Blockchain and impact on science

Gotthold Fläschner[*], Martin Etzrodt[*] [#] & Sebastian Bürgel[#]

[*] ETH Zurich, [#] Validity Labs AG, Zug

CERN, 27.4.2018

Validity Labs AG
Postplatz 1
6300 Zug | Switzerland

ValidityLabs™

Dr. Sebastian Bürgel | co-founder & CTO
+41 44 77 00 282
sebastian.buergel@validitylabs.org

Dr. Martin Etzrodt | Research head
+41 44 77 00 280
martin.etzrodt@validitylabs.org

André Wolke | co-founder & CEO
+41 44 77 00 281
andre.wolke@validitylabs.org

Research branch of Validity Labs: Design, test and deploy tools for decentralized research institutions of the future.

Research

Build, break & improve platforms running on smart contract & crypto- economic architectures

Education

Educate about the potential of blockchain in research and development.

Collaboration

Collaborate with academia, funding agencies & industry. Build open source tools.

Agenda

- Blockchain for “dummies”
- Smart Contracts
- ‘Blockchain for Science’:
  Data integrity, protection & collaboration

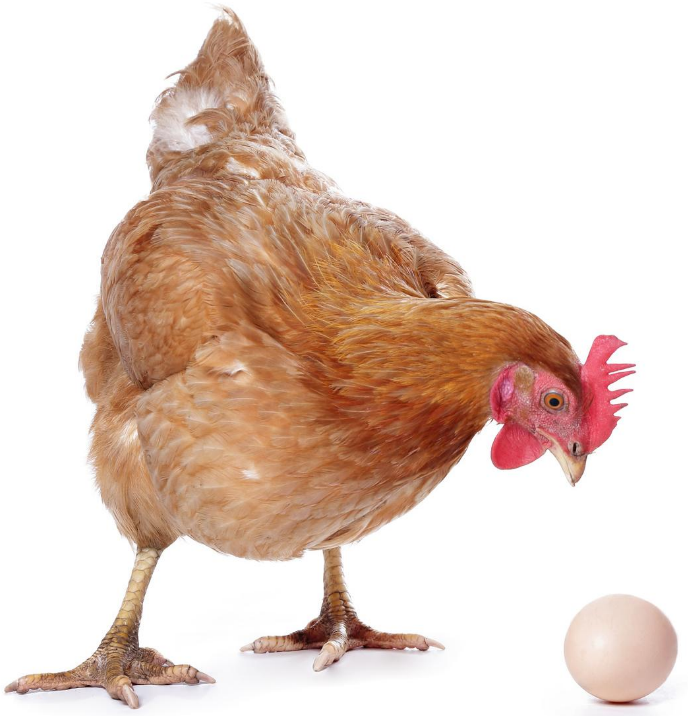
Agenda

- **Blockchain for “dummies”**
- Smart Contracts
- ‘Blockchain for Science’:
  Data integrity, protection & collaboration

Blockchain vs Bitcoin

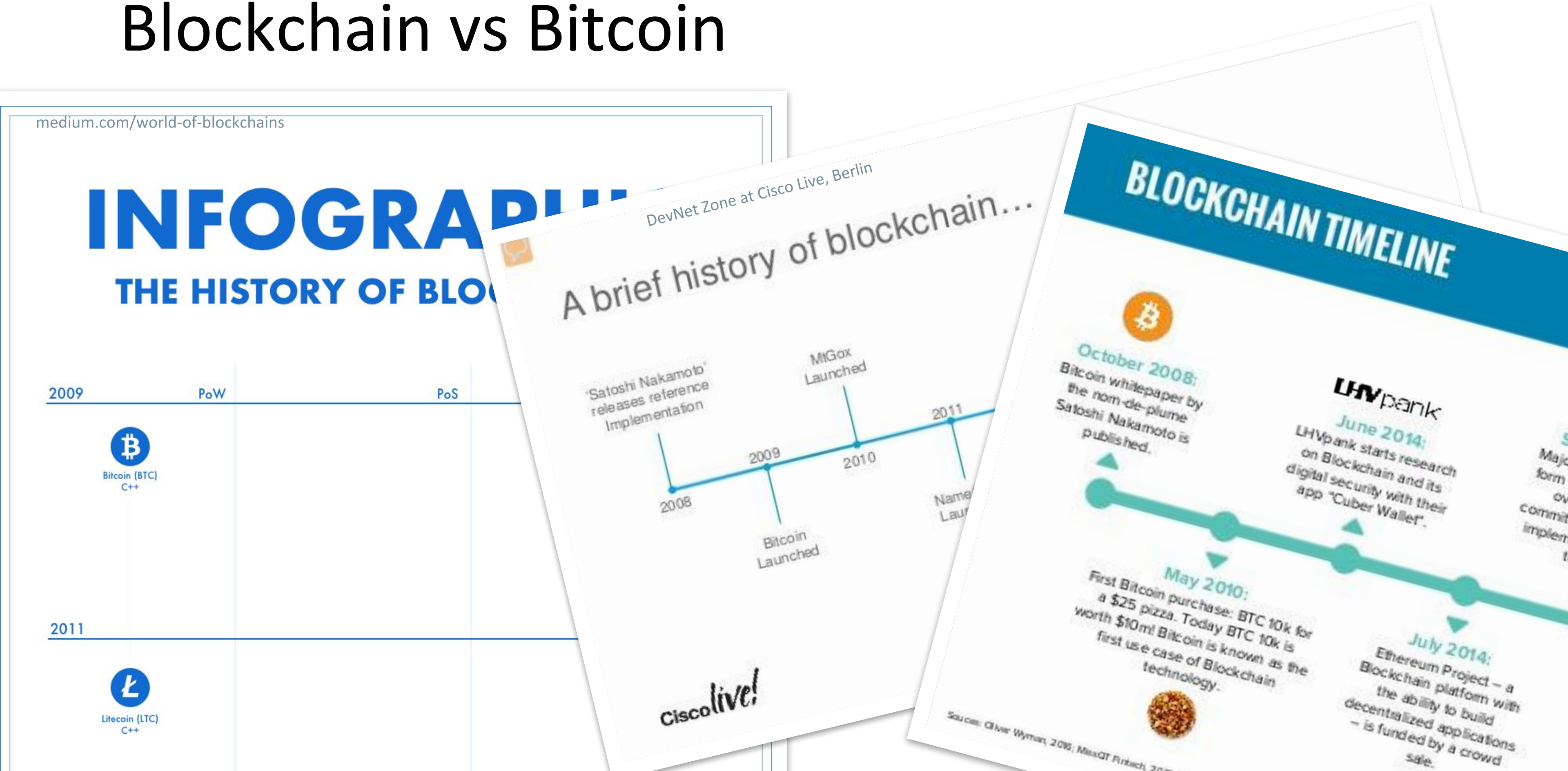
- A blockchain is an open database
- Decentralized & trustless verification through math
- Blockchain: early 1990s

  Bitcoin: 2008



thegoodeggfellas.co.uk

Blockchain vs Bitcoin



medium.com/world-of-blockchains

INFOGRAPH

THE HISTORY OF BLO

DevNet Zone at Cisco Live, Berlin

A brief history of blockchain…

BLOCKCHAIN TIMELINE

October 2008: Bitcoin whitepaper by the nom-de-plume Satoshi Nakamoto is published.

June 2014: LHVpank starts research on Blockchain and its digital security with their app "Cuber Wallet".

May 2010: First Bitcoin purchase: BTC 10k for a $25 pizza. Today BTC 10k is worth $10m! Bitcoin is known as the first use case of Blockchain technology.

July 2014: Ethereum Project – a Blockchain platform with the ability to build decentralized applications – is funded by a crowd sale.

Sources: Oliver Wyman, 2016; MaxxQT Fintech, 20

Let‘s build a blockchain

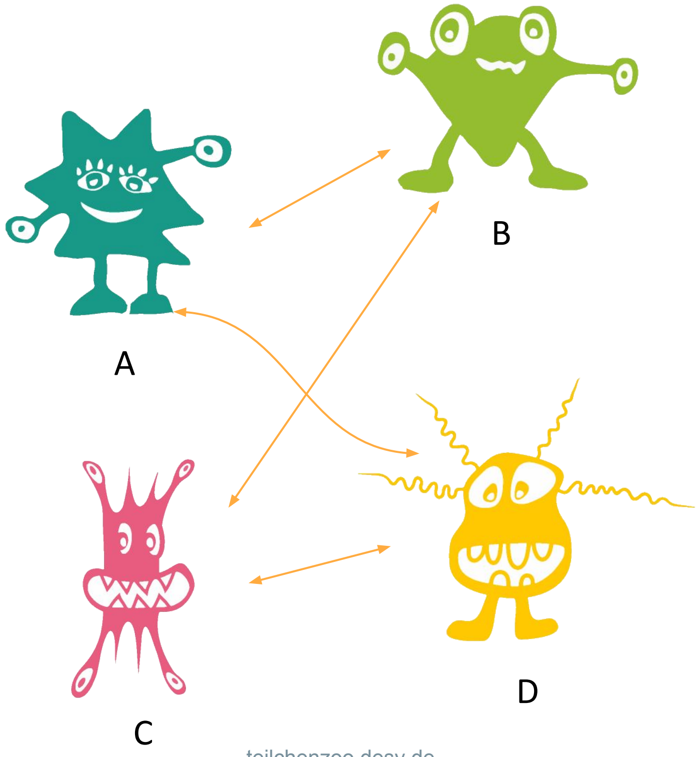
- Money is exchanged. Or information. The data flow is logged!
- After a certain size a block is formed

Ledger - April ‘18

A *pays* B 20 CHF
B *pays* C 10 CHF
C *pays* A 30 CHF
D *pays* C 10 CHF

Science contributions

A *contributed...*
B *proposed...*
C *proposed...*
D *researched...*

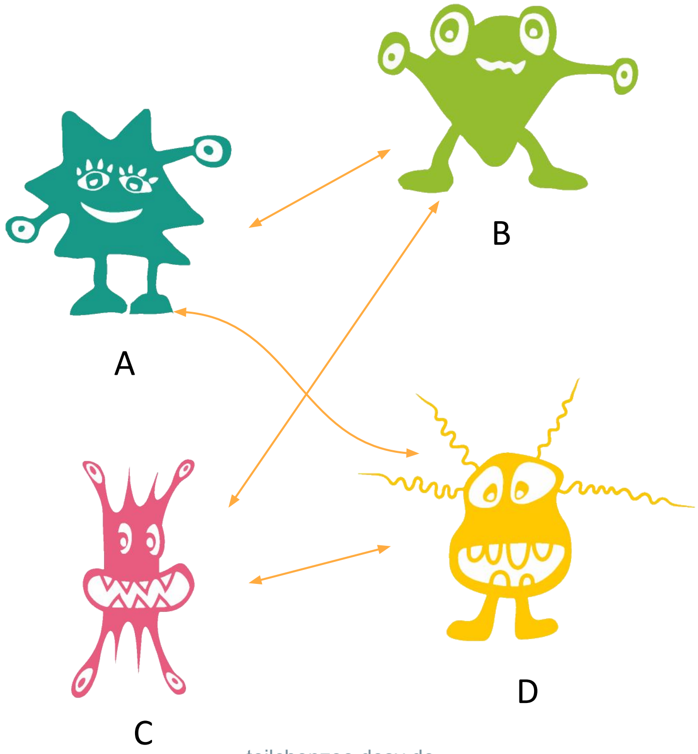


teilchenzoo.desy.de

Let‘s build a blockchain

- Protocol:
  - Everybody can add lines
  - After time t, settle up (blocks)
- How to prevent cheating?

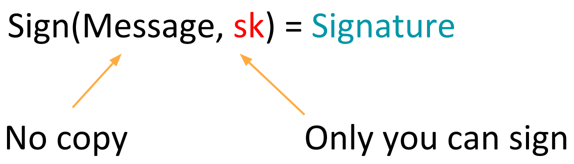
→ ***Signatures***



teilchenzoo.desy.de

Signatures

- Digital signatures change with every message!
- Private/secret key and public key pair



Sign(Message, sk) = Signature

No copy

Only you can sign

- Easy to compute, impossible to break

Verify(Message, pk, Signature) = **T**rue / **F**alse

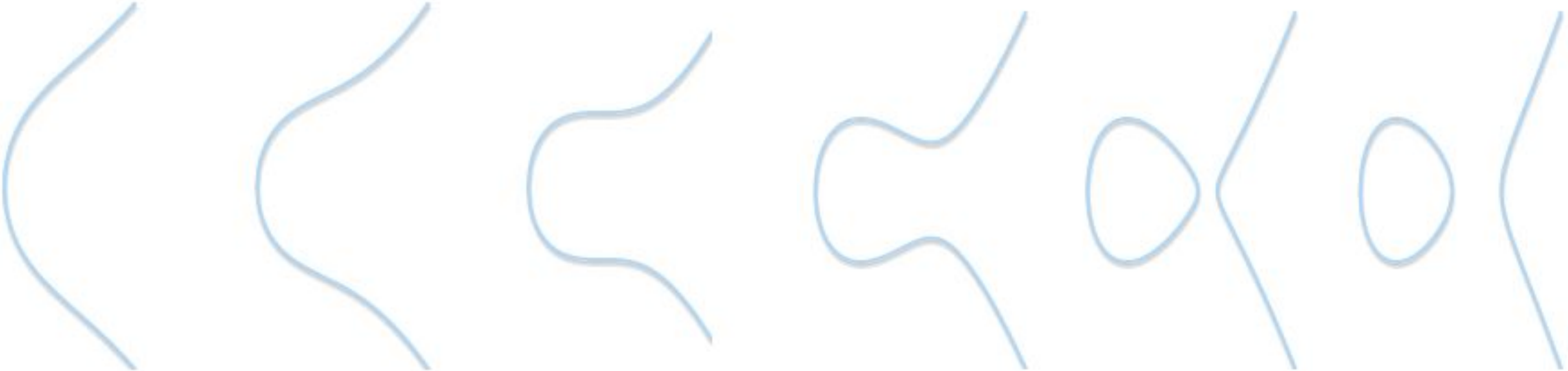
I hereby enact the shut-down of CERN to protect humanity of black holes.

And I order to inform them about the power of blockchain.

created with hepwori.github.io/execorder

Making Trap-doors: Elliptic Curves

For our purpose:



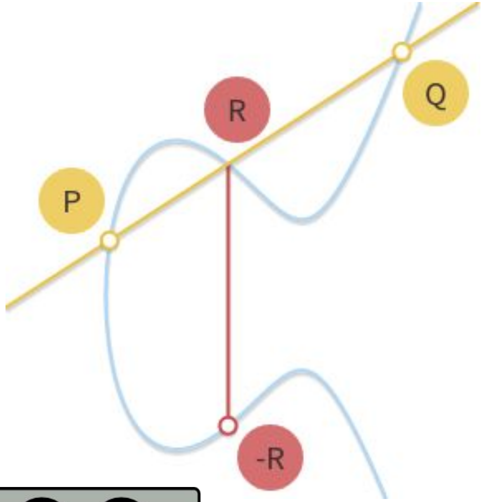
andrea.corbellini.name

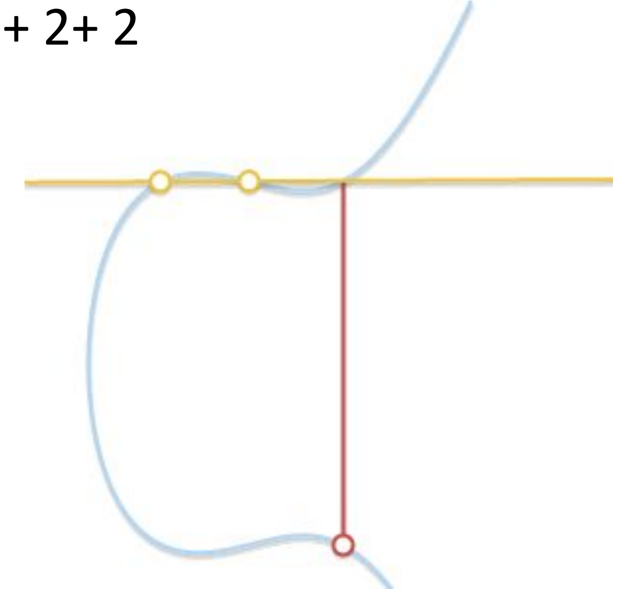
$$\{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} \cup \{\infty\}$$

Making Trap-doors: Elliptic Curves

Define an *addition*

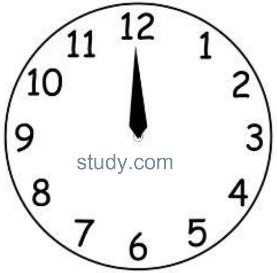
Get a *multiplication*: 5 * 2= 2+ 2+ 2+ 2+ 2





andrea.corbellini.name

Making Trap-doors: Modular Arithmetic



Modulus 12

(10 + 4) mod 12 = 2

For our needs: mod p, p is prime

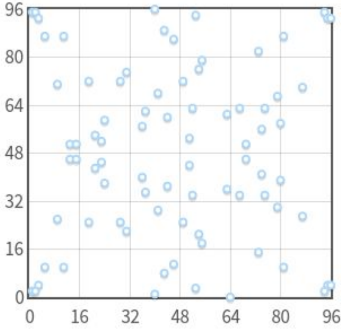
$$\{(x,y) \in F_p \,|y^2 = x^3 + ax + b \bmod p,\ 4a^3 + 27b^2 \neq\ 0 \bmod p\} \cup \{\infty\}$$

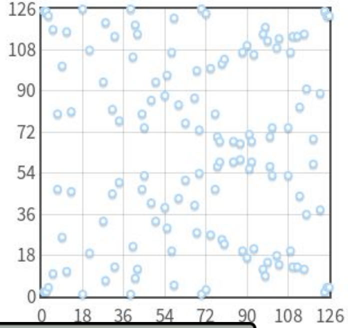
Some numbers don‘t exist anymore!

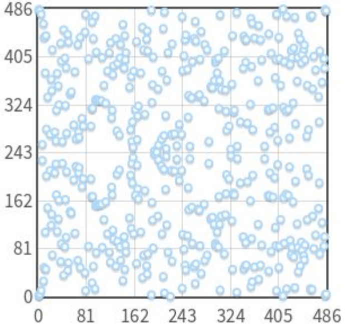
Elliptic Curve Geometry in a Finite Field

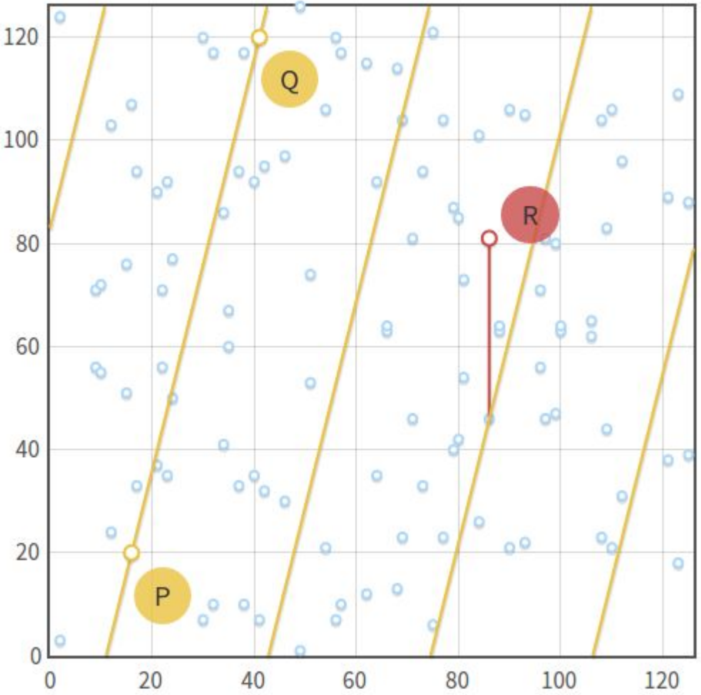
12
1
2
3
4
5
6
7
8
9
10
11

Modulus 12









andrea.corbellini.name

Cryptography

Generator point G

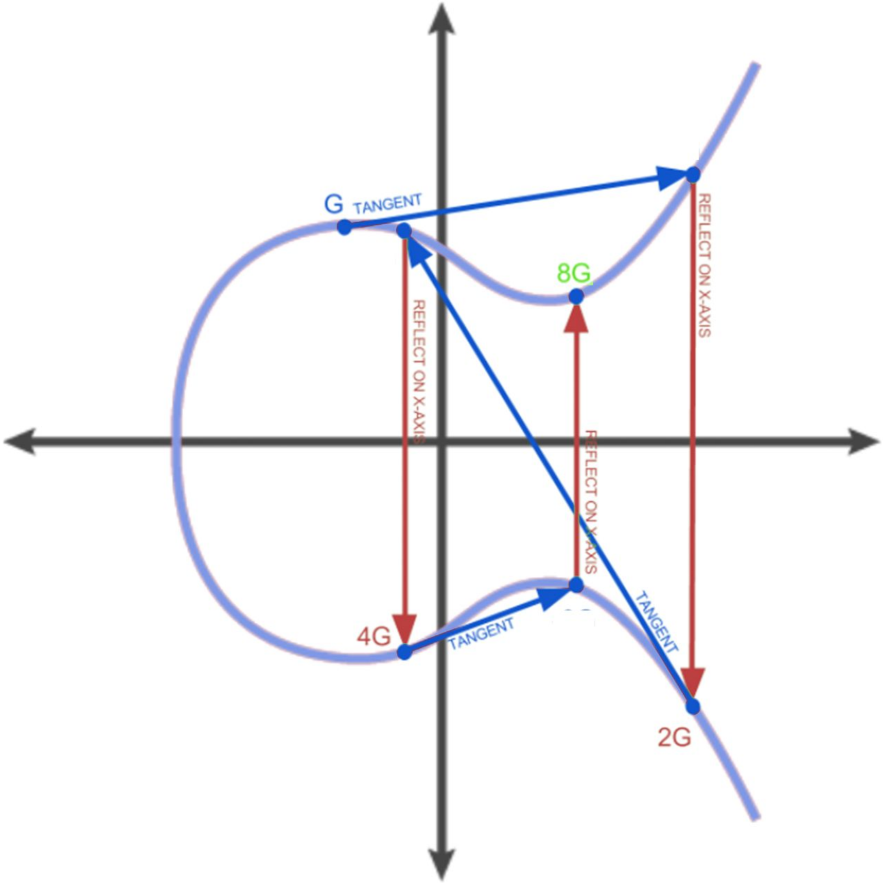
Pick random sk

1 out of 1.15E77 - 256 bit

pk = sk * G

Calculation of:

- pk is $O(\log n)$ complex
- sk is $O(2^{n/2})$ complex



modified from crypto.stackexchange.com

Back to the Blockchain

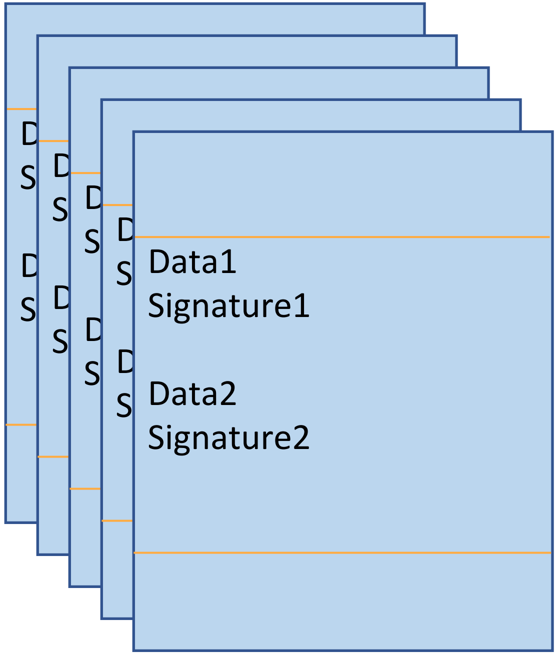
pk is the address

0x74abbdc4e5d62210194f503a871a6bf68744b1a1

Verify(Message, pk, Signature) = **T**rue / **F**alse

Protocol:

- Everybody can add lines
- Only valid with signature
- Make blocks



Where is the database?

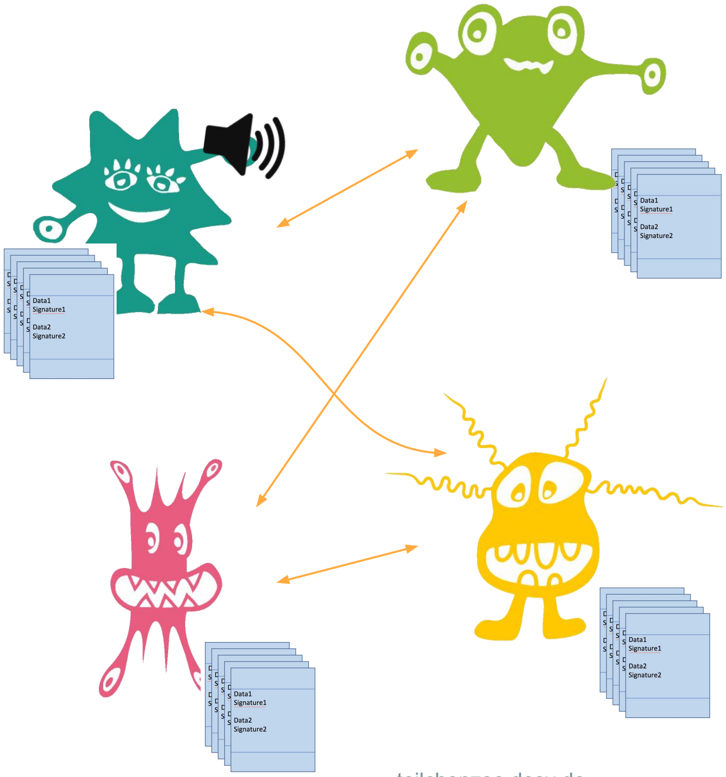
Back to the Blockchain

Everybody has/can have a copy
New entries get broadcasted

How to keep the database consistent?

Proof of Work:

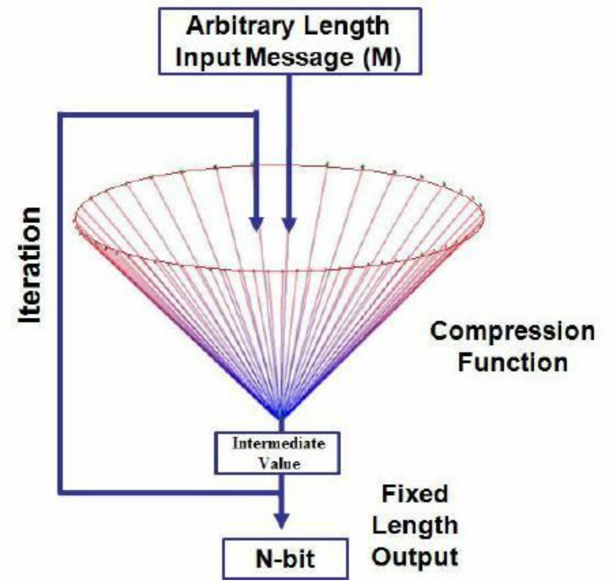
Make fraud computationally infeasible



teilchenzoo.desy.de

Cryptographic Hash function

- SHA (Secure Hash Algorithm) was developed by the NSA…



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

de.wikipedia.org/wiki/Fingerabdruck

Hello World

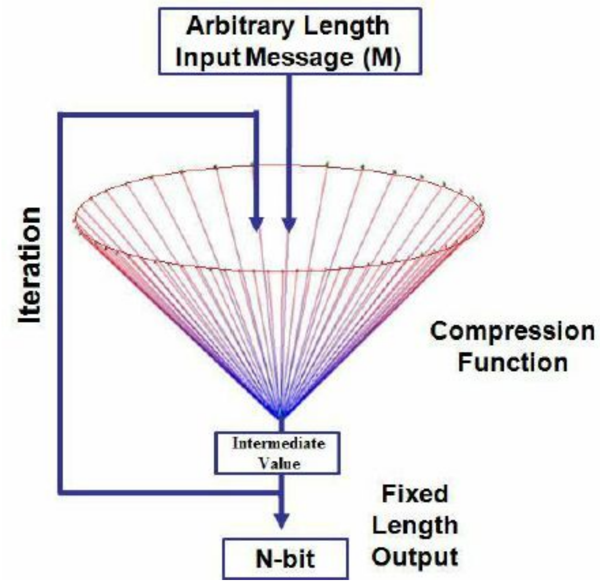
↓

a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Cryptographic Hash function

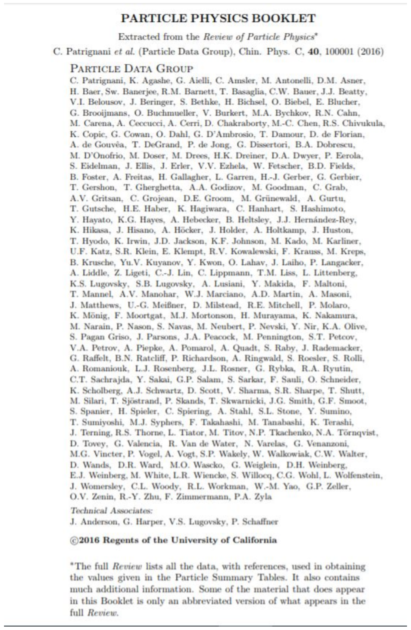
- SHA (Secure Hash Algorithm)

  was developed by the NSA…



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

de.wikipedia.org/wiki/Fingerabdruck



PARTICLE PHYSICS BOOKLET

Extracted from the *Review of Particle Physics**

C. Patrignani *et al.* (Particle Data Group), Chin. Phys. C, **40**, 100001 (2016)

PARTICLE DATA GROUP

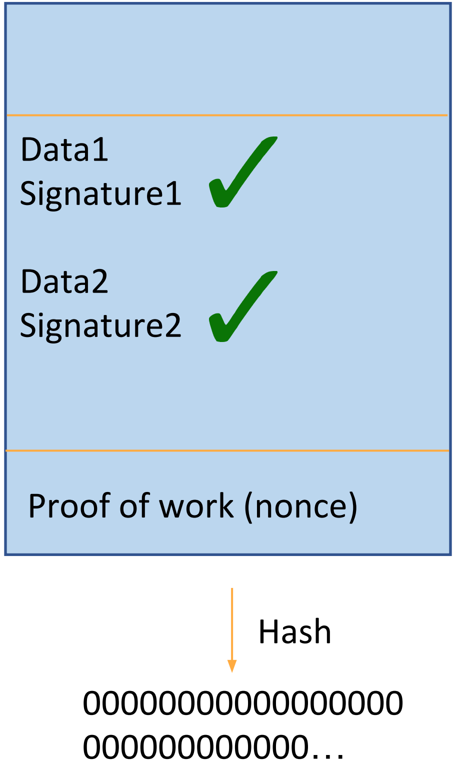
C. Patrignani, K. Agashe, G. Aielli, C. Amsler, M. Antonelli, D.M. Asner, H. Baer, Sw. Banerjee, R.M. Barnett, T. Basaglia, C.W. Bauer, J.J. Beatty, V.I. Belousov, J. Beringer, S. Bethke, H. Bichsel, O. Biebel, E. Blucher, G. Brooijmans, O. Buchmueller, V. Burkert, M.A. Bychkov, R.N. Cahn, M. Carena, A. Ceccucci, A. Cerri, D. Chakraborty, M.-C. Chen, R.S. Chivukula, K. Copic, G. Cowan, O. Dahl, G. D'Ambrosio, T. Damour, D. de Florian, A. de Gouvêa, T. DeGrand, P. de Jong, G. Dissertori, B.A. Dobrescu, M. D'Onofrio, M. Doser, M. Drees, H.K. Dreiner, D.A. Dwyer, P. Eerola, S. Eidelman, J. Ellis, J. Erler, V.V. Ezhela, W. Fetscher, B.D. Fields, B. Foster, A. Freitas, H. Gallagher, L. Garren, H.-J. Gerber, G. Gerbier, T. Gershon, T. Gherghetta, A.A. Godizov, M. Goodman, C. Grab, A.V. Gritsan, C. Grojean, D.E. Groom, M. Grünewald, A. Gurtu, T. Gutsche, H.E. Haber, K. Hagiwara, C. Hanhart, S. Hashimoto, Y. Hayato, K.G. Hayes, A. Hebecker, B. Heltsley, J.J. Hernández-Rey, K. Hikasa, J. Hisano, A. Höcker, J. Holder, A. Holtkamp, J. Huston, T. Hyodo, K. Irwin, J.D. Jackson, K.F. Johnson, M. Kado, M. Karliner, U.F. Katz, S.R. Klein, E. Klempt, R.V. Kowalewski, F. Krauss, M. Kreps, B. Krusche, Yu.V. Kuyanov, Y. Kwon, O. Lahav, J. Laiho, P. Langacker, A. Liddle, Z. Ligeti, C.-J. Lin, C. Lippmann, T.M. Liss, L. Littenberg, K.S. Lugovsky, S.B. Lugovsky, A. Lusiani, Y. Makida, F. Maltoni, T. Mannel, A.V. Manohar, W.J. Marciano, A.D. Martin, A. Masoni, J. Matthews, U.-G. Meißner, D. Milstead, R.E. Mitchell, P. Molaro, K. Mönig, F. Moortgat, M.J. Mortonson, H. Murayama, K. Nakamura, M. Narain, P. Nason, S. Navas, M. Neubert, P. Nevski, Y. Nir, K.A. Olive, S. Pagan Griso, J. Parsons, J.A. Peacock, M. Pennington, S.T. Petcov, V.A. Petrov, A. Piepke, A. Pomarol, A. Quadt, S. Raby, J. Rademacker, G. Raffelt, B.N. Ratcliff, P. Richardson, A. Ringwald, S. Roesler, S. Rolli, A. Romaniouk, L.J. Rosenberg, J.L. Rosner, G. Rybka, R.A. Ryutin, C.T. Sachrajda, Y. Sakai, G.P. Salam, S. Sarkar, F. Sauli, O. Schneider, K. Scholberg, A.J. Schwartz, D. Scott, V. Sharma, S.R. Sharpe, T. Shutt, M. Silari, T. Sjöstrand, P. Skands, T. Skwarnicki, J.G. Smith, G.F. Smoot, S. Spanier, H. Spieler, C. Spiering, A. Stahl, S.L. Stone, Y. Sumino, T. Sumiyoshi, M.J. Syphers, F. Takahashi, M. Tanabashi, K. Terashi, J. Terning, R.S. Thorne, L. Tiator, M. Titov, N.P. Tkachenko, N.A. Törnqvist, D. Tovey, G. Valencia, R. Van de Water, N. Varelas, G. Venanzoni, M.G. Vincter, P. Vogel, A. Vogt, S.P. Wakely, W. Walkowiak, C.W. Walter, D. Wands, D.R. Ward, M.O. Wascko, G. Weiglein, D.H. Weinberg, E.J. Weinberg, M. White, L.R. Wiencke, S. Willocq, C.G. Wohl, L. Wolfenstein, J. Womersley, C.L. Woody, R.L. Workman, W.-M. Yao, G.P. Zeller, O.V. Zenin, R.-Y. Zhu, F. Zimmermann, P.A. Zyla

Technical Associates:
J. Anderson, G. Harper, V.S. Lugovsky, P. Schaffner

*The full *Review* lists all the data, with references, used in obtaining the values given in the Particle Summary Tables. It also contains much additional information. Some of the material that does appear in this Booklet is only an abbreviated version of what appears in the full *Review*.

60fae91769c446c650a1bf85d65ea5950c0911578747af17698847a36ccb761f

Proof of Work: Nonce-sense



Data1
Signature1 ✓

Data2
Signature2 ✓

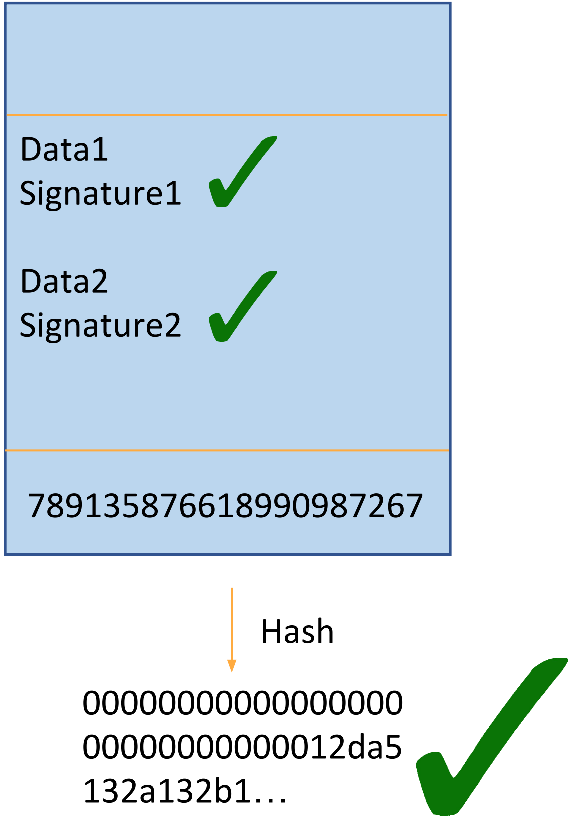
Proof of work (nonce)

Hash

00000000000000000
000000000000…

- SHA256 hash: first n bits are 0
- Proof of work: special number (nonce)
- 2^{-30} for the right guess

A Block …



Data1
Signature1 ✓

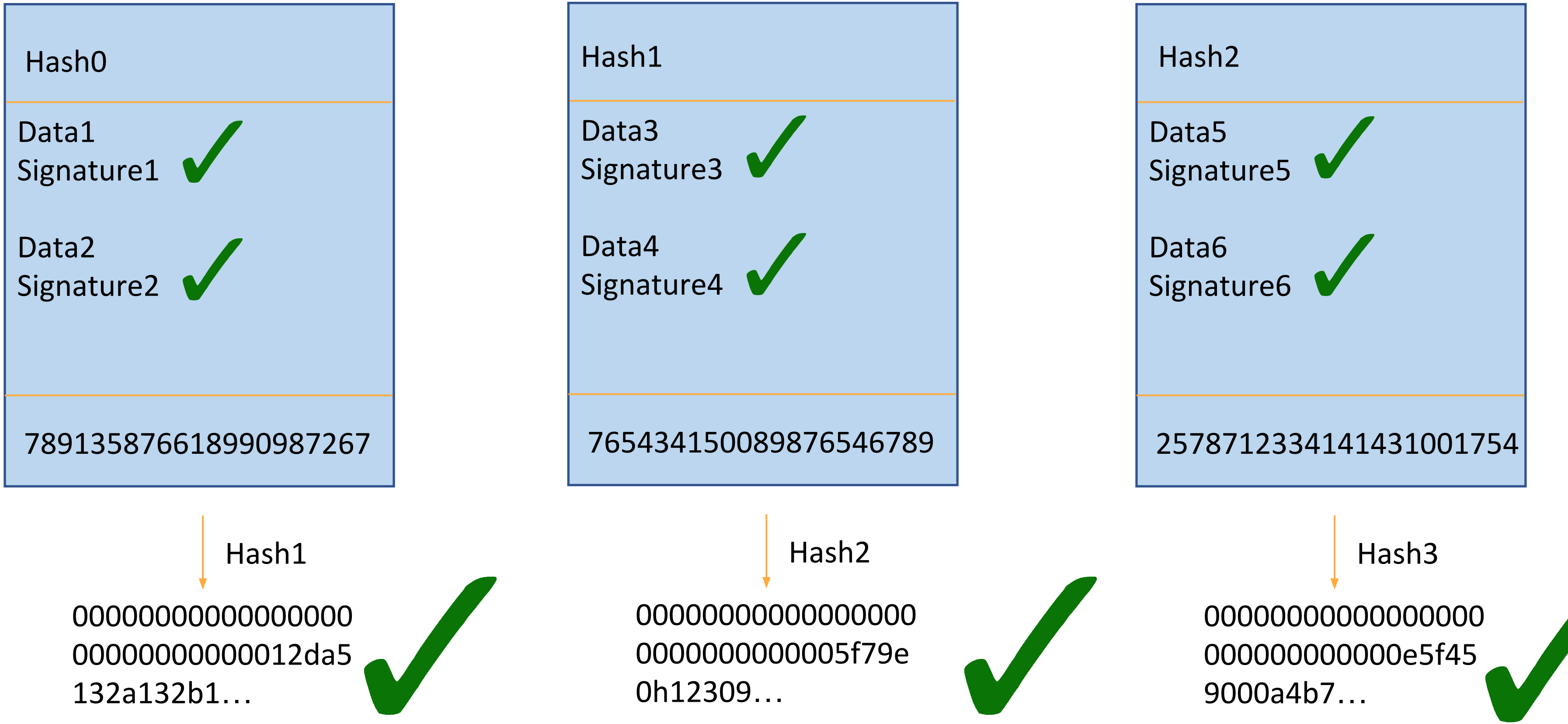
Data2
Signature2 ✓

7891358766189909872677

Hash

000000000000000000
000000000000012da5
132a132b1… ✓

A Blockchain



Hash0

Data1
Signature1 ✓

Data2
Signature2 ✓

789135876618990987267

Hash1

00000000000000000
00000000000012da5
132a132b1… ✓

Hash1

Data3
Signature3 ✓

Data4
Signature4 ✓

765434150089876546789

Hash2

00000000000000000
000000000005f79e
0h12309… ✓

Hash2

Data5
Signature5 ✓

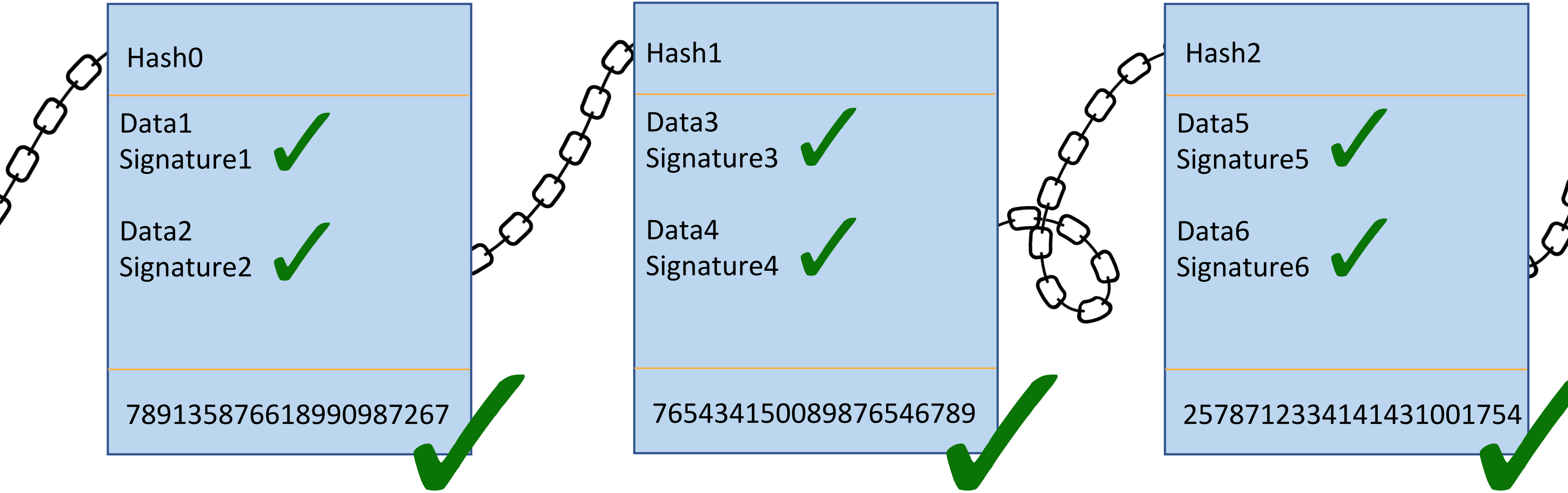
Data6
Signature6 ✓

2578712334141431001754

Hash3

00000000000000000
000000000000e5f45
9000a4b7… ✓

A Blockchain



Hash0

Data1
Signature1 ✓

Data2
Signature2 ✓

789135876618990987267 ✓

Hash1

Data3
Signature3 ✓

Data4
Signature4 ✓

765434150089876546789 ✓

Hash2

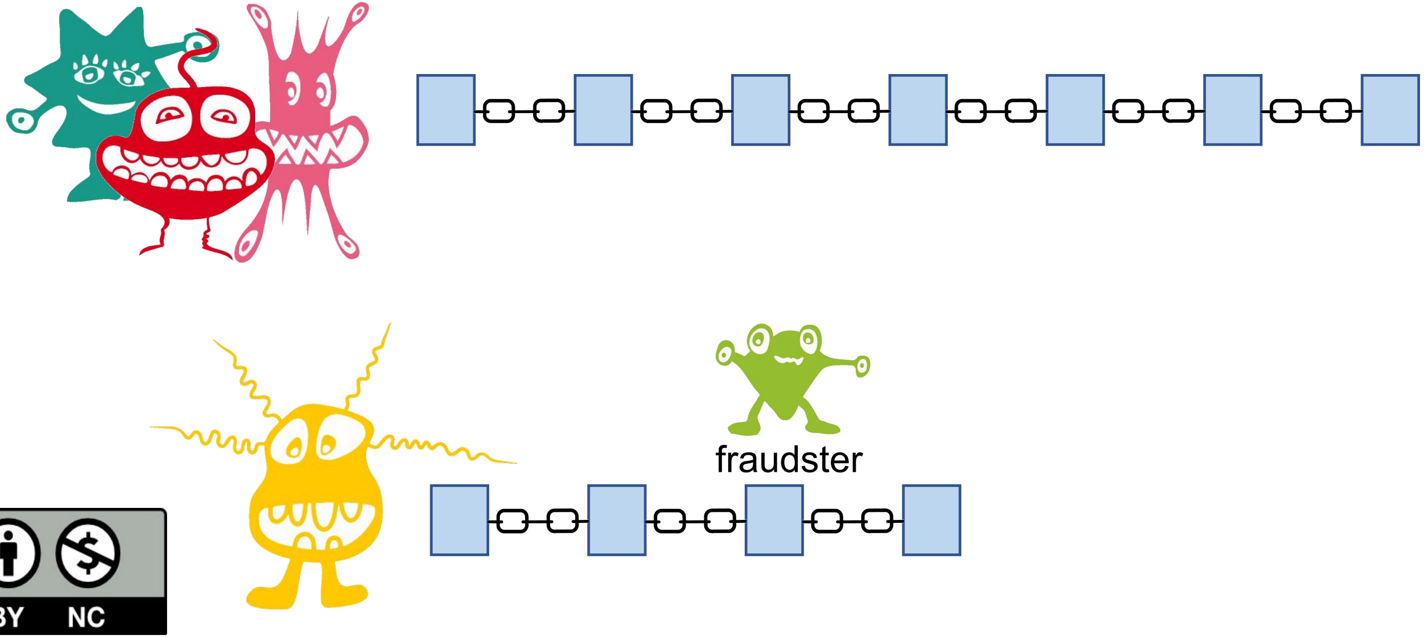
Data5
Signature5 ✓

Data6
Signature6 ✓

2578712334141431001754 ✓

Proof of Work: Decentralized Consensus

Trust the longest chain, it is backed by the majority



Miners

Miners are the housekeepers, doing the proof of work

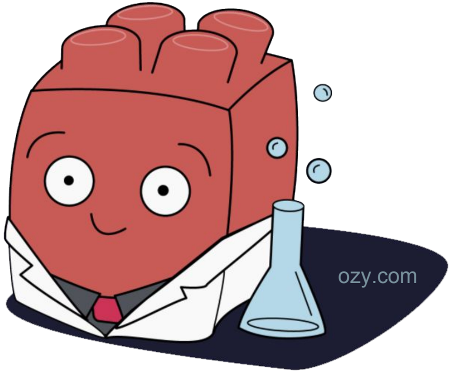
- ➢ Decentralised consensus

Other *proofs:* stake, activity, capacity...

Incentiv: *Blockreward* and *fees*

“Consens-uela”
“Miner-craft”

Summing it up


ozy.com

- Blockchain is a database
- Everybody can write
- Validity by cryptography
  - Data have a signature
  - Blocks have proof of work
- Database is decentralized, miners are it’s “good spirit”
  - Incentivised via block rewards

Agenda

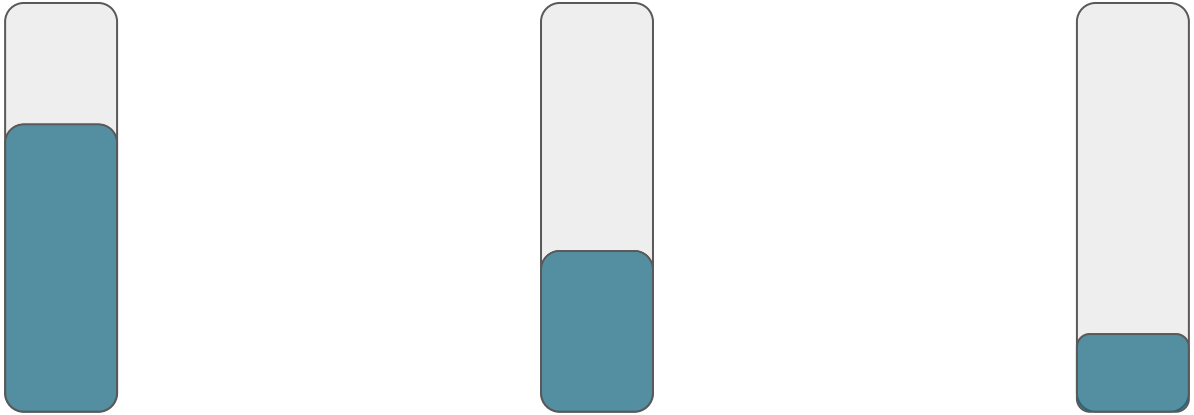
- Blockchain for “dummies”
- **Smart Contracts**
- ‘Blockchain for Science’:
  Data integrity, protection & collaboration

Introducing a database that is:

“A fundamental possibility to perform (financial) transactions.”

- Censorship resistant,
- Tamper-resistant,
- Auditable

Access to finance



75% of population (planet earth)

40% in developing nations

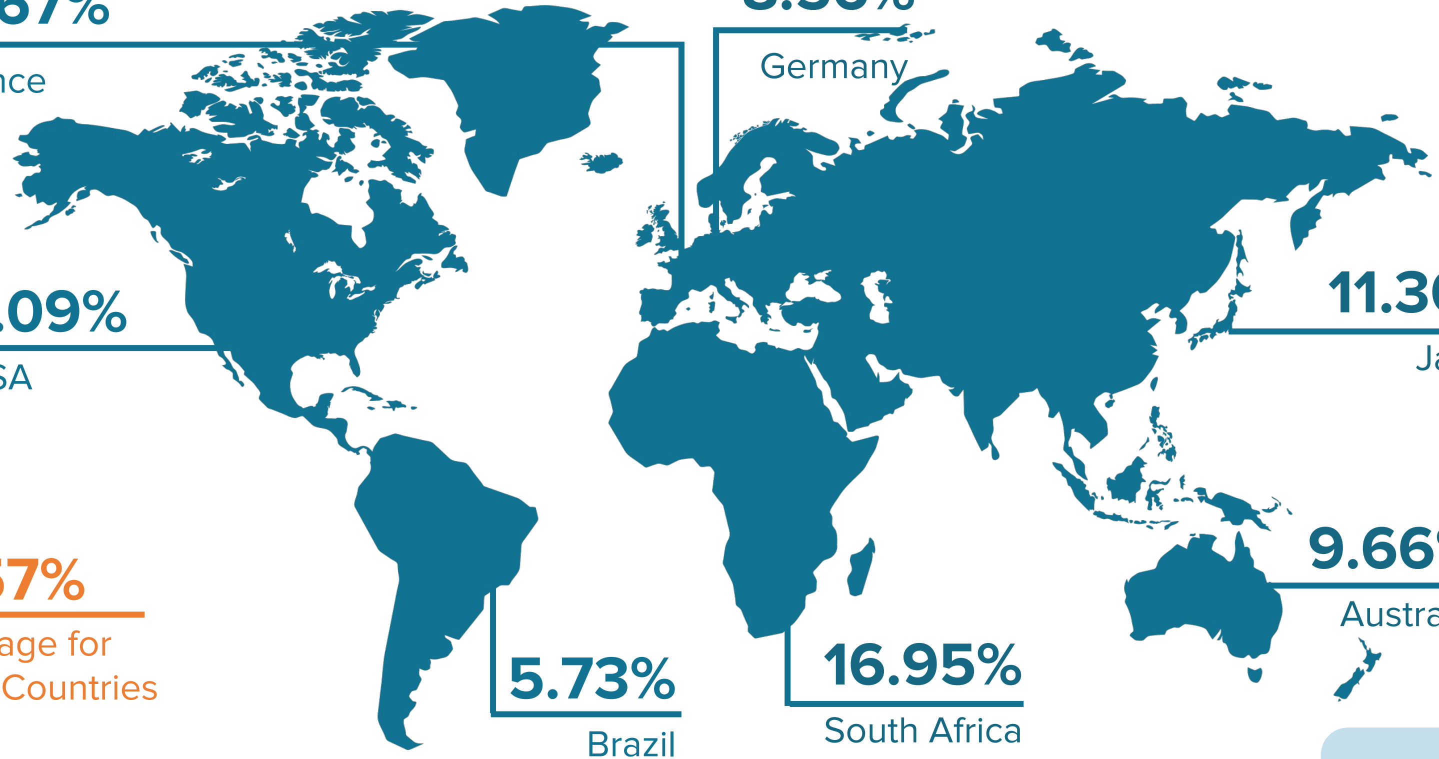
20% of adults with daily income under $2

But 1 billion people without bank account have a mobile phone!

Cost of Remitting from G20 countries

Source

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP



6.67%
France

8.56%
Germany

6.09%
USA

11.30%
Japan

9.66%
Australia

5.73%
Brazil

16.95%
South Africa

7.57%
Average for
G20 Countries

ValidityLabs

The weird issue of Dole

Claimed shares: 49,164,415

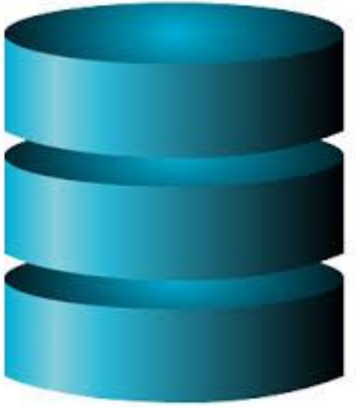
Δ over 30% !!!

Outstanding shares: 36,793,758

Separate systems were unable to correctly reconcile.
(owner of the share / actual owner of the share / really real owner of the share)

Blockchain will drive intermediaries out of business!

Blockchain and Smart Contracts



Bitcoin blockchain
= database

Crypto Valley

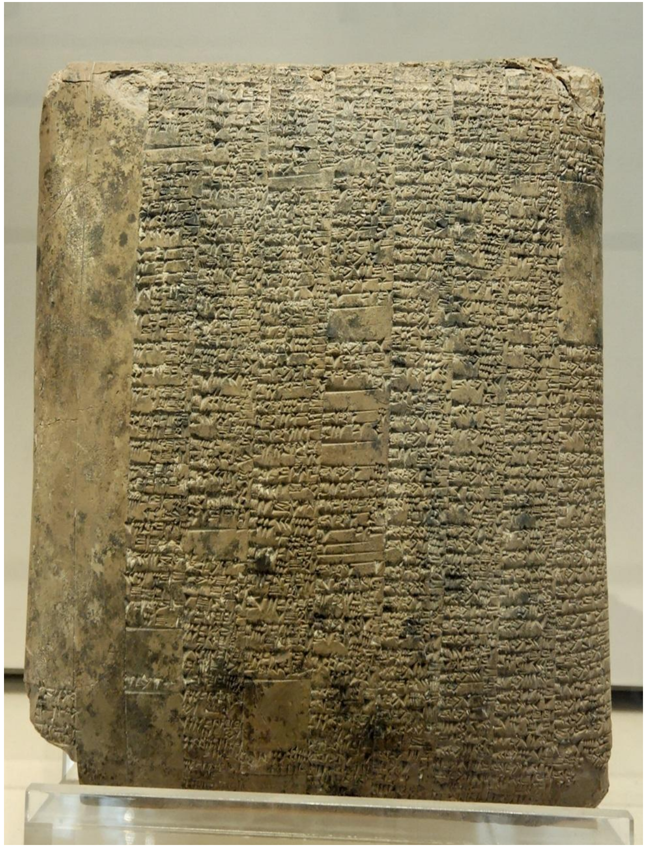
Ethereum blockchain
with smart contracts

= World Computer

SMART CONTRACT

=

Program on a blockchain that can control (financial) assets.



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

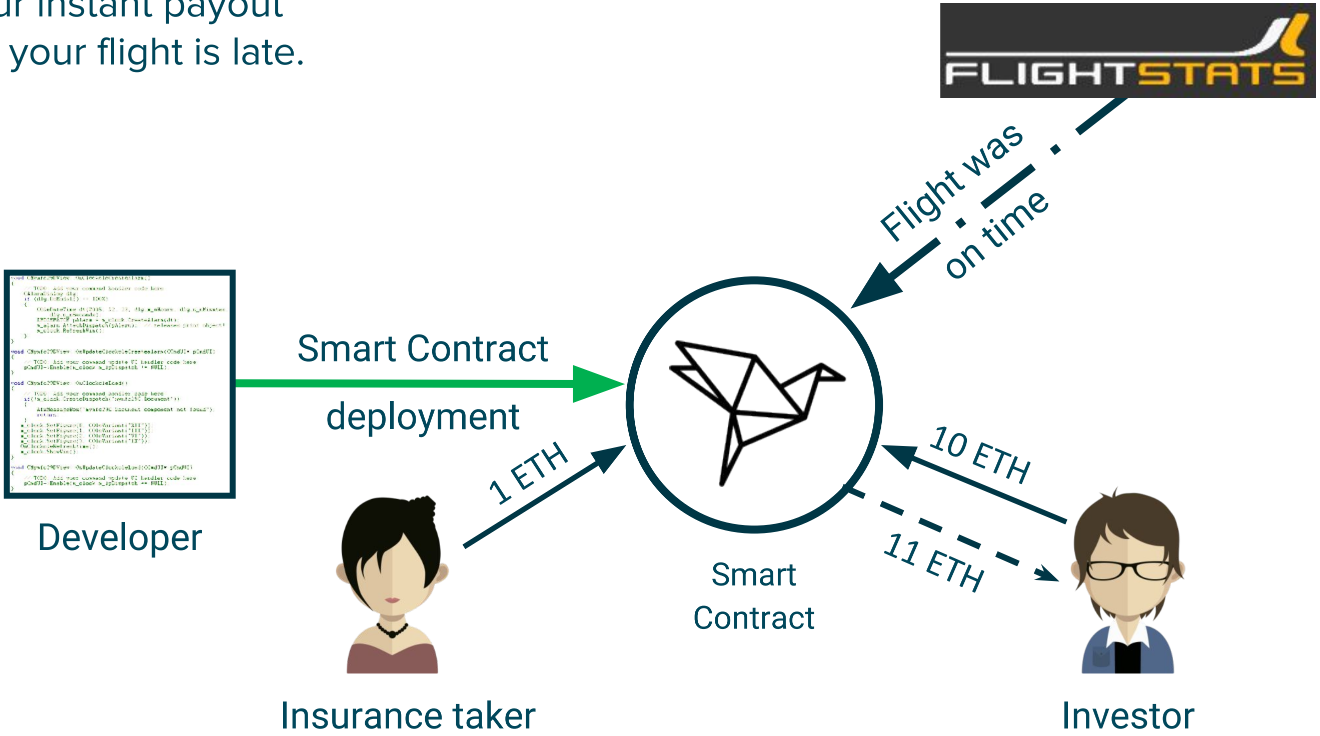
Organizations

Programs

EXAMPLE: Decentralized insurance

Get your instant payout
in case your flight is late.

Data Source (Oracle)

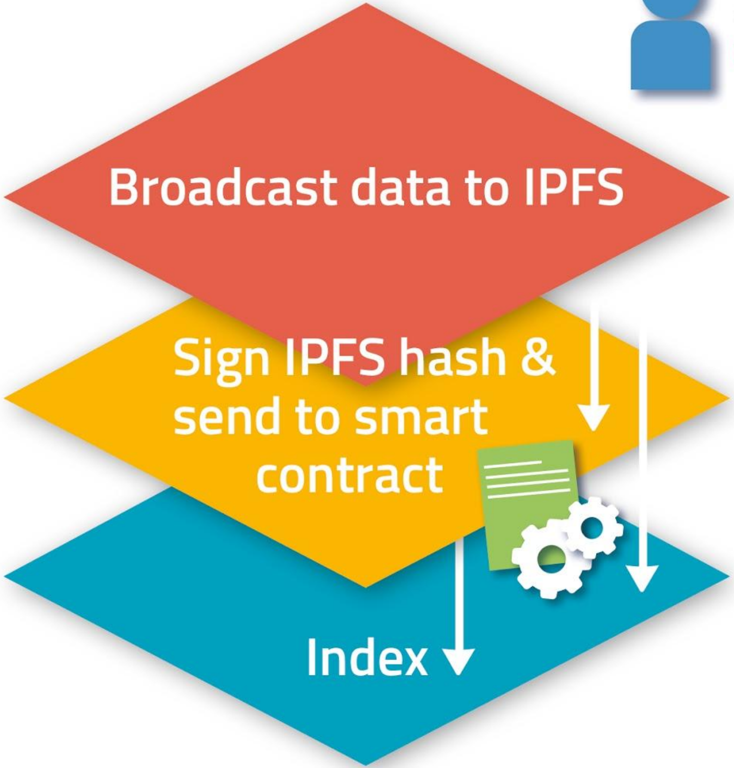


```
void CMyatc29DView::OnClockctlCreatealarm()
{
    // TODO: Add your command handler code here
    CAlarmDialog dlg;
    if (dlg.DoModal() == IDOK)
    {
        COleDateTime dt(2005, 12, 23, dlg.m_nHours, dlg.m_nMinutes,
            dlg.m_nSeconds);
        LPDISPATCH pAlarm = m_clock.CreateAlarm(dt);
        m_alarm.AttachDispatch(pAlarm);  // releases prior object!
        m_clock.RefreshWin();
    }
}

void CMyatc29DView::OnUpdateClockctlCreatealarm(CCmdUI* pCmdUI)
{
    // TODO: Add your command update UI handler code here
    pCmdUI->Enable(m_clock.m_lpDispatch != NULL);
}

void CMyatc29DView::OnClockctlLoad()
{
    // TODO: Add your command handler code here
    if(!m_clock.CreateDispatch("myatc29C.Document"))
    {
        AfxMessageBox("myatc29C.Document component not found");
        return;
    }
    m_clock.SetFigure(0, COleVariant("XII"));
    m_clock.SetFigure(1, COleVariant("III"));
    m_clock.SetFigure(2, COleVariant("VI"));
    m_clock.SetFigure(3, COleVariant("IX"));
    OnClockctlRefreshtime();
    m_clock.ShowWin();
}

void CMyatc29DView::OnUpdateClockctlLoad(CCmdUI* pCmdUI)
{
    // TODO: Add your command update UI handler code here
    pCmdUI->Enable(m_clock.m_lpDispatch == NULL);
}
```

Agenda

- Blockchain for “dummies”
- Smart Contracts
- **‘Blockchain for Science’:**
  Data integrity, protection & collaboration

Blockchain solution architecture.



Operator/ machine:

- creates data
- analyses data
- interprets data

Notarization:

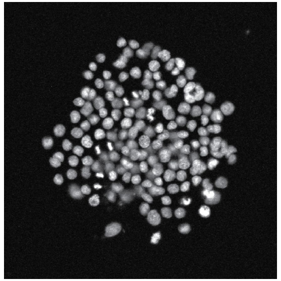
- attributable
- timestamped
- can trigger processes

Storage:

- open
- immutable
- censorship-resistant

Example

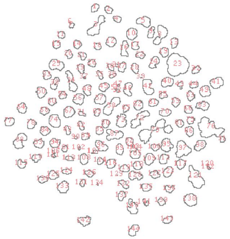
1. Acquisition



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:
0x74abbdc4e5d62210194f503a8
71a6bf68744b1a1

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

Analyst:
0x74abbdc4e5d62210194f503a8
71a6bf68744b1a1

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

Publisher:
0x74abbdc4e5d62210194f503a8
71a6bf68744b1a1

Martin Etzrodt and Sebastian C. Bürgel

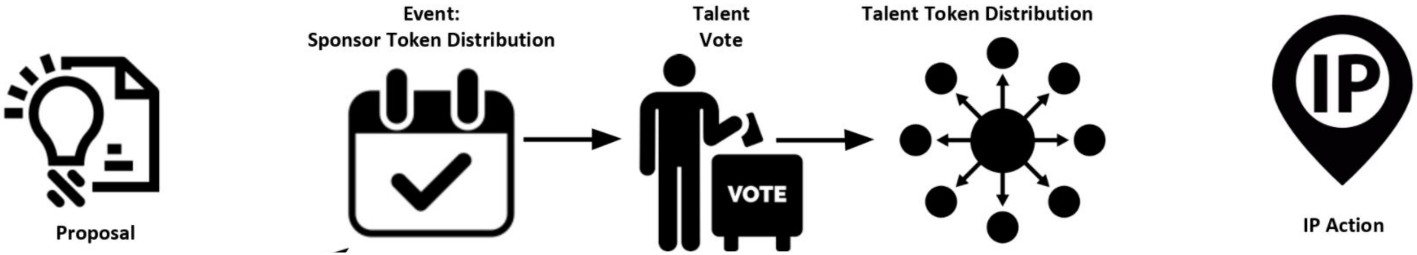
What did we gain?

- Permanent publication of results
- Attribution of researchers’ contributions
- Interoperability to enable incentives (grants, publications, IP)

Blockchain 1.0 → #BeYourOwnBank (Bitcoin)

Blockchain 2.0 → #BeYourOwnJournal (now)

Example: Mindfire



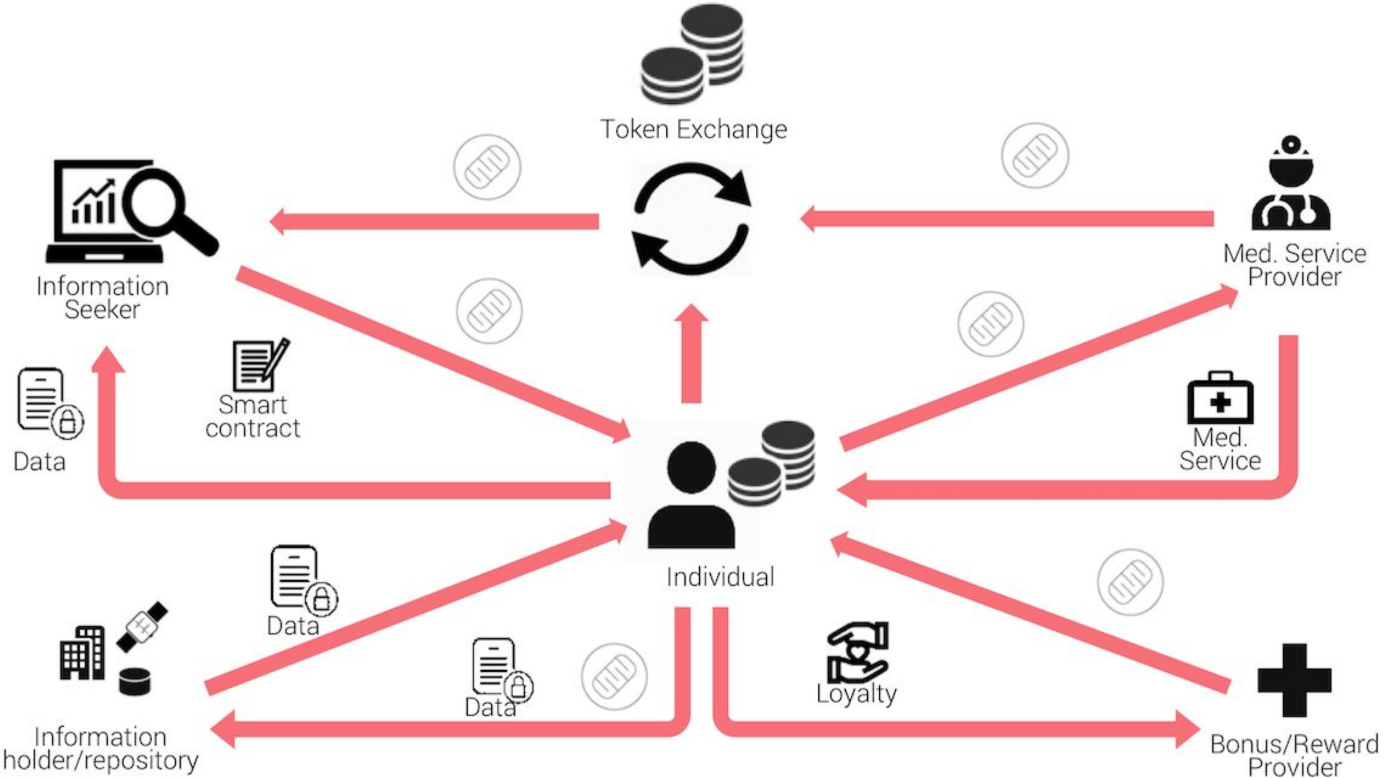
Token backed governance of:

Funding, IP and participant R&D efforts towards true AI

mindfire.global

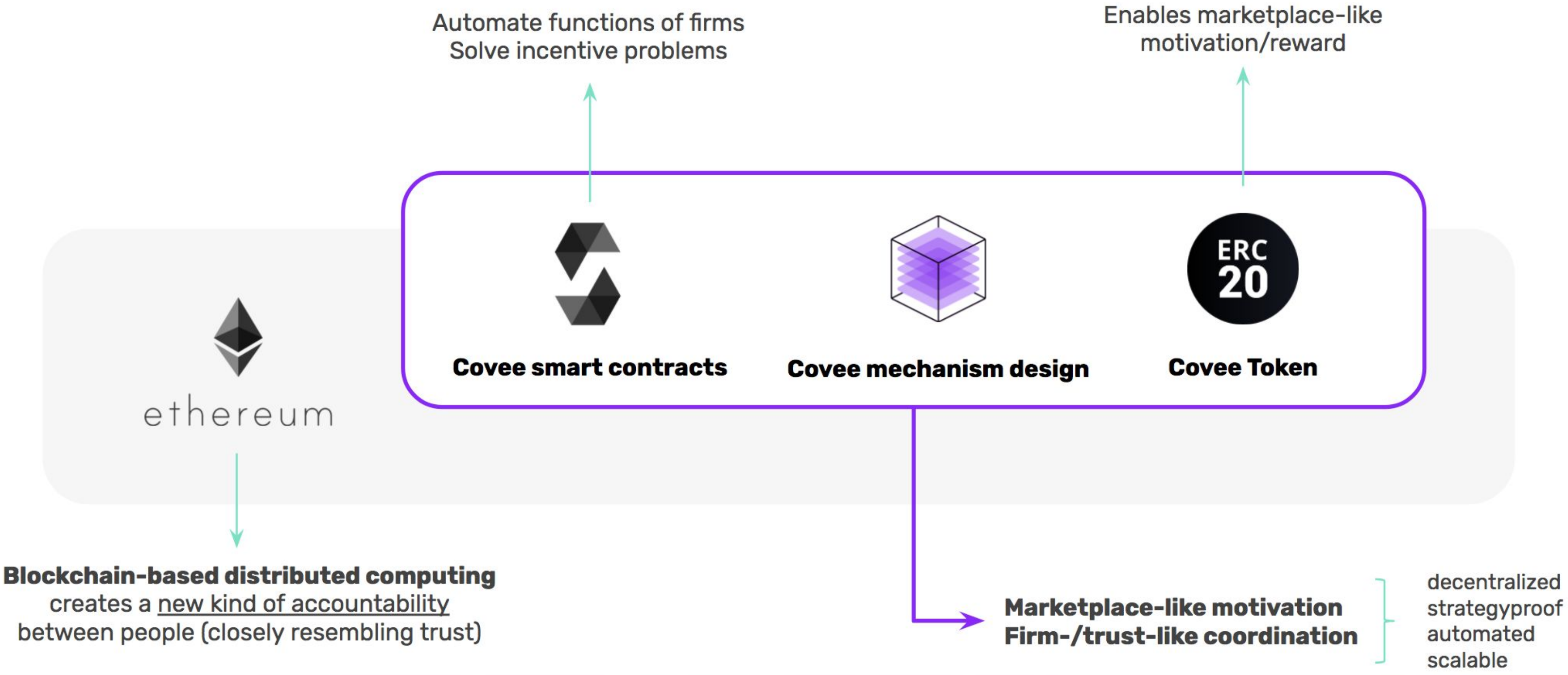
Example: HIT.foundation

token ecosystem for medical data



Example: Covee

trust network for collaborative data science



Automate functions of firms
Solve incentive problems

Enables marketplace-like
motivation/reward

Covee smart contracts

Covee mechanism design

Covee Token

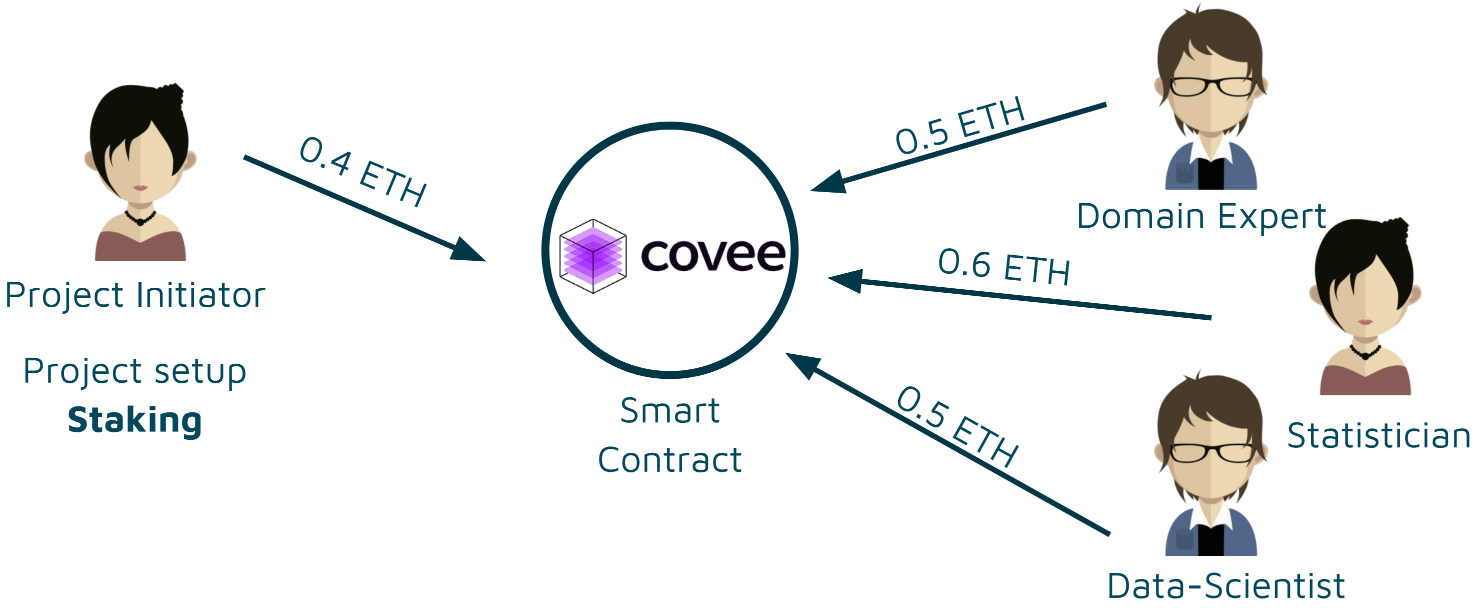
Blockchain-based distributed computing
creates a new kind of accountability
between people (closely resembling trust)

Marketplace-like motivation
Firm-/trust-like coordination

decentralized
strategyproof
automated
scalable

Architecture

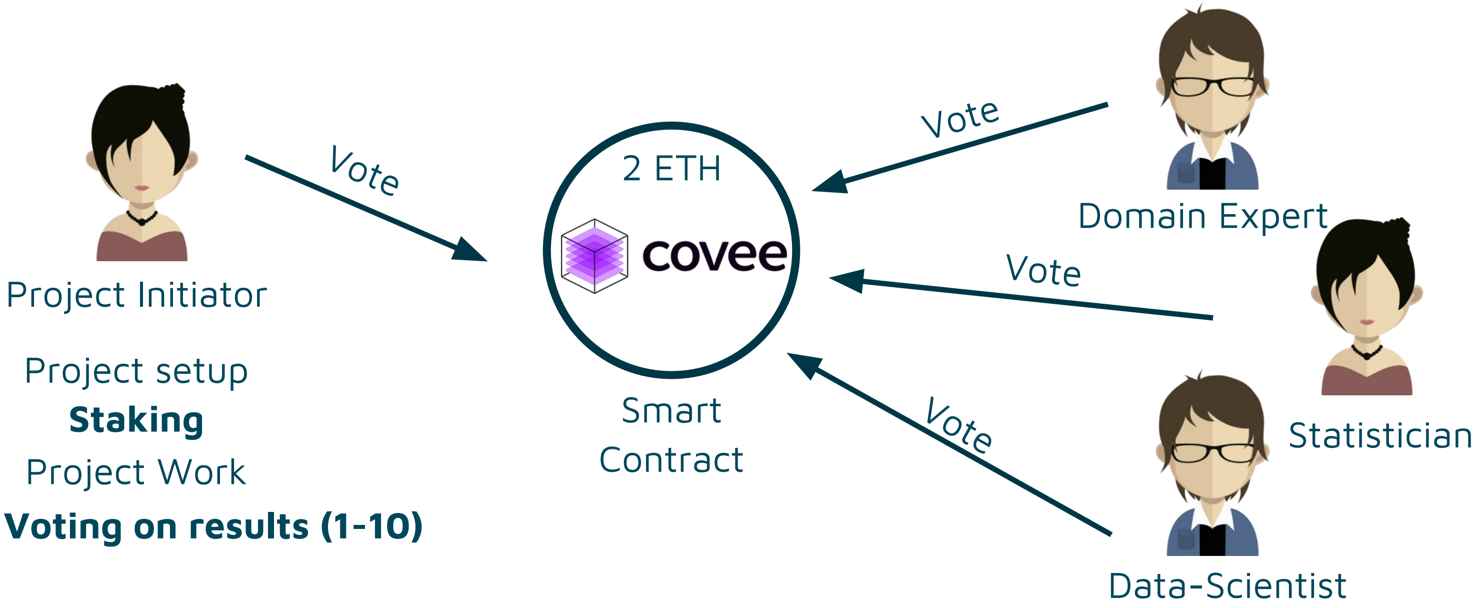
Decentralized team-work powered by smart contracts
You want to work with others on a project and be sure that nobody is free-riding/lazy/misbehaving



Architecture

Decentralized team-work powered by smart contracts

You want to work with others on a project and be sure that nobody is free-riding/lazy/misbehaving



Project setup

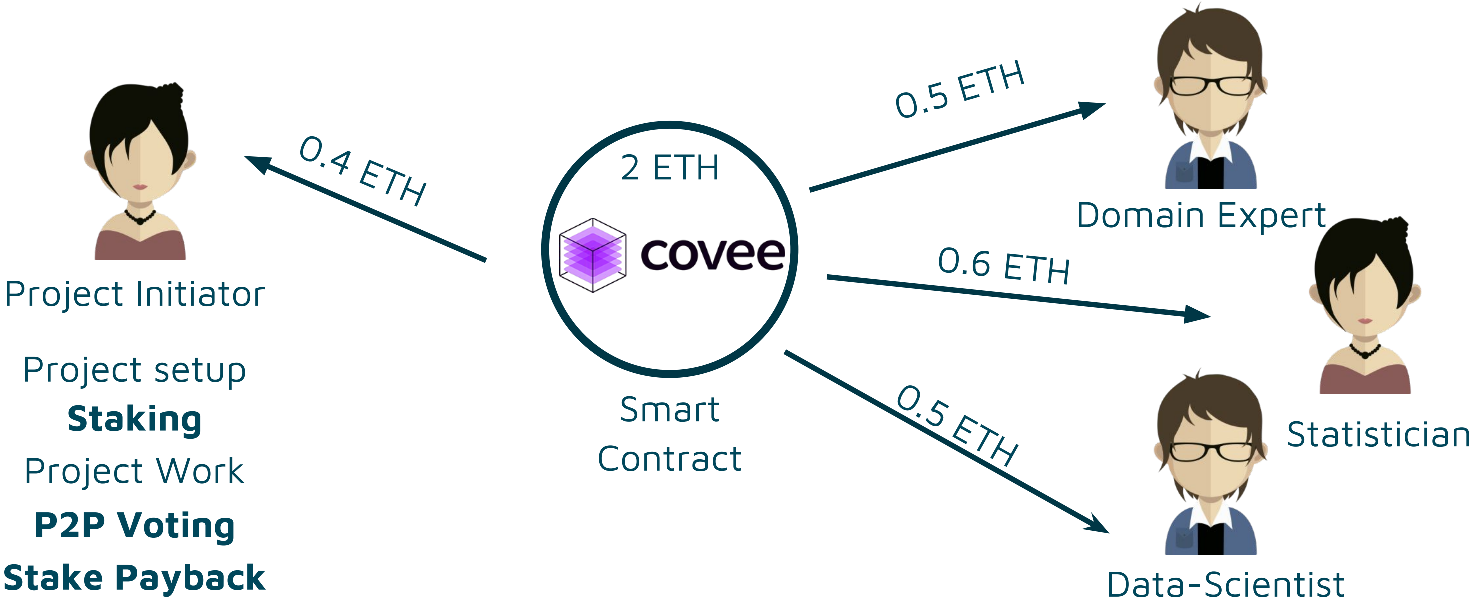
Staking

Project Work

Voting on results (1-10)

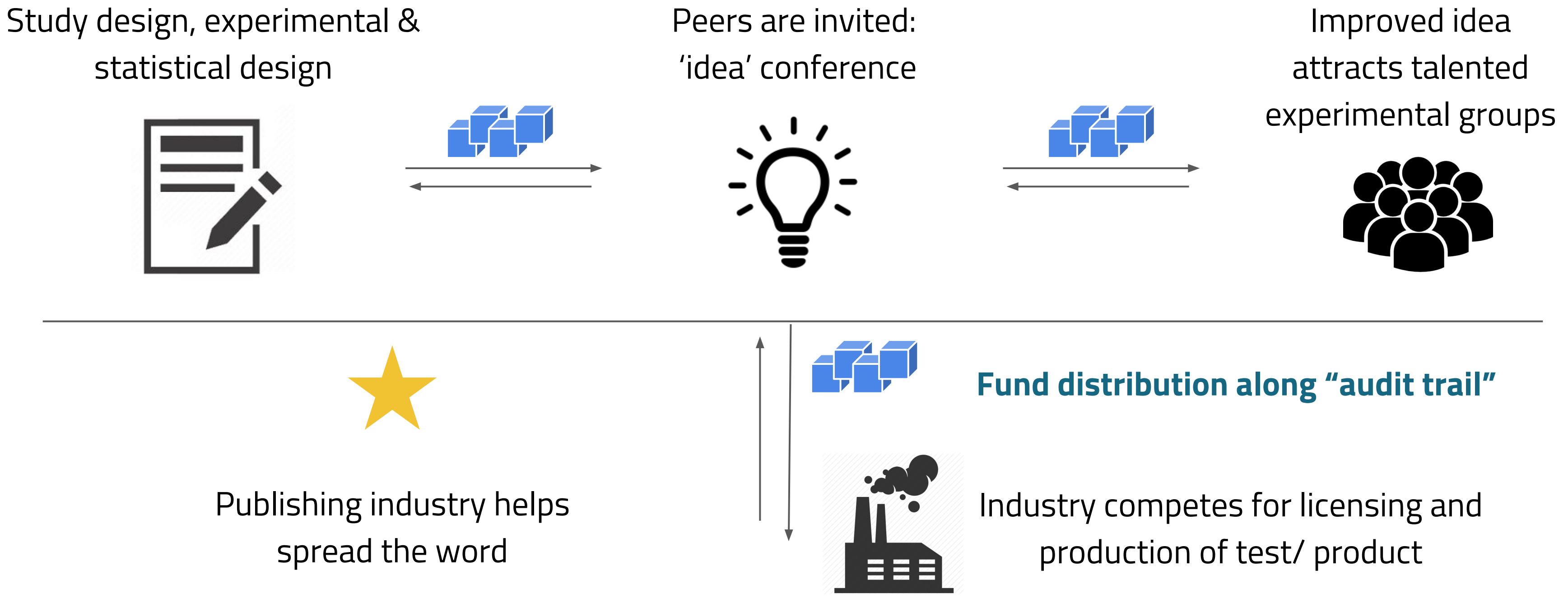
Architecture

Decentralized team-work powered by smart contracts
You want to work with others on a project and be sure that nobody is free-riding/lazy/misbehaving



Project setup
Staking
Project Work
P2P Voting
Stake Payback

A blockchain backed social media platform for science



Study design, experimental & statistical design

Peers are invited: 'idea' conference

Improved idea attracts talented experimental groups

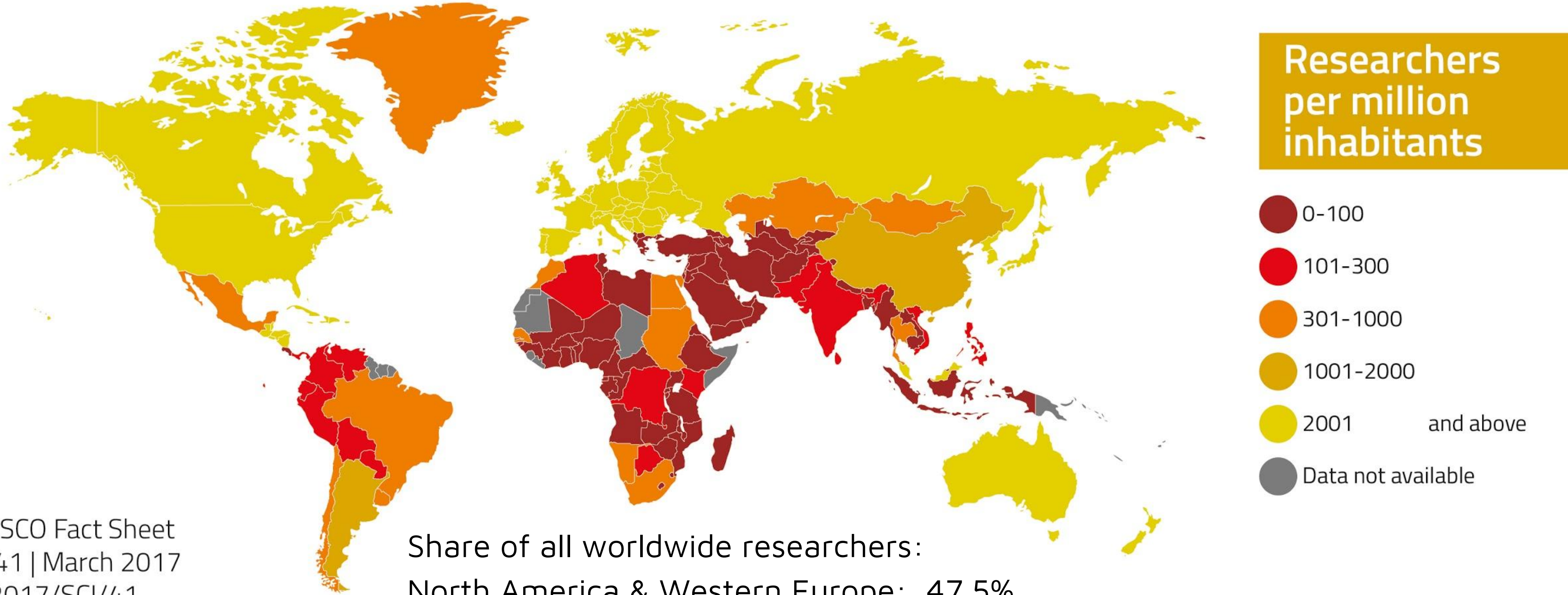
Fund distribution along "audit trail"

Publishing industry helps spread the word

Industry competes for licensing and production of test/ product

PROBLEM: LOST HUMAN POTENTIAL

We miss out on human potential to address global challenges. There are unnecessary entry barriers to participate in scientific discovery & research.



UNESCO Fact Sheet
No. 41 | March 2017
FS/2017/SCI/41

Share of all worldwide researchers:

North America & Western Europe: 47.5%

SOLUTION: Creating global blockchain-backed networks for collaborative research.

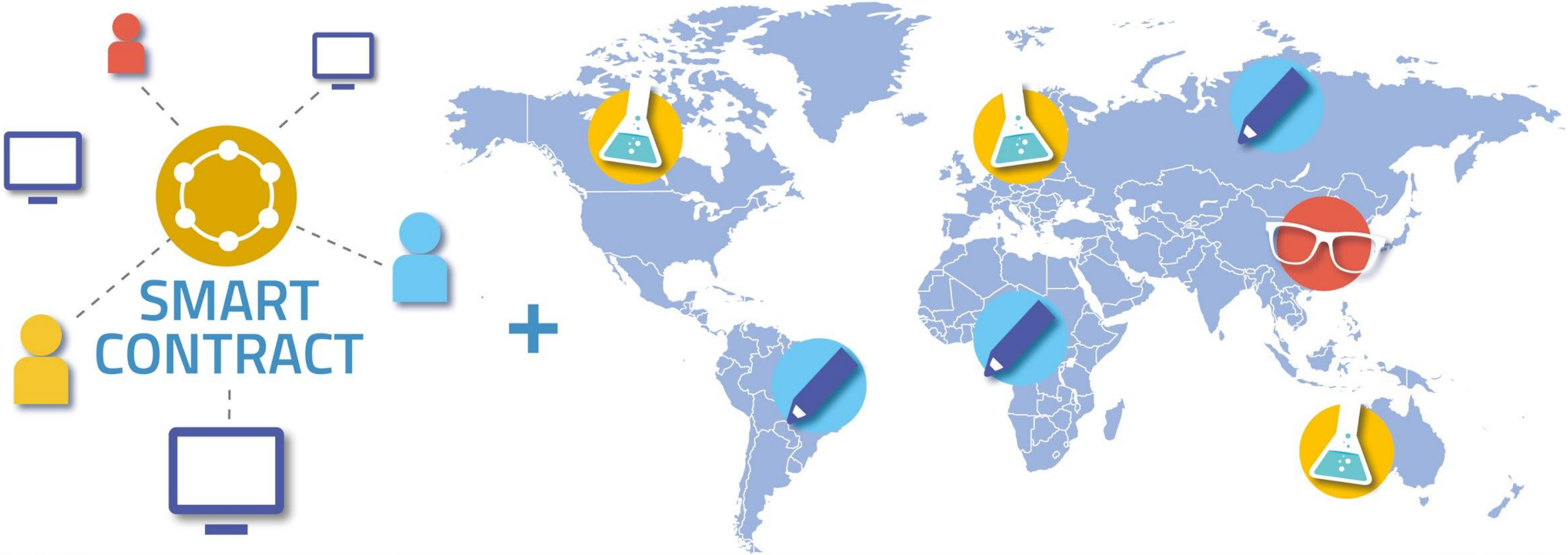
Incentivize collaboration to find the best solution for a problem

Harness collective intelligence

Reward all contributors to the best solution

ValidityLabs™

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



SMART CONTRACT

+

Blockchain for Science and Collaborative Research

September 17-21 2018, Davos, WEF Congress Center

Goals:

- Educate & explore
- Create use cases & roadmap for implementation.
- Follow up: 11 month dev team implement pilot projects

Target groups:

- Academic & industrial scientist

2 da

Kick-off symposium:

Social scientists, economists, blockchain developers, scientist & industry representatives discuss & learn about trust networks for collaborative research

3 days

Workshops explore tools & identifiy implementable R&D projects.

Verticals: Pharma, Healthcare, Mobility, Energy, Big Data & IoT

FOLLOW UP IMPLEMENTATION

3 month

Dev team performs **assessment** of platform performance for given tasks.

Feasibility & work plan of required adaptation for specific problem (UI/ Data management...)

9 month

Implementation, adjustment of UIs, integration through dev team, financing & roll out

Launch

Dr. Sebastian Bürgel | co-founder & CTO
+41 44 77 00 282
sebastian.buergel@validitylabs.org

Dr. Martin Etzrodt | Research head
+41 44 77 00 280
martin.etzrodt@validitylabs.org

André Wolke | co-founder & CEO
+41 44 77 00 281
andre.wolke@validitylabs.org

Validity Labs AG
Postplatz 1
6300 Zug | Switzerland