Blockchain for Science

Martin Etzrodt

CERN, 11.7.2018

Overview

- Basics
- Application
- Future of science communication & knowledge creation

Overview

- **Basics**
- Application
- Future of science communication & knowledge creation (work in progress...)

In short...

- ❑ Blockchain is a database

- ❑ Everybody can write

- ❑ Validity by cryptography

  - ❑ Data have a signature

  - ❑ Blocks have proof of work

- ❑ Database is decentralised, miners are it's "good spirit"

  - ❑ Incentivised via block rewards
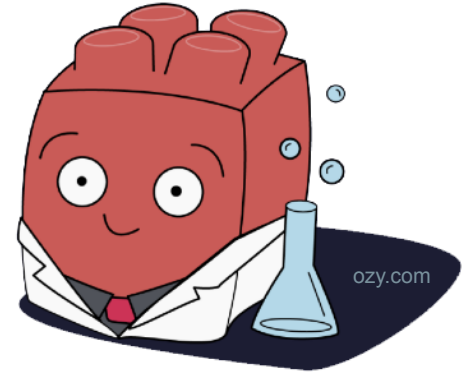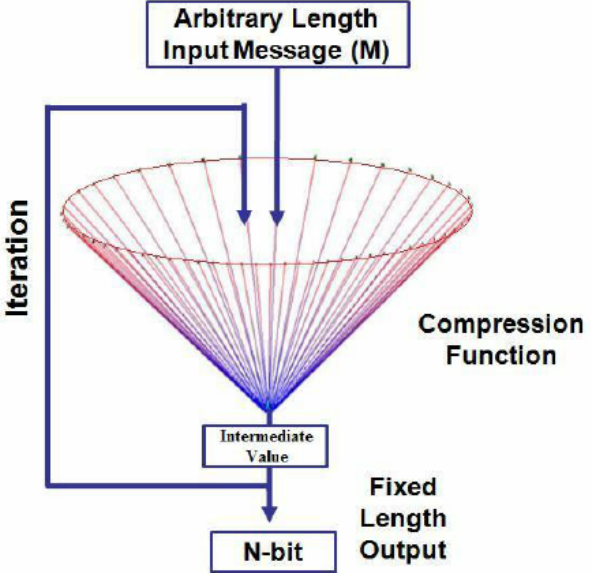
Cryptographic Hash function

- SHA 256 (Secure Hash Algorithm) - a 256 bits long digital finger print for data:

Hello World

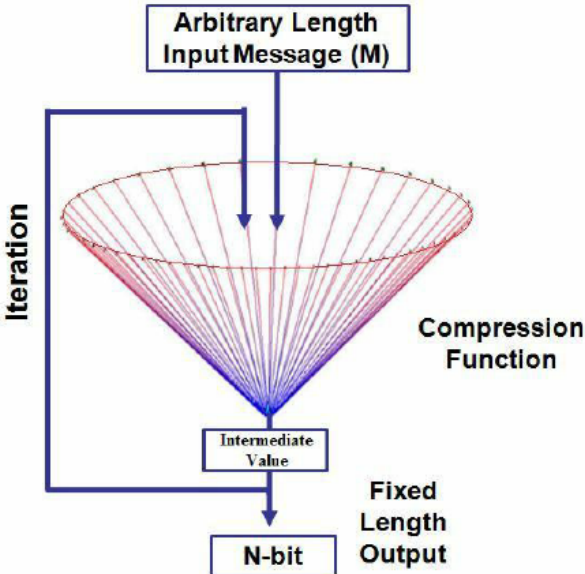a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Arbitrary Length Input Message (M)

Iteration

Compression Function

Intermediate Value

N-bit

Fixed Length Output

- Given the output its impossible to determine the input ("one way" hash)

- Its impossible to find two different inputs which give the same output.

Cryptographic Hash function

- Same hash length, no matter how many data
- Same data = same hash

M. Maqableh (2011), DOI: 10.13140/2.1.2021.0886

60fae91769c446c650a1bf85d65ea5950c0911578747af17698847a36ccb761f

Martin Etzrodt, 11.6.2018, CC-BY NC

A New Dimension For Payments

Since ~ 10.000 years

Transaction of financial assets from and to:

People

Organizations

A New Dimension For Payments

Since 07/30/2015 3:26 UTC (Ethereum genesis block):

Transaction of financial assets from and to:

People

Organizations

Programs

SMART CONTRACT
=

Program on a blockchain that can control distribution of assets.

Blockchain and Smart Contracts
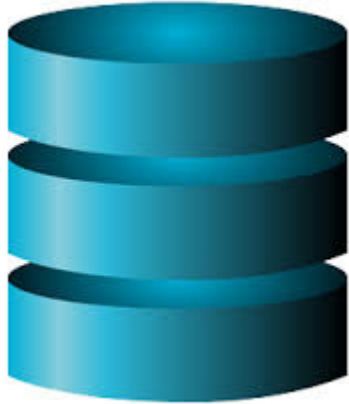
Bitcoin blockchain
= database

Crypto Valley

Ethereum blockchain
with smart contracts

= World Computer

EXAMPLE: Decentralised insurance

ValidityLabs

Get your instant payout
in case your flight is late.

Data Source (Oracle)

FLIGHTSTATS

Flight was
on time

Smart Contract
deployment

Developer

1 ETH

Smart
Contract

10 ETH

11 ETH

Insurance taker

Investor
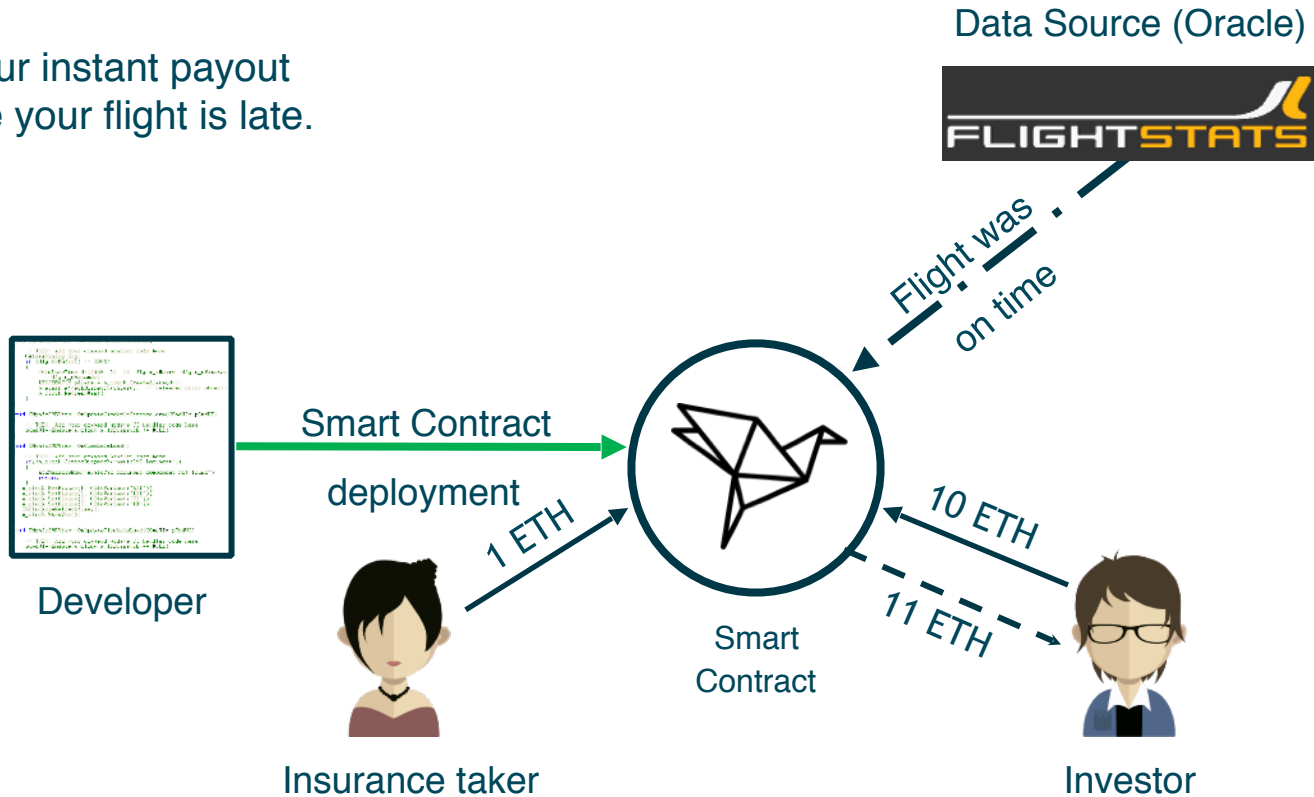
Blockchain will drive intermediaries out of business!

- Basics
- **Application**
- Future of science communication & knowledge creation

Decentralizing Science

Scientific publishers have traditionally served two important roles for science:

1. Efficient collection and distribution of scientific information:

- Distribution of physically printed articles

2. Publishers serve as a trusted third party:

- Filtering content
- Handle "peer review" process
- Serve as a solicitor to attribute scientific findings

http://elephantinthelab.org/decentralizing-science/

ELEPHANT
IN THE LAB

Blockchain solution architecture.

ValidityLabs™

Broadcast data to IPFS

Sign IPFS hash & send to smart contract

Index

Operator/ machine:
- creates data
- analyses data
- interprets data

Notarization:
- attributable
- timestamped
- can trigger processes

IPFS Storage:
- open
- immutable
- censorship-resistant

slide prepared by Martin Etzrodt with Validity Labs

Example

1. Acquisition
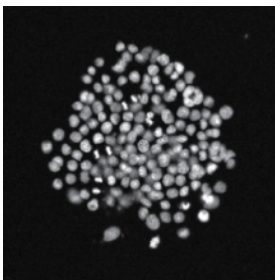
2. Analysis

```
//run("Brightness/Contrast...");
setMinAndMax(59, 186);
run("Smooth");
run("Apply LUT");
//run("Threshold...");
setThreshold(0, 120);
setOption("BlackBackground", false);
run("Convert to Mask");
run("Analyze Particles...", " show=Outlines
display clear include summarize record add");
```

3. Interpretation

Permanent content-addressed storage (IPFS)

Notarization (who and when) on blockchain

Timestamp:
Jul-05-2017 11:36:07 PM

Operator:
0x74abbdc4e5d62210194f503a871a6bf68744b1a1

Timestamp:
Jul-05-2017 11:45:52 PM

Analyst:
0x74abbdc4e5d62210194f503a871a6bf68744b1a1

Timestamp:
Jul-05-2017 11:43:07 PM

Publisher:
0x74abbdc4e5d62210194f503a871a6bf68744b1a1

What did we gain?

- Permanent publication of results

- Attribution of researchers' contributions

- Interoperability to enable incentives (grants, publications, IP)

- Trigger processes (via smart contract)

Blockchain 1.0 → #BeYourOwnBank   (Bitcoin)

Blockchain 2.0 → #BeYourOwnJournal   (now)

- Basics
- Application
- **Future of science communication & knowledge creation (WARNING: incomplete, work in progress...)**

The race for a "Blockchain for Science"

All talks of the meeting on: https://hackmd.io/c/r11YTzX9f/%2FQTaG8S3LQAeBfnCT-EFFfQ

ALETHEIA

DaMaHub

AKASHA
A Next Generation Social Media Network

Knowbella Tech

DEIP

matters
Stories can wait. Science can't.

covee

DIGITAL science

EUREKA
by sciencematters

sci napse

frankl FL

pluto
Decentralized
Scholarly Communication
Breaking down barriers in academia

SCIENCEROOT

MINDFIRE

FRACTAL FLOWS

Orvium

Zug, May 10, 2018
https://www.blockchainforscience.com/2018/02/20/cryptscience2018/

PUBLISHERS BEGIN CO-OPTING THE BLOCKCHAIN REVOLUTION

T&F and CUP join Springer Nature blockchain pilot

Published April 27, 2018 by Benedicte Page

Share

Academic houses Taylor & Francis and Cambridge University Press have joined a pilot project on using blockchain technology for peer review announced by publisher Springer Nature and start-up Katalysis last month.

Digital Science and Katalysis Lead Initiative to Explore Blockchain Technologies for Peer Review

TAGS: #blockchainforresearch , Blockchain

The initiative is an important step towards a fairer and more transparent ecosystem for peer review and explores the utility of decentralized data stores in supporting trusted assertions that connect researchers to their activities.

https://www.blockchainpeerreview.org/

Decentralised Scholarly Communication Platforms aim to break down the "barriers of academia".

Problem: Focus on publication process

"Wealth creation has shifted from prior knowledge to the ability to gain new-knowledge-in-action.

… its more cost-effective to invest in processes for insight than in material possessions or present-day intellectual property (IP)."

Economy of insight - Conversations as Transactions, Paul Pangaro (2011)

In Pablo Garcia Tello's words:

-> It is interesting to know who is "trading" with whom and "what".

Relevant resources: http://pangaro.com/futurecom/

Data, information & knowledge are...
Anti-rival goods

- Anti-rival goods: *The more persons share an anti-rival good the more utility each person receives.*

+Public goods:
Not excludable (freely available to all)
+ non-rival: consumption by one person does not reduce the amount available for others.

Examples: Knowledge, natural language, software....

Intellectual Property (IP) and copyright is a means to turn anti-rival resources into scarce elements: to make them sellable.

Today content **is** already freely accessible

Table 1. Coverage for the ten journals with the most articles.

| Journal	Sci-Hub	Crossref	Coverage
The Lancet	457,650	458,580	99.8%
Nature	385,619	399,273	96.6%
British Medical Journal (Clinical Research Edition)	17,141	392,277	4.4%
Lecture Notes in Computer Science	103,675	356,323	29.1%
Science	230,649	251,083	91.9%
Journal of the American Medical Association	191,950	248,369	77.3%
Journal of the American Chemical Society	189,142	189,567	99.8%
Scientific American	22,600	186,473	12.1%
New England Journal of Medicine	180,321	180,467	99.9%
PLOS ONE	4,731	177,260	2.7%

The total number of articles published by each journal is noted in the Crossref column. The table provides the number (Sci-Hub column) and percentage (Coverage column) of these articles that are in Sci-Hub's repository.
DOI: https://doi.org/10.7554/eLife.32822.005

SciHub: "An international network of piracy and copyright infringement by circumventing legal and authorised means of access" (Elsevier) ...

Publisher's responses: "Amazonification"
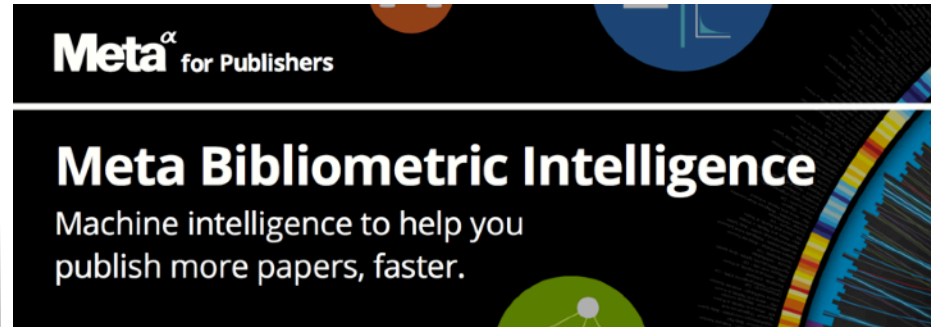
federated ID systems for publishers

- Offer personalised services to accelerate insight...
- **"individualised and differentiated access" means: (= exact stats on Who is researching What and Where at any given time)**

- Pinpoint high impact manuscripts
- Publish more content and drive revenue
- Pre-rank manuscripts
- Grow number of papers published without sacrificing quality standards

Information about those create knowledge is worth more than the published papers.

Commons based peer production

- Large numbers of people work cooperatively

- Less rigid hierarchical structures

- Often no financial compensation (but now possible)

Examples:
Linux, GNU, Wikipedia, SETI@home, Clickworker (NASA), open source hardware, …
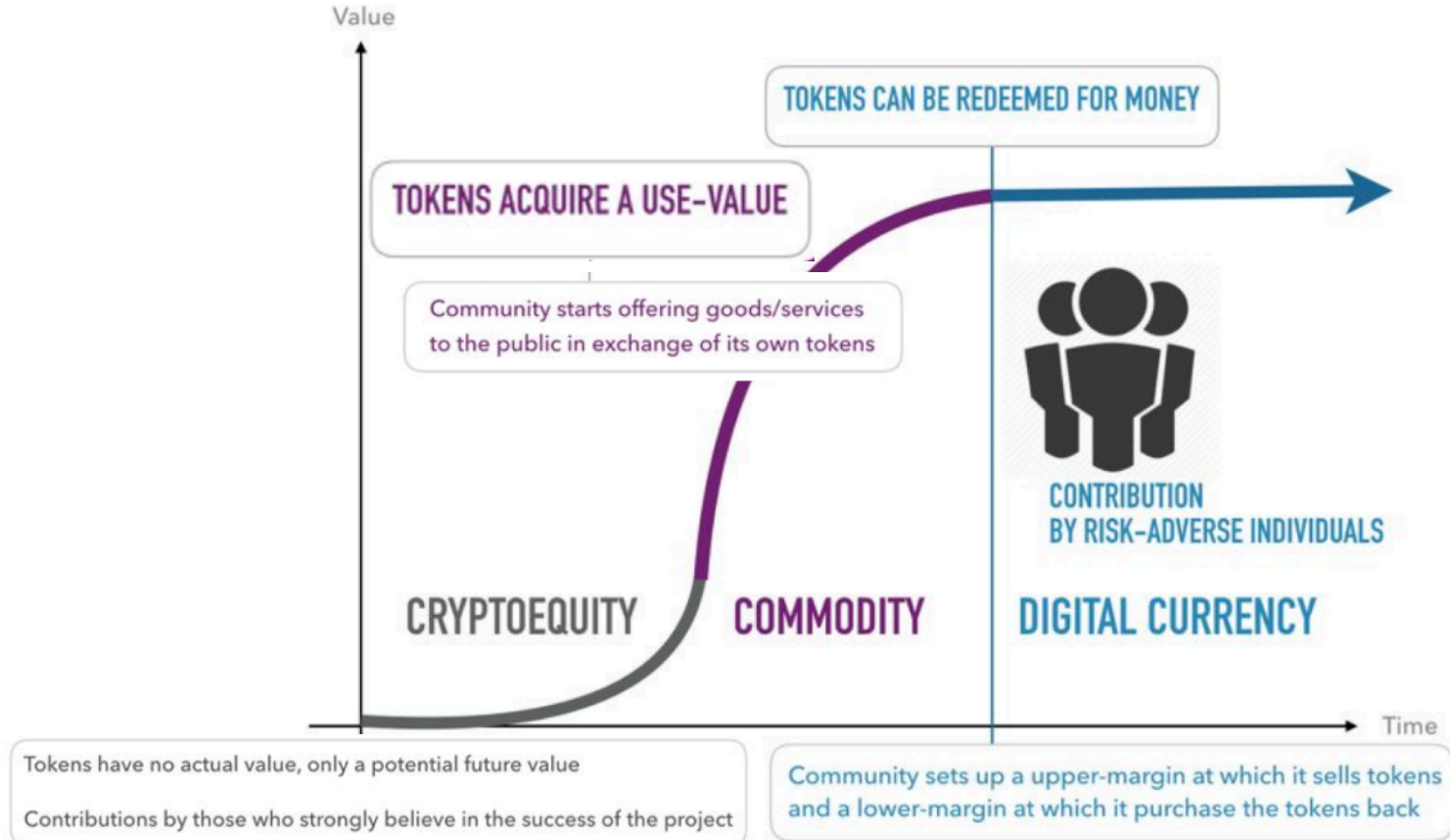
Why blockchain?

Internet:

+ Real-time information exchange at a worldwide scale.

- No internal value distribution, lacks inherent economic incentive model for engagement.

Blockchain: Reliable (*third party independent*) open (*decentralised*) and programmable (*smart contracts*) accounting system (*ledger*).
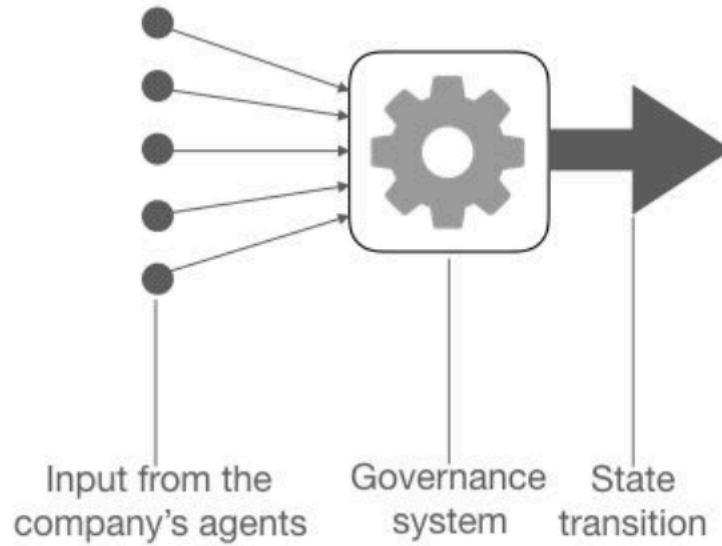
-> Fundamental possibility of value exchange for coordination and global peer-production.

Cave: "Value" does not mean you can buy anything for it...

Sources: i.e. DAOstack.io,

Token valuation proposal

Source: http://backfeed.cc/assets/docs/BackfeedEconomicModel.pdf

Governance

Input from the company's agents   Governance system   State transition
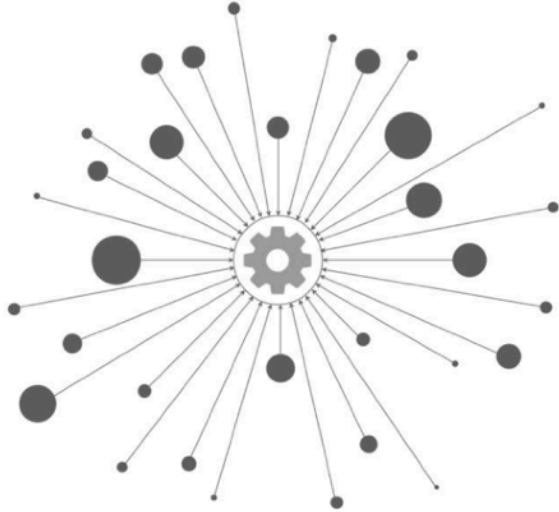
A blockchain governance system collects inputs from blockchain addresses and under certain rules spells out an output in terms of the blockchain global state transition.

DAO - Decentralised autonomous organisations

The assembly mode of a DAO.

Assembly node:

a large number of agents are interacting in decision making within a single agency via its smart contract, assuming that reputation, and thus decision-making power is fairly distributed.

Large scale commons-based and value bearing projects can be created in absence of a central authority (publisher, institution, government).

Source: daostack.io

SCIENTIFIC PEER PRODUCTION USING "SMART CONTRACTS" - incomplete proposal
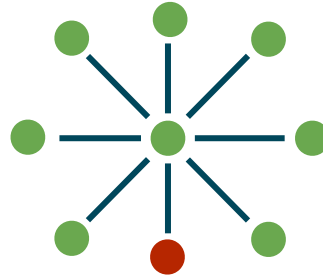
Smart contracts:

operate recursively & create a
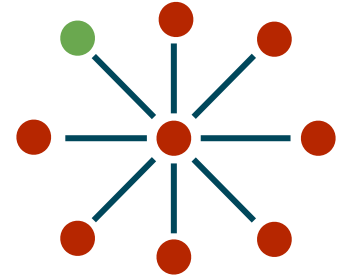'tree' for a given seeding problem

Discovery status:

🟢 accepted

🔴 closed/ rejected

accept

reject

Blockchain projects building on this paradigm:
https://www.eurekatoken.io/
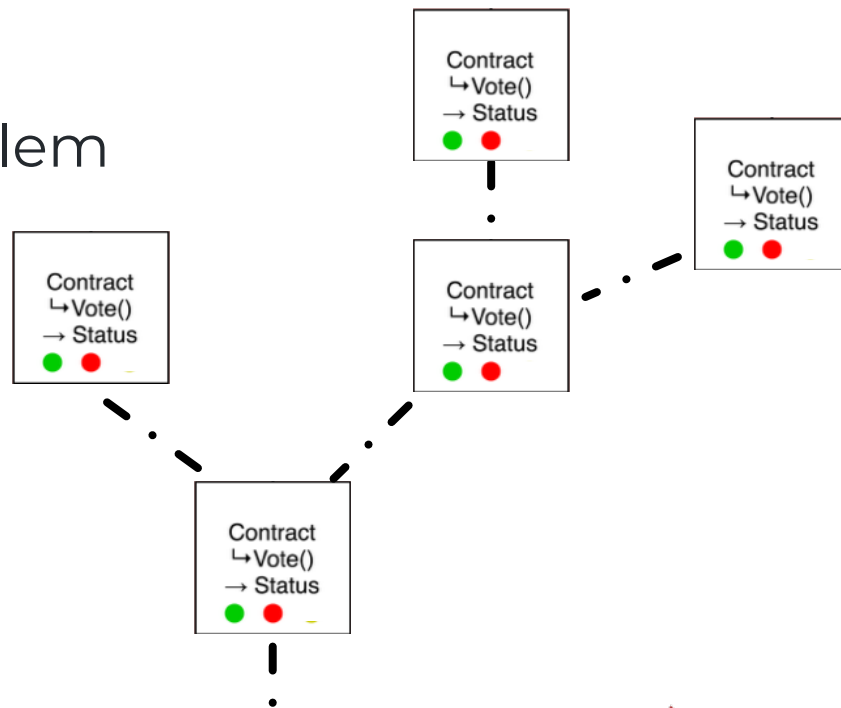https://fractalflows.com/

THE TREE OF KNOWLEDGE

Smart contracts:

operate recursively & create a

'tree' for a given seeding problem
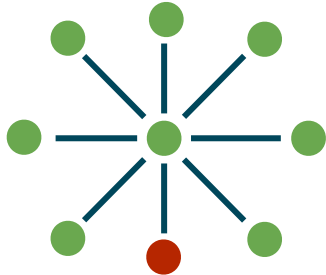
Discovery status:
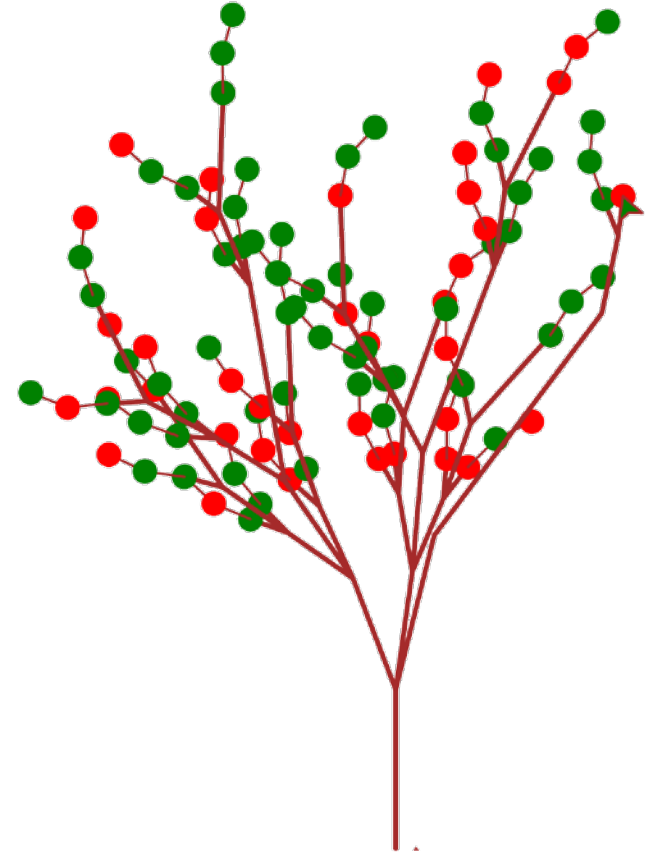
🟢 accepted

🔴 closed/ rejected

THE TREE OF KNOWLEDGE

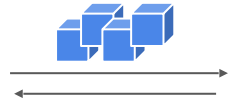Contract
↳Vote()
→ Status
● ●

accept   reject

Projects building on this paradigm:
 https://fractalflows.com/
 https://www.eurekatoken.io/

ETH *zürich*

Proposal: A blockchain backed "social media" platform for science & knowledge creation

Study design, experimental
& statistical design

Peers are invited:
'idea' conference

Improved idea
attracts talented
experimental groups

Fund distribution along "audit trail"

Publishing industry helps
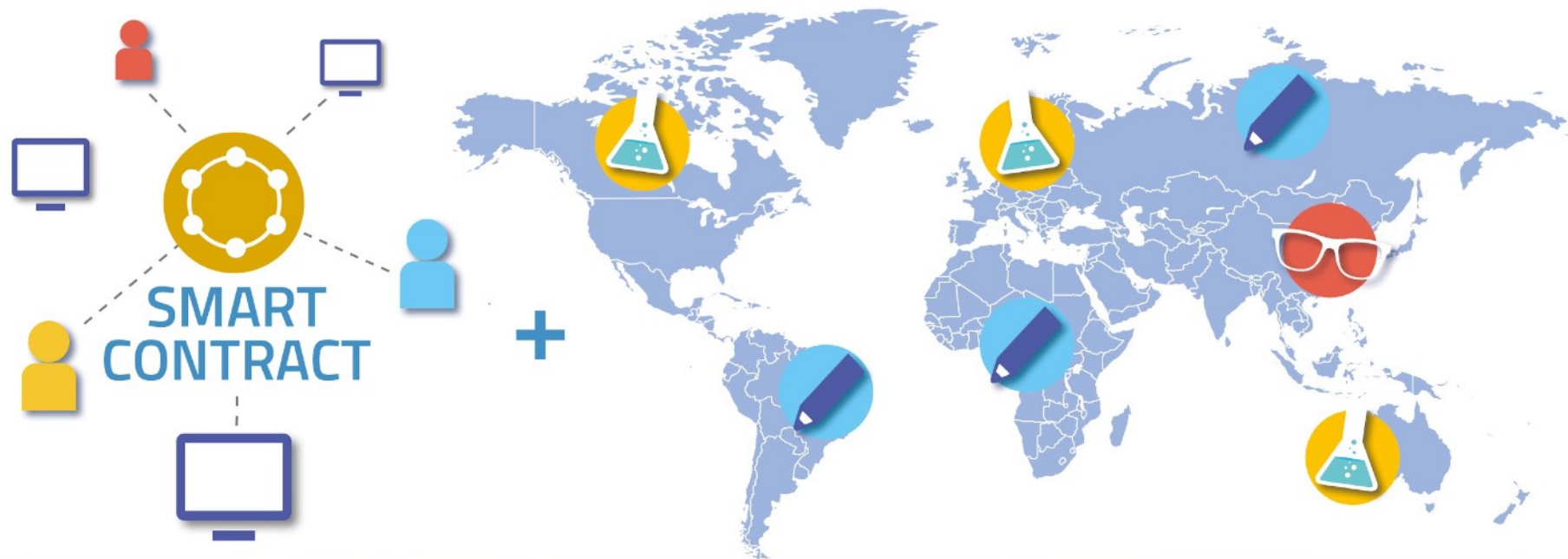spread the word

Industry competes for licensing and
production of test/ product

REINVENTING DISCOVERY: Decentralized R&D markets emerging outside of corporate, academic or governmental silos.

SMART CONTRACT

+

slide prepared by Martin Etzrodt with Validity Labs

Akasha - an experimental decentralised social media platform

Akasha.world

> Decentralised social media experiment by Ethereum co-founder Mihai Alisie

> Crypto-economic experiment for re-evaluating information processing