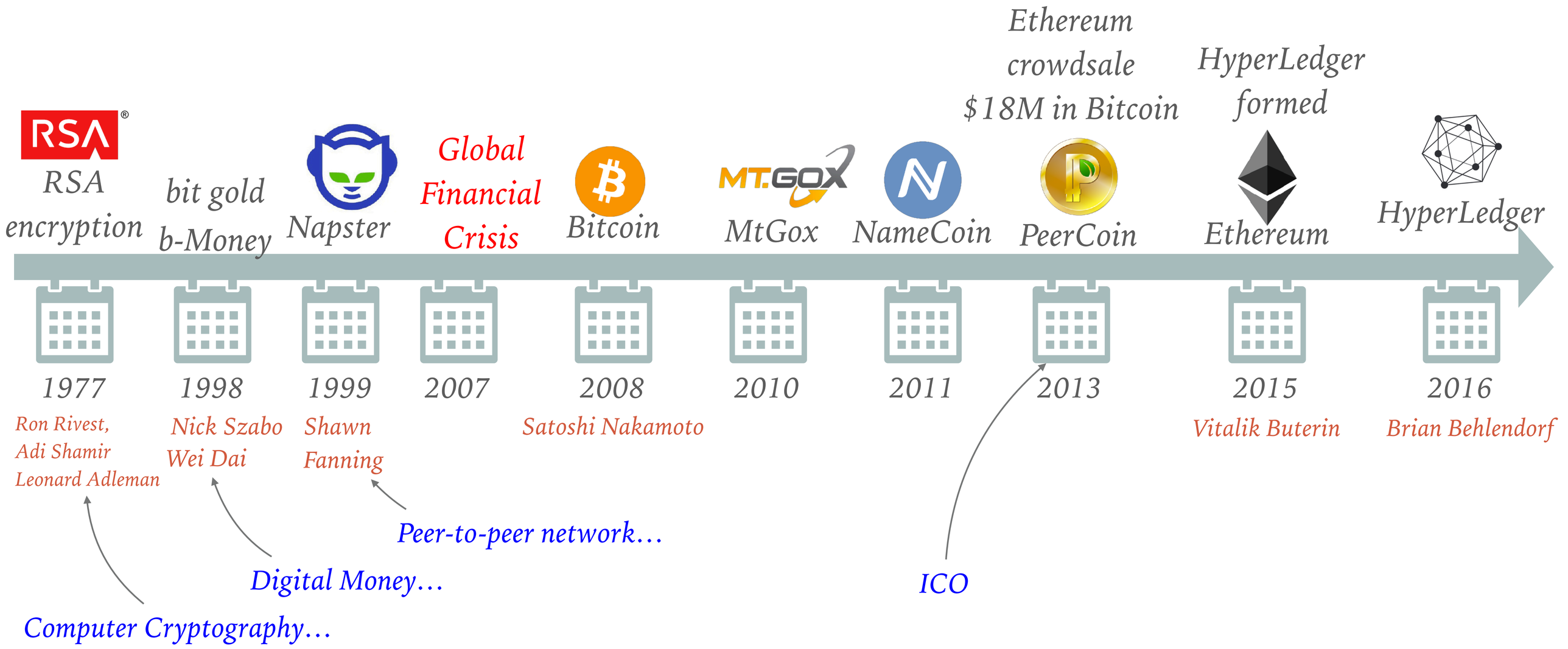
ACE DIGITAL
Resource Advisory Services

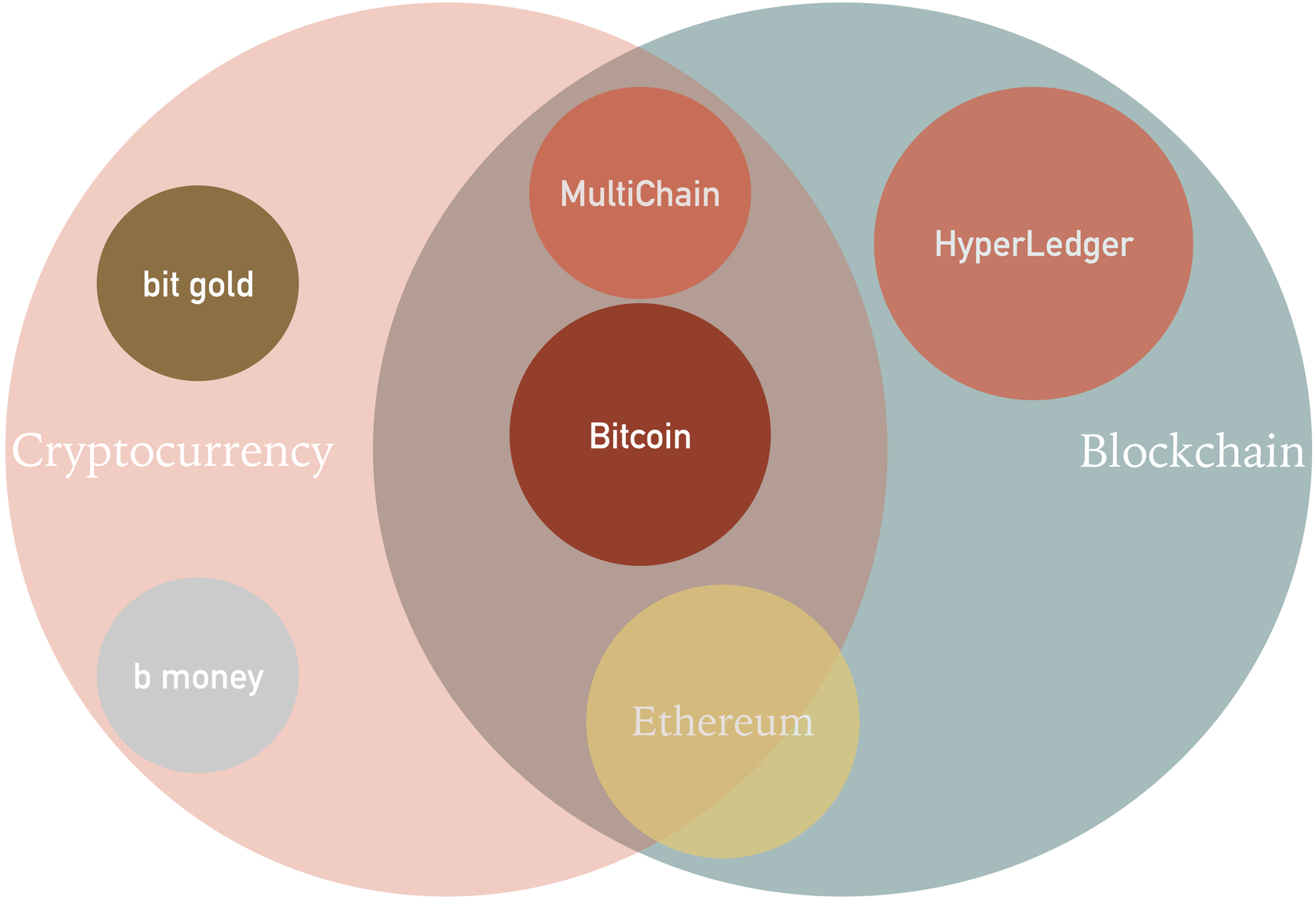
BLOCKCHAIN – MASTERCLASS

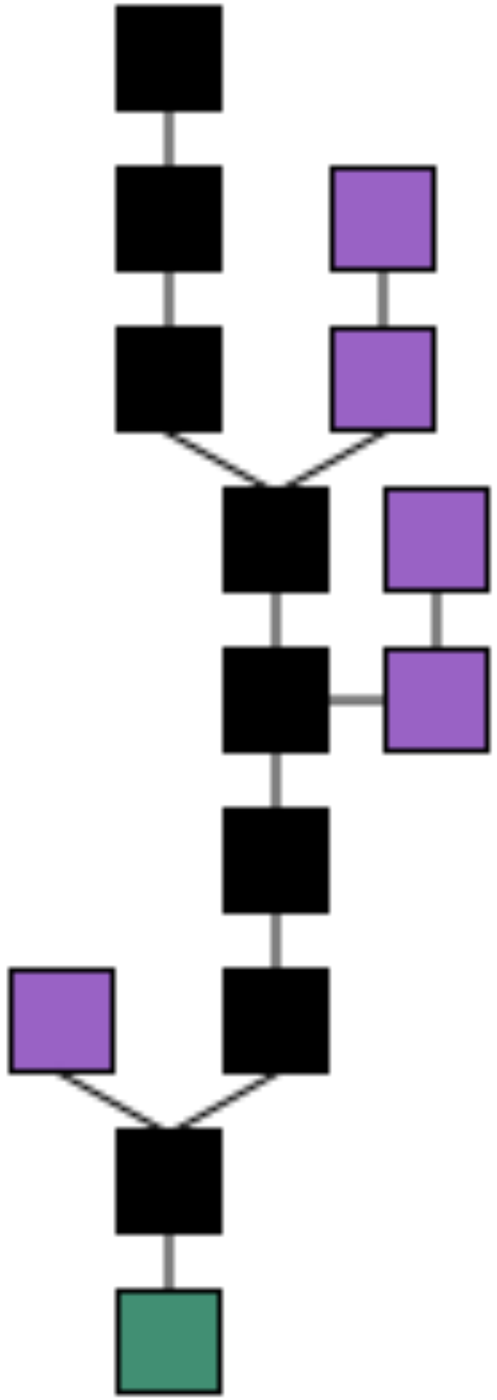
25 January 2019

HISTORY & BACKGROUND



HISTORY & BACKGROUND





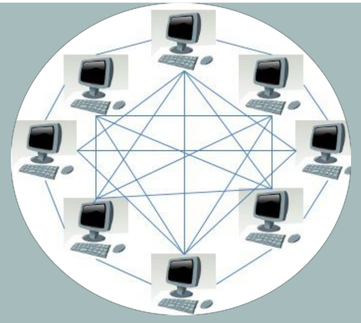
KEY CONCEPTS – WHAT IS BLOCKCHAIN?

- A blockchain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash)

KEY CONCEPTS – COMPONENTS OF A BLOCKCHAIN

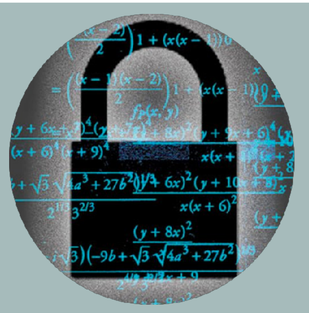
Digital Assets

Consensus Protocol



Peer to Peer Network

Distributed Ledger



Cryptography

- **Cryptography** is the practice and study of techniques for secure communication in the presence of third parties called adversaries

- A device for recording the ownership and state of an asset

- **Peer-to-peer** (**P2P**) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes

A **Consensus Protocol** is a process in computer science used to achieve agreement on a single data value among distributed processes or systems. The real world applications include clock synchronization, PageRank, load balancing, etc.

- Anything that is capable of being owned or controlled to produce value, is an asset. E.g. House, Mortgage, Intellectual Property, Patents, Copyright, etc.

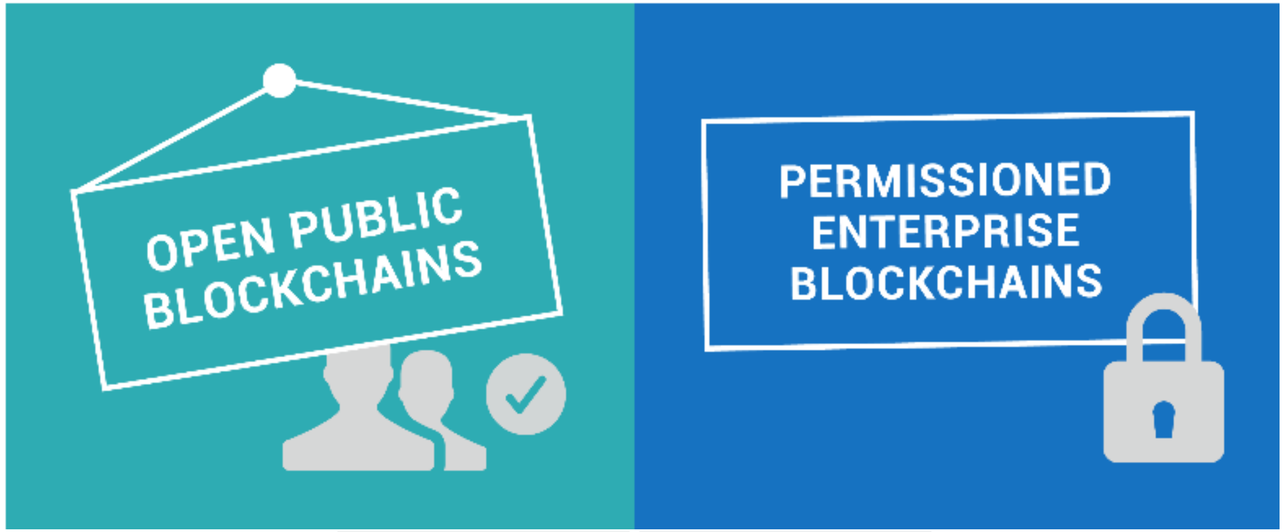
KEY CONCEPTS – TECHNOLOGY BREAKTHROUGH

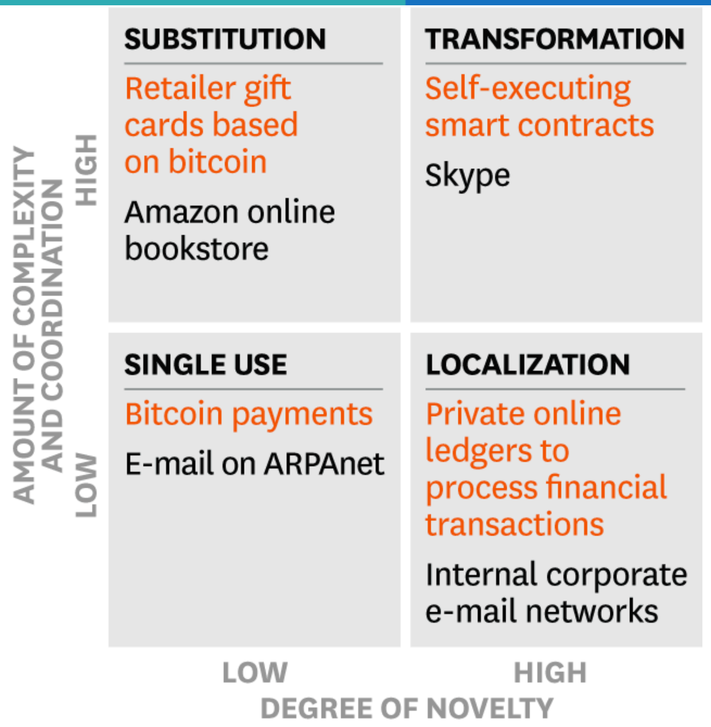
- **Byzantine Fault Tolerance** is the dependability of a fault-tolerant computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component has failed. In a "Byzantine failure", a component such as a server can inconsistently appear both failed & functioning to failure-detection systems, presenting different symptoms to different observers. (Also known as ***disintermediation of trust***)
- **Double Spend** - A potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. Solved using the crytographic protocol Proof-of-work protocol (invented by Markus Jakobsson and Ari Juels)

KEY CONCEPTS – INNOVATIONS

- Smart Contracts
- Provenance, Immutability and Finality

INDUSTRY USE CASES – TOOLS





FROM "THE TRUTH ABOUT BLOCKCHAIN," BY MARCO IANSITI AND KARIM R. LAKHANI, JANUARY–FEBRUARY 2017

- Hyperledger - A collaborative effort created to advance cross-industry blockchain technologies for business

- Hyperledger Fabric - An implementation of blockchain technology that is intended as a foundation for developing blockchain applications
- Key technical features:
  - A shared ledger and smart contracts implemented as "chaincode"
  - Privacy and permissioning through membership services
  - Modular architecture and flexible hosting options

- V1.0 released July 2017: contributions by 159 engineers from 27 organizations
  - IBM is one contributor to Hyperledger Fabric

INDUSTRY USE CASES – EXAMPLE

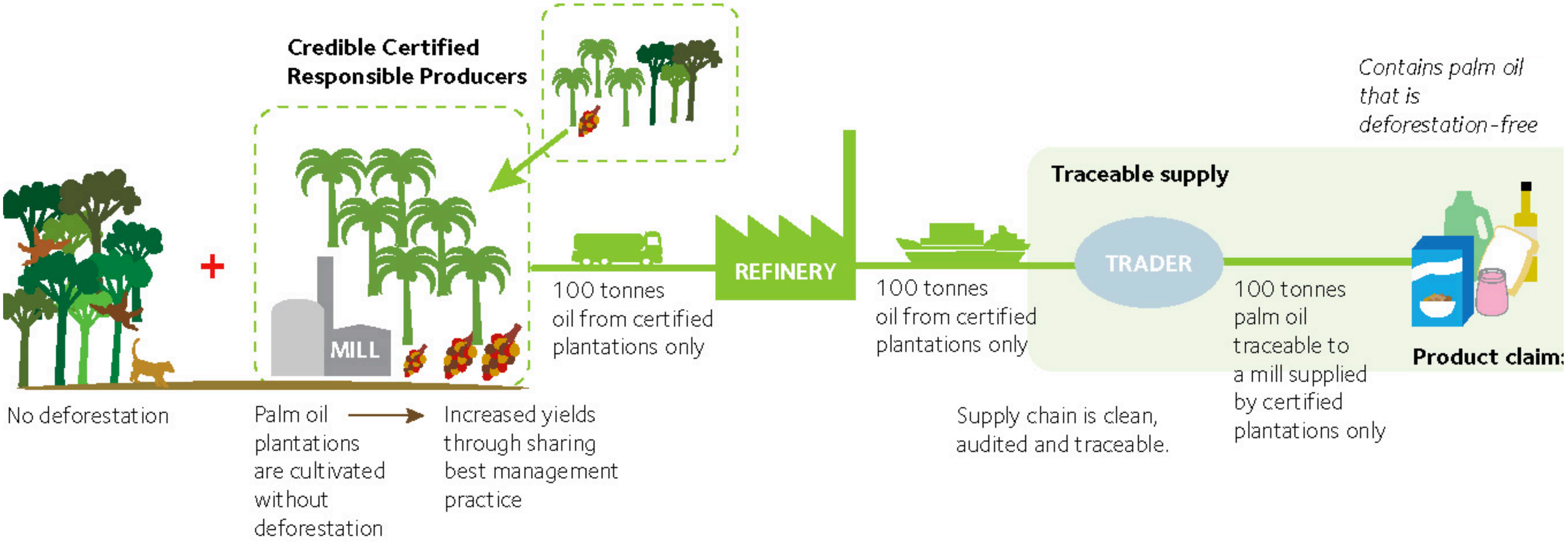
- Ocean to Table - Tuna/Seafood Use Case (using Sawtooth of Hyperledger)

- Farm to table - Coffee use case (using Colored Coin)

HANDS ON ASSIGNMENT

- Problem Identification
  - Digital Asset
  - Trust
  - Multi-party
  - Double Spend
- Problem Definition
  - Business Goal
- Solution Development
  - How to establish consensus?
- Value Articulation

INDUSTRY USE CASE SAMPLE – PALM OIL SUPPLY CHAIN



- Digital Asset - Palm Oil from a land parcel
- Trust - Farmer to mill to NGO
- Multi-party - Yes
- Double Spend - Yes

- Problem Definition - Tracking the provenance of Palm oil from a plantations
- Business Goal - Segregate sustainably sourced palm oil from the rest

- Solution Development
  - How to establish consensus?
- Value Articulation

Cross Industry	Financial	Government	Healthcare	Insurance	Manufacturing Retail &CP
Shared reference data	Letter-of-Credit	Land Registry	Medical records	Claims processing	Supply chain
Internal financial ledger	Cross currency payments	Vehicle Registry	Medicine supply chain	IoT integration for policy monitoring	Product parts
Audit and compliance enablement	Mortgages (and Contracts)	Citizen ID			Provenance tracking
Regulatory view	Collateral Management	Education Certification			Digital Property Management
Improved efficiencies	Post trade settlement	Voting			Real Estate Cars
IoT Cars, Robots, Drones					Trade Agreements, Contract

Telegram

SINGAPORE AIRLINES KRISFLYER

Filecoin

TRADE LENS

Financial Use Cases

Currency Exchange & Remittance	P2P Transfers	Ride Sharing	Data Storage	Trading Platforms	Gaming
Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma	BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)	La'zooz	Storj.io, Peernova	equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares	PlayCoin, Play(on DACx platform), Deckbound

Non-Financial Use Cases

Digital Content/Documents, Storage & Delivery	Authentication & Authorization	Digital Identity	Marketplace
BitProof, Blockcai, Ascribe, ArtPlus, Chainy.Link, Stampery, Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN	The Real McCoy, Degree of Trust, Everpass, BlockVerify,	Sho Card, Uniquid, Onename, Trustatom	Providing premium rights & brand based coins: MyPowers

Smart Contracts	Real Estate	Diamonds	Gold & Silver	Reviews/Endorsement
Otonomos, Mirror, Symbiont, New system Technologies	Factom	Everledger	BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve	TRST.im, Asimov (recruitment services), The World Table

Blockchain in IoT	App Development	Network Infrastructure & APIs	Other
Filament, Chimera-inc.io, ken Code – ePlug	Proof of ownership for modules in app development: Assembly	Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher	Prediction platform: Augur Election Voting: Follow My Vote Patient Records management: BitHealth

INDUSTRY USE CASES SAMPLES & EXAMPLES

SELF LEARNING

1. Hyperledger Composer Playground - https://composer-playground.mybluemix.net/editor

2. Hyperledger Composer Tutorial - https://ibm-blockchain.github.io/develop/tutorials/playground-tutorial

3. Hyperledger Sawtooth (Tuna Supply Chain Video) - https://www.youtube.com/watch?v=8nrVlICgiYM

4. Hyperledger Vehicle Lifecycle Video - https://youtu.be/cNvOQp8r0xo?t=243

5. Blockchain Hyperledger Website - https://www.hyperledger.org/

6. Ethereum Platform Website - https://www.ethereum.org/

7. Bitcoin White Paper - https://bitcoin.org/bitcoin.pdf

RSA CRYPTOGRAPHY

The **public key** is (n = 3233, e = 17). For a padded Plain-Text message m, the encryption function is:

$c = m^{17} \bmod 3233$

Suppose m=65 then cipher text c

$c = (65)^{17} \bmod 3233 = 2790$

Encryption

The **private key** is (n = 3233, d = 2753). For an encrypted cipher-text c, the decryption function is:

$m = c^{2753} \bmod 3233$

In the above example c=2790 if we get message m again then:

$m = (2790)^{2753} \bmod 3233 = 65$

Decryption