A Distributed Future: Blockchain and its Potential

Brian Rogers & Nir Kabessa

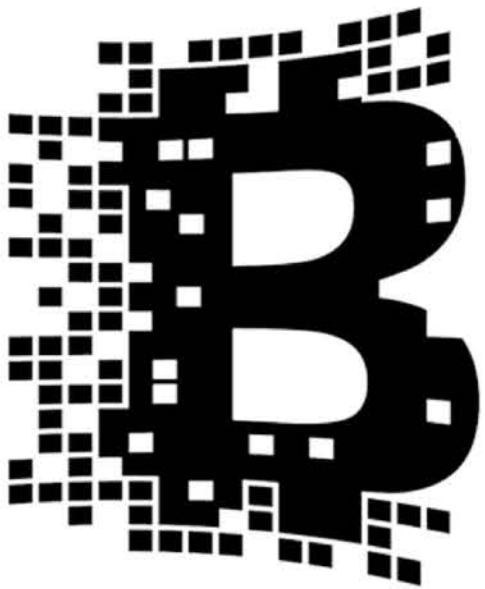
COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

EMERGING TECHNOLOGIES

COLUMBIA BLOCKCHAIN ALLIANCE

BLOCKCHAIN @ COLUMBIA

WHAT IS THE INTERNET (1994)?



=

NOT REALLY

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

COLUMBIA BLOCKCHAIN ALLIANCE

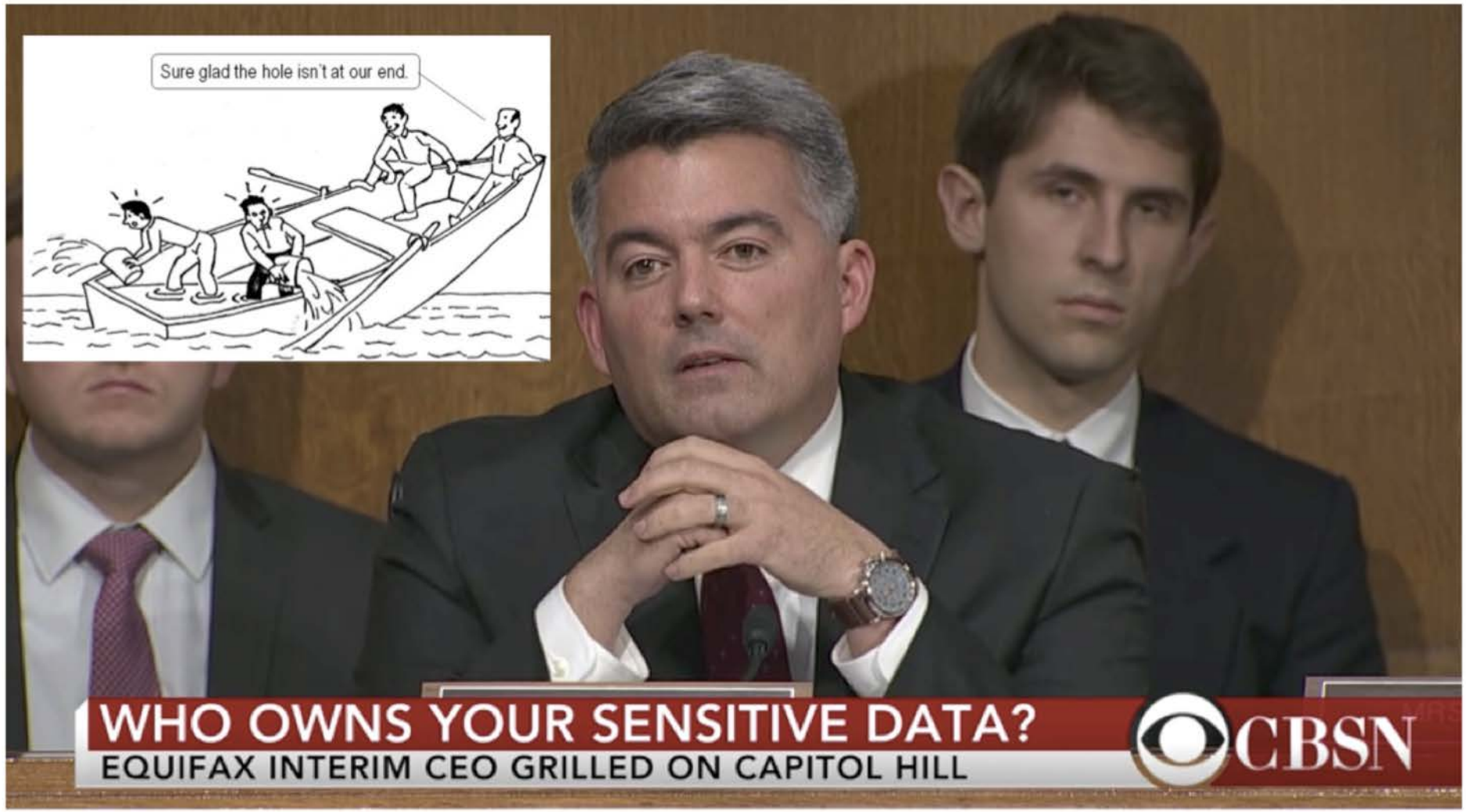
BLOCKCHAIN @ COLUMBIA

“virtually every programmer that has started to understand blockchain technology will say – This is the big breakthrough. This is the thing we’ve been waiting for!”

“He solved all the problems. Whoever he is, he should get the Nobel Prize – he’s a genius.”

- Marc Andreessen, co-founder Netscape

“All the consumer [my] data that defines my life I have no control over?”

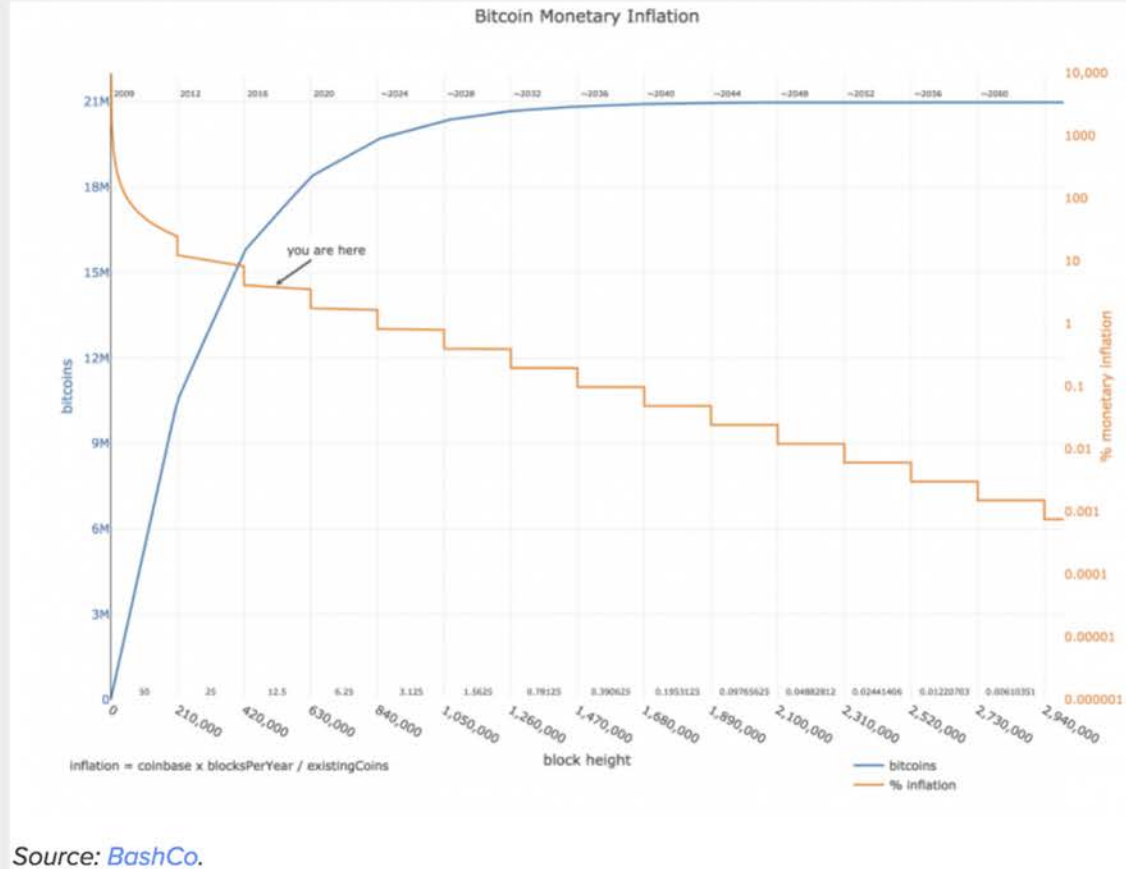


U.S. Senator Cory Gardner of Colorado

Bitcoin: A Peer-to-Peer Electronic Cash System

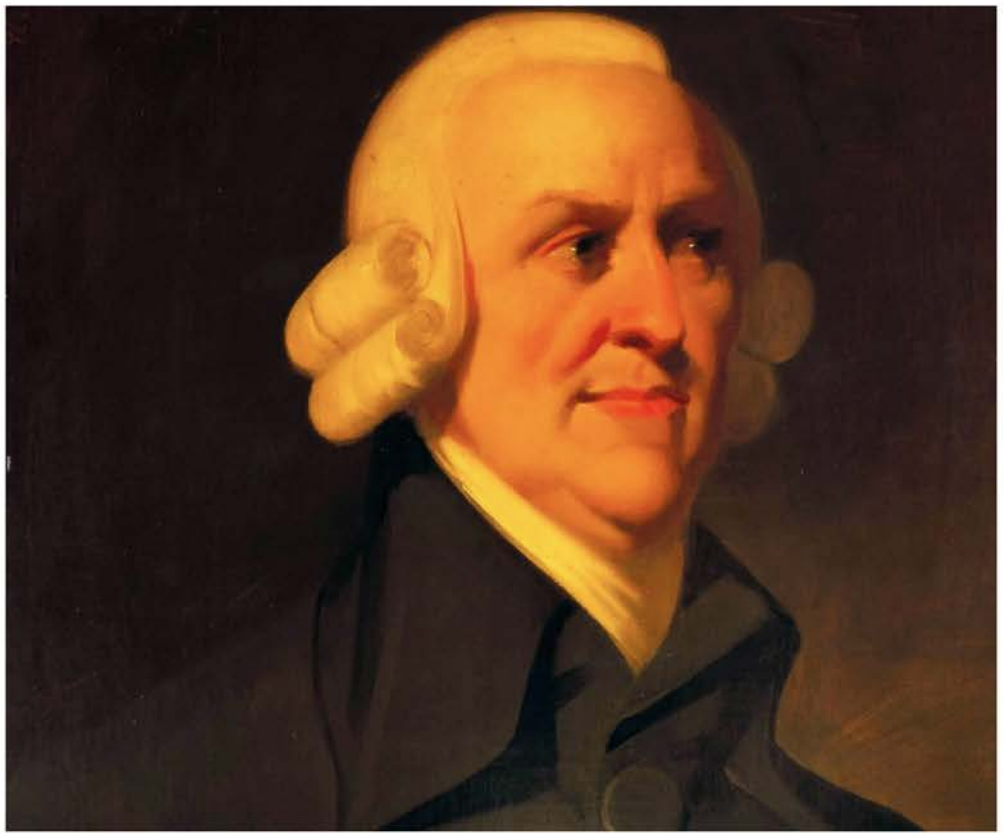
bitcoin

- Only 21 million coins will be mined, roughly 17 million mined to date
- Network reward started at 50 Bitcoin, every 4 years it's reduced by 50% – today it's at 12.5
- A block of transactions is added to the Bitcoin Blockchain every 10 minutes (~546k now)
- On average 2020 transaction/block (1 MB)
- Difficulty changes every 2016 blocks
- Supply will continue to increase, but at a decreasing rate, asymptotically approaching 21 million by 2140 (include graph)
- Each unit of Bitcoin is divided into 100,000,000 units



Source: BashCo.

A person's self-interest - service the public need



"It is not from the benevolence of the butcher, the brewer or the baker, that we expect our dinner, but from their regard to their own self interest."

- Adam Smith

Adam Smith

Announce

Asymmetric
Cryptographically sign
(strong control of ownership)

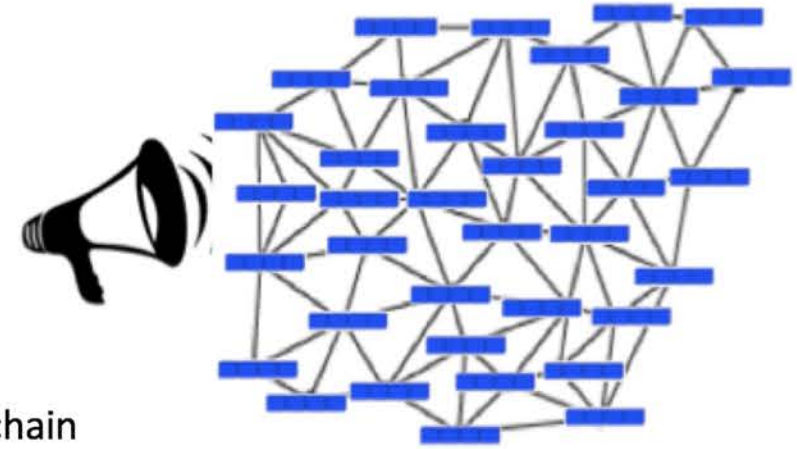
```
0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50
```

Validators/Miners
Every 10 minutes a few hundred transactions are collected.

Show how much
& to who

One Solves the problem

Add the new block to the blockchain and broadcast to all nodes



Proof of Work (PoW)
Each node has to show that it has performed some amount of work. The work is in the form of solving a difficult math (difficulty).

Proof of Stake (PoS)
Involving a user's stake or ownership of virtual currency in the blockchain system.

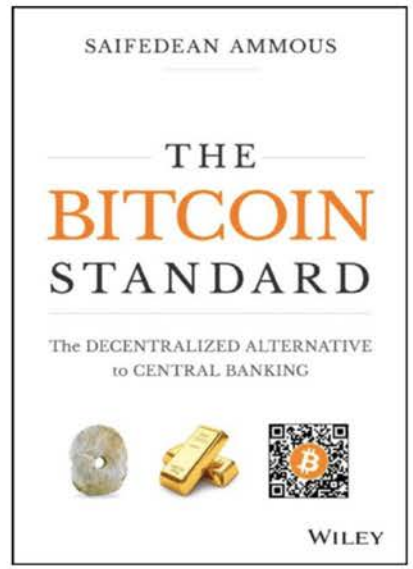
Proof of Authority (PoA)
uses a set of "authorities" - nodes that are explicitly allowed to create new blocks and secure the blockchain

Consensus mechanisms allow secure updating of a distributed shared state, ensuring the sanctity of data.

How Safe Is Bitcoin From Hackers?

1. It's barebones simplicity
2. It's vast processing power doing nothing but ensuring safety.
3. Distributed nodes with need to achieve consensus

You wouldn't be hacking one person, but rather every record in the Bitcoin network since its inception all at once.



Hash Rate/hashes per second (attempts made SHA-256)
Measure of how much power it takes to solve the problem

Current hash rate 50 TH/s or **300,000x** more powerful than the most powerful supercomputer the Tianhe-2. Or equivalent of **2 trillion laptops**


China's Intel-based Tianhe-2 Super computer

51% Attack
If a single entity had more capacity than the existing network, it could continue the blockchain with a new block

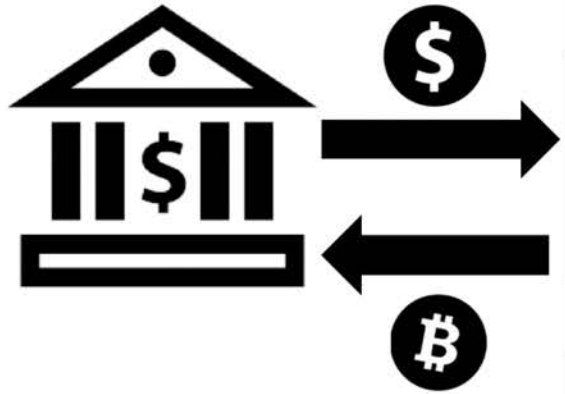
- 1 hour of electricity ~$550,000 & ~$1 billion in hardware costs*

* According to ccn.com

Fly in Amber: Immutable & Clearly Visible

18.9: © PjrStudio/Alamy.

– Nick Szabo



Centralized Exchanges

coinbase POLONIEX BINANCE

kraken GEMINI

Decentralized Exchanges (DEXs)

IDEX waves Oasis dDEX

HOT

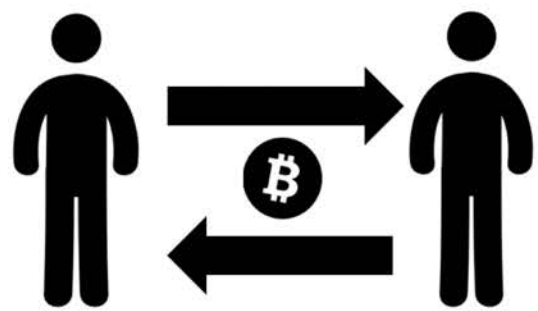
mycelium ad-hoc economy Jaxx

bread

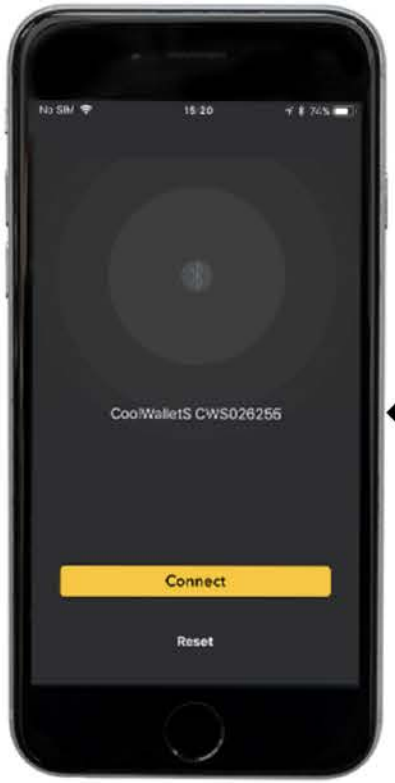
COLD

TREZOR keepkey

Ledger CoolWallet S



The Future of Banking?



Your new Bank!

If you want to deposit

celsius

Earn up to 7% on crypto deposits

Or simply use the card's NFC to pay directly

1. Using encrypted Bluetooth pair with your phone
2. Enter the amount you want to pay

No Exchange Rates, and transfer in SECONDS

2018 Q1 Binance was more profitable than Deutsche Bank and only $9 million shy of NASDAQ
On track to have $1 billion in profits by end of 2018

BLOCKCHAIN/DISTRIBUTED LEDGER TECHNOLOGY (DLT)

Not just a breakthrough in financial technology
To move data of value securely and privately

Types of Blockchain

Permissionless (Public)

- Consensus algorithms open sourced and not permissioned.
- Anyone can participate without permission.
- Network is held together by strangers in trustless state of aligned economic incentives.
- Examples: Bitcoin, Ethereum, Monero, Dash, and Litecoin

Permissioned (Private)

- Validator is a member of a consortium or separate legal entities of the same organization.
- Permission is restricted to a single organization/consortium, pre-approved parties to write on the blockchain.
- Much faster, no need to wait for confirmation from thousands of nodes

Inflection Point for Blockchain

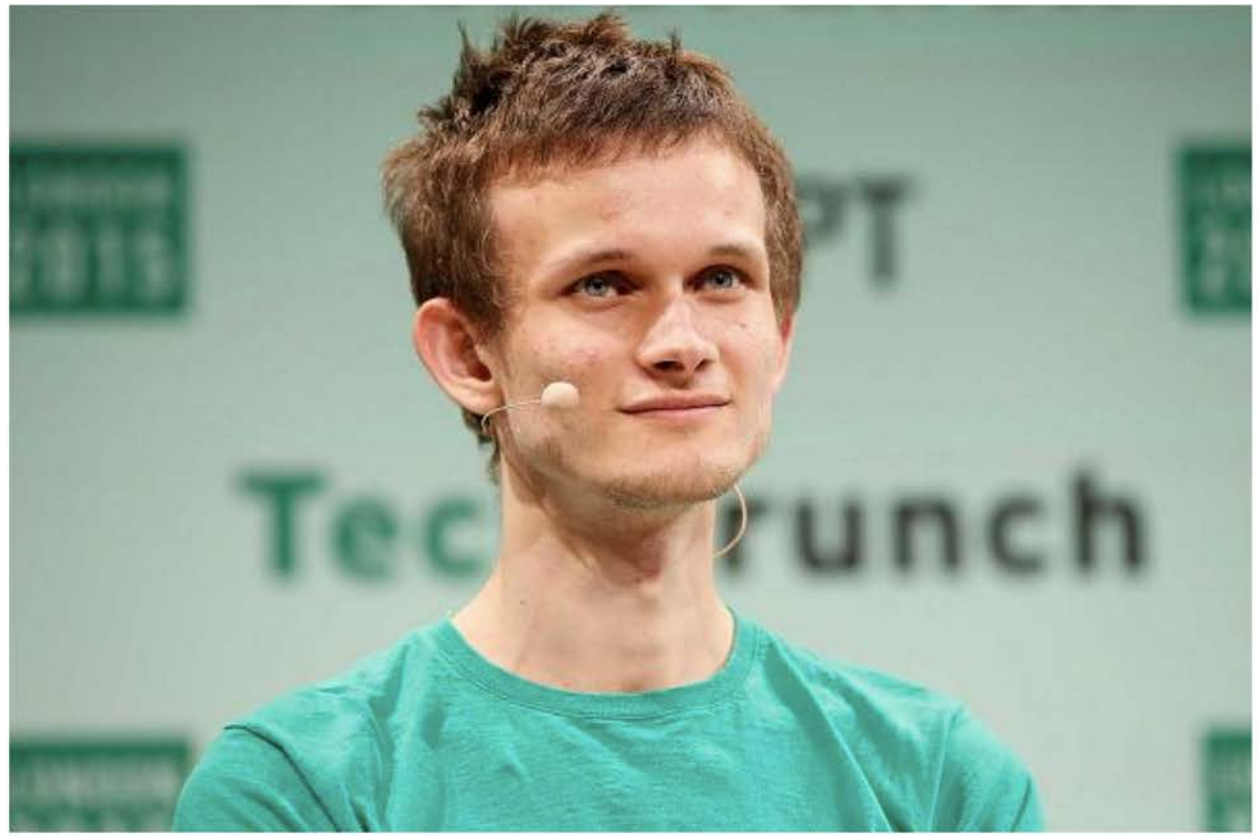
July 2015

ETHEREUM

Virtual Machine

$31.5B Market Cap

2017 value increased 3000%



Vitalik Buterin

TURING-COMPLETENESS

Turing complete contract scripting language Solidity, making the creation of more sophisticated logic possible in blockchains;

Why Turing-Completeness Matters

DApps

&

Smart Contracts

Decentralized Applications DApp

With just the Internet, an open protocol, and a new kind of asset, we can instantiate networks that dynamically assemble the resources necessary to provide many kinds of services.

DApp

Smart Contracts

Not Smart Nor a Contract
- Self-executing contracts, which avoids the services of a middleman

- *An asset or currency is transferred into a program*
- *Program runs this code*
- *It automatically validates a condition*
- *Automatically determines whether the asset should go to one person or back to the other person*
- *The decentralized ledger stores and replicates the document which gives it a certain security and immutability.*

- Vitalik Buterin

Objective versus Subjective

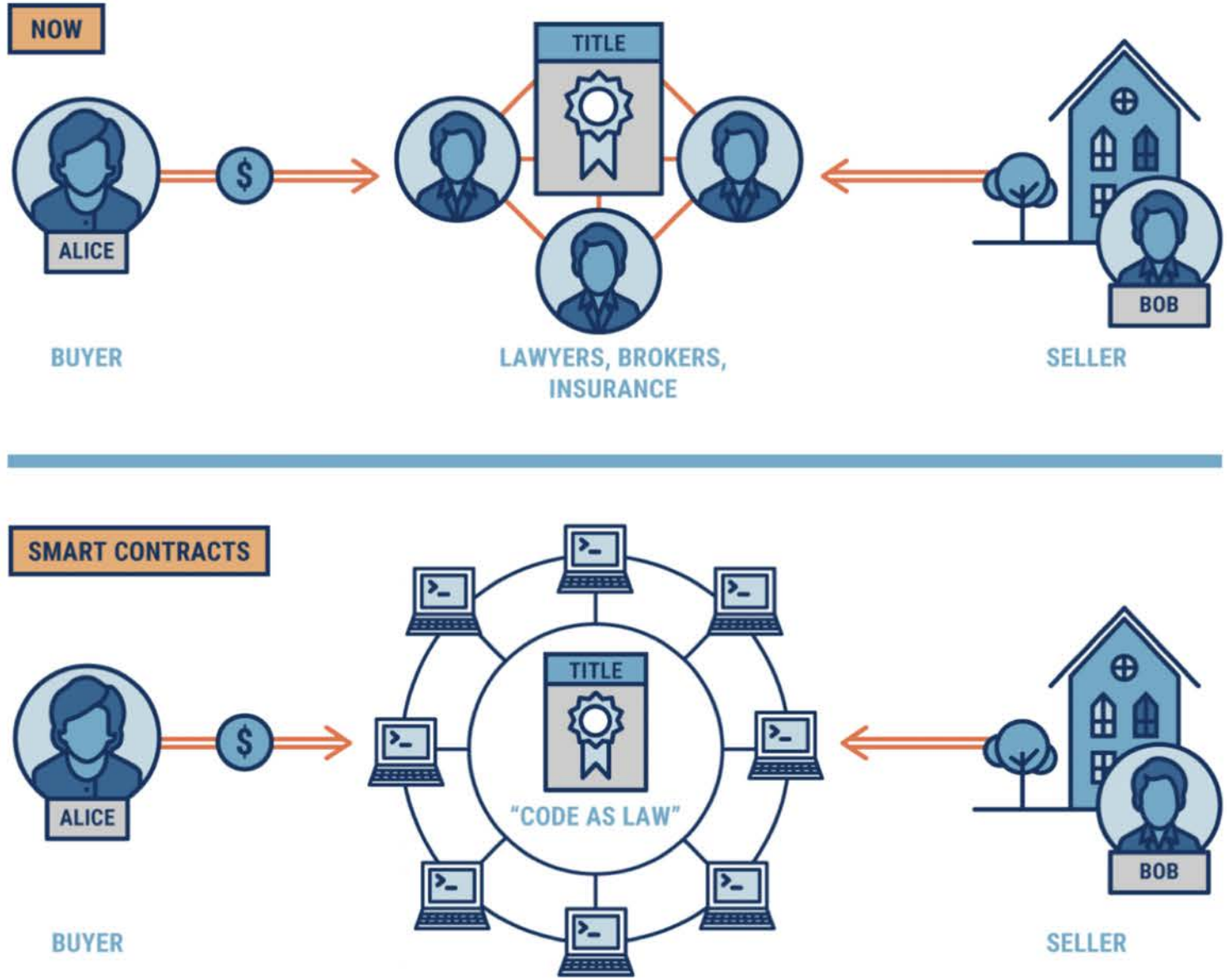
```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

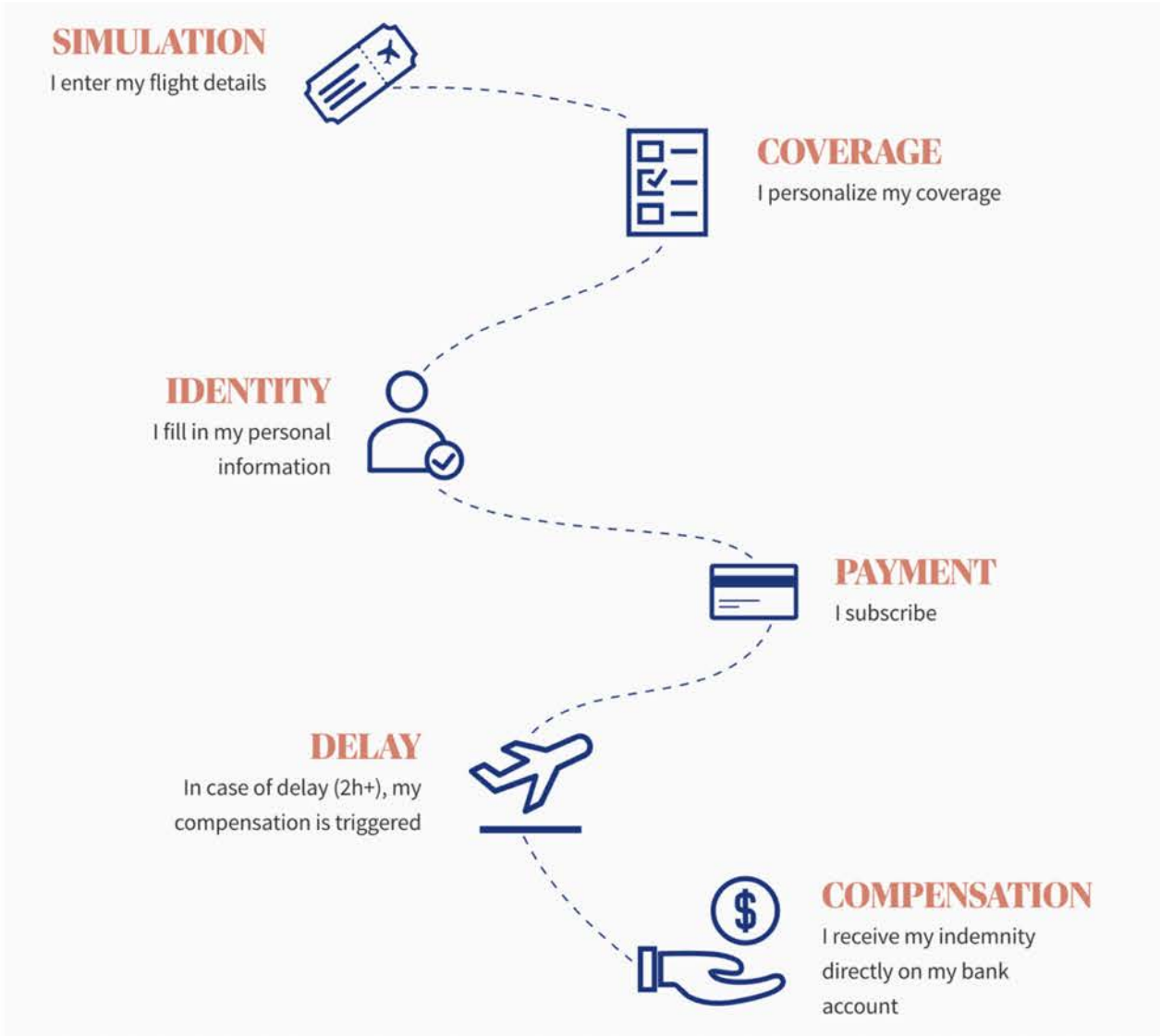
Allow another contract to spend some tokens in your behalf

Approve & then communicate the approval

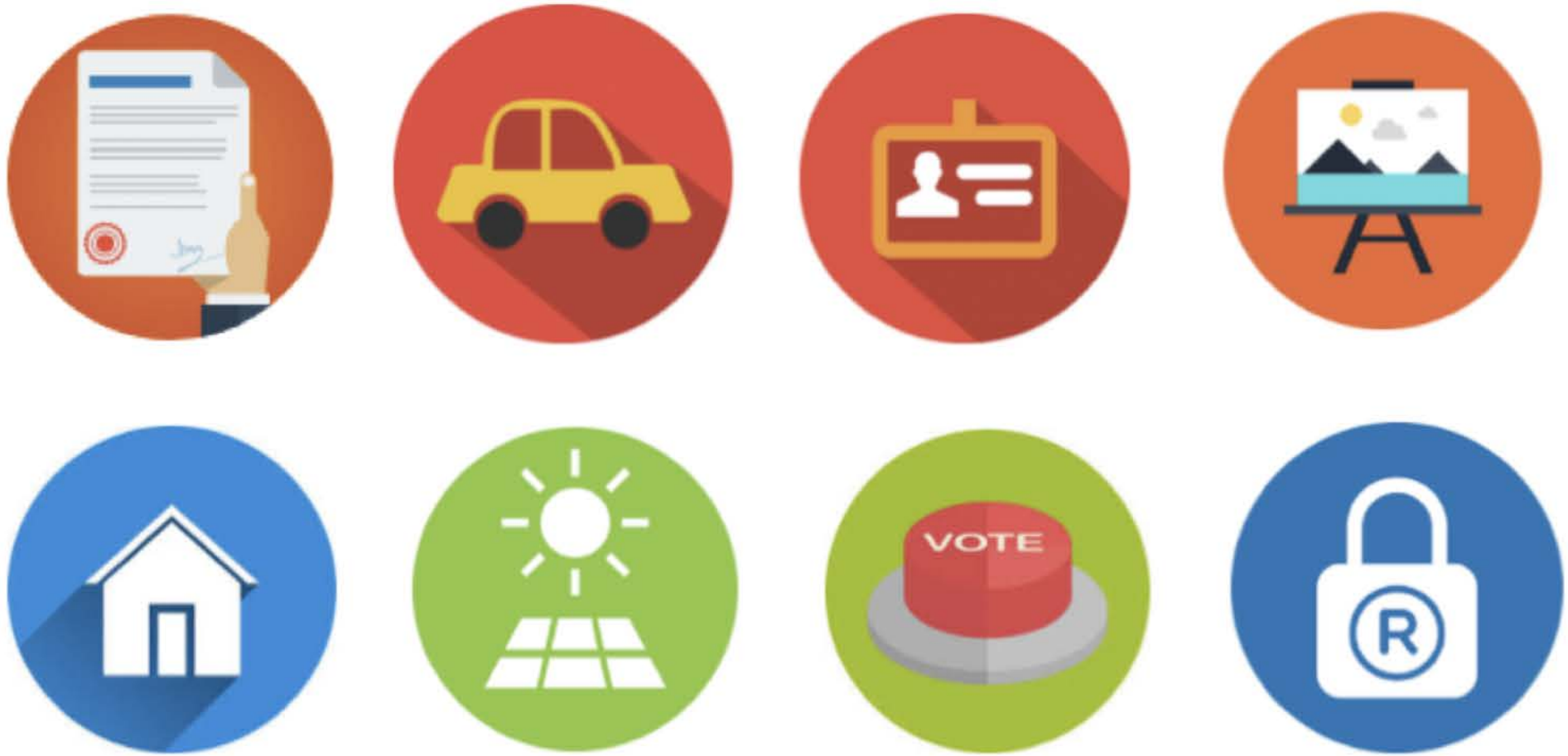
A contract attempts to get the coins

Function is called whenever someone tries to send cryptocurrency to it


NOW
TITLE
ALICE
$
BOB
BUYER
LAWYERS, BROKERS, INSURANCE
SELLER
SMART CONTRACTS
TITLE
ALICE
$
"CODE AS LAW"
BOB
BUYER
SELLER
CBINSIGHTS


SIMULATION
I enter my flight details
COVERAGE
I personalize my coverage
IDENTITY
I fill in my personal information
PAYMENT
I subscribe
DELAY
In case of delay (2h+), my compensation is triggered
COMPENSATION
I receive my indemnity directly on my bank account

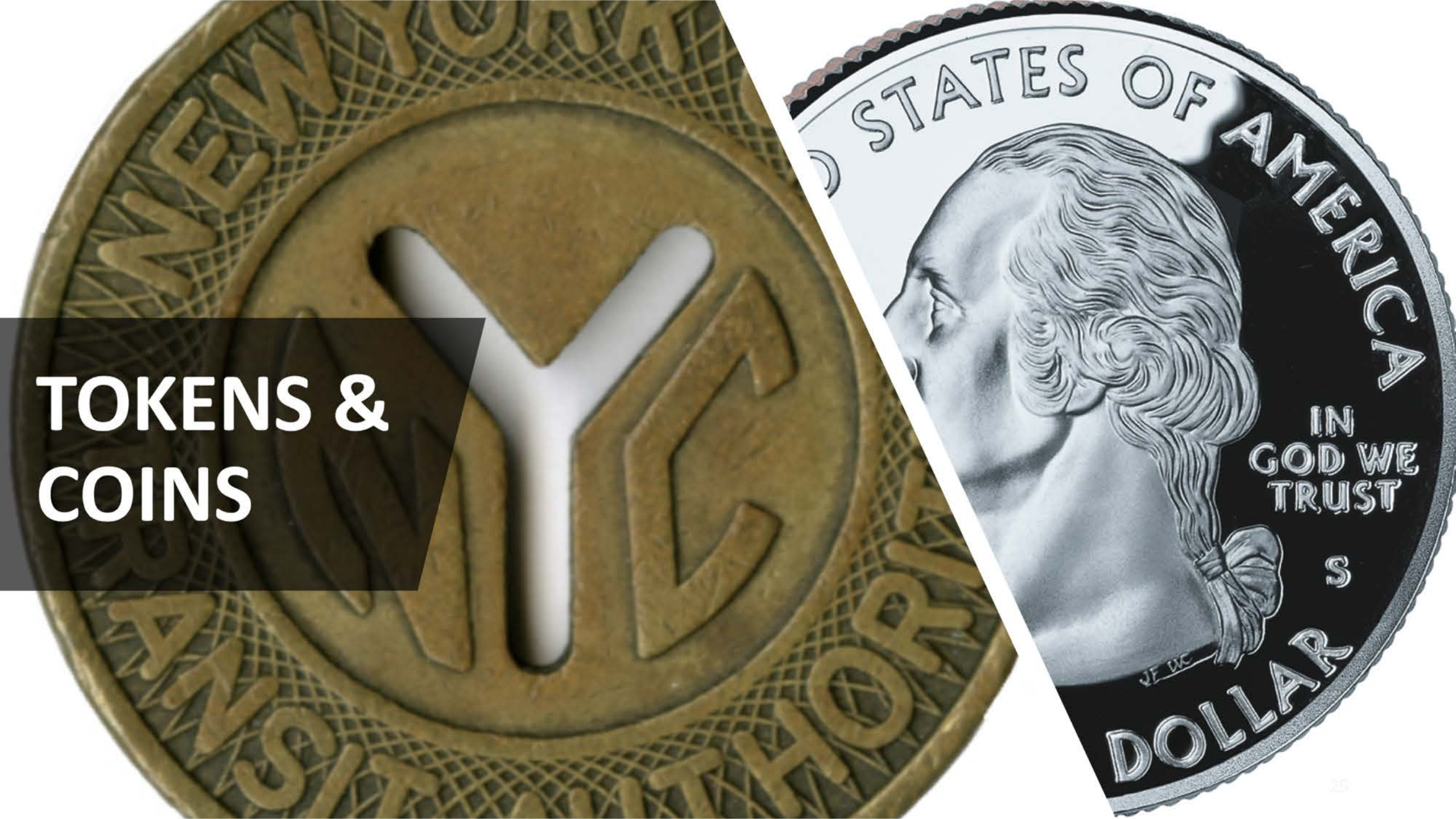
THINGS OF VALUE



2005 Land Rover Discovery		
001	Sold to Frank	10/5/16
002	Oil change	12/1/16
003	Install brush guard	12/15/16
004	Sold to Lisa	01/12/17

2005 Land Rover Discovery				
Last Owner	001	Sold to Frank	10/5/16	
Roof Us	003	Moon roof leaking	11/2/16	
LR Service	004	Frt pass window	11/5/16	
Jiffy Oil	005	Oil Change	12/1/16	
LR Service	006	Audio system failure	12/7/16	
British GR	007	Install brush guard	12/15/16	
LR Service	008	Transmission issue	12/27/16	
Frank	001	Sold to Lisa	01/12/17	

TOKENS & COINS



Simplified – Some sources will represent differently

Protocol Tokens/Coins

Provide the financial incentives needed to drive a cryptoeconomic protocol – **standardized**, with global value (i.e. bitcoin, Zcash, Filecoin, Litecoin).

App/Asset Tokens

Enabling decentralized applications, providing no cryptoeconomic mechanism. DApps merely facilitate access to protocols – **non-standardized**.

Types of App Tokens

Payment Tokens - Cryptocurrency

Digital currency operating independently of a central bank

Securities Token

Cryptographically represents underlying traditional assets such as equity, real estate, gold, etc

Utility Token

Provides a user access to a digital service/application or to act as a key for the execution of digital transactions (i.e. Filecoin: use & contribute storage space).

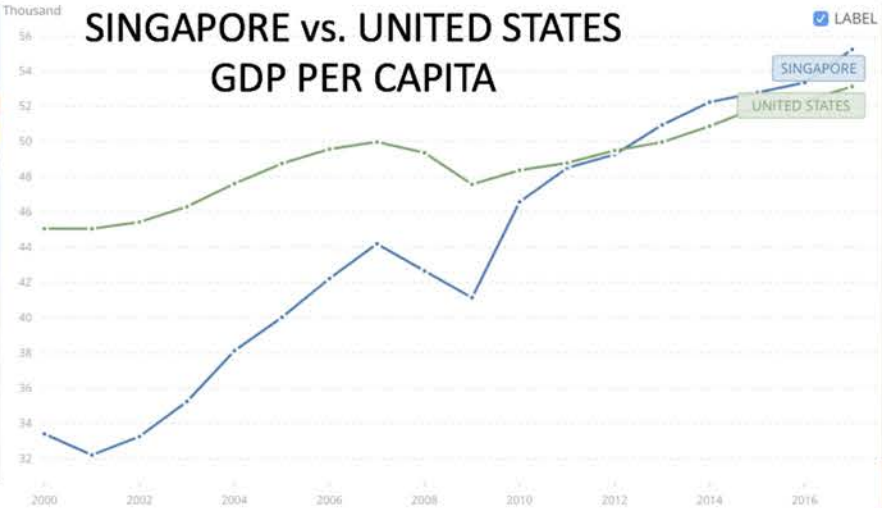

U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV
IGNORE
ME

A New Asset Class – Crypto asset or Security?

Crypto assets are a new asset class that enable decentralized applications. And like every other asset class, they exist as a mechanism to allocate resources to a specific form of organization.

AS other Asset Classes;

- **Corporate equities** serve **companies**
- **Government bonds** serve **nations, states, municipalities**
- **Mortgages** serve **property owners**
- **Crypto** assets serve **decentralized applications**



Jay Clayton, SEC Chairman

"There's no token that I have seen – that are not securities"

"We are not going to do any violence to the traditional definition of a security that has worked for a long time"

Damien Pang, Head of Technology Infrastructure Monetary Authority of Singapore

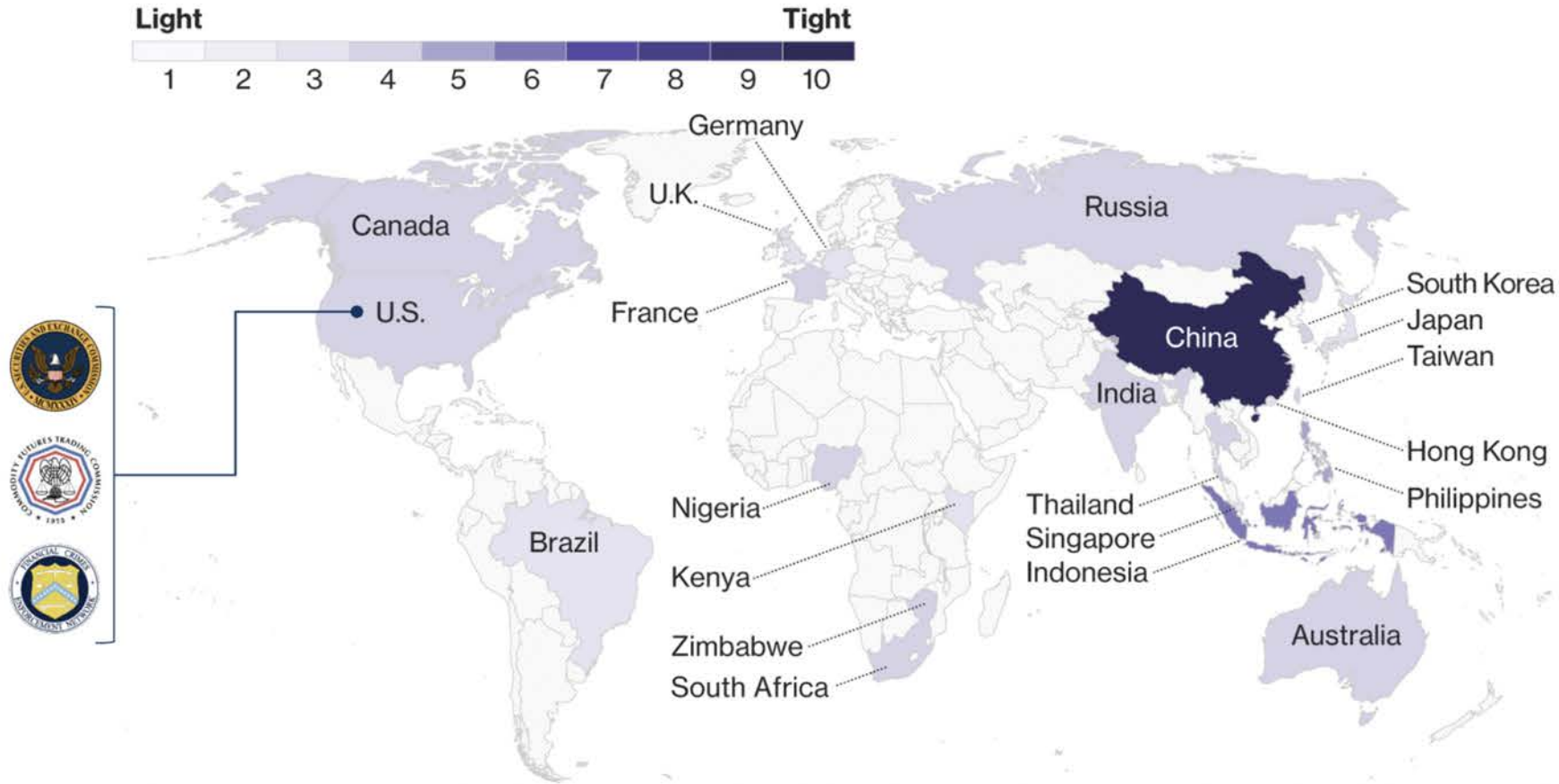
"MAS does not intend to regulate utility tokens that are used to access certain services….Most tokens I've seen are NOT securities" – Consensus Singapore 2018

Hester M. Pierce, SEC Commissioner (dissent on ETF disapproval)

"I reject the role of gatekeeper of innovation"

Types of Regulation

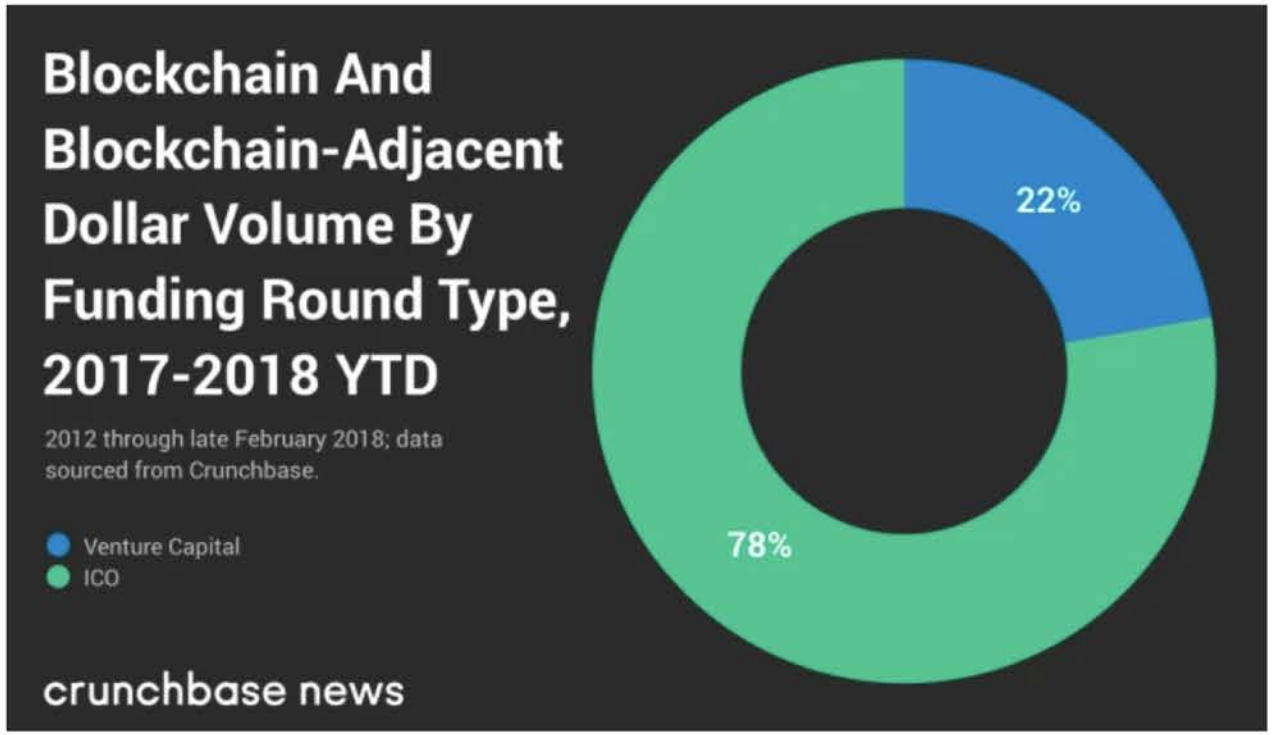
- Closed – China
- Open but Strict (proceed with caution) – USA
- Open and Liberal – Switzerland & Malta



CBINSIGHTS Source: Bloomberg

Initial Coin Offerings (ICOs)

2016 - $98.6 million
2017 - $6.2 billion
2018 - $20.8 billion



EOS™ **$4 billion**

Telegram **$1.7 billion**

DRAGONCHAIN **$320 million**

Filecoin **$257 million**
$200 million in 60 min!

Tezos **$232 million**

https://www.coinschedule.com/stats.html

Jamie Dimon. Photo by David A. Grogan | CNBC 2017

"I'd fire them in a second. For two reasons: It's against our rules, and they're stupid. And both are dangerous."

"It's a fraud" and "worse than tulip bulbs."

"There is a use case for bitcoin. If you live in Venezuela, North Korea … if you're a criminal. Great product,"

JPMorgan Chase & Co.

Launching a payment processing network on their Quorum – Canada, Australia, and New Zealand

Bank of America

Filed 20 patents on blockchain technology

Goldman Sachs

Considering a **bitcoin** trading operation
Granted SETLcoin patent
Lead investor $50 million Circle Financial

citi

Partnering with Nasdaq blockchain cross-borders payments

WELLS FARGO

Partnering with Swift's blockchain initiative. Has submitted patent applications

Permissioned Private Ledgers

Permissioned (Private)

- Validator is a member of a consortium or separate legal entities of the same organization.
- Permission is restricted to a single organization/consortium, allowing only internal, pre-approved parties to write on the blockchain.
- Much faster, no need to wait for confirmation from thousands of nodes
- Examples: Hyperledger Fabric, R3 (Corda),

HYPERLEDGER

r3 corda

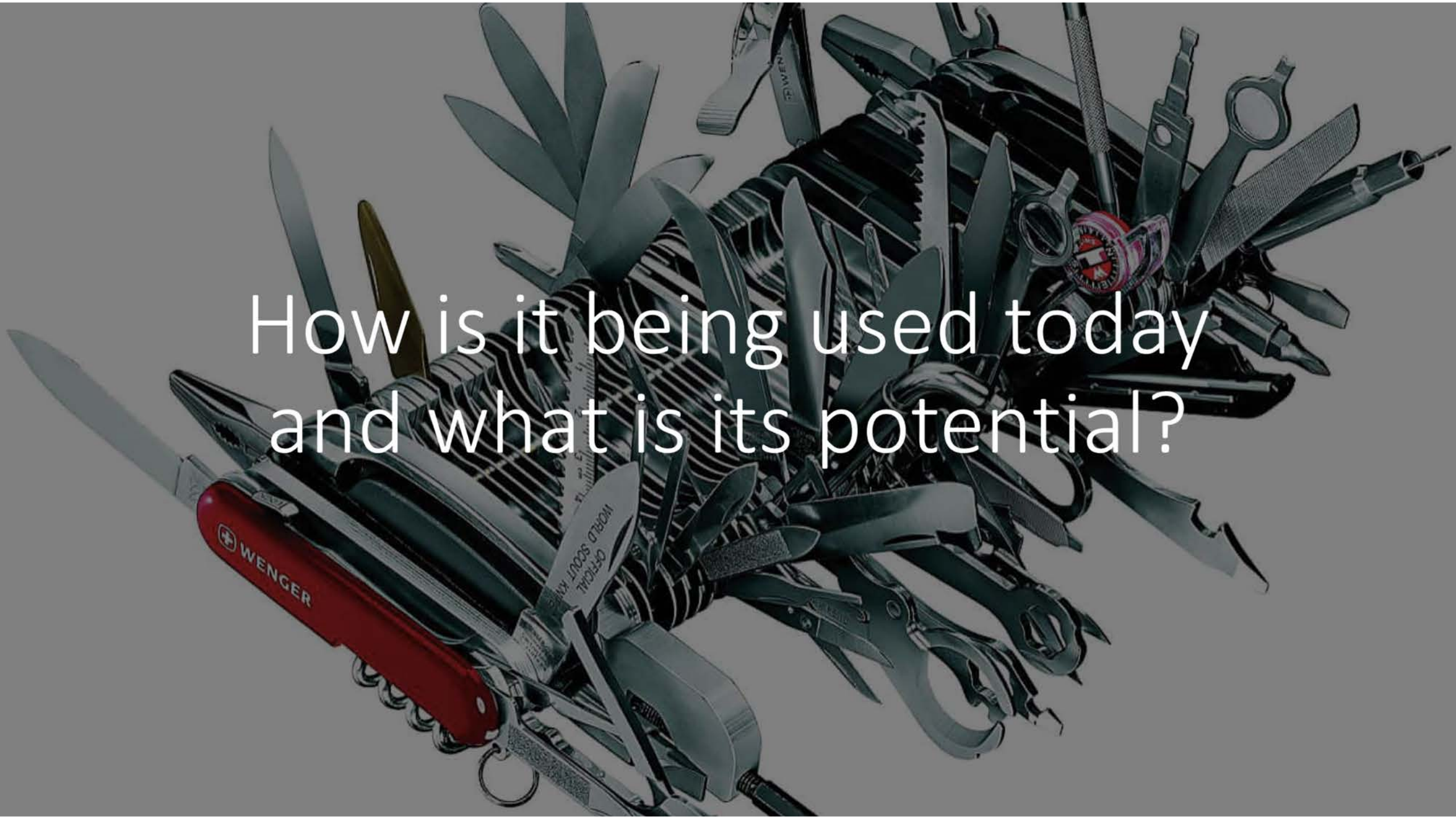
Quorum

Notable Organizations Moving to Blockchain

DTCC

ripple

MOBI



How is it being used today and what is its potential?

Trustless Voting

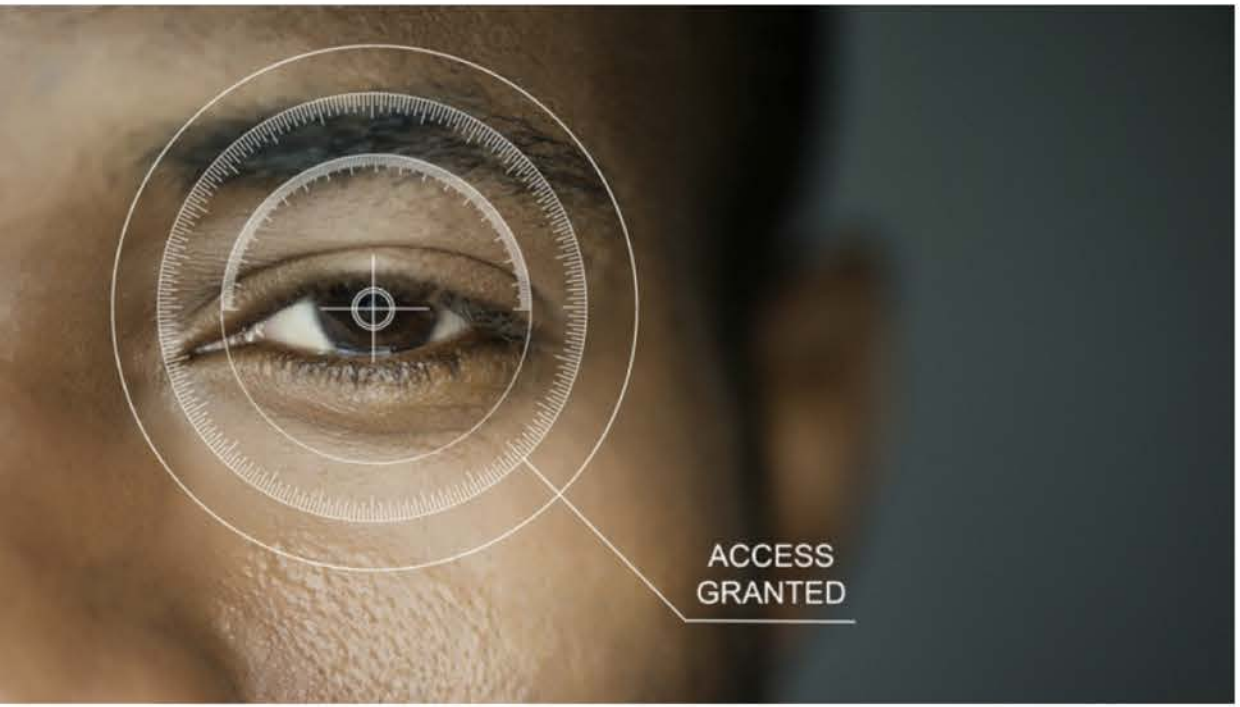
- Anonymous yet transparent voting
- Sierra Leone Elections
- Governments, institutions, board rooms, DAOs

Democracy.Earth

Agora

MAKER

Identity / Personal Data



- Refugee identities
  - Iris-scanning IDs
  - Direct Aid
  - Syrian Refugees in Jordan

- Medical Health Records
  - Emergency Situations
  - Research

Columbia University in the City of New York

Columbia Blockchain Alliance

Blockchain @ Columbia

Tokenization of Illiquid/Non-Fungible Assets

Est $11 Trillion Market*

"Tokenization of everything allows us to have fundamentally new avenues for sharing value globally…. in the same way that we can share information and content"
- Jeremy Allaire, CEO of Circle

Commodities

Exclusive Goods

Securitized Assets

Private Capital

Natively Digital Assets

*Source: AlphaPoint

Asset-Backed Tokens or USDs? Fungible/Non-Fungible

ST REGIS
ASPEN

18.9% Tokenized

"Tokenization of everything allows us to have fundamentally new avenues for sharing value globally…. in the same way that we can share information and content" - Jeremy Allaire, CEO of Circle

Diamonds Moving From Non-Fungible to Fungible

Provenance Financial Products

VULT

Financial Trade in Gold is 275x the Physical Trade

Actual
Gold Trade (US$ Billion p.a.)

Potential for Financialized
Polished Diamond Trade (US$ Billion p.a.)

Financial Trade in Gold is 275X the Physical Trade Source: Gold – A Physical Investment Asset Class Case Study, World Gold Council, Bloomberg

Tokenization of Gold

Bars of Gold divisible and transferable on the blockchain

1 gram = 1 Token

DIGIX

ONEGRAM

Collectibles

- Baseball Cards! MLB Crypto
  - Augmented Reality
  - Magic the Gathering, Pokémon…

- Art, Crypto Collectibles
  - CryptoKitty sold for $170k
- Fantasy Sports

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

COLUMBIA BLOCKCHAIN ALLIANCE

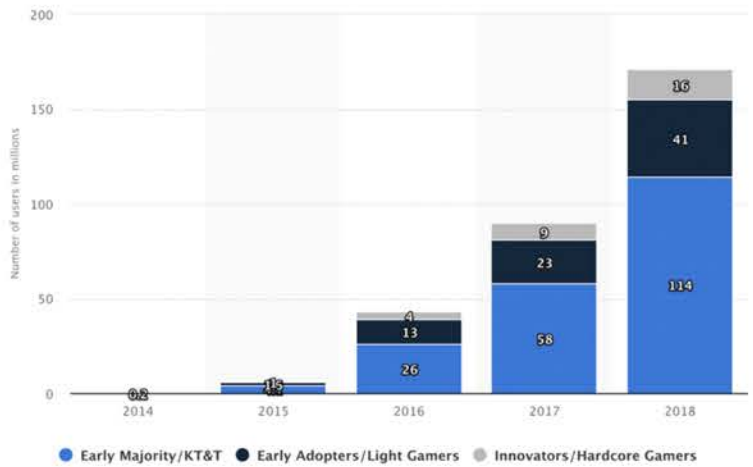
BLOCKCHAIN @ COLUMBIA

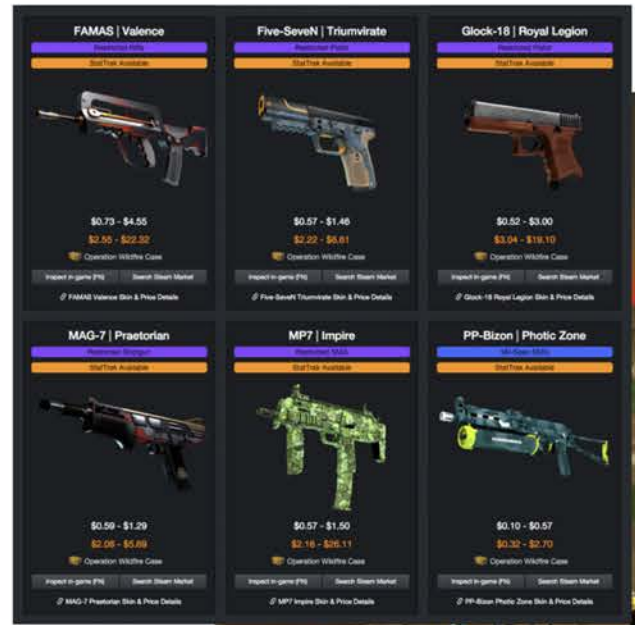
PlayerShare

Digital Scarcity

DECENTRALAND

- Value in virtual realities
  - Transferrable assets





>150M Users worldwide

- Immutable accounts, characters, worlds.

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

COLUMBIA BLOCKCHAIN ALLIANCE

BLOCKCHAIN @ COLUMBIA

loom

Exchange

- Cheap and swift exchange of digital assets

0x

- Decentralized orderbooks and relays connect markets and provide liquidity

paradigm

STUDENT PROJECT

Bancor

Columbia University in the City of New York

Columbia Blockchain Alliance

Blockchain @ Columbia

My Project – Head of Product (Permissionless & Permissioned)

AUGMATE

CONSUMER COMMERCIAL INDUSTRIAL

HYPERLEDGER RChain COOPERATIVE IOTA

ups verizon accenture High performance. Delivered. PEUGEOT Pfizer

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

COLUMBIA BLOCKCHAIN ALLIANCE

BLOCKCHAIN @ COLUMBIA

Permissionless

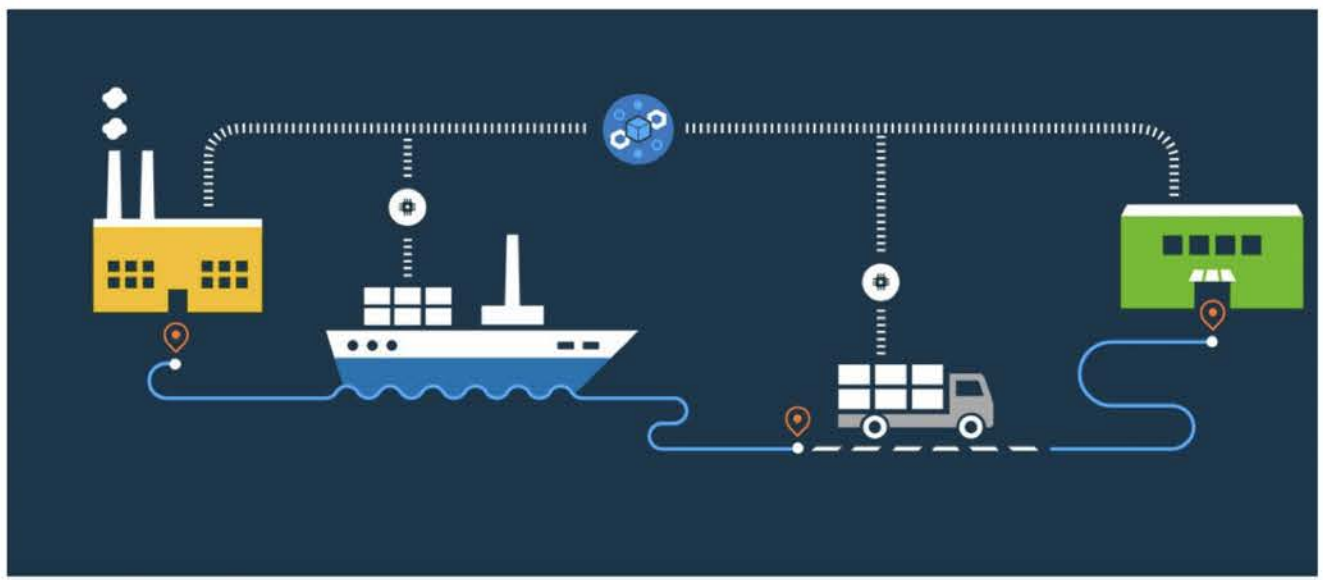
Permissioned

How Enterprises are Using DLT (Permissioned)

IBM Food Trust Hyperledger consortium – Dole, Unilever, Walmart, Golden State Foods, Kroger and Nestle, as well as Tyson Foods, McLane Company and McCormick and Company

Walmart Test Trace Mango Origin

- Traditional – 6 days, 18 hours, and 26 minutes
- Blockchain – 2.2 seconds



Source: IBM blockchain

Content

- Content licensing rights / royalties / contracts

BitRights

STUDENT PROJECT

- Media Platforms
  - Avg 1,300 streams/m at a $10/m = $0.00769 /stream, Spotify pays $0.00397 to artists

Choon

- Attention Economies

Basic Attention Token (BAT)

Columbia University in the City of New York

Columbia Blockchain Alliance

Blockchain @ Columbia

Decentralized File Storage and Compute

Compute

golem

iexec

Storage

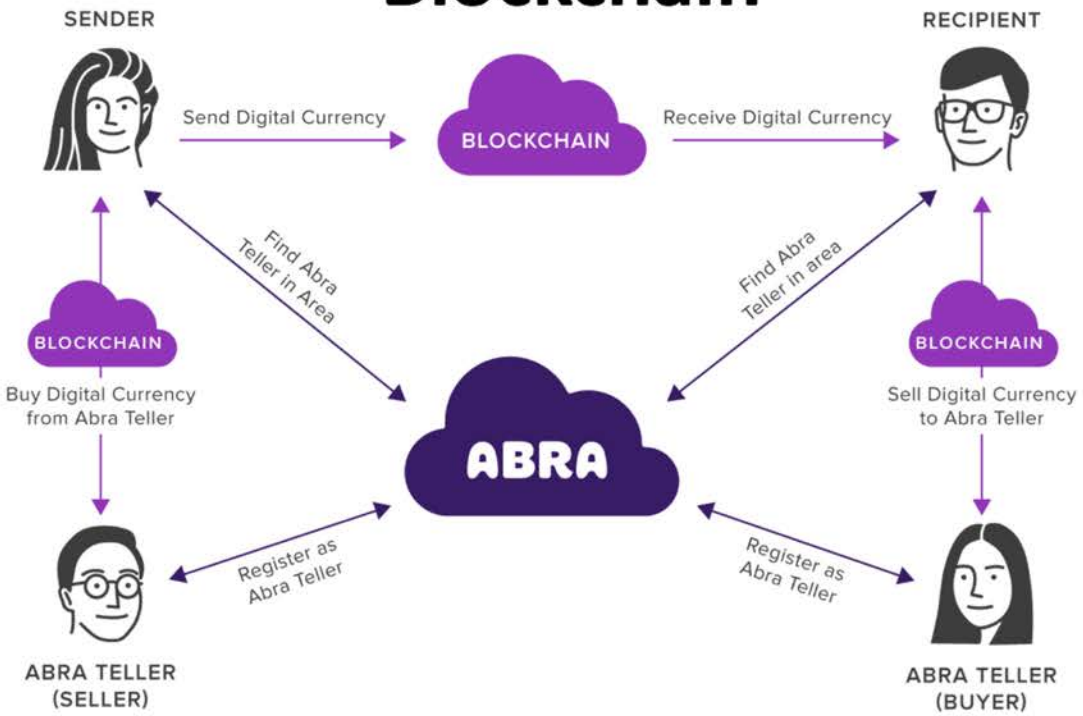
Filecoin

IPFS

STORJ

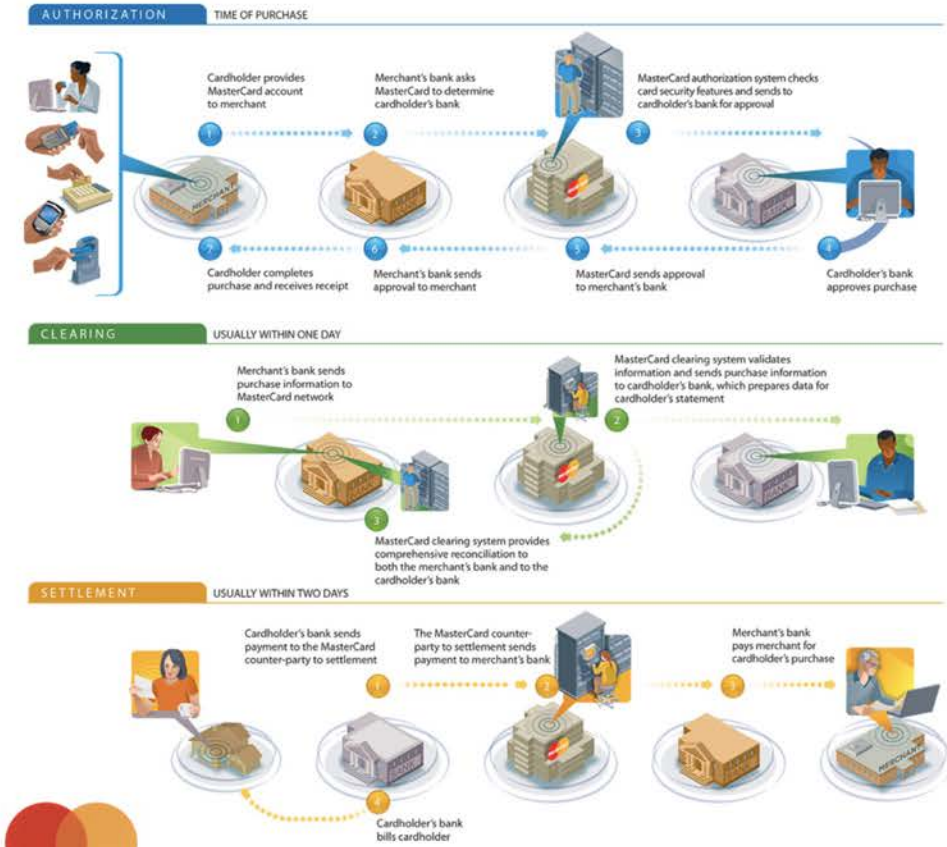
Clearing & Settling Money

Blockchain



veem ABRA BitPesa Bitspark

Current Banking



mastercard.

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

COLUMBIA BLOCKCHAIN ALLIANCE

BLOCKCHAIN @ COLUMBIA

Incentives Work

Inspired by the DARPA Challenge to find 10 balloons placed all over America
The balloons were all found by a team at MIT in **less than 9 hours**!

nCent is a new blockchain that tracks the value users contribute to an incentive program

Team from MIT promised $2000 to the first person who submitted the correct coordinates for a single balloon
…$1000 to whomever invited that person
…$500 to the person who invited the inviter
….and so on

Essentially they created an incentive market

"Our network tokens, called NCNT, efficiently track the provenance (or referral) chain of a user and provide the exchange mechanism for correct payouts."

SEQUOIA

WINKLEVOSS CAPITAL

Steve Jurvetson

Stanford University

Columbia University in the City of New York

Columbia Blockchain Alliance

Blockchain @ Columbia

Brian Rogers

Co-Founder & Chair
Columbia Blockchain Alliance
bdr2124@columbia.edu
https://www.linkedin.com/in/brogers/
@brdotcom

Nir Kabessa

President
Blockchain @ Columbia
nir.k@columbia.edu
https://www.linkedin.com/in/nir-kabessa-483878116/
@nirkabessa

References

https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/#133489681183
https://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf
https://docs.google.com/spreadsheets/d/1QxOV2dgxO3C_TyVE0-41ZwLlzPmB-EE1NNshJGuedCU/edit#gid=0
https://www.scribd.com/document/360469179/The-SAFT-Project-Whitepaper\
https://news.21.co/thoughts-on-tokens-436109aabcbe
http://www.usv.com/blog/fat-protocols
https://medium.com/@tonywillenberg/fractional-reserve-banking-the-bitcoin-crypto-economy-b2a9f2e28073
https://plato.stanford.edu/entries/convention/
https://medium.com/@getongab/announcing-the-worlds-first-reg-a-ico-e9965c61669b
https://bitcoinexchangeguide.com/blockchain-distributed-ledger-technology/
https://medium.freecodecamp.org/how-does-blockchain-really-work-i-built-an-app-to-show-you-6b70cd4caf7d
https://www.trulioo.com/blog/bitcoin-regulation/
https://amlbitcoin.com/
https://medium.com/blockchain-review/how-to-do-an-ico-d02c54a990c2
http://www.loc.gov/law/help/bitcoin-survey/#_ftn60
https://www.coindesk.com/understanding-segwit2x-bitcoins-next-fork-might-different/
https://en.wikipedia.org/wiki/Bitcoin
https://medium.com/@Join_Civil/the-civil-cryptoeconomic-whitepaper-1a42a7ff038d
https://www.forbes.com/sites/rogeraitken/2017/08/22/ibm-forges-blockchain-collaboration-with-nestle-walmart-for-global-food-safety/#11f184af3d36
https://gridplus.io/assets/Gridwhitepaper.pdf
https://pages.riskbasedsecurity.com/hubfs/Reports/2017%20MidYear%20Data%20Breach%20QuickView%20Report.pdf
https://smartasset.com/mortgage/the-50-worst-charities-in-america-how-to-keep-from-being-scammed
https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80

References (continued)

https://medium.com/@earndotcom/21-is-an-open-source-library-for-the-machine-payable-web-4f30d1437fde
https://bitnodes.earn.com/
https://earn.com/lists/
https://www.buybitcoinworldwide.com/mining/pools/
http://exonum.com/doc/advanced/consensus/specification/
https://bitcoin.org/bitcoin.pdf
https://www.icoalert.com/
https://www.coindesk.com/framework-valuing-crypto-tokens/
https://blog.0xproject.com/the-difference-between-app-coins-and-protocol-tokens-7281a428348c
https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/
https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf
http://www.unrisd.org/brett-scott
https://saftproject.com/static/SAFT-Project-Whitepaper.pdf
http://www.thepowerofthepoor.com/concepts/c6.php
https://hackernoon.com/all-you-need-to-know-about-cryptocurrencies-an-overview-for-the-savvy-investor-bdc035b14982
https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74
https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae
https://medium.com/@EtherSportz/how-to-hold-an-ico-in-2018-and-beyond-83f4555705fc
https://data.worldbank.org/indicator/NY.GDP.PCAP.CD
https://www.cbinsights.com/research/what-is-ethereum/
https://news.crunchbase.com/news/icos-delivered-least-3-5x-capital-blockchain-startups-vc-since-2017/
https://thecontrol.co/on-token-value-e61b10b6175e
https://www.aspentimes.com/news/local/in-18-million-deal-nearly-one-fifth-of-st-regis-aspen-sells-through-digital-tokens/
https://www.seedinvest.com/blog/crowdfunding/regulation-crowdfunding-rules