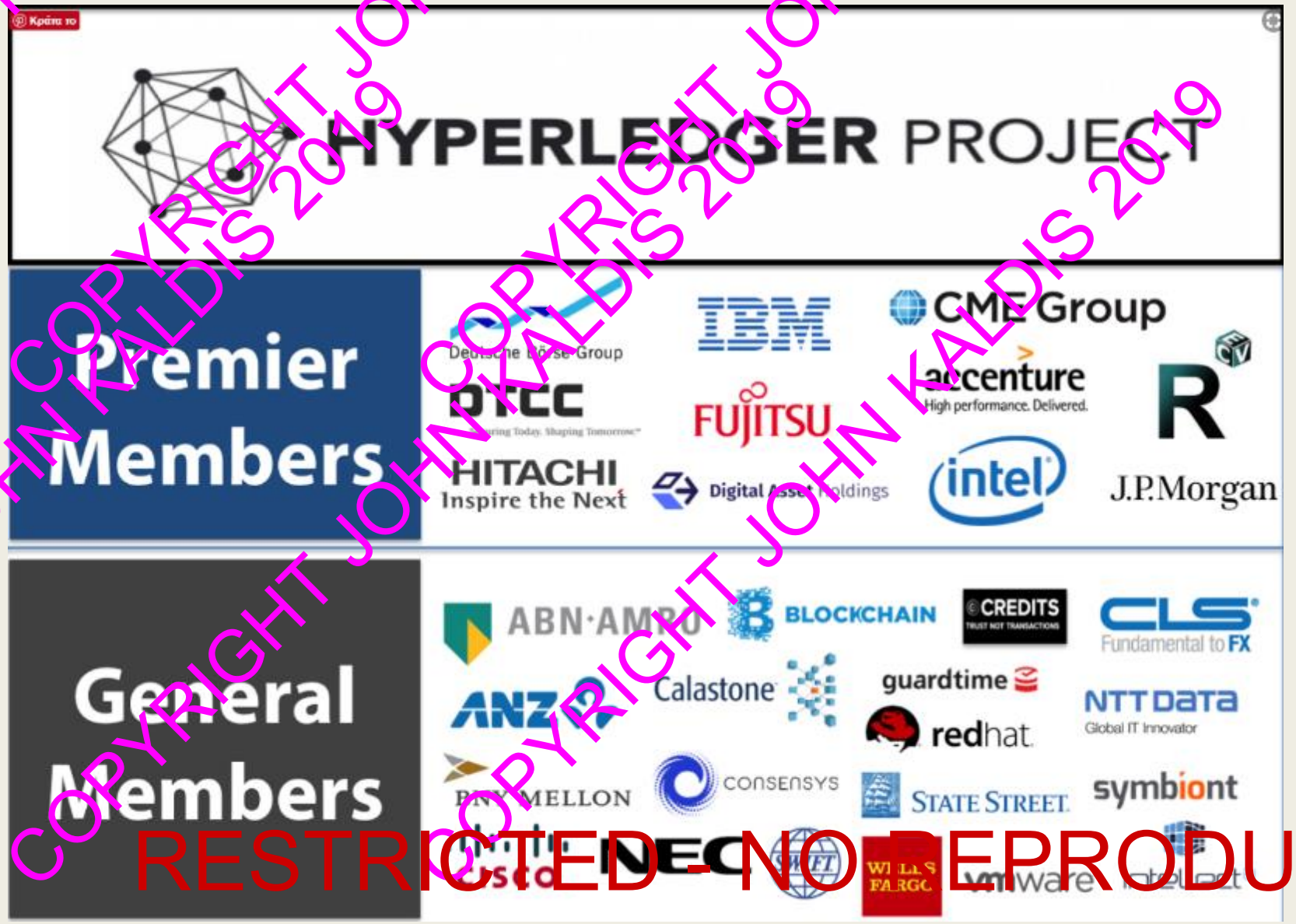
- Reduced Time to deploy new automation concepts and technologies
- Better Exploitation of Data
- Increase automation in factories
- Improve process agility
- Enable factory collaboration
- RAMI Compliant implementation

Hyperledger

- Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, IoT, supply chain, manufacturing, and technology.
- Business Blockchain Frameworks are hosted with Hyperledger.
- Hyperledger addresses important features for a cross-industry open standard for distributed ledgers. The Linux Foundation hosts Hyperledger as a Collaborative Project under the foundation.
- To learn more, visit: https://www.hyperledger.org/.

www.hyperledger.org

Hyperledger

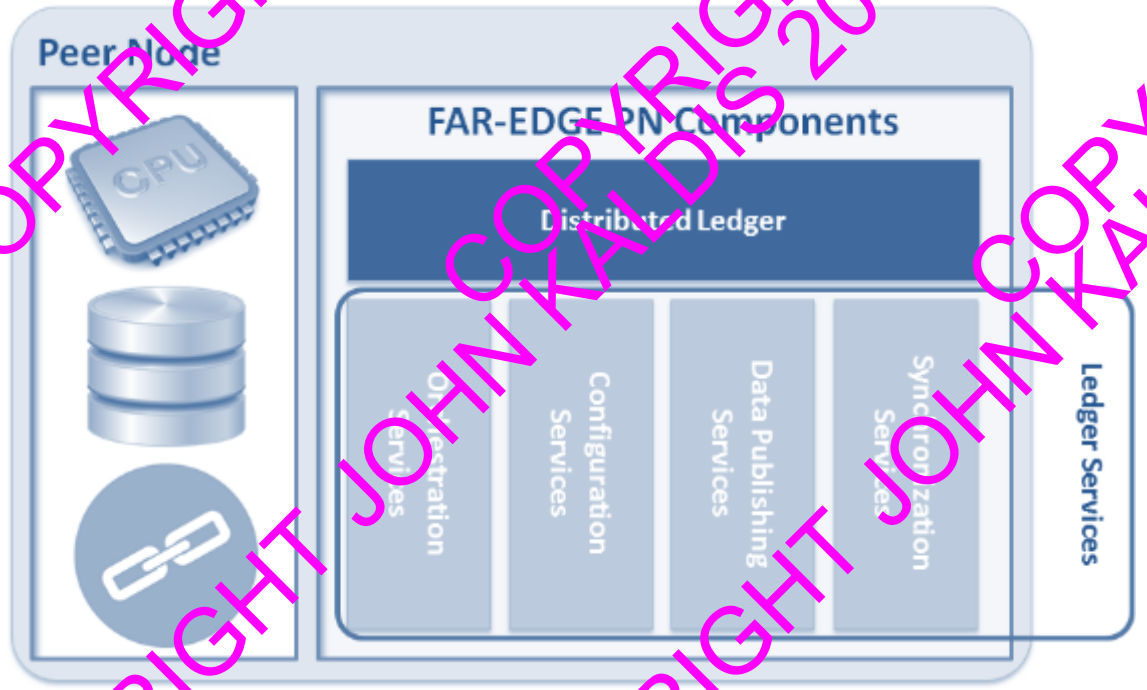


Hyperledger Projects

A few of the Hyperledger Projects include:

- Hyperledger Burrow – Permissible smart contract machine with a modular blockchain client, built in part to the specification of the Ethereum Virtual Machine (EVM)
- Hyperledger Fabric – Foundation for developing plug-n-play solutions within a modular architecture
- Hyperledger Iroha – Simple and easy blockchain framework designed to be incorporated into infrastructure projects requiring distributed ledger technology
- Hyperledger Sawtooth – A modular platform for building, deploying, and running distributed ledgers

Ledger Tier



- Key Innovation of Far Edge Project
- distributed ledger and smart contract patterns
- truly distributed process logic without any centralized service being in charge
- No constraints of Deployment

FAR-EDGE Pilots (Volvo)

Wheel alignment station (WAS) in Goteborg

- Each single truck requires a specific configuration (i.e., rotation angle and torque) of a nut driver tool
- The tool supports remote configuration, but is not connected to the workstation control system: setting is done manually for each work item
  - Problem #1 (UC enhancement): error prone
  - Problem #2 (UC expansion): Volvo needs to deploy a great number of WAS equipment all over the world (e.g., at service shops) and each deployment requires a substantial configuration and training effort on site

FAR-EDGE Pilots (Whirlpool)

FAR-EDGE experimentation

- Implement a sorting algorithm which gets input from existing sensors that identify product items along the conveyor belt
- Make each exit bay an autonomous system that:
  - Is aware of its own pains and needs (requires new sensors and an embedded controller)
  - Can negotiate with a Factory-level smart contract (blockchain) the items to be received
  - May be hot swapped at need (i.e., switched on/off, added/removed without any discontinuity)

H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No

FAR-EDGE Pilots (Smart Factory)

- Test the full fledged functionality of FAR-EDGE solution and validate the following enablers:
  - Automation
  - Analytics
  - Real to Digital Synchronization
  - Simulation
  - Ledger Services

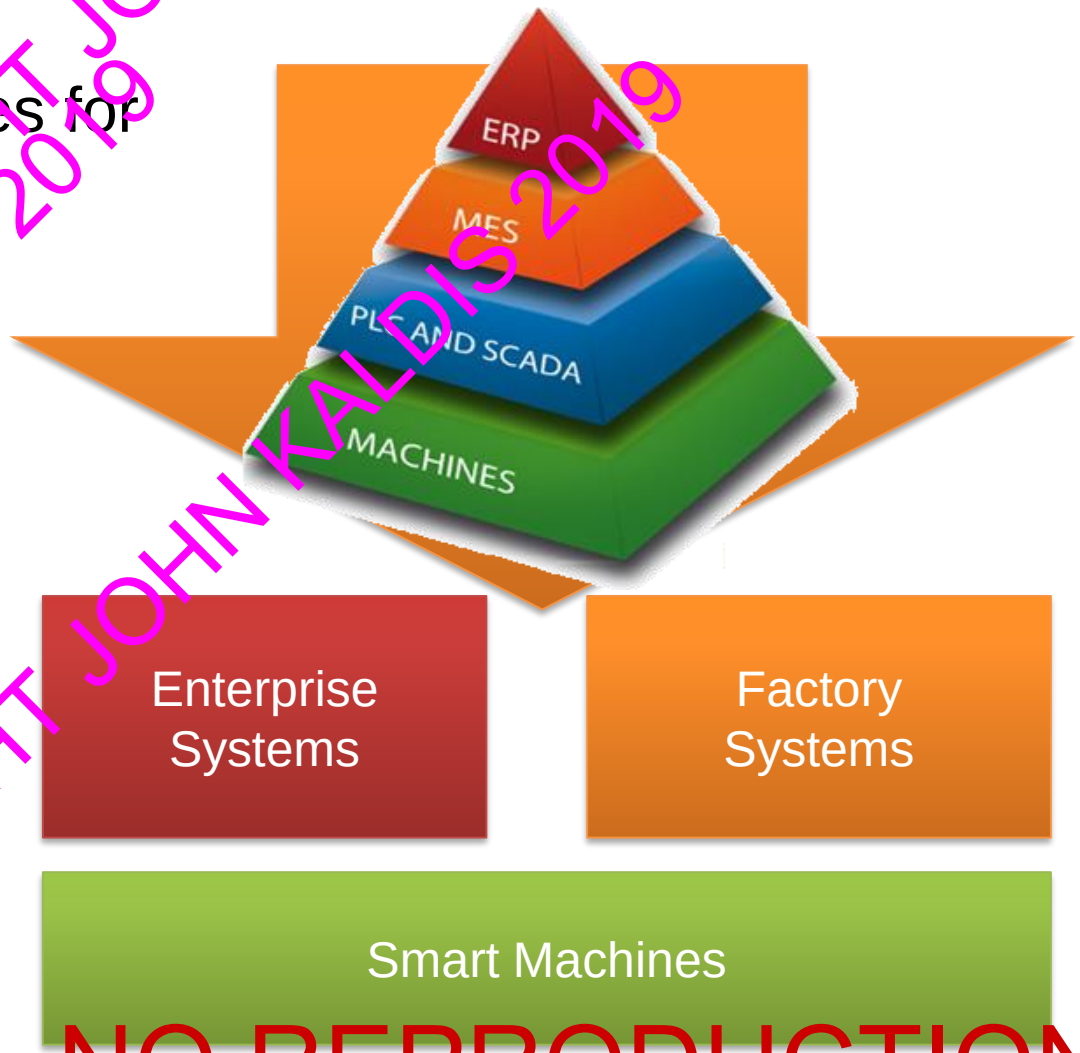
H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 723094

Vision and Values

Edge Computing as a key enabling technologies for **Autonomous Shopfloor Systems**

EC **PROs** (goals)
- plug-and-produce machinery and tools
- more reactive automation
- bandwidth-wise data processing
- no single point of failure

EC **CONs** (problems)
- more difficult to manage
- more vulnerable systems



H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 723094

Approach

- A **Blockchain** infrastructure can synchronize & orchestrate local processes across a factory, an enterprise or even an entire supply chain ecosystem:
  - Global process state stored and shared on a distributed ledger

H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 723094

Validation

Green Field scenario
Smart Machines
@Whirlpool

Brown Field scenario
Legacy Shopfloor
@Volvo

Green Field

Brown Field

H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 723094

Pilot: Whirlpool's Collaborative Sorter

H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 723094

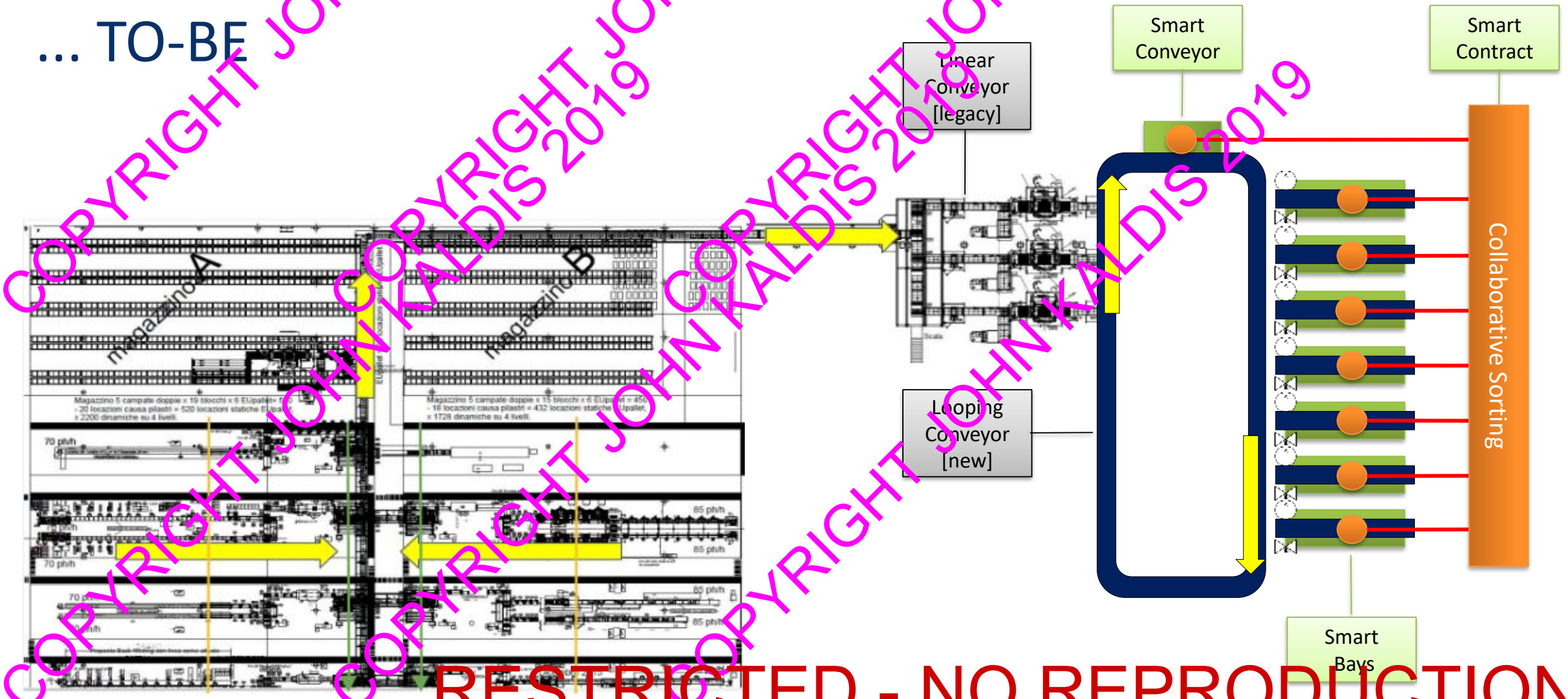
Pilot: Whirlpool's Collaborative Sorter

AS-IS...

H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 723094

Pilot: Whirlpool's Collaborative Sorter

... TO-BE



H2020 Research and Innovation Action - This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 723094

THE END

- Discussion
- Questions