Knowledge Media Institute

HUB4NGI

hub4ngi.eu

The Open University

Questions to: feedback@hub4ngi.eu

Blockchains as a Component of the Next Generation Internet

Prof. John Domingue (@johndmk)
Director, Knowledge Media Institute,
the Open University, UK

Agenda

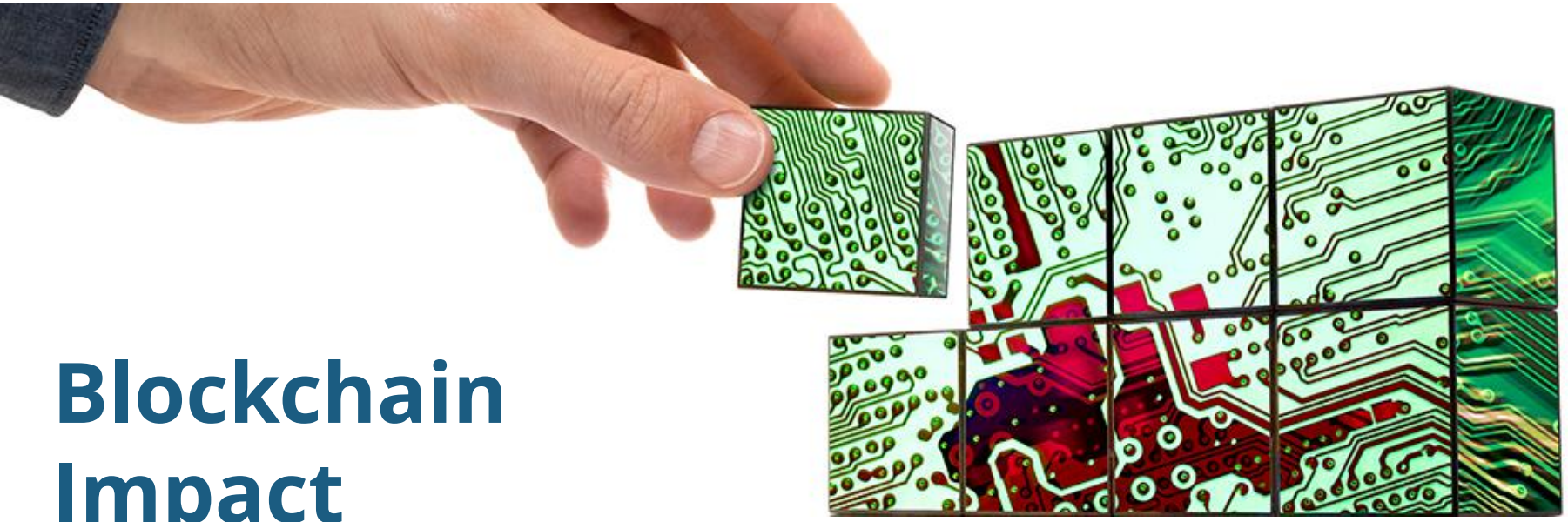
- Blockchain Impact
- Blockchain Elements
- Ethereum Blockchain Platform
- Distributed Autonomous Organisations and ICOs
- An Example DApp
- EU Funding Opportunities
- Summary

The Open University

Knowledge Media Institute

Knowledge Media Institute

The Open University



Blockchain Impact

Blockchain

The Open University

IBM Adapts Bitcoin Technology for Smart Contracts

Tech giant developing its own version of blockchain technology, plans to release open source software within next few months

WORLD ECONOMIC FORUM

World Economic Forum Survey Projects Blockchain 'Tipping Point' by 2023

Santander

Santander: Blockchain Tech Can Save Banks $20 Billion a Year

KMi Knowledge Media Institute

MARKETS

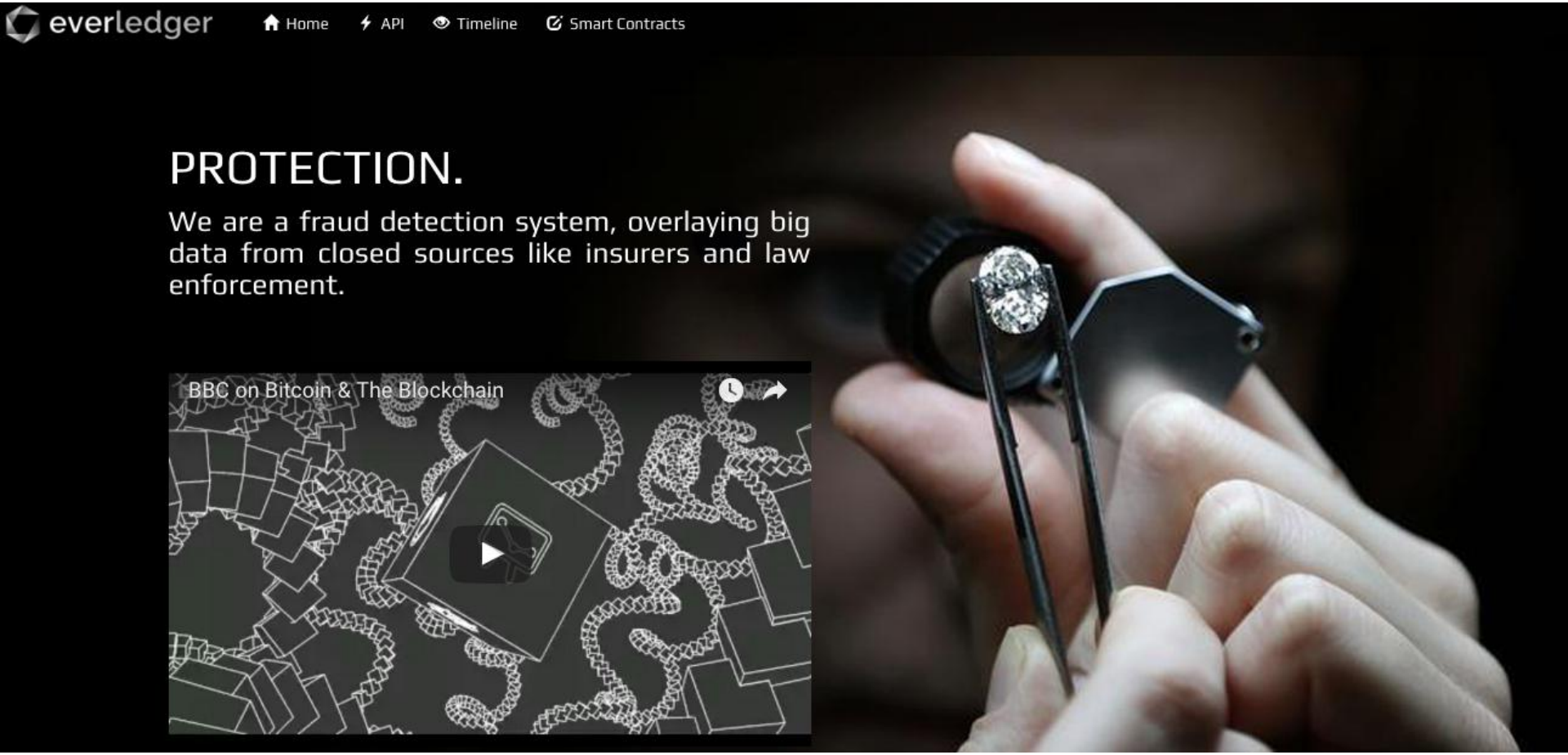
Bitcoin's Blockchain Technology Proves Itself in Wall Street Test

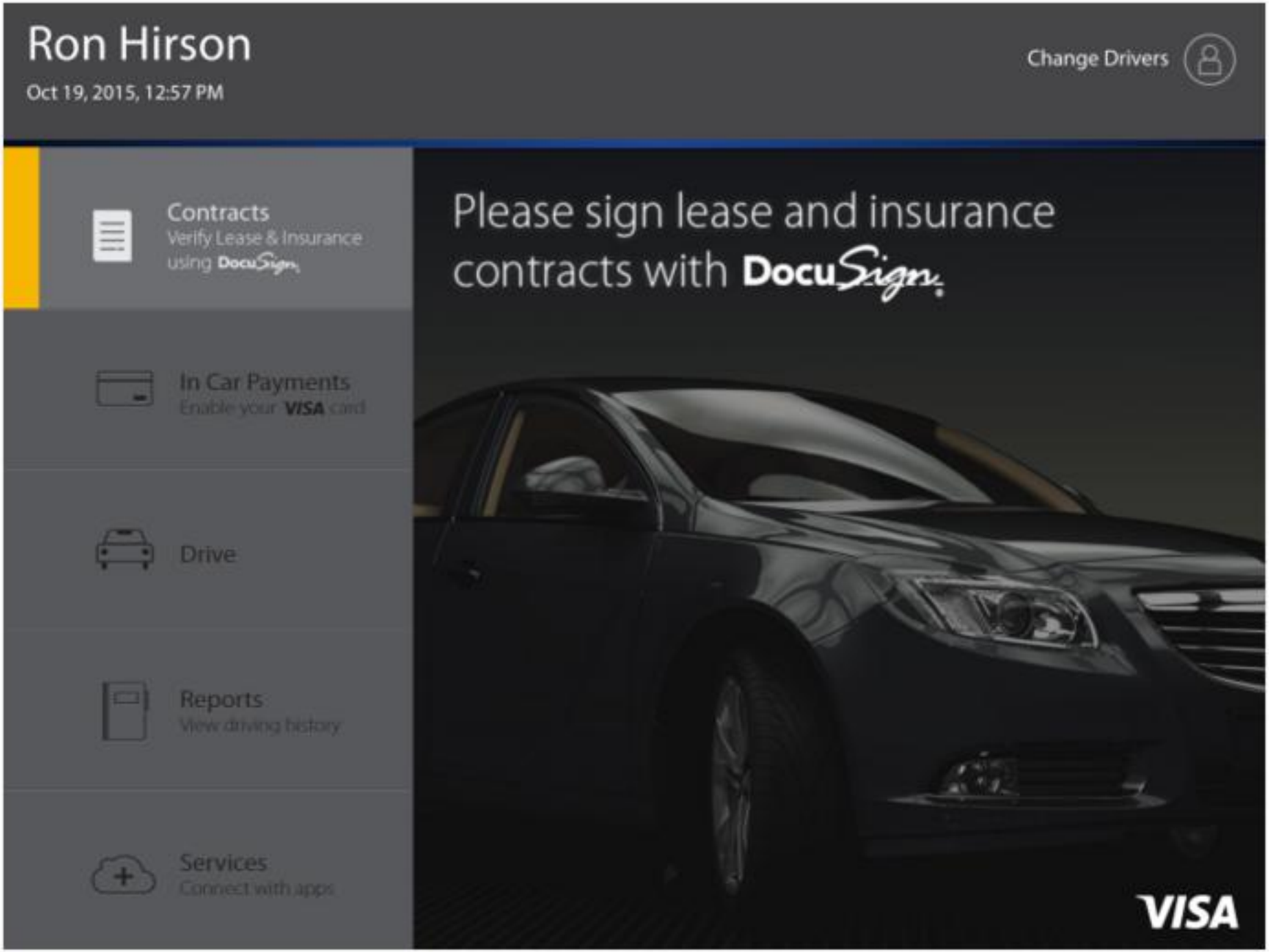
Success in credit-default-swap record keeping may help technology gain finance foothold

Citigroup took part in a successful test of the record-keeping technology behind bitcoin. *PHOTO: MARCOS BRINDICCI/REUTERS*

Everledger

www.everledger.io





https://www.docusign.com/blog/the-future-of-car-leasing-is-as-easy-as-click-sign-drive/

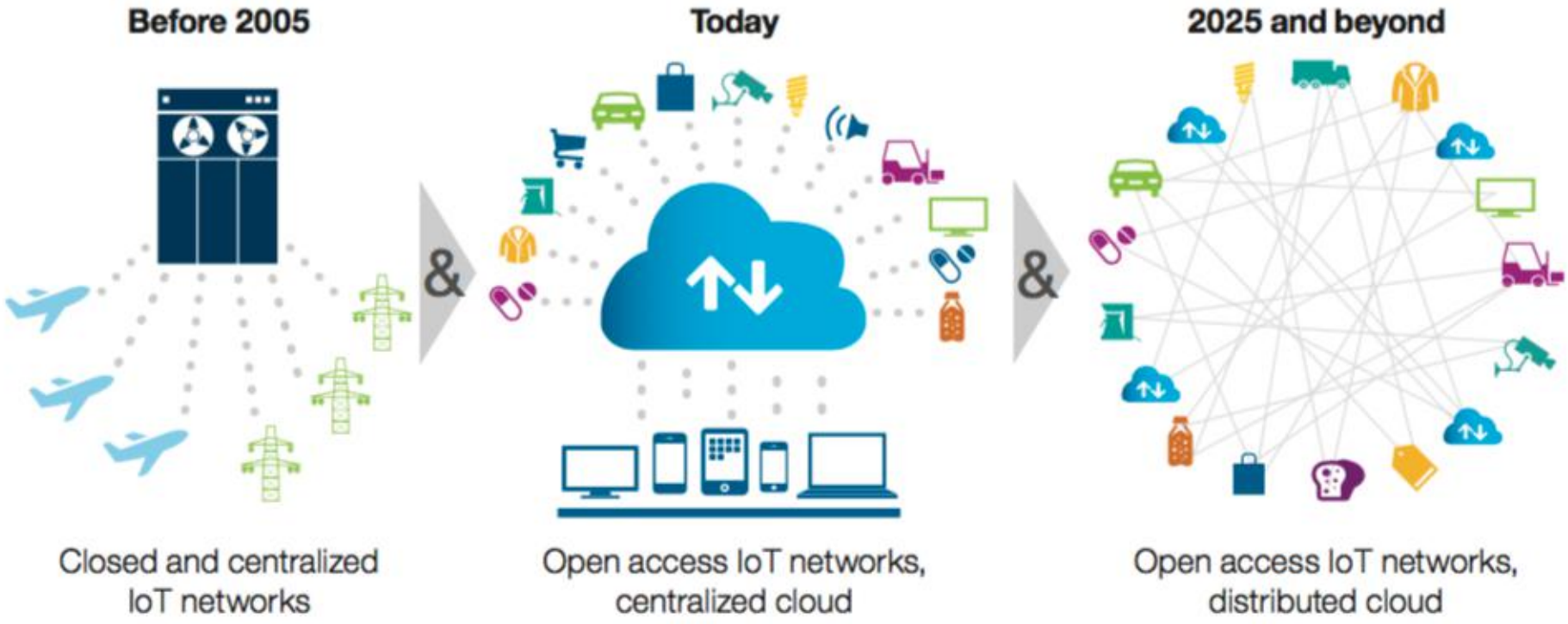
Brooklyn's 'Microgrid' Did Its First Solar Energy Sale

12 April 2016 // 11:00 AM CET

http://motherboard.vice.com/read/transactive-grid-ethereum-brooklyn-microgrid

Solar panels on top of Frumin's apartment in Park Slope. Image: Clinton Nguyen

IBM: Device Democracy

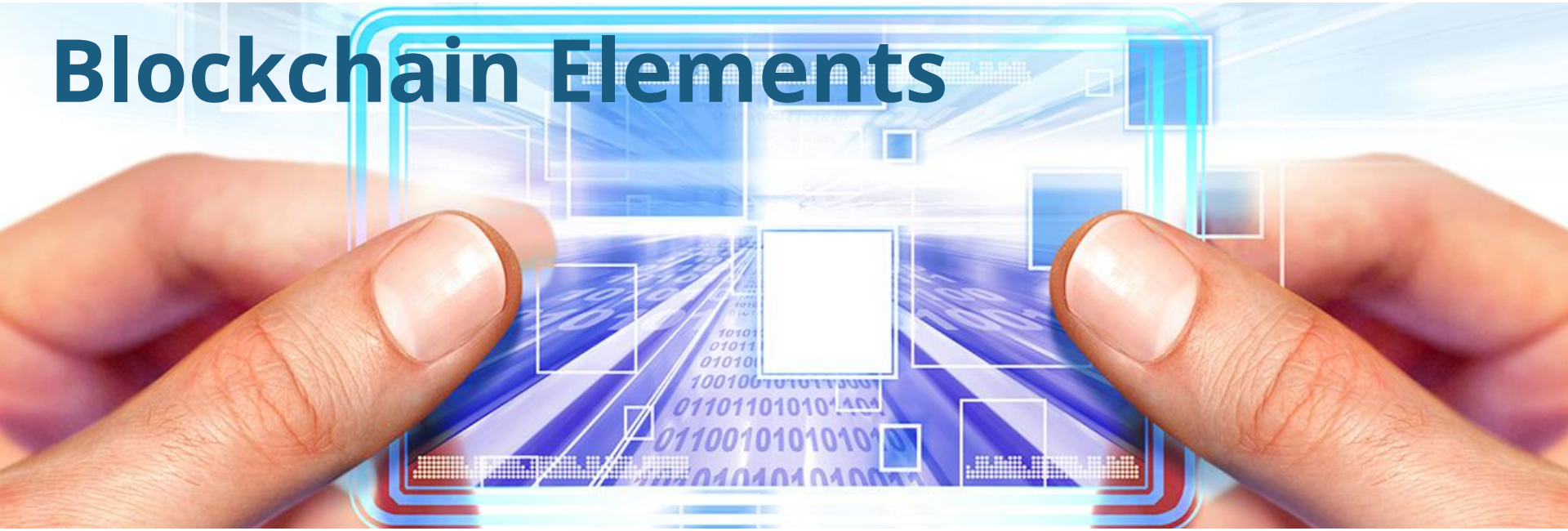


http://www-935.ibm.com/services/multimedia/GBE03620USEN.pdf

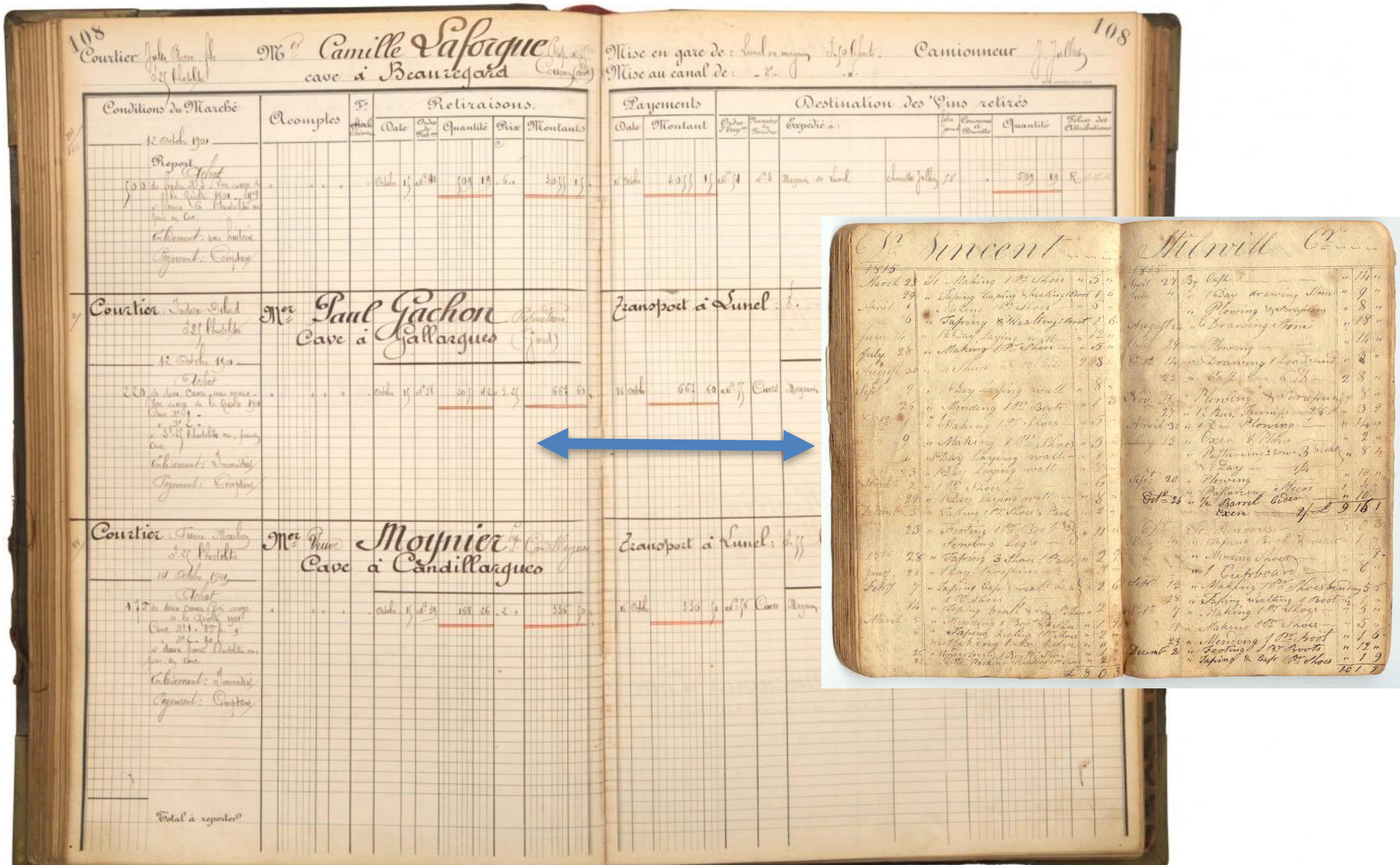
Knowledge Media Institute

The Open University

Blockchain Elements

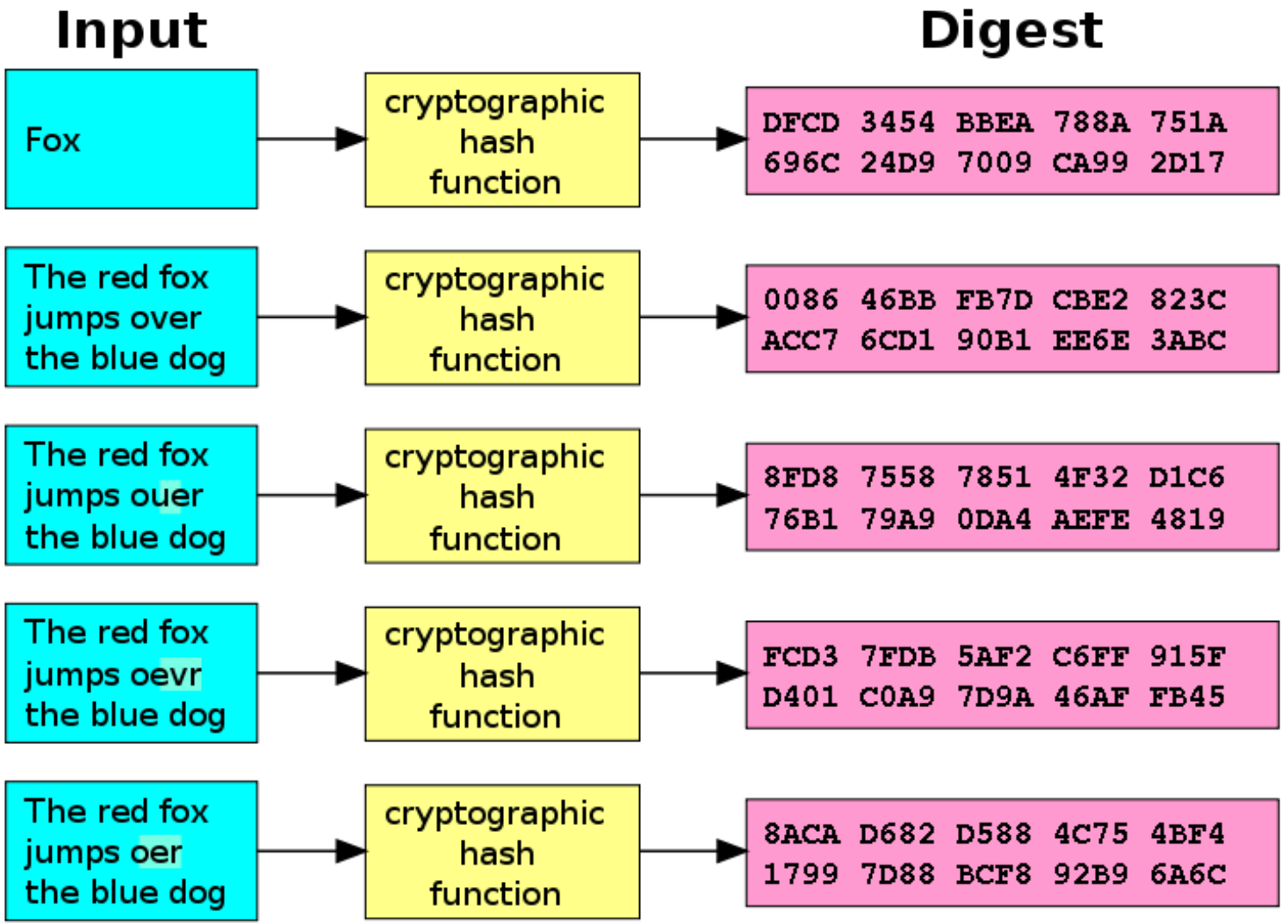


Ledgers



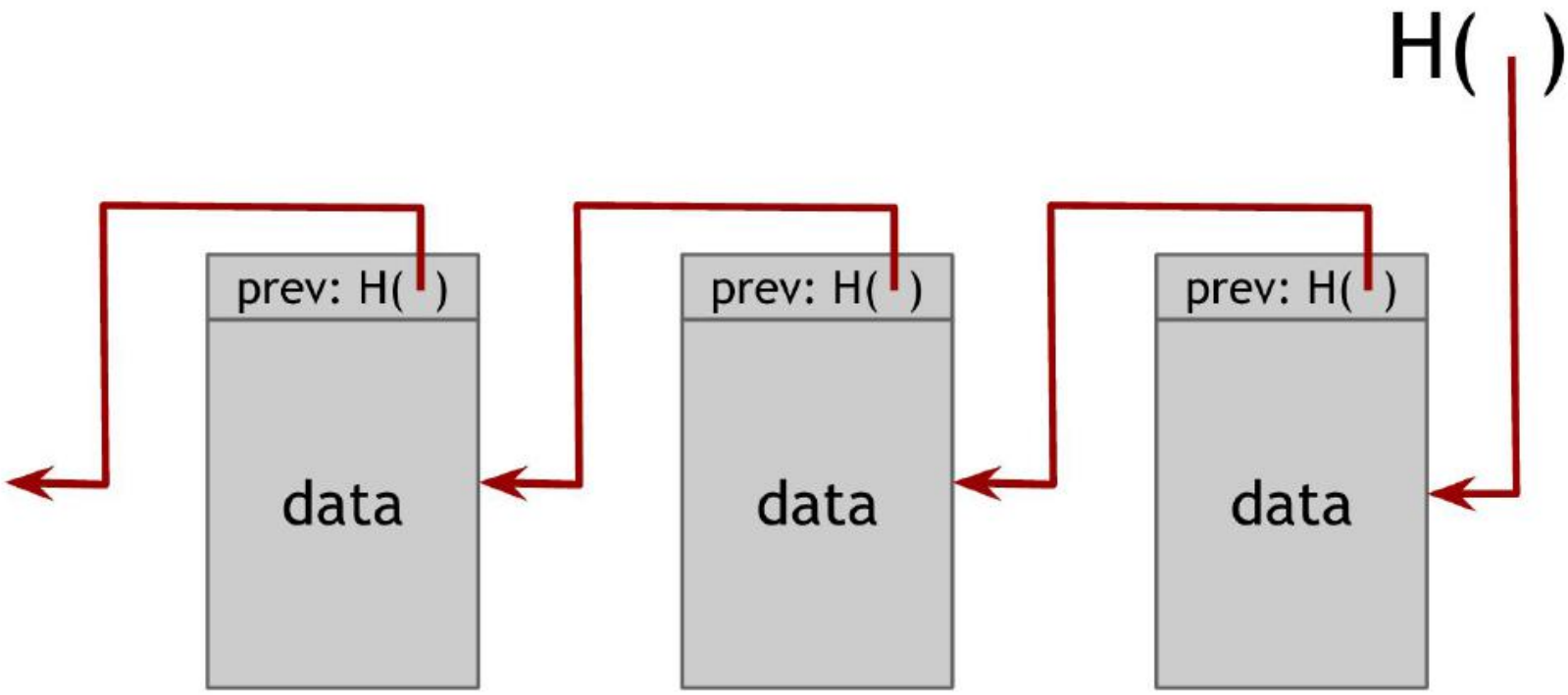
108
Courtier
Camille Laforgue
cave à Beauregard
Mise en gare de :
Mise au canal de :
Camionneur
Conditions du Marché
Acomptes
Retiraisons
Date
Quantité
Prix
Montant
Payements
Date
Montant
Destination des Vins retirés
Expédié à :
Quantité
Paul Gachon
Cave à Gallargues
Transport à Lunel
Moynier
Cave à Candillargues
Total à reporter

Cryptographic Hash Function



https://en.wikipedia.org/wiki/Cryptographic_hash_function

Blockchain is a Linked List



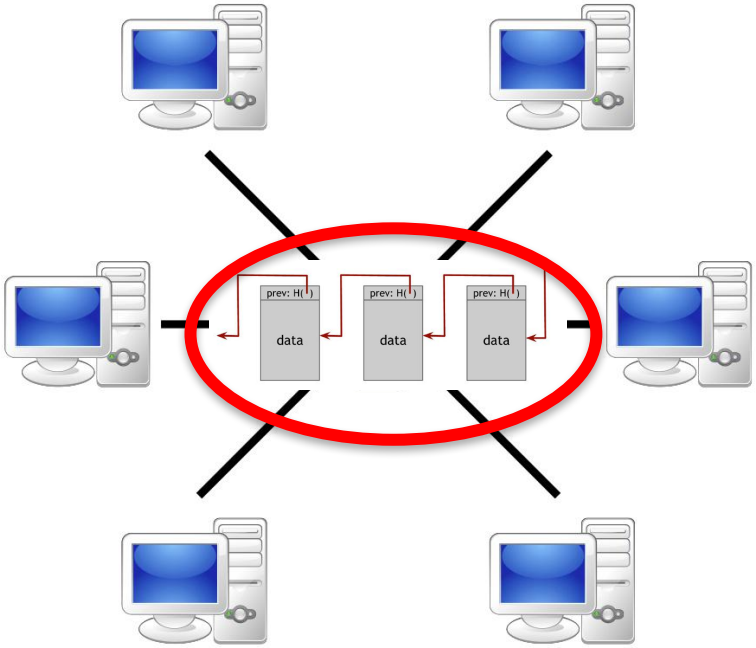
A blockchain can be thought of as a linked list of transactions that is built with hash pointers instead of pointers

Source: Bitcoin and Cryptocurrency Technologies - Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

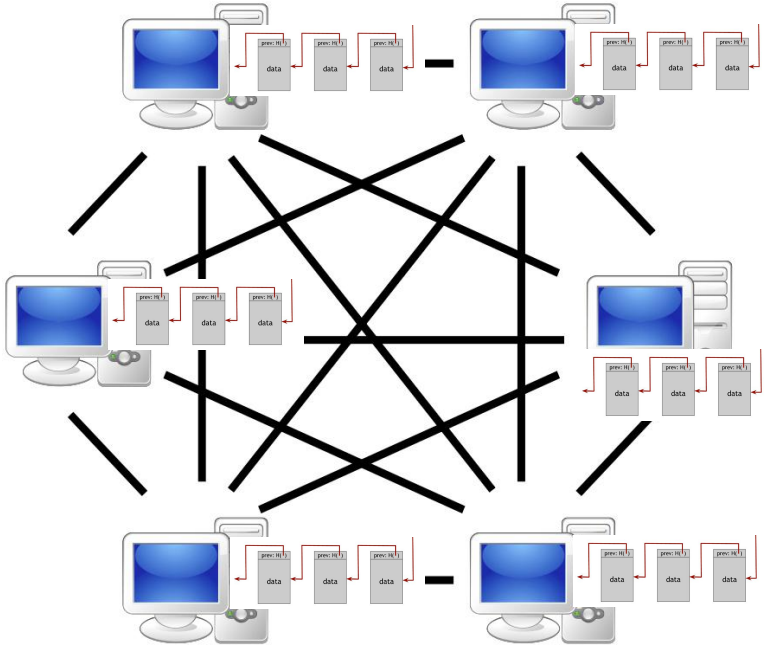
Peer to Peer Network

Add everyone has a complete copy of the data

Who Next?



Server-based



P2P-network

http://www.terndrup.net/2015/10/27/Building-a-P2P-Peer-Client-with-Node-js/

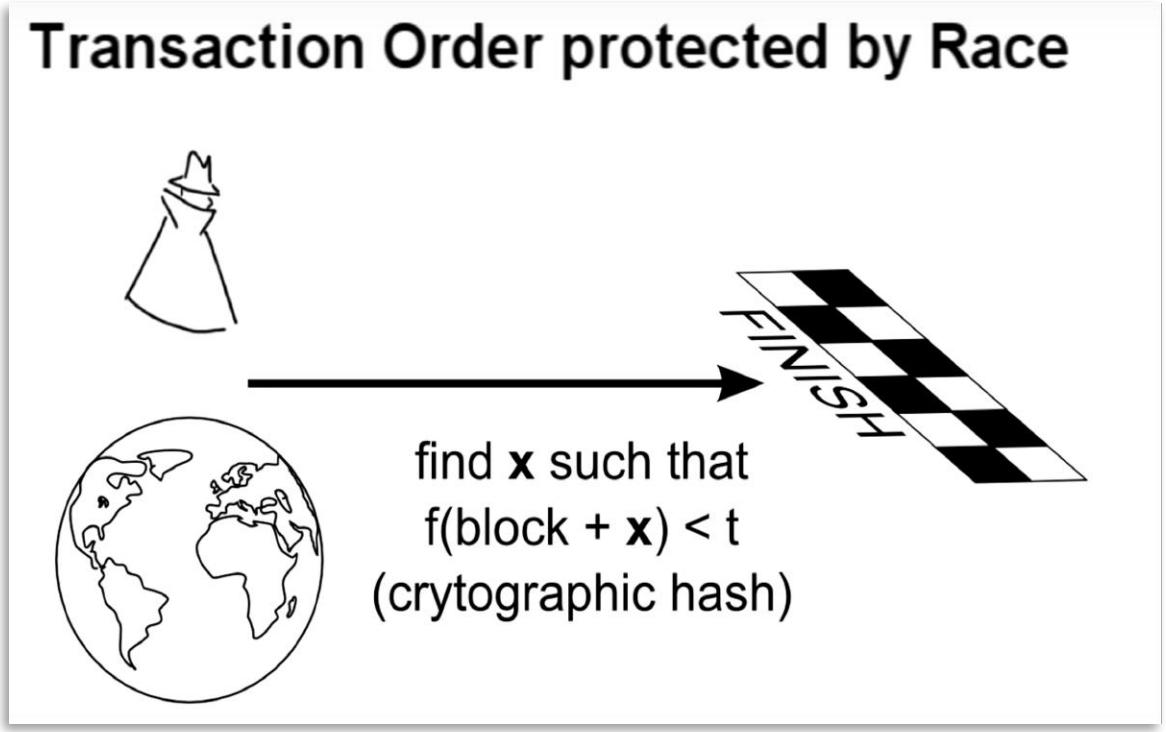
Proof of Work

- Find x such that f(nonce + x) < t (cryptographic hash)

"Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" =>
ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7 ...

"Hello, world!4248" =>
6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

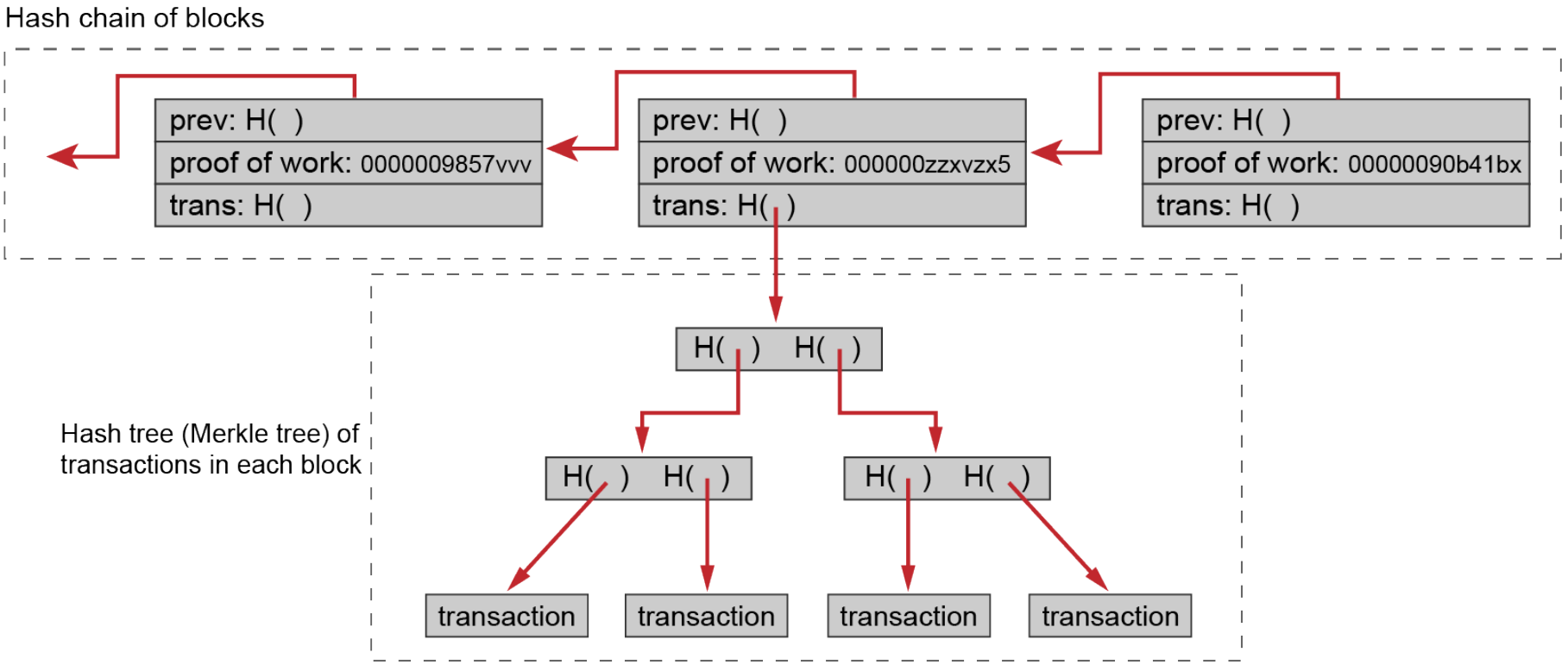
Proof of Work



- Hard to outpace the entire rest of the network… a 51% attack could do it, but otherwise it is like buying thousands of lottery tickets – doesn't help you that much!

Source: Marc Eisenstadt 'What is the genius behind Bitcoin'

Blockchain is a Linked List (2/2)



A blockchain actually contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another.

The second is internal to each block and is a Merkle Tree of transactions within the blocks.

This allows for efficiently verifiable proofs that a transaction was included in a block.

Source: Bitcoin and Cryptocurrency Technologies - Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

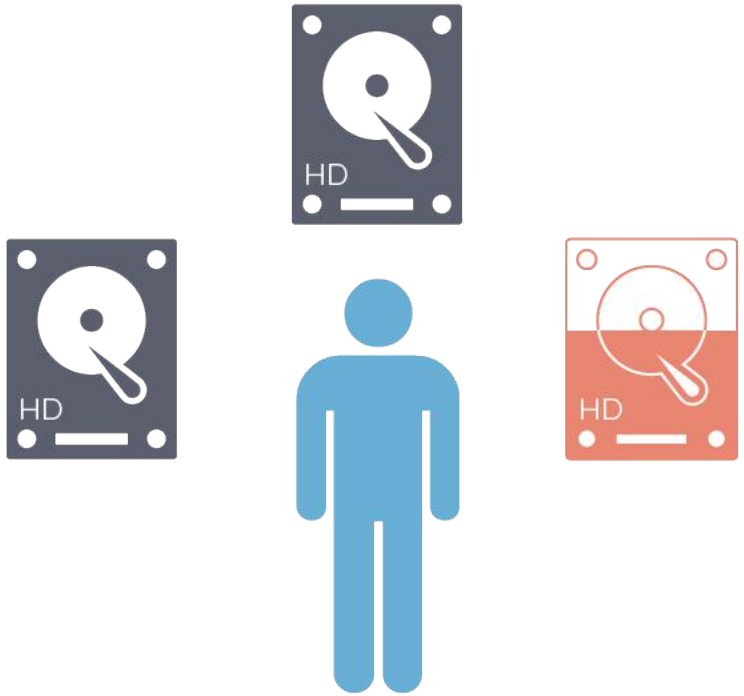
BitCoin Mining

http://knkx.org/post/central-wash-home-nations-biggest-bitcoin-mine-more-coming

Consensus Mechanisms (1/6)

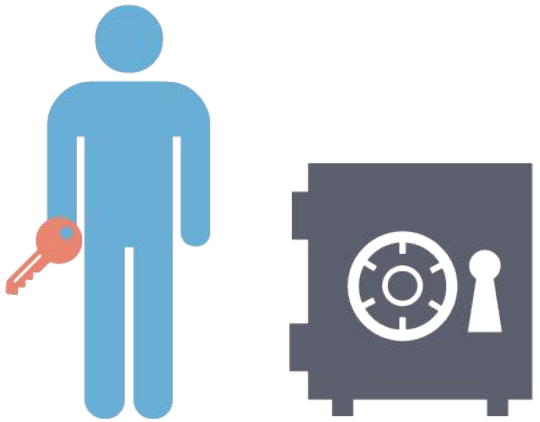
Proof of Work

Consensus Mechanisms (2/6)



Proof of Capacity

Consensus Mechanisms (3/6)



Proof of Stake

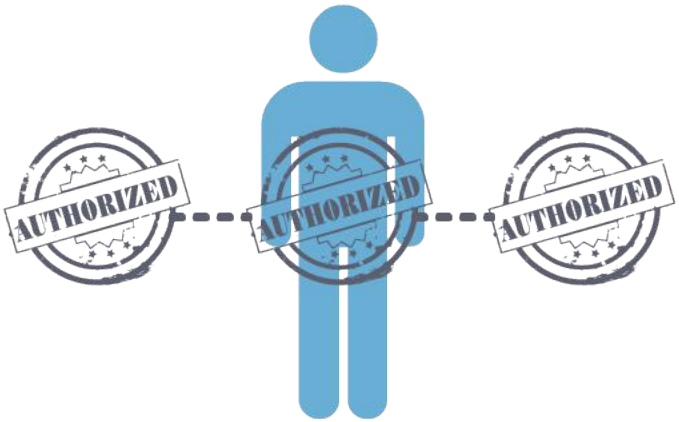
Consensus Mechanisms (4/6)

Proof of Burn

Consensus Mechanisms (5/6)

Proof of Elapsed Time

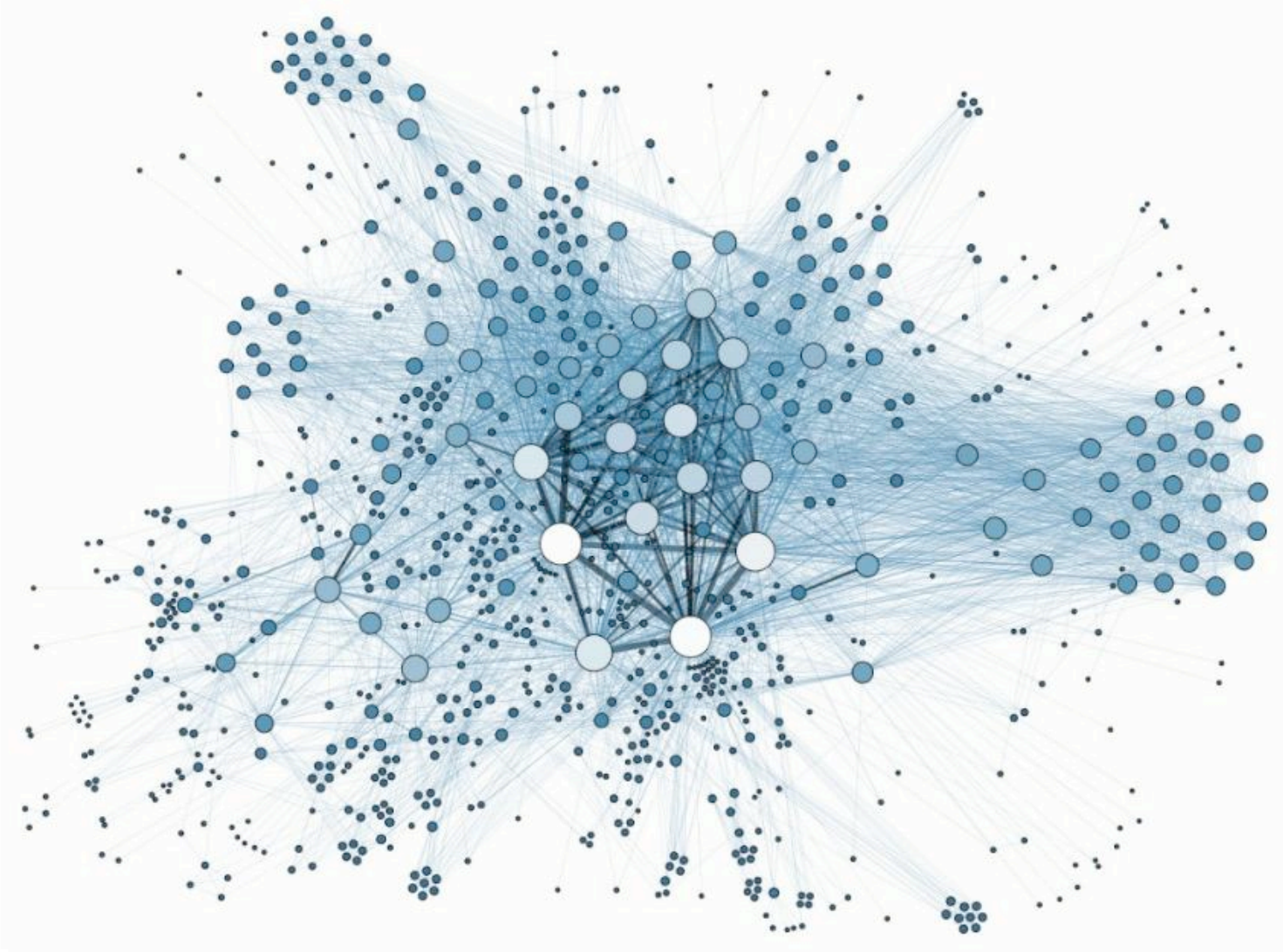
Consensus Mechanisms (6/6)



Proof of Authority

Knowledge Media Institute

Ethereum Blockchain Platform



Ethereum Virtual Machine

The Open University

The Ethereum Virtual Machine can be thought of as a large decentralized computer containing millions of objects, called "accounts", which have the ability to maintain an internal database, execute code and talk to each other.
There are 2 types of Accounts:

Externally owned account (EOA): an account controlled by a private key that has the ability to send ether and messages from it.

'Smart' **Contract**: an account that has its own code, and is controlled by code.

Any user can trigger an action by sending a transaction from an EOA, setting Ethereum's wheels in motion.

If the destination of the transaction is another **EOA**, then the transaction may transfer some ether but otherwise does nothing

However, if the destination is a 'Smart' **Contract**, then the contract in turn activates, and automatically runs its code.

KMi
Knowledge Media Institute

Sources: Ethereum Development Tutorial

Ethereum External Accounts

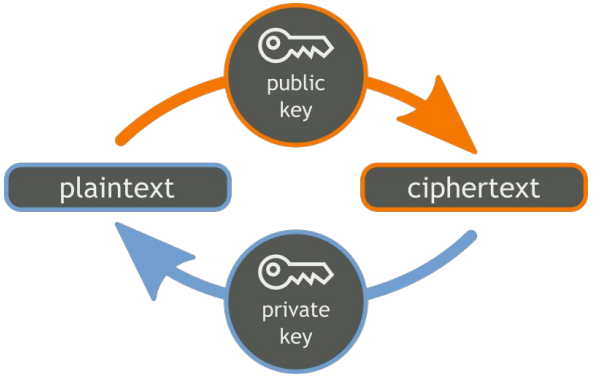
The Open University

Every account is defined by a pair of **keys**, a private key and public key

A **keyfile** holds encoded key pair data as JSON with the private key encrypted with a user given password

Accounts are indexed by their **address** which is derived from the public key by taking the last 20 bytes

Accounts use public key cryptography to **sign transaction**.



Knowledge Media Institute

http://ethdocs.org/en/latest/account-management.html

Ethereum External Accounts

The Open University

Server side external Accounts

Server side account keyfiles are held in the **keystore folder** where your Ethereum node data is located

Ease of Use

Client side external Accounts

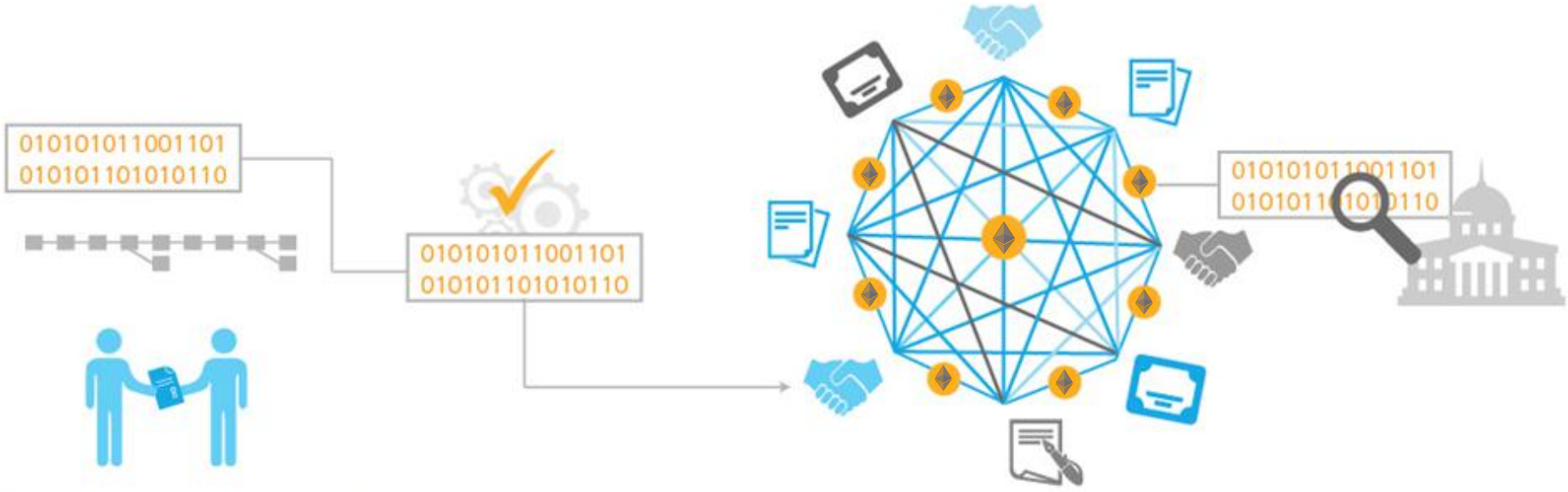
Client side keyfiles are held in a keystore managed by **wallet Software** running either in a browser or on the client computer

Control

KMi Knowledge Media Institute

http://ethdocs.org/en/latest/account-management.html

Contracts in Ethereum



Contracts in Ethereum generally serve 4 purposes:

- Maintain a data store representing something which is useful to either other contracts or to the outside world
- Serve as a sort of externally owned account with a more complicated access policy
- Manage an ongoing contract or relationship between multiple users
- Provide functions to other contracts; essentially serving as a software library.

Knowledge Media Institute

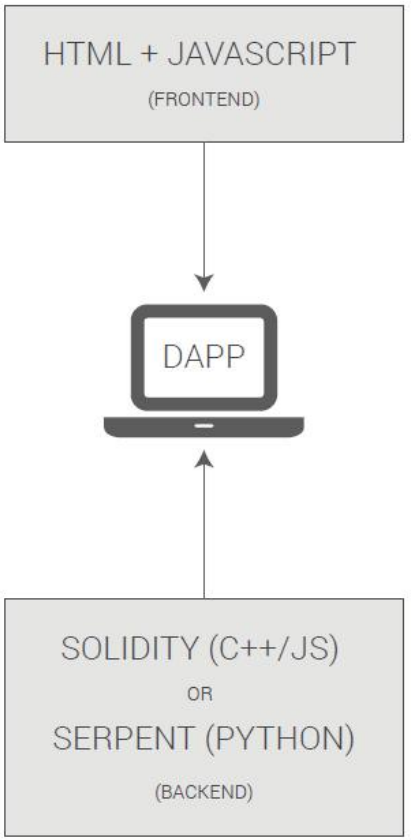
source: Richard Gendal Brown "A Simple Model for Smart Contracts"
http://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/

DApps

A Đapp is a decentralised application which serves some specific purpose to its users, but which has the important property that the application itself does not depend on any specific party existing.

Rather than serving as a front-end for selling or providing a specific party's services, a Đapp is a tool for people and organizations on different sides of an interaction use to come together without any centralized intermediary.

A Dapp consists of two parts: a frontend, written in HTML or QML, and a backend (think of it as the 'database' for your frontend).



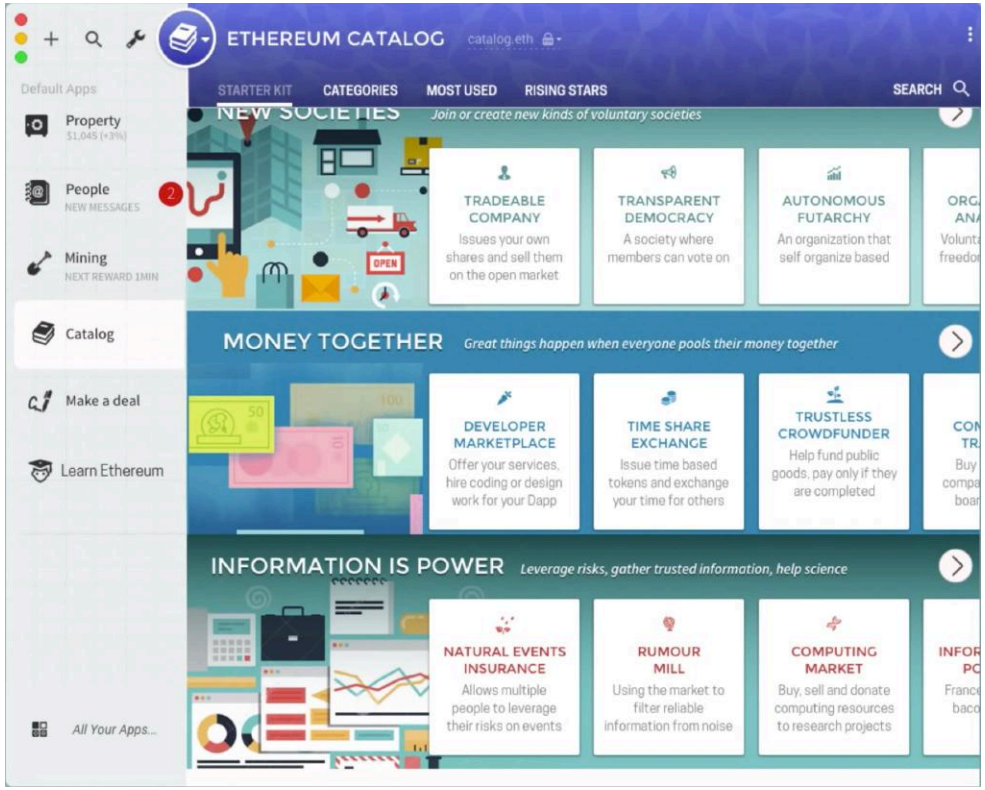
Source: Ethereum - Stephan

DBrowsers

It is an end user interface onto the Ethereum blockchain.

A DBrowser is how users will find and interact with DApps

‘Mist’ is the name of the Ethereum DBrowser.



Knowledge Media Institute

Characteristics of Blockchain DApps

- Shared database
- Multiple writers
- Absence of trust
- Disintermediation
- Transaction interaction
- Set rules
- Validators
- Asset backing

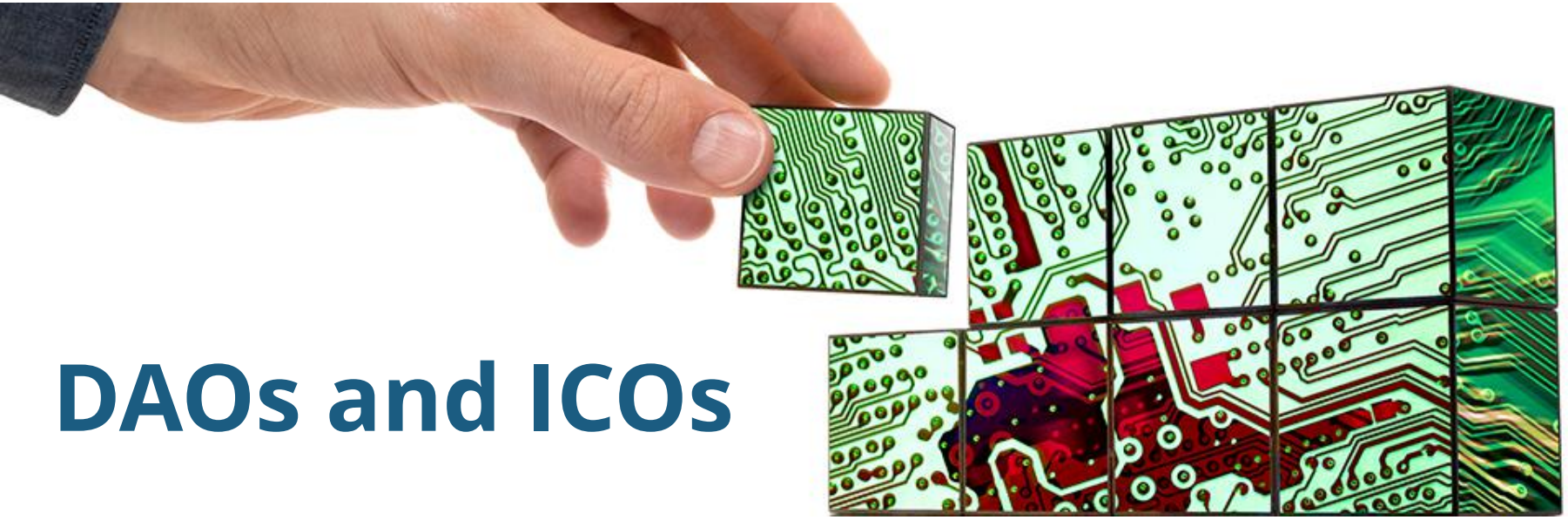
The Open University

KMi Knowledge Media Institute

http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

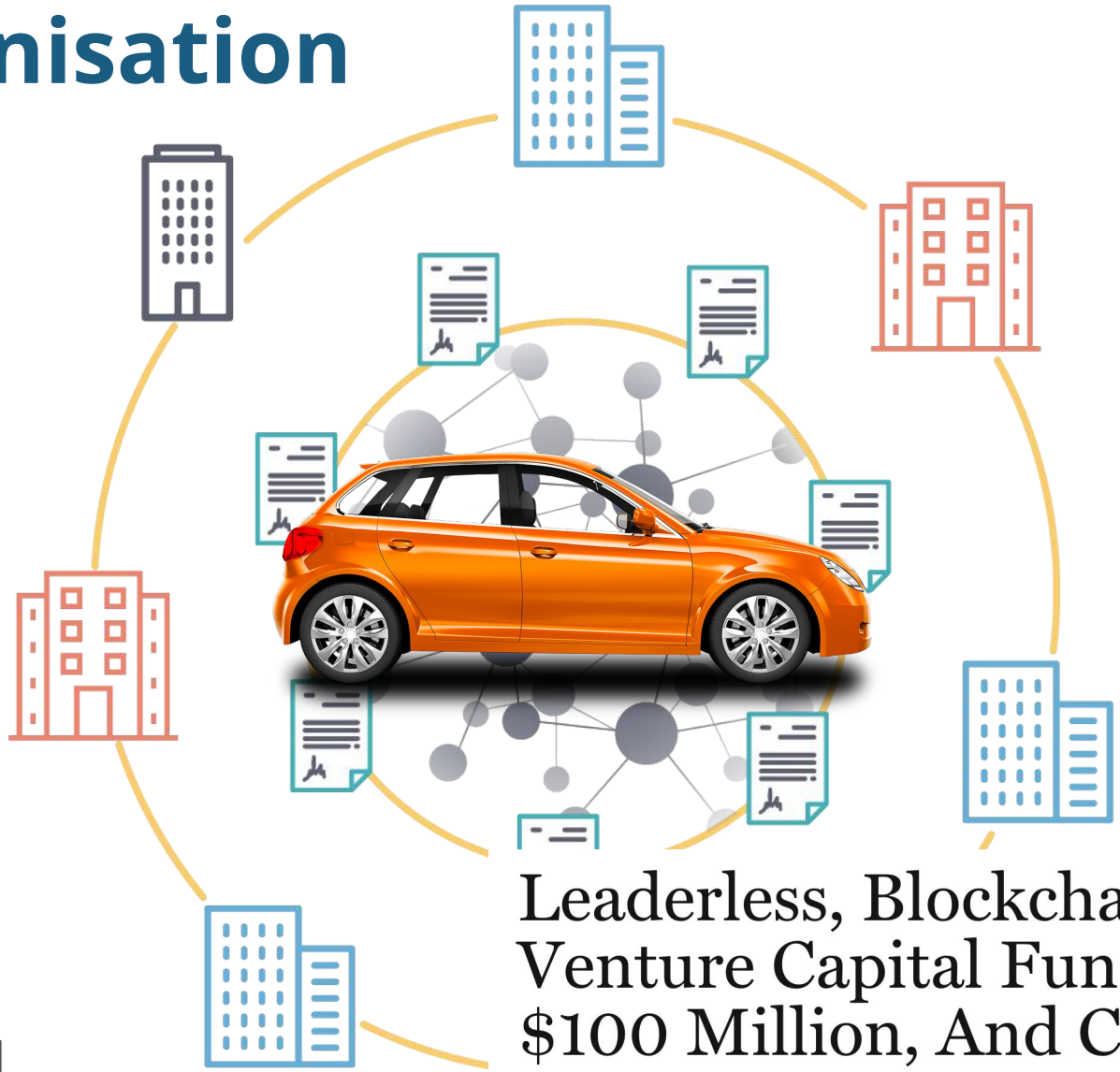
Knowledge Media Institute

The Open University



DAOs and ICOs

Distributed Autonomous Organisation



Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting

by David Z. Morris @davidzmorris MAY 15, 2016, 5:04 PM EDT

Knowledge Media Institute

The Open University

Initial Public Offering

Knowledge Media Institute

Services with value

Shareholders

Customer/User

Initial Public Offering

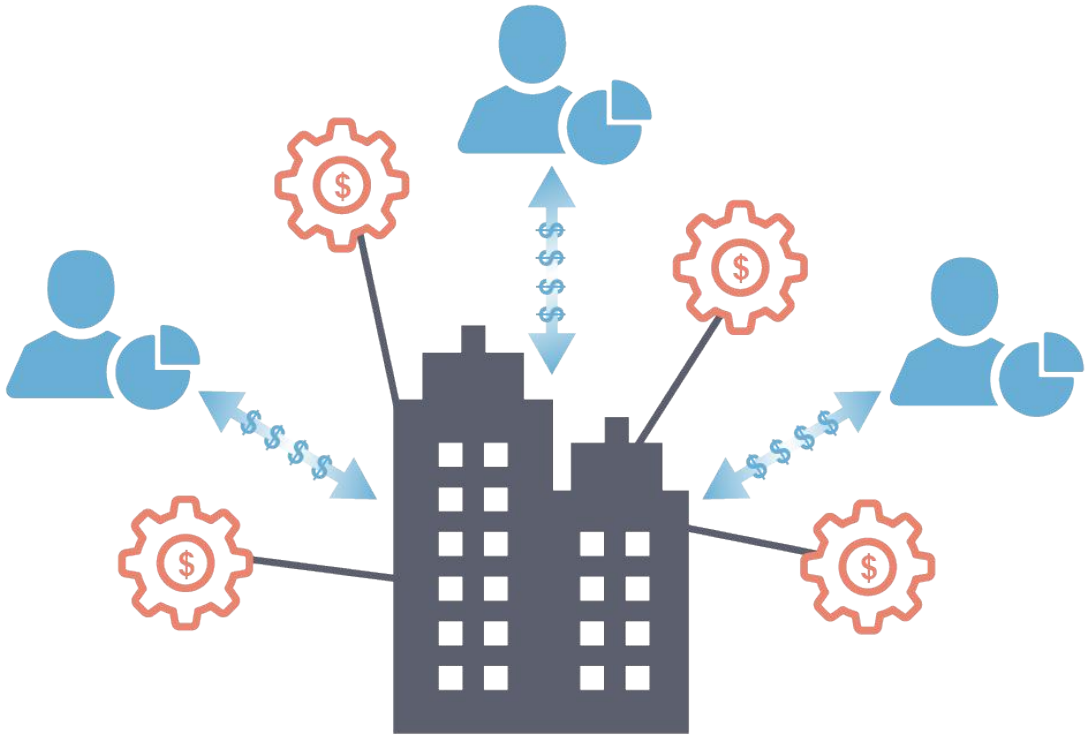
Knowledge Media Institute

Services with value

Shareholders

Customer/User

Initial Public Offering



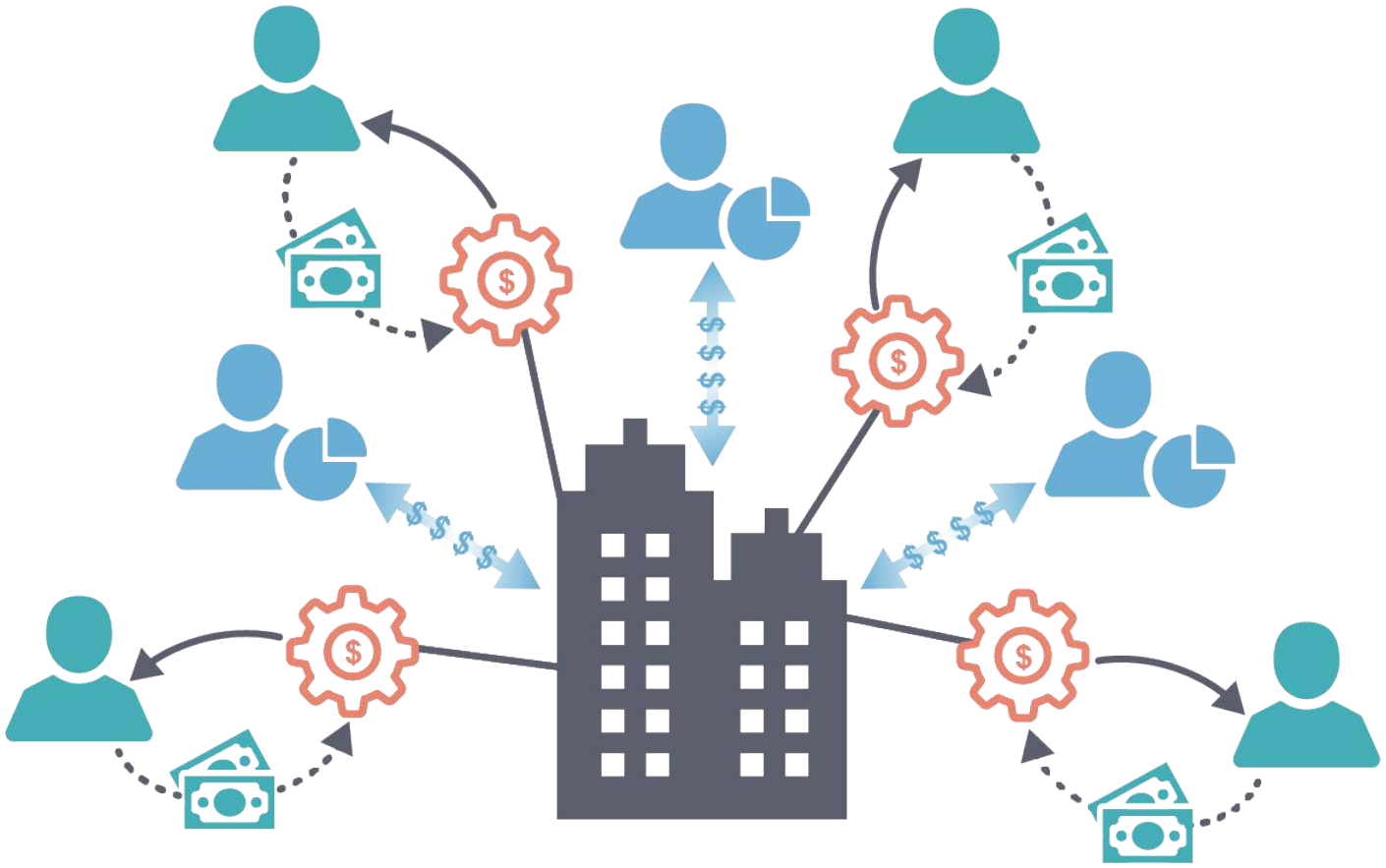
Knowledge Media Institute

Services with value

Shareholders

Customer/User

Initial Public Offering



Knowledge Media Institute

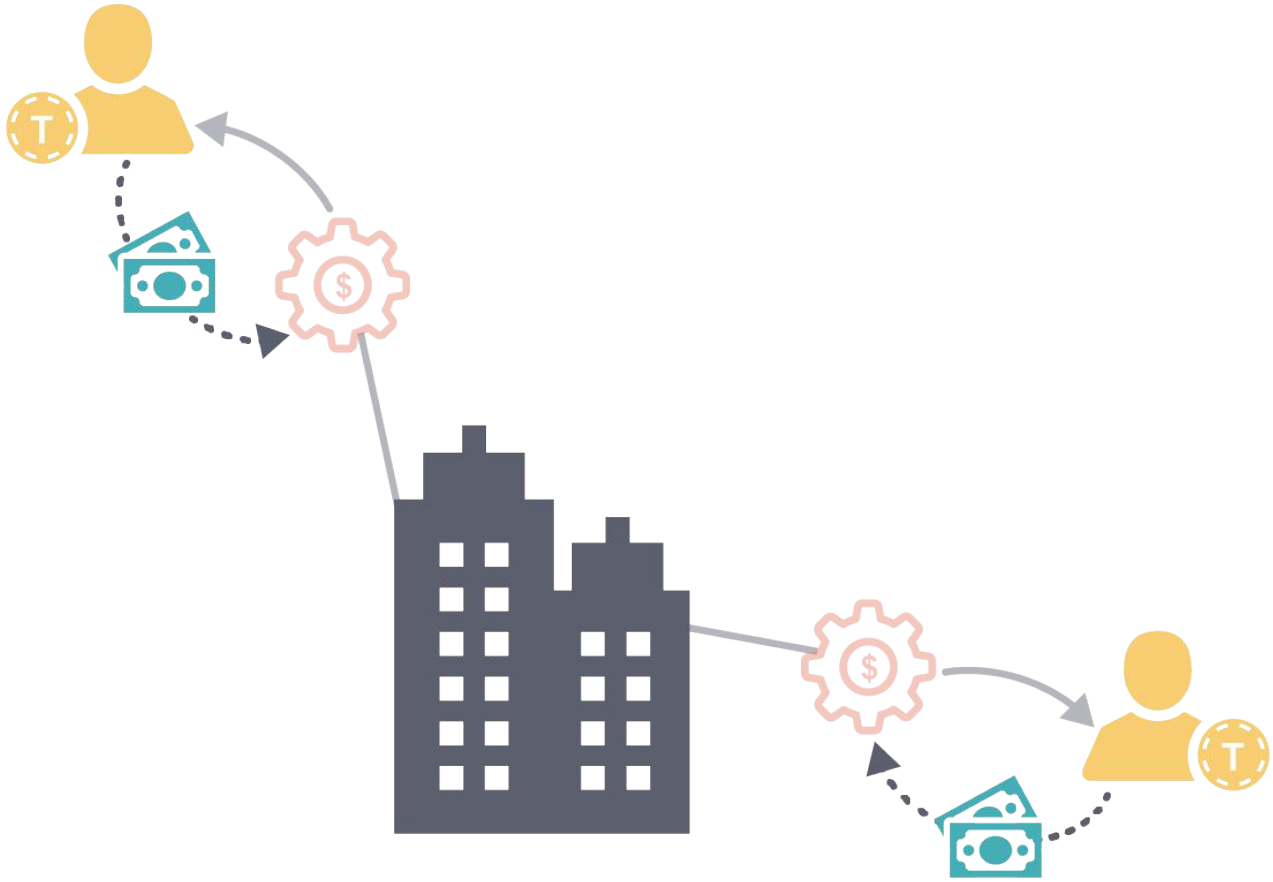
Services with value

Shareholders

Customer/User

The Open University

Initial Coin Offering



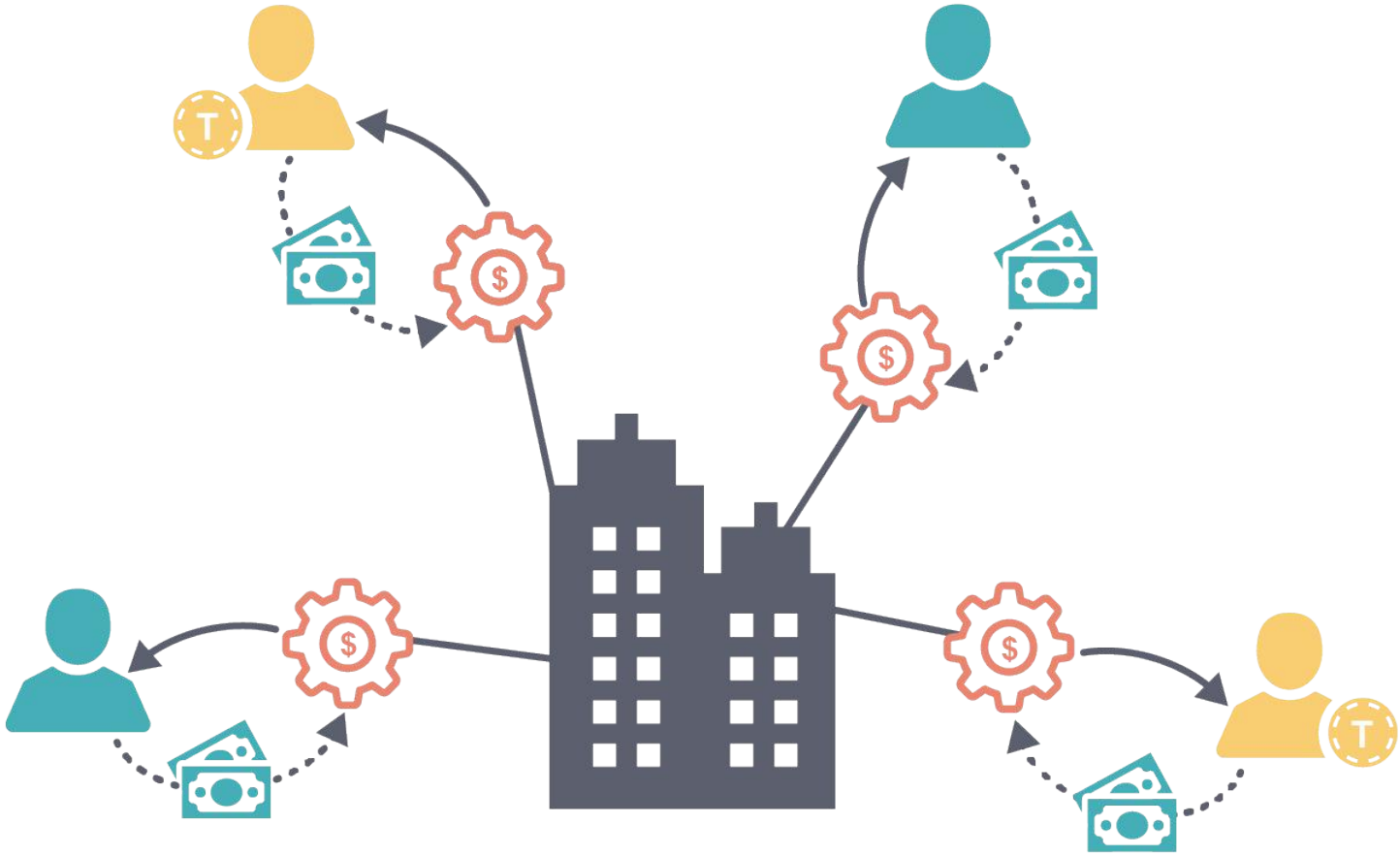
Knowledge Media Institute

Services with value

Shareholders with tokens

Customer/User

Initial Coin Offering



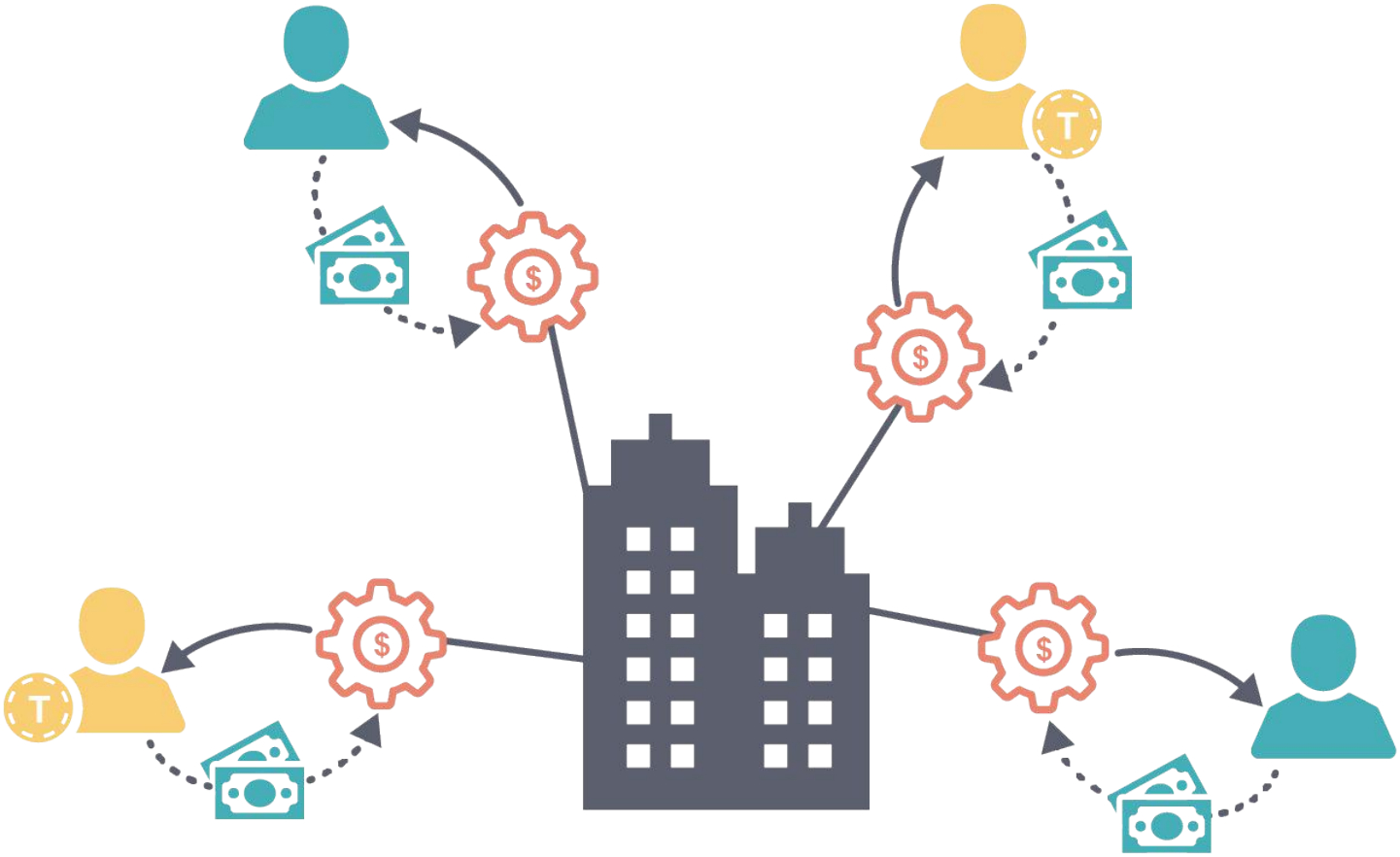
Knowledge Media Institute

Services with value

Shareholders with tokens

Customer/User

Initial Coin Offering



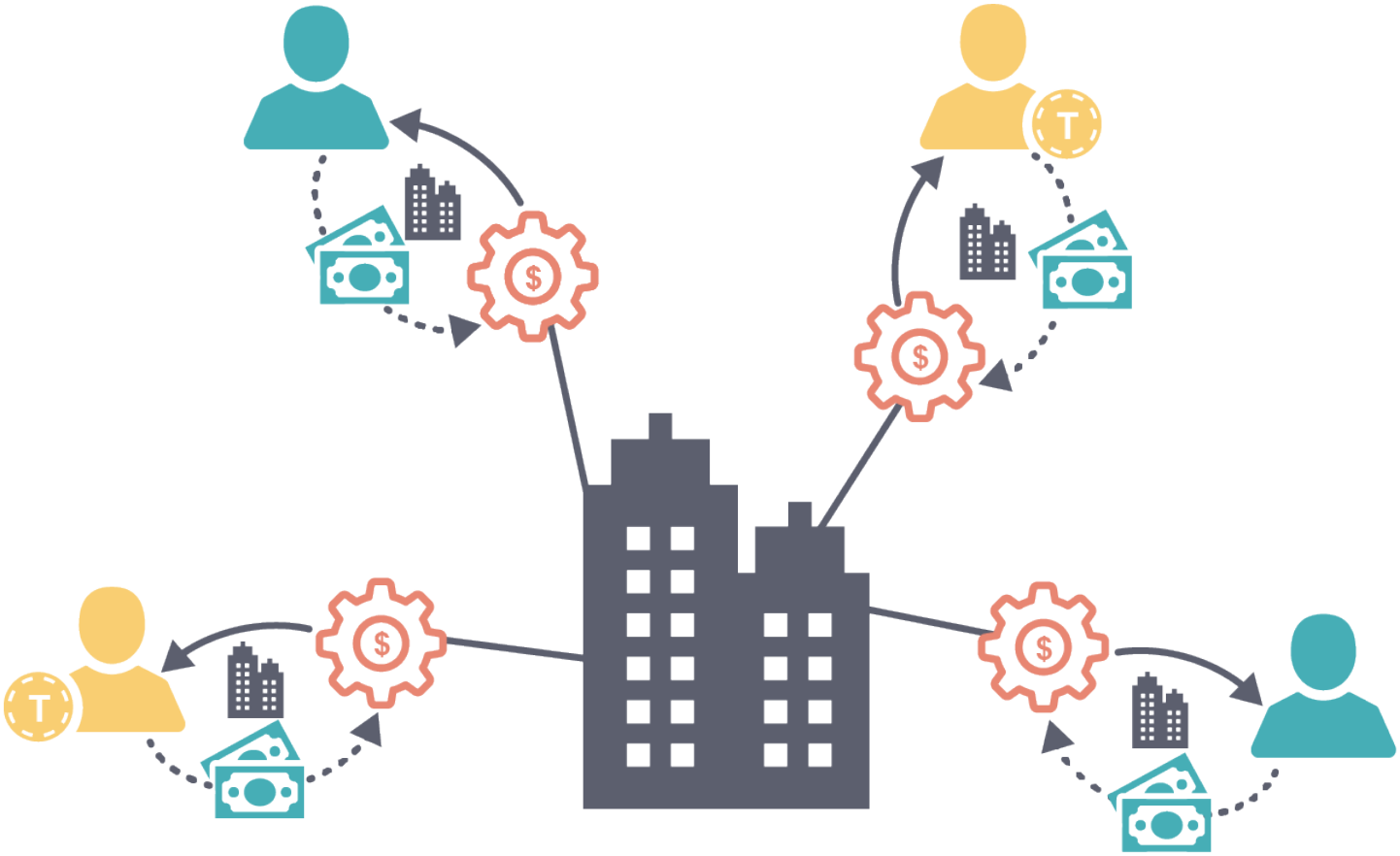
Knowledge Media Institute

Services with value

Shareholders with tokens

Customer/User

Initial Coin Offering



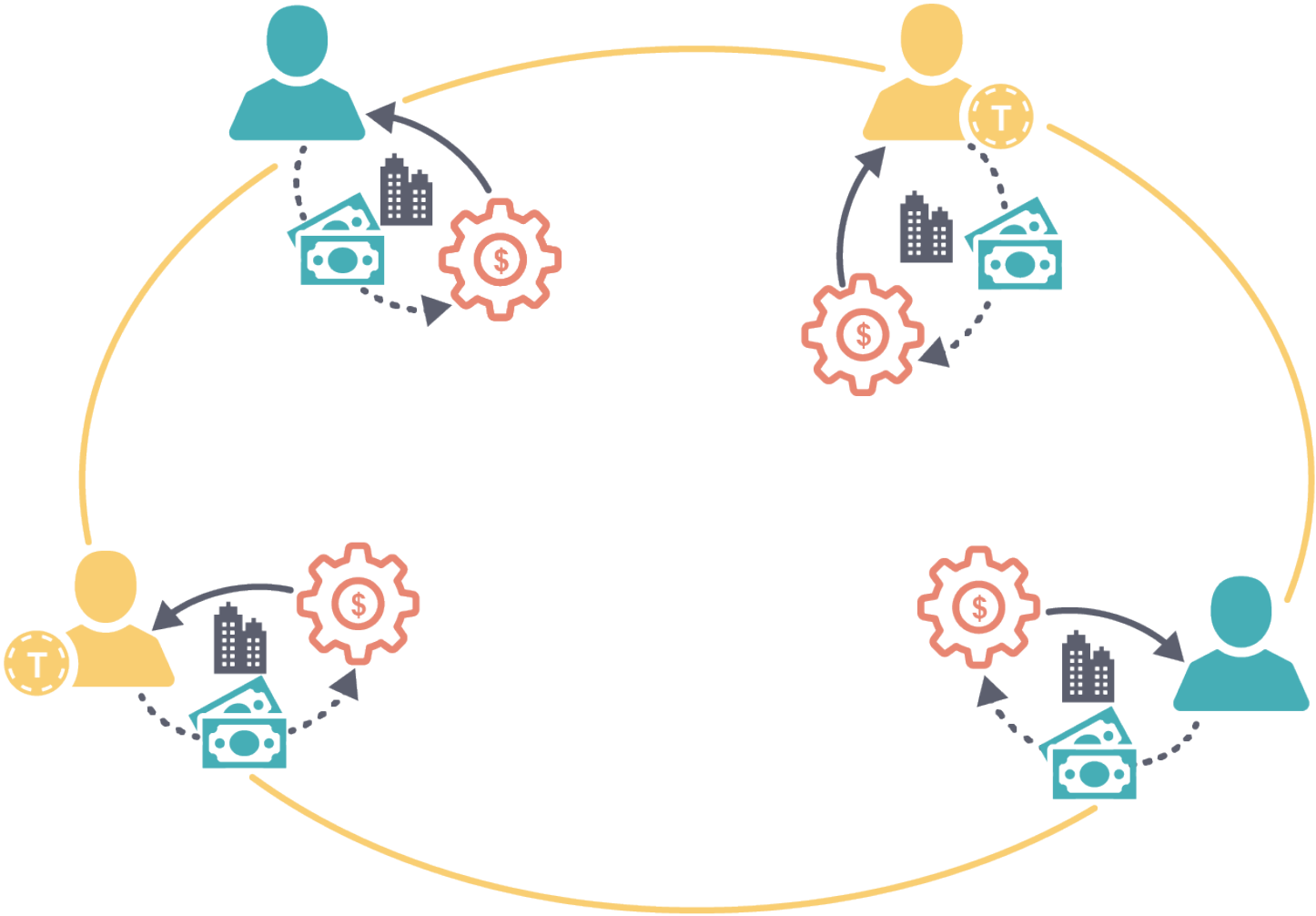
Knowledge Media Institute

Services with value

Shareholders with tokens

Customer/User

Initial Coin Offering



Knowledge Media Institute

Services with value

Shareholders with tokens

Customer/User

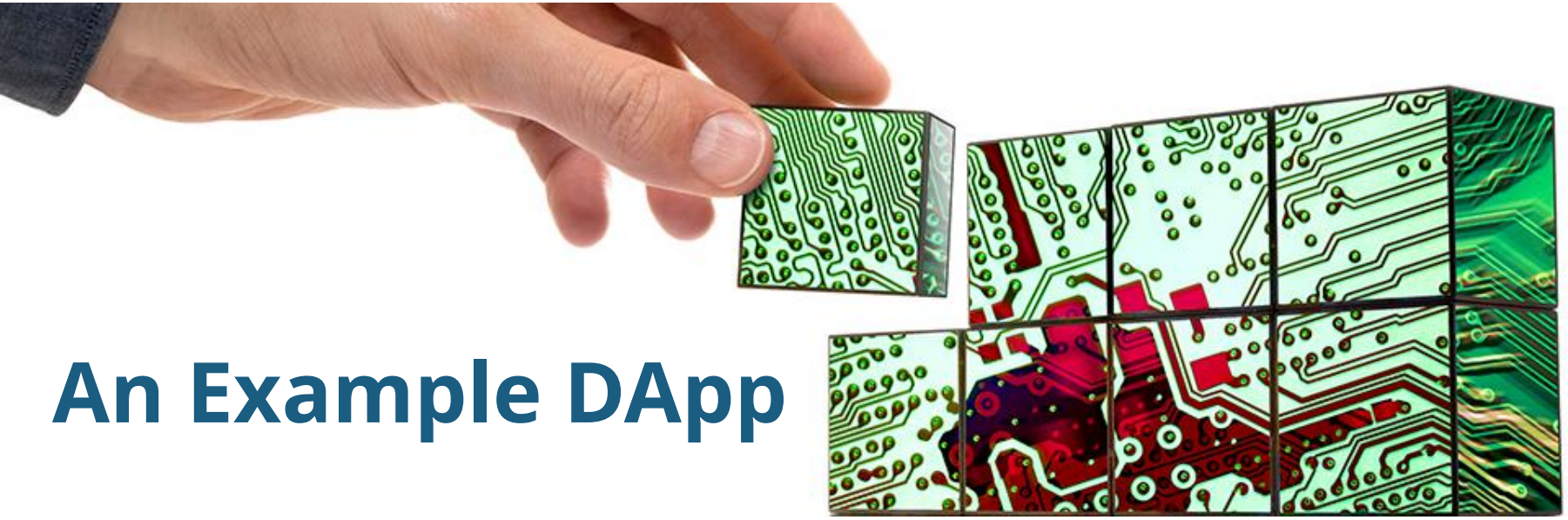
The Open University

Interplanetary File System (IPFS)

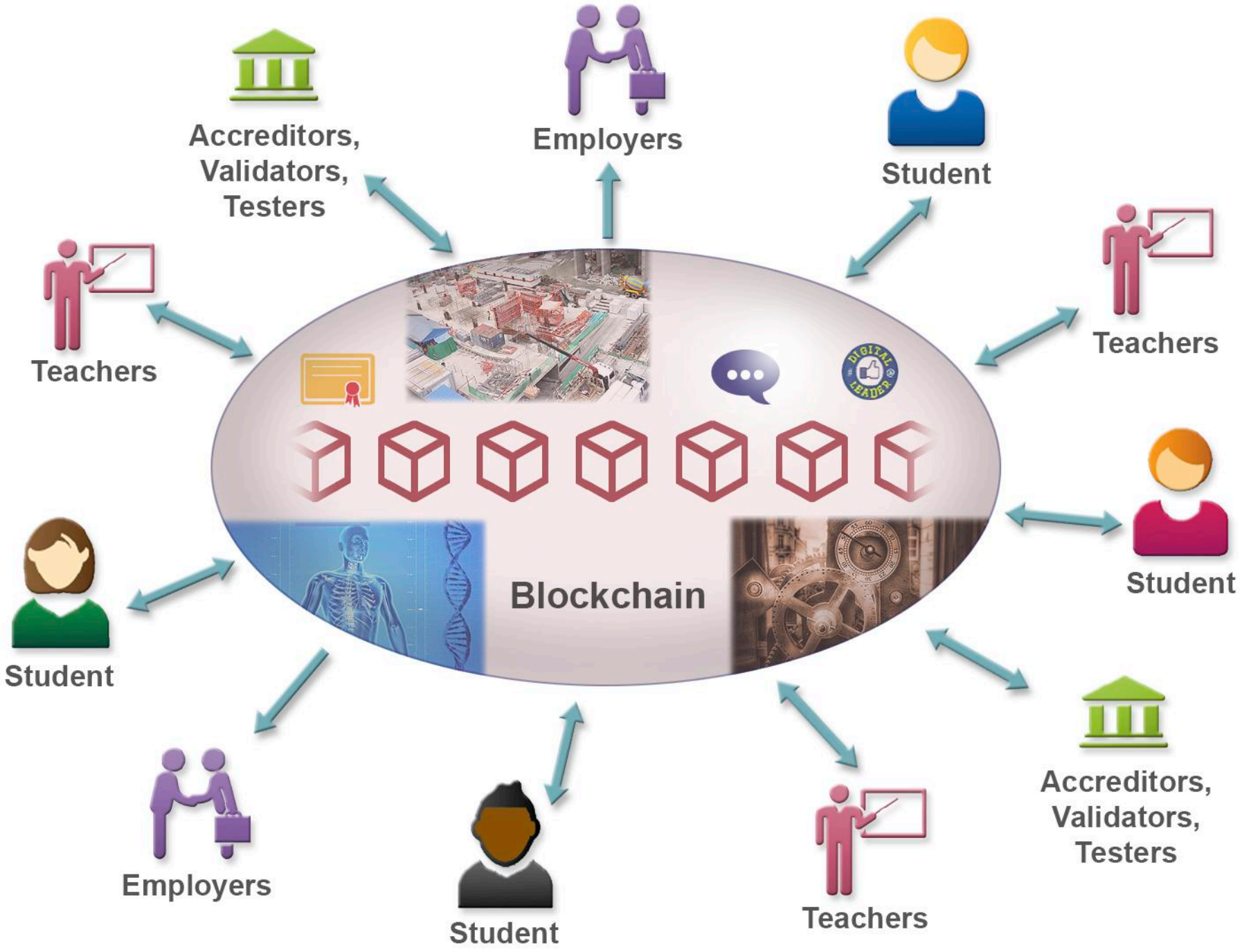
- Content-addressed distributed storage (CADS)
- Files identified by hash of contents
- Shared across BitTorrent-based network

Knowledge Media Institute

The Open University



An Example DApp


Accreditors, Validators, Testers
Employers
Student
Teachers
Teachers
Student
Blockchain
Student
Employers
Student
Teachers
Accreditors, Validators, Testers

OpenLearn Badges on the

The Open University

Blockchain Badge Viewer

Badge Assertion Address: 0xca7c1ff5612e8fde71a87504ef6d0989c78f1c55 [View badge]

Assertion

Assertion Blockchain address: 0xca7c1ff5612e8fde71a87504ef6d0989c78f1c55
Assertion Contract Owner: 0x4e475617f95ce4b2e50fb52fa798a8d7356beec8

Badge Contract Address: 0x8c76d957a25a5f742024448a5e970638983db347
Recipient Contract Address: 0x0cdc2e08b7b94b75328dac465a7b92db2e9c94c4
Evidence Contract Address: 0x62d0cd0c2ebce10dae0c3a05f2e4c80277b93ea6
Issued on: 26 Aug 2015
Expires on: never
Revoked: false
Revoked Reason:

Recipient

Recipient Blockchain address: 0x0cdc2e08b7b94b75328dac465a7b92db2e9c94c4
Recipient Contract Owner: 0x28ad986bf1f51676d89a968103e9eeeb1b409219

Identity: sha256$0f110300986c7d30daee547509eeb412c22138bc4a27452f21685e4b24c4b15a
Identity type: email
Identity hashed: true
Identity salt: badges1343741481

Badge

Badge Blockchain address: 0x8c76d957a25a5f742024448a5e970638983db347
Badge Contract Owner: 0x4e475617f95ce4b2e50fb52fa798a8d7356beec8

Name: English skills for learning
Description: This badge has been issued for participating in the activities in the free non-accredited course English: skills for learning. This course supported demonstration of the following learning outcomes: follow an active reading method to help you read academic texts and make notes; critically read source texts and appropriately use the information they contain in your writing; link ideas in your writing so that your readers can easily understand your ideas; make use of vocabulary and grammatical structures to express yourself more formally; make the most of online dictionaries

Image:

Issuer Contract Address: 0x9aef0a92fd8e7f0a3431515bd0a0e9e1767830d7
Criteria Contract Address: 0x0000000000000000000000000000000000000000
Alignment Contract Address: 0x0000000000000000000000000000000000000000

Issuer

Issuer Blockchain address: 0x9aef0a92fd8e7f0a3431515bd0a0e9e1767830d7
Issuer Contract Owner: 0x4e475617f95ce4b2e50fb52fa798a8d7356beec8

Name: OpenLearn
Description: The home of free learning from The Open University
Image:

Email: http://www.open.edu
Url: openlearn@open.ac.uk

Evidence

Evidence Blockchain address: 0x62d0cd0c2ebce10dae0c3a05f2e4c80277b93ea6
Evidence Contract Owner: 0x4e475617f95ce4b2e50fb52fa798a8d7356beec8

Evidence Links:
http://www.open.edu/openlearn/ocw/badges/badge.php?hash=933512f2a6b53b9ba73b5985c58209b6f839bbf5

Criteria

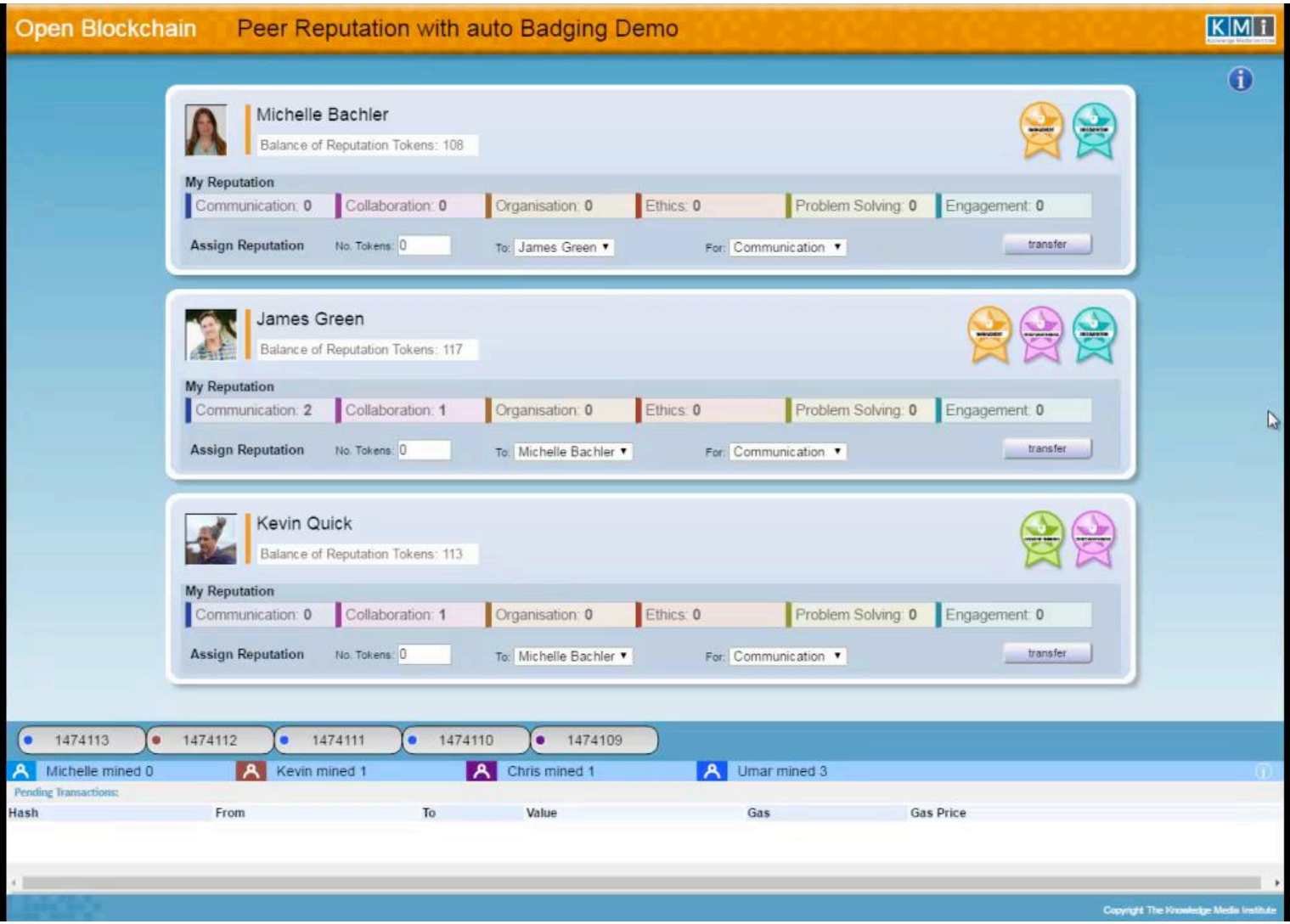
Criteria Blockchain address: 0x0000000000000000000000000000000000000000
Criteria Contract Owner:

Alignment

Alignment Blockchain address: 0x0000000000000000000000000000000000000000
Alignment Contract Owner:

KMi
Knowledge Media Institute

Peer Reputation and Badging

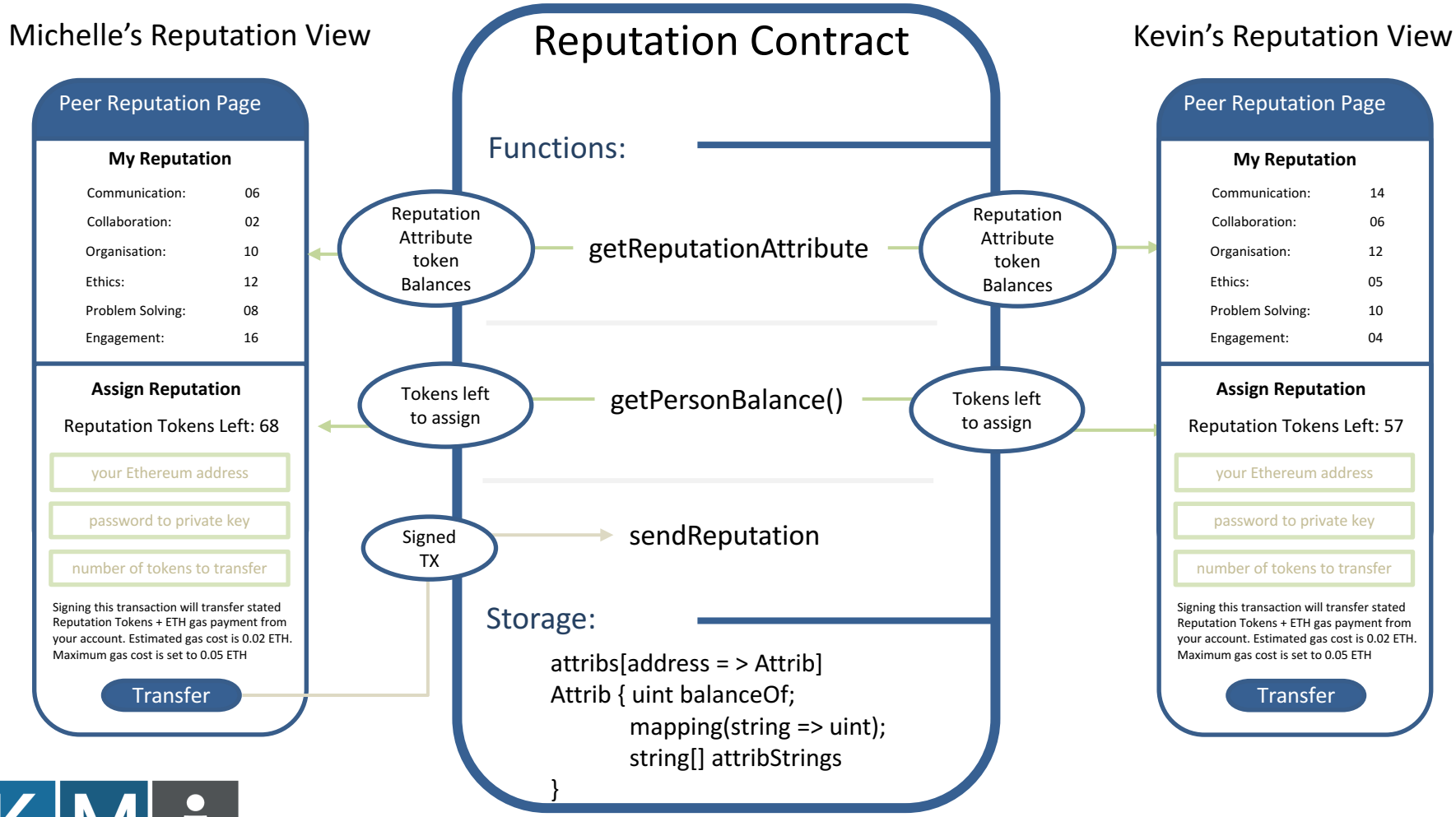


Demos of movies available at: http://blockchain.open.ac.uk/

Reputation Smart Contract

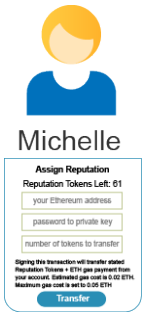
The Open University

Michelle transfers 4 Reputation tokens for 'Organisation' to Kevin



KMi Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin

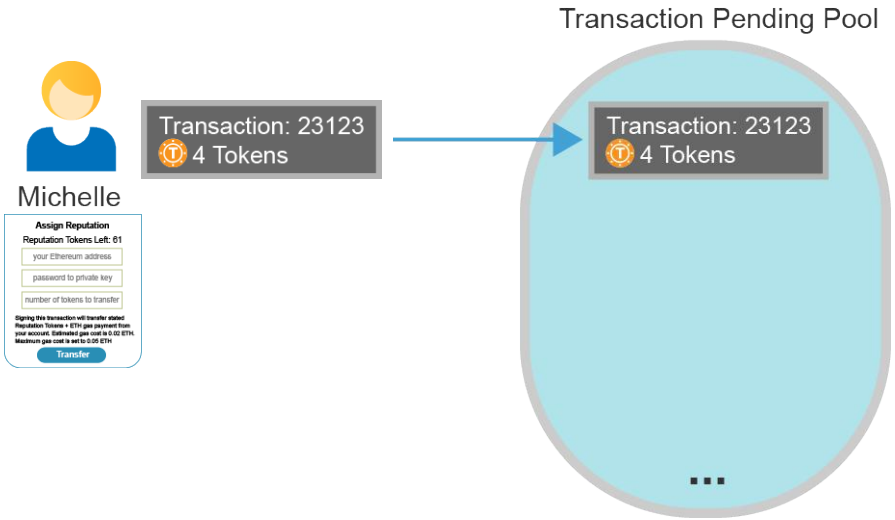


Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin

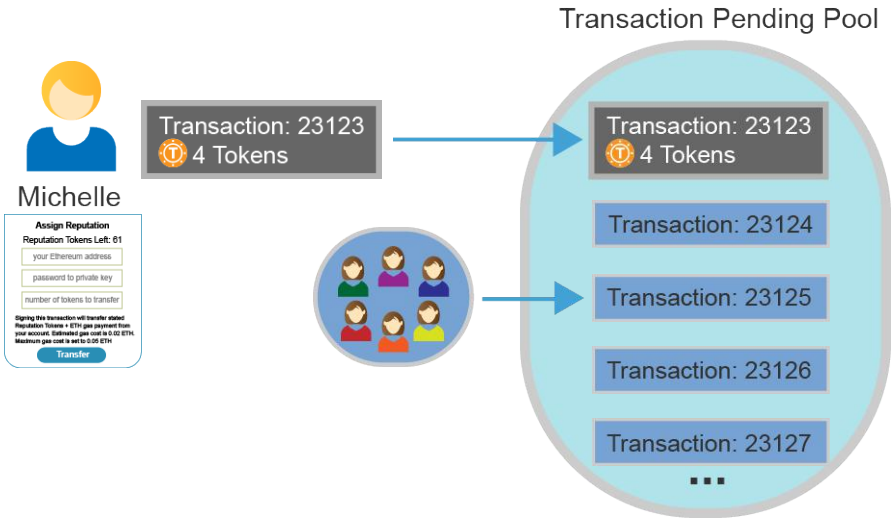
Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin



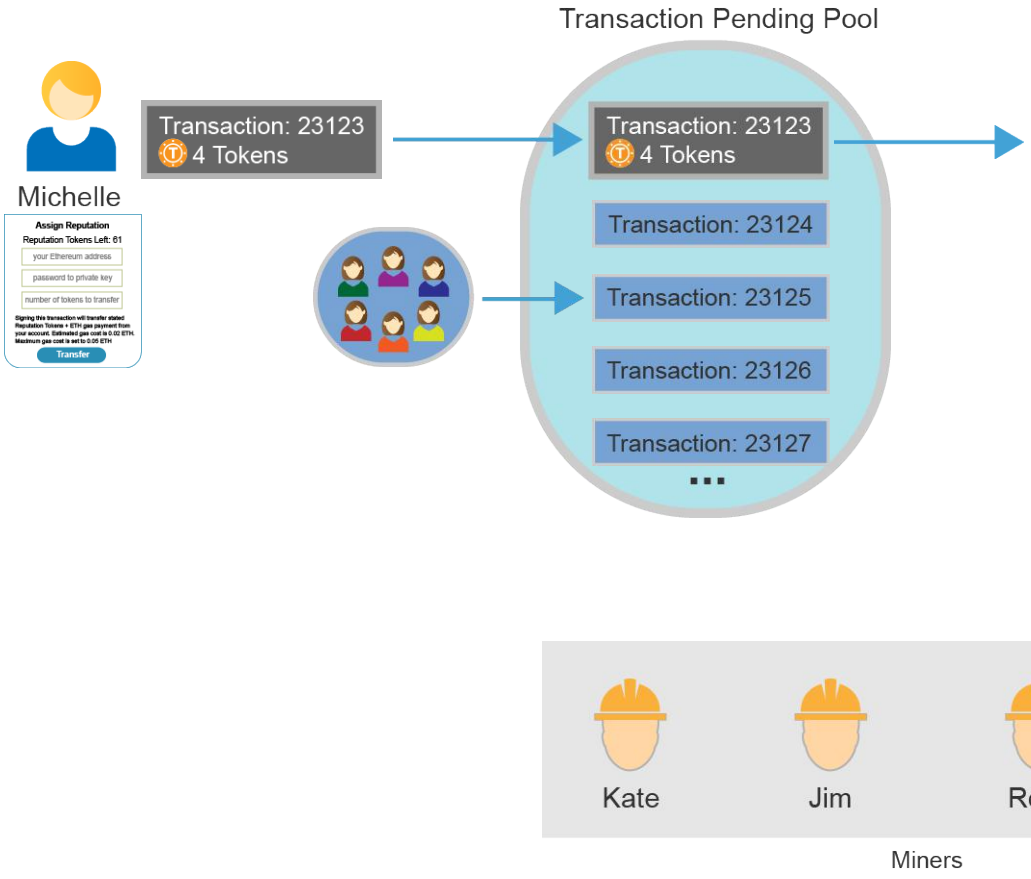
Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin



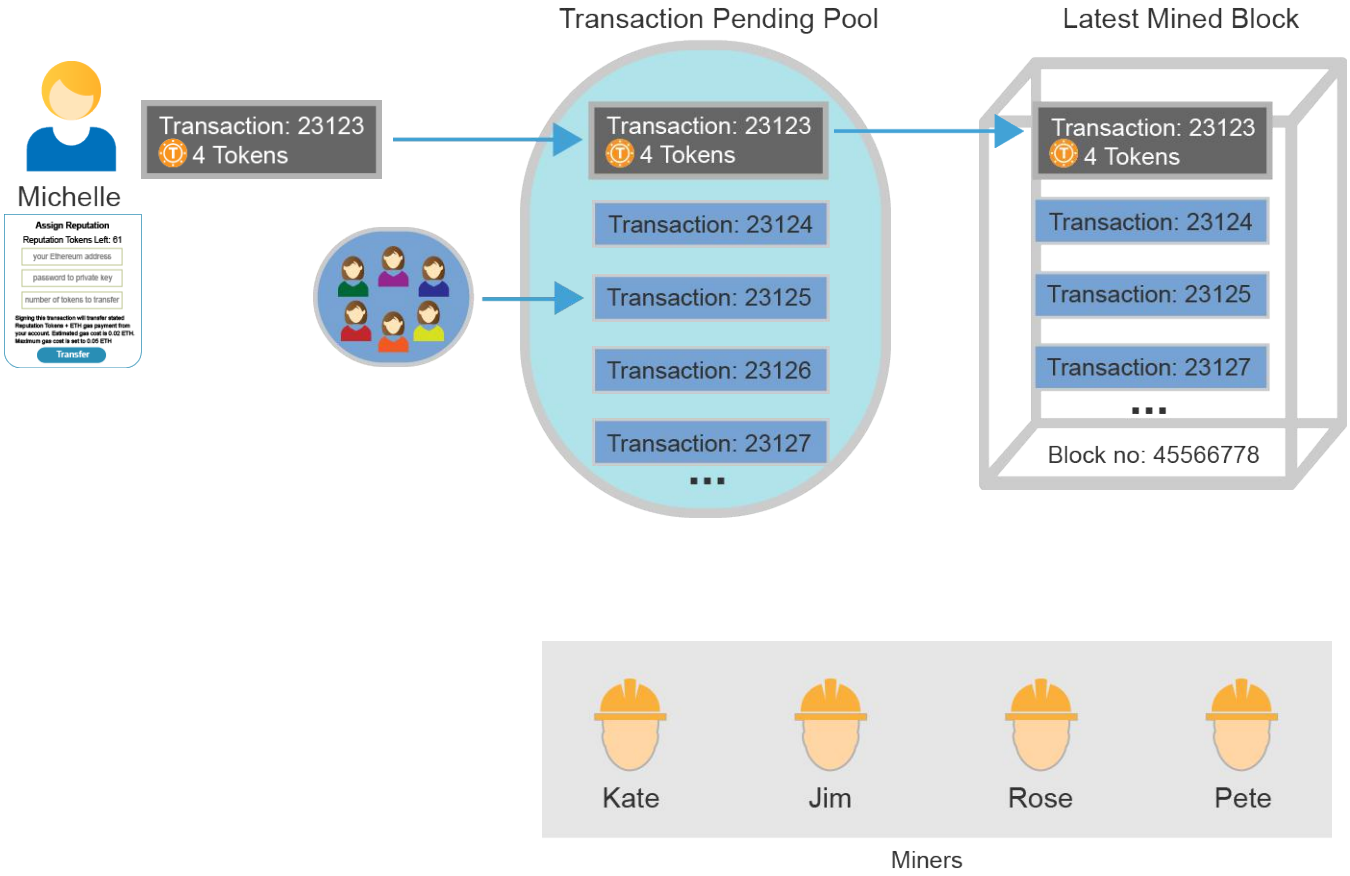
Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin



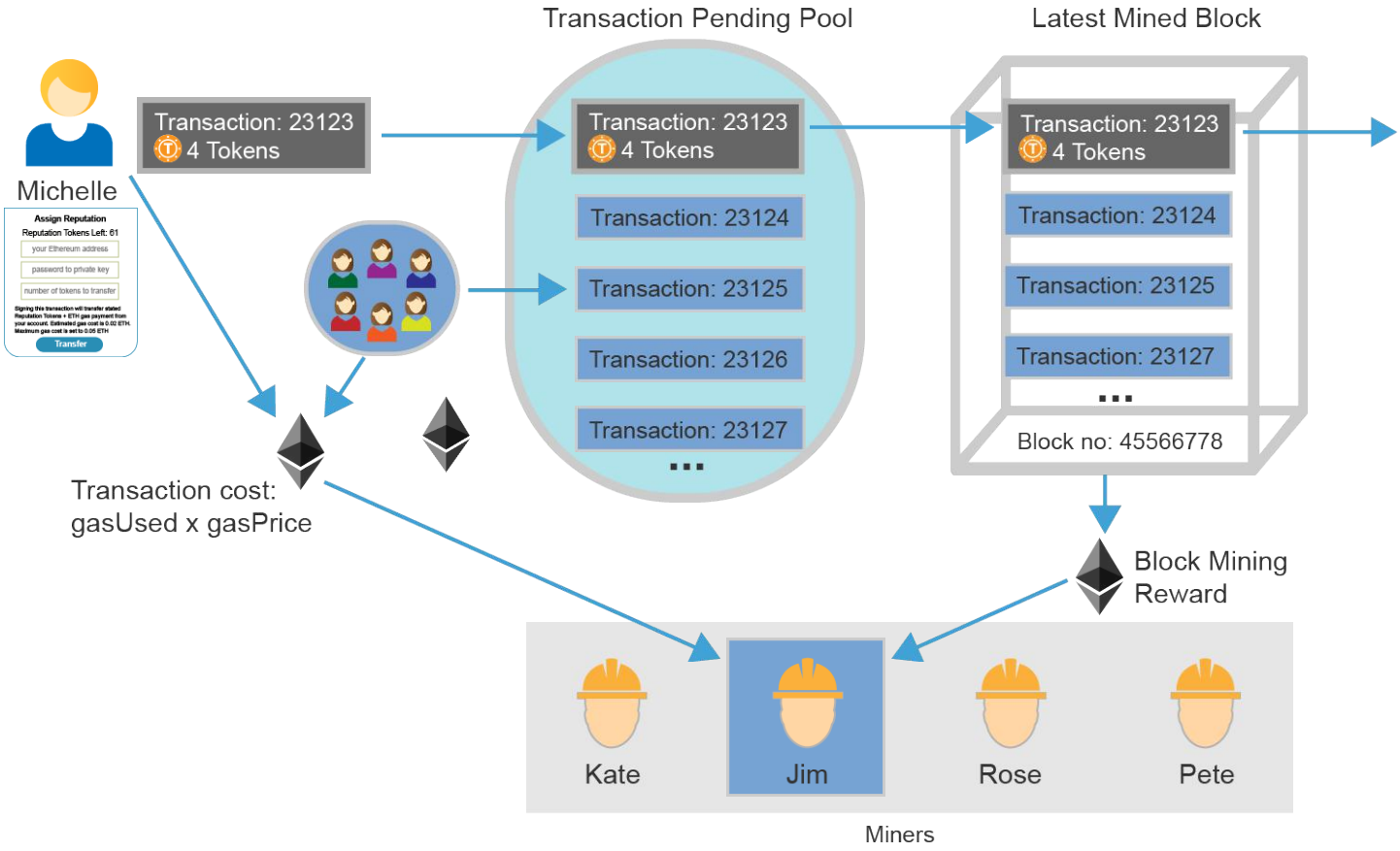
Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin



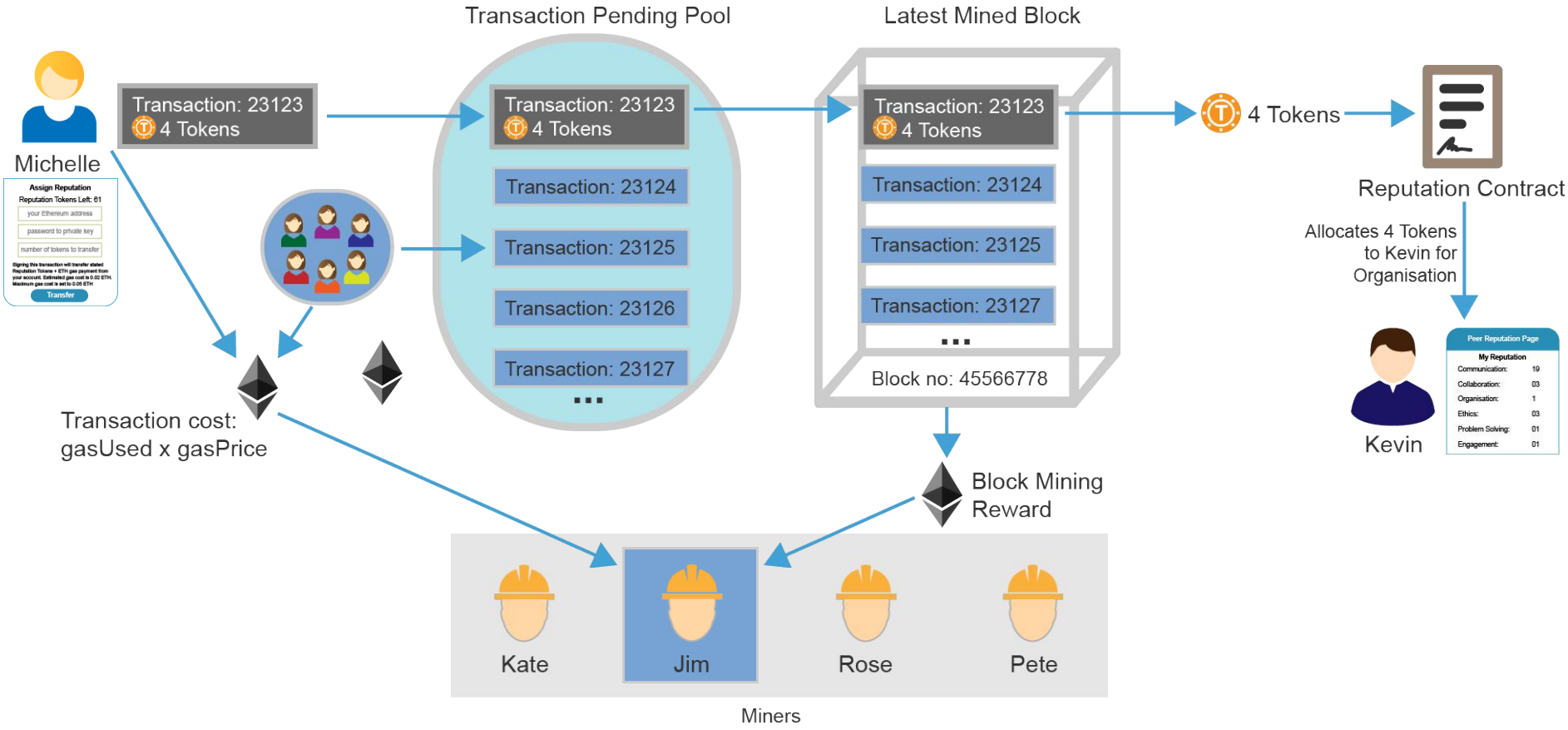
Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin



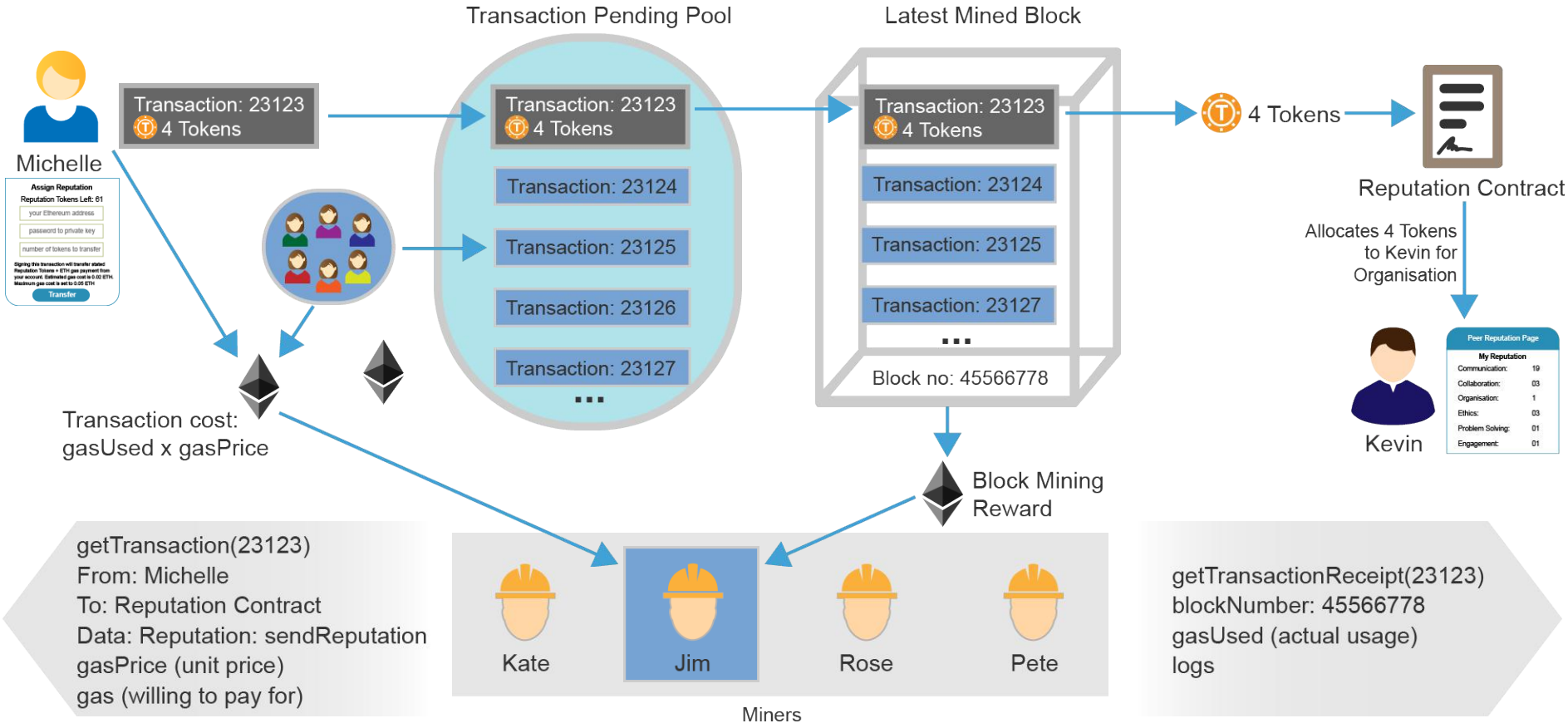
Knowledge Media Institute

Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin



Knowledge Media Institute

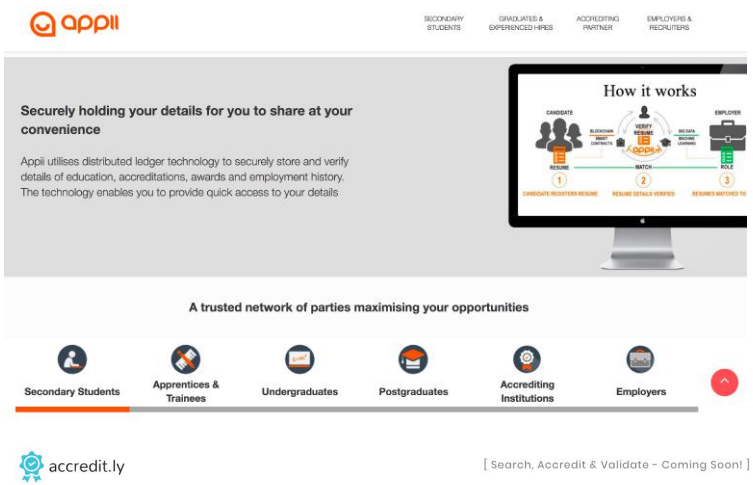
Michelle transfers 4 Reputation tokens for ‘Organisation’ to Kevin

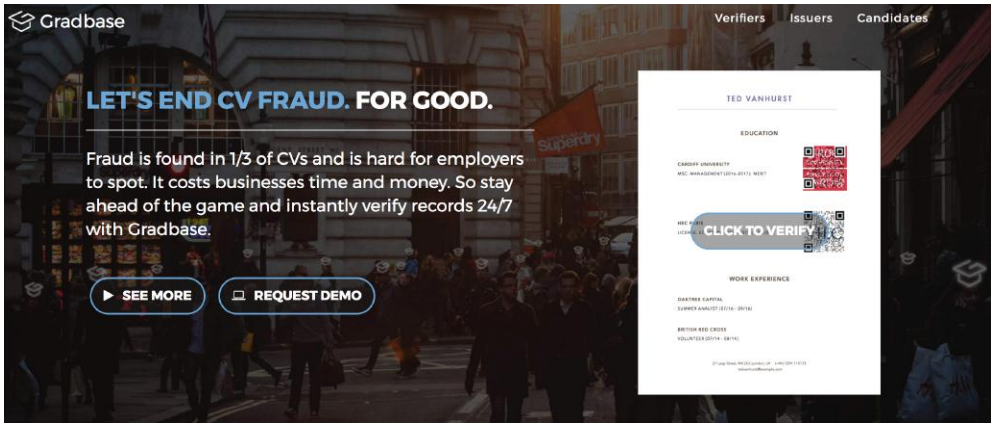


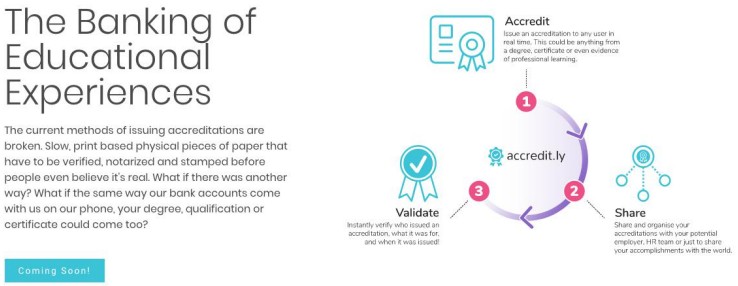
Knowledge Media Institute

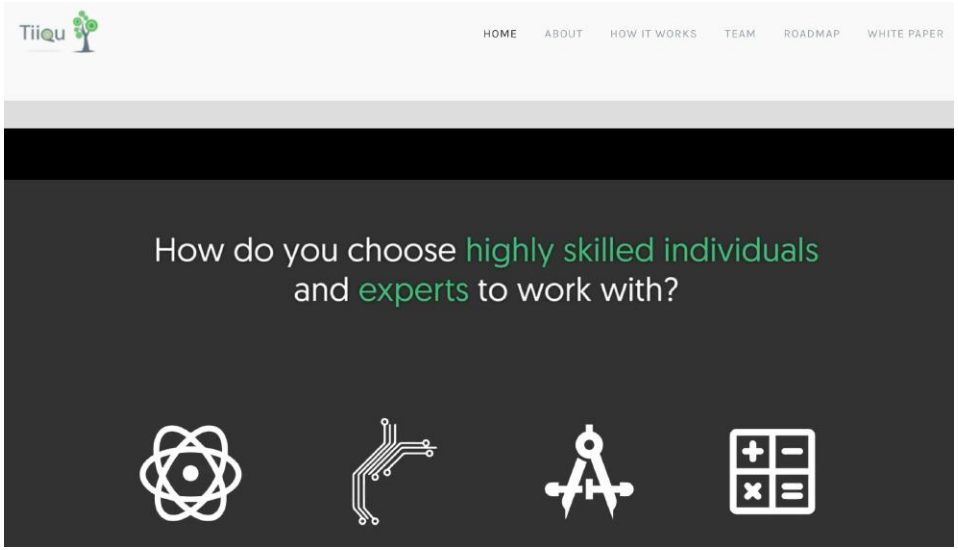
Startups in the CV/Accreditation Space

The Open University









Knowledge Media Institute

Knowledge Media Institute

The Open University

EU Funding Opportunities

NEXT GENERATION INTERNET

NGI Open Internet Initiative: Objective ICT-24

Call 1: 2018

Closure: 17 April 2018

- 3 research & innovation projects with a total budget Euro 21.5 million

  Use of cascading grants (financial support to third parties, 80%)

- 3 CSAs, total budget Euro 7 million

Call 2: 2019

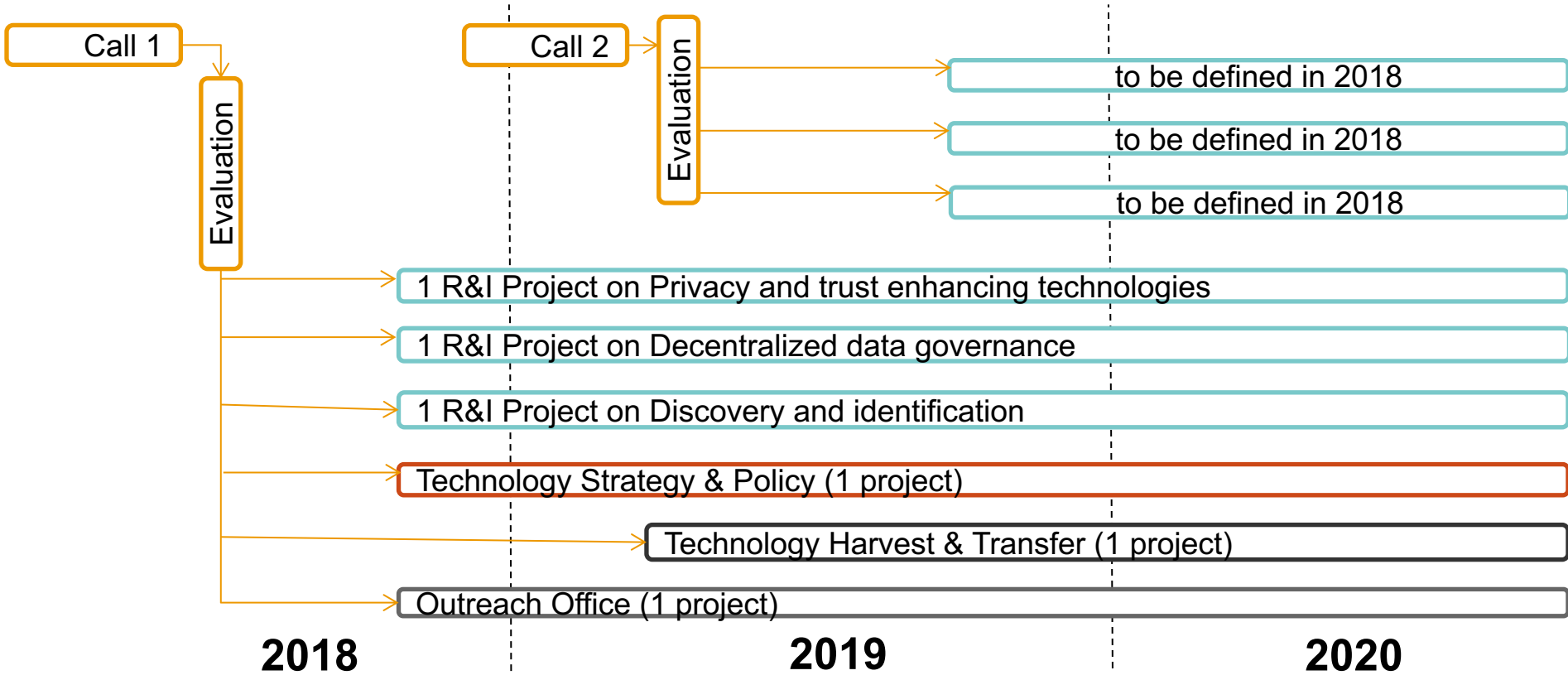
Closure: 28 March 2019

- 3 research & innovation projects with a total budget Euro 21.5 million

  Use of cascading grants (financial support to third parties, 80%)

Programme logic of objective ICT-24

NEXT GENERATION INTERNET



NEXT GENERATION INTERNET

R&I project implementation through sub-granting

Project submitted to EC call:

Euro 7-7.5 mil, 2-3 years,
80% for sub-grantee
Pan European
Procedures adapted to stakeholders
Run by organisations in the ecosystem

R&I Action:
Privacy and trust enhancing technologies

Activities include inter-alia:

- Call for & selection of top-teams
- Monitoring
- Mentoring, Coaching, Sharing
- Communications
- Community building

Sub-grantee:

- One legal entity with one specific project
- **Young researchers from outstanding academics, hi-tech startups and SMEs**
- Carry out the R&I work
- 50.000 – 200.000 Euro, 9 – 12 month

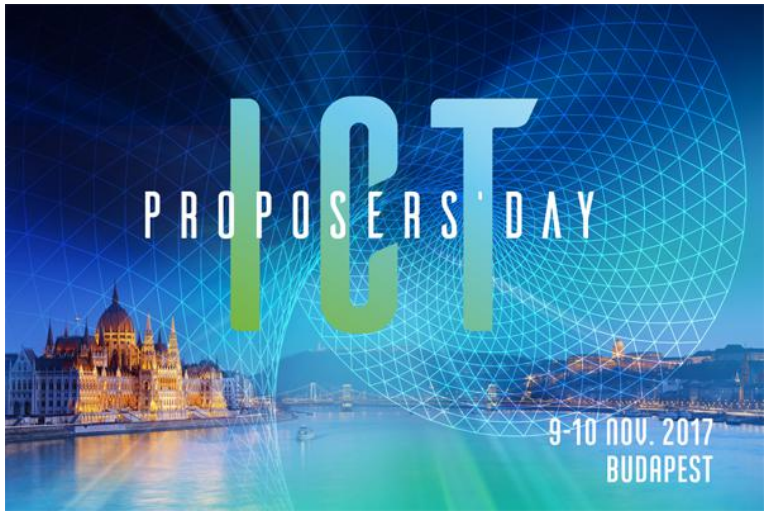
NGI @ ICT PROPOSERS' DAY 2017

NEXT GENERATION INTERNET

The **Next Generation Internet (NGI) networking session - 10/11/2017 (09:30-11:00)**

The NGI networking session focuses on 2 calls:

- The NGI Open Internet Initiative ICT-24-2018:
  - 3 Research & Innovation (R&I) Actions; 21.5 M€; 2-3 years; 1 R&I project per topic:
    - Privacy and trust enhancing technologies
    - Decentralized data governance
    - Discovery and identification technologies
  - supported by 3 Coordination and support actions (CSAs); 7 M€
- The EU-US collaboration on NGI ICT-31-2018;
  - 2 CSAs (2.5 M€; 3 years)
    - CSA 1: Organise & other support activities
    - CSA2: A Fellowship programme.
- Feel free to propose your project ideas for the 2 NGI calls above!



THE NGI BOOTH

- More information about the ICT-24-2018 and ICT-31-2018 Calls

EU-US Collaboration on NGI

Deadline 17 April 2018

Support Actions
- **Think-tank**
- **Fellowships**

Budget Euro 2.5 million

Deadline 28 March 2019

Research and Innovation Action
- **Joint experimentation**

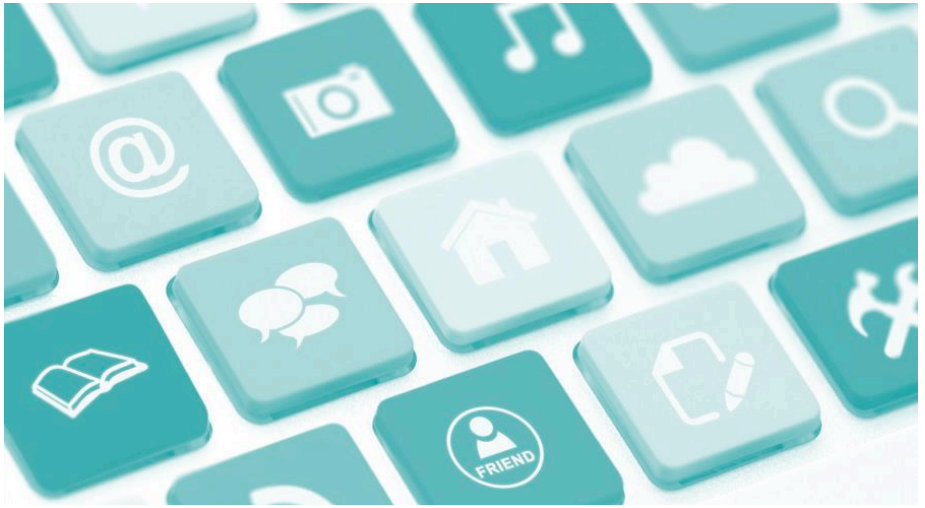
Budget: Euro 3.5 million

Stay Connected

NEXT GENERATION INTERNET

WHERE TO FIND MORE INFO

- The NGI Corner on Futurium
  https://ec.europa.eu/futurium/en/next-generation-internet
- The NGI Twitter Channel @NGI4EU
- The NGI web portal www.ngi.eu
- The NGI map of actors www.hub4ngi.eu/map/



Summary

- A blockchain is a distributed ledger
- Smart contracts add trusted computational layer
- Benefits include
  - Inbuilt identity management
  - Decentralised control/ownership
  - Increases transparency
  - Reduces risk of fraud
  - Dramatic lowering of process costs
  - Enables collaboration/interoperability
  - Facilitates disaggregation and disintermediation
  - Transform online and physical objects into DAOs

THANK YOU FOR YOUR ATTENTION

WWW.HUB4NGI.EU

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732569