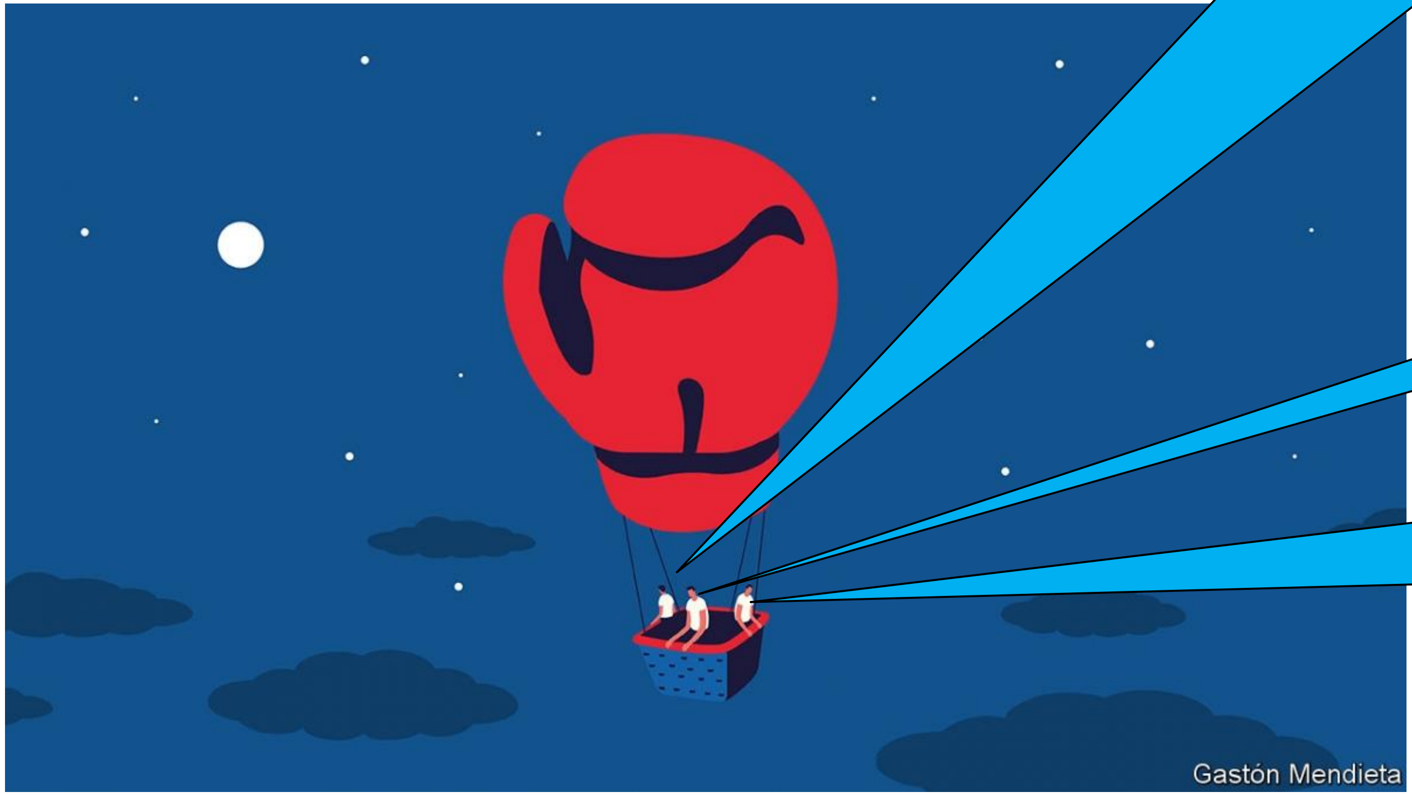
University of Applied Sciences and Arts Northwestern Switzerland
School of Business

Higher Education Expert Conference
The New Student: Flexible Learning Paths and Future Learning Environments
20-21 September 2018
Vienna

The Blockchain Principles and their Potential

Walter Dettling

A distant view: What matters?



Diffuse economic and political power
Hayek

Think freely
Popper

Creative destruction
Schumpeter

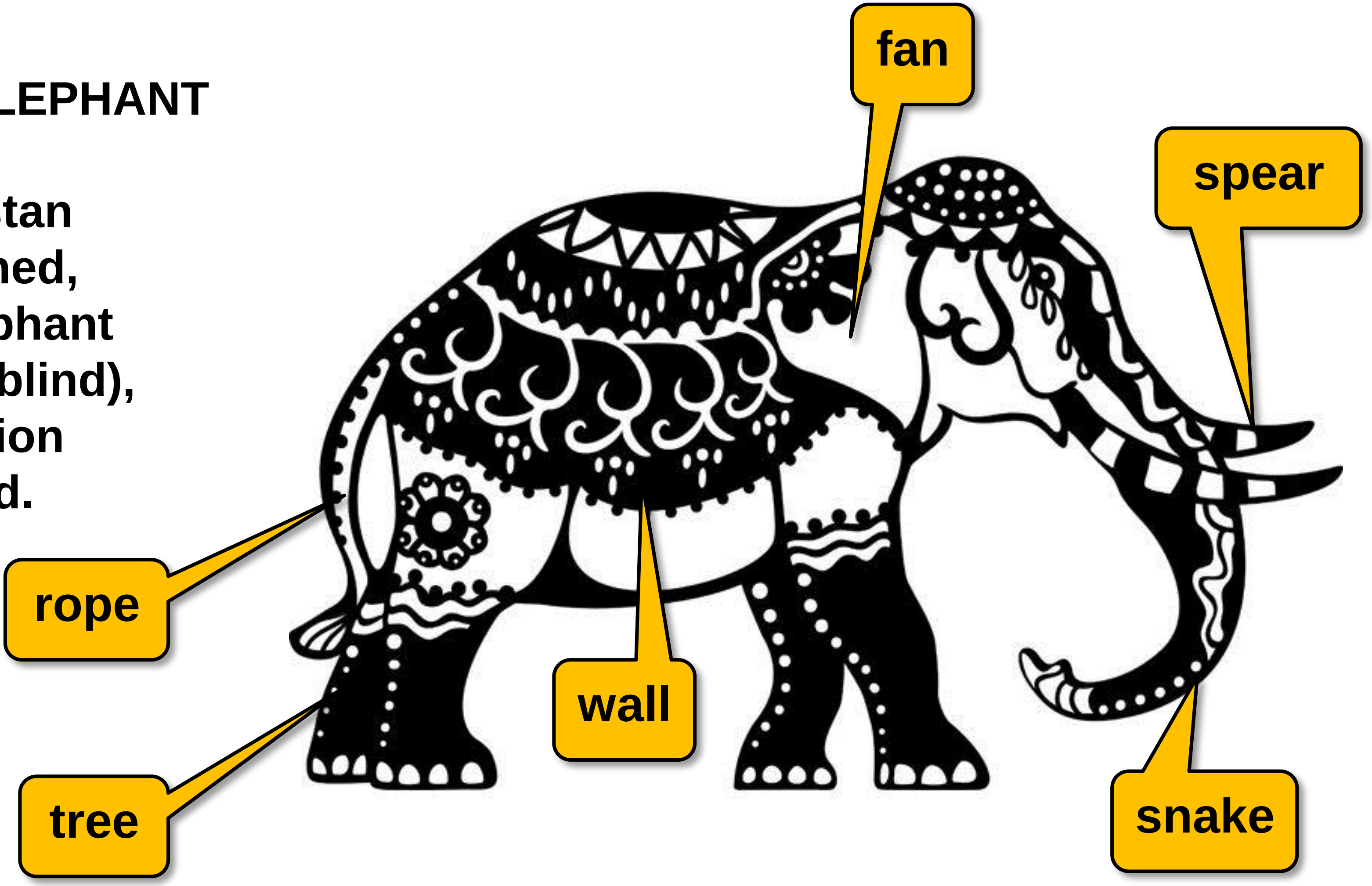
Source: Economist, Aug 23rd 2018

A close view: What is a Blockchain?

THE BLIND MEN AND THE ELEPHANT

It was six men of Indostan
To learning much inclined,
Who went to see the Elephant
(Though all of them were blind),
That each by observation
Might satisfy his mind.

John Godfrey Saxe



Source: https://www.ims.de; https://en.wikisource.org/wiki/The_poems_of_John_Godfrey_Saxe/The_Blind_Men_and_the_Elephant

Possible Perspectives on Blockchain

Financial perspective

Ex. Bitcoin, crypto assets, speculation, ...

Technical perspective

Ex. RSA, SHA256, proof of work, proof of stake, consensus protocol, ...

Business perspective

Ex. Ethereum, smart contracts, new business models, …

Legal and political perspective

Ex. Compliance, fraud, control, legal services, ...

Education

Ex. Certificates, transfer of credits, collecting fees, sovereign identities, …

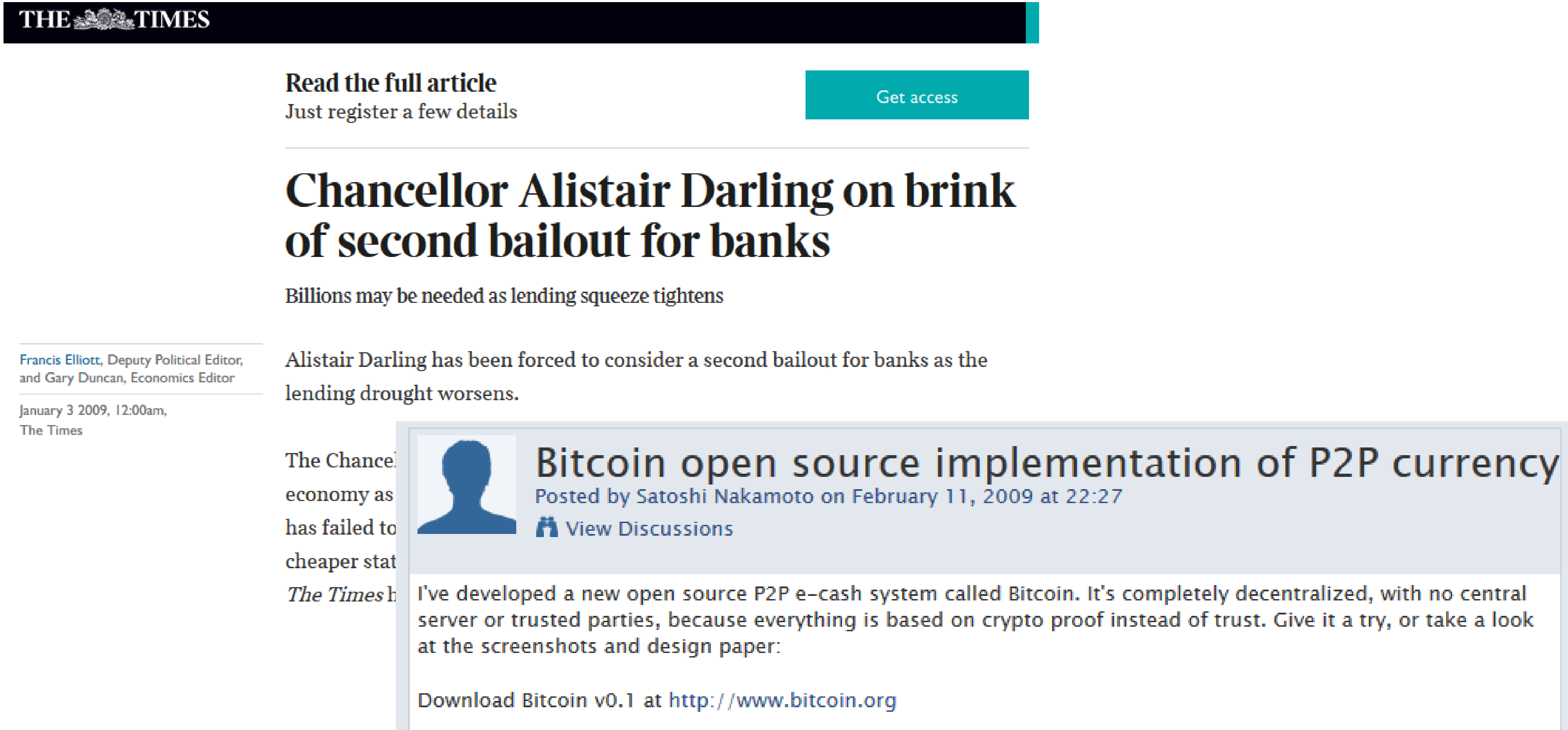
The problem statement of Bitcoin’s founders

«The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. *We have to trust them with our privacy, trust them not to let identity thieves drain our accounts*. Their massive overhead costs make micropayments impossible.»

Satoshi Nakamoto, 2008

Source: *http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source*

Bitcoin makes a distinguished political statement …



THE TIMES

Read the full article
Just register a few details

Chancellor Alistair Darling on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott, Deputy Political Editor, and Gary Duncan, Economics Editor

January 3 2009, 12:00am, The Times

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancel
economy as
has failed to
cheaper stat
The Times h

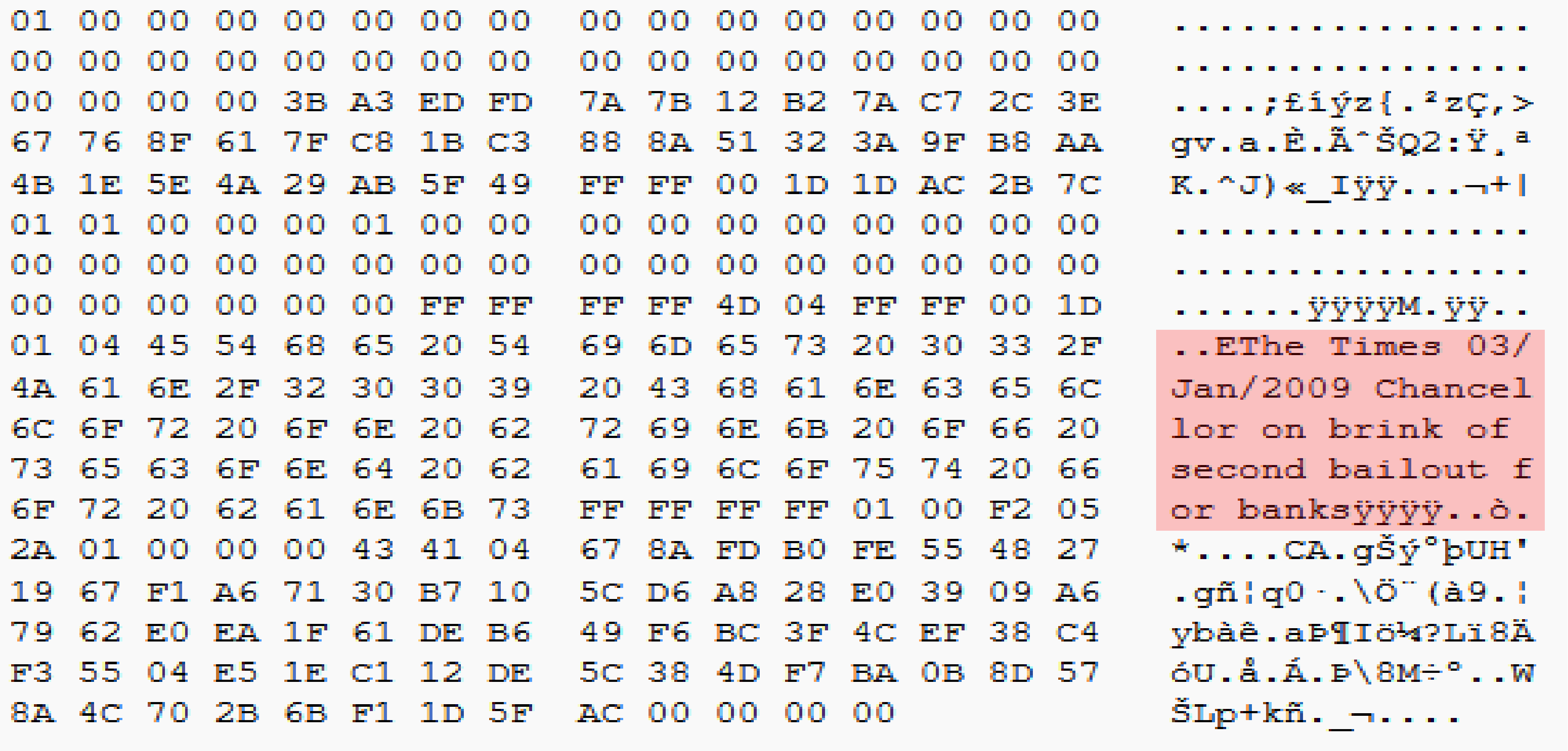
Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The Genesis Block of Bitcoin refers to the financial crisis



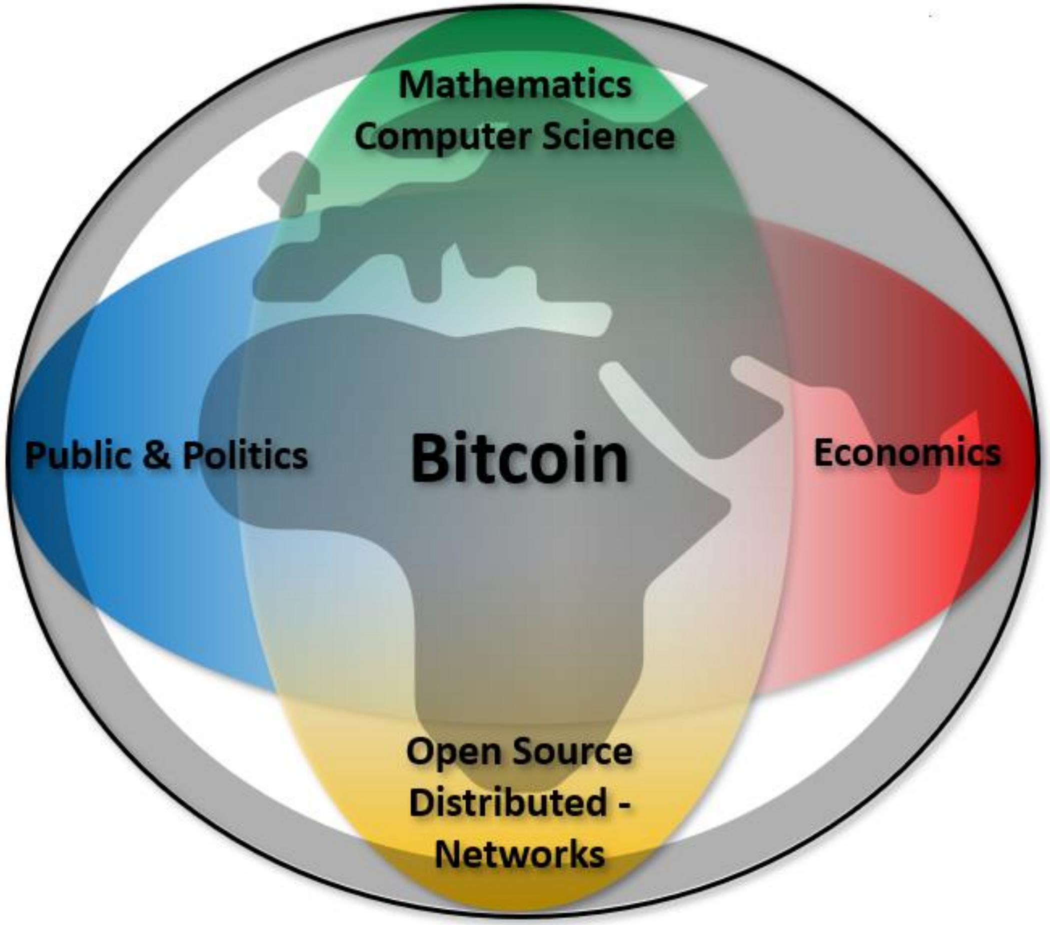
```
01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.ÃˆŠQ2:Ÿ¸ª
4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷°..W
8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

Source: *https://en.bitcoin.it/wiki/Genesis_block*

Design principles of Bitcoin

Bitcoin is a global system which uses mathematics and computer science to build an open source software which is deployed on a global distributed network.

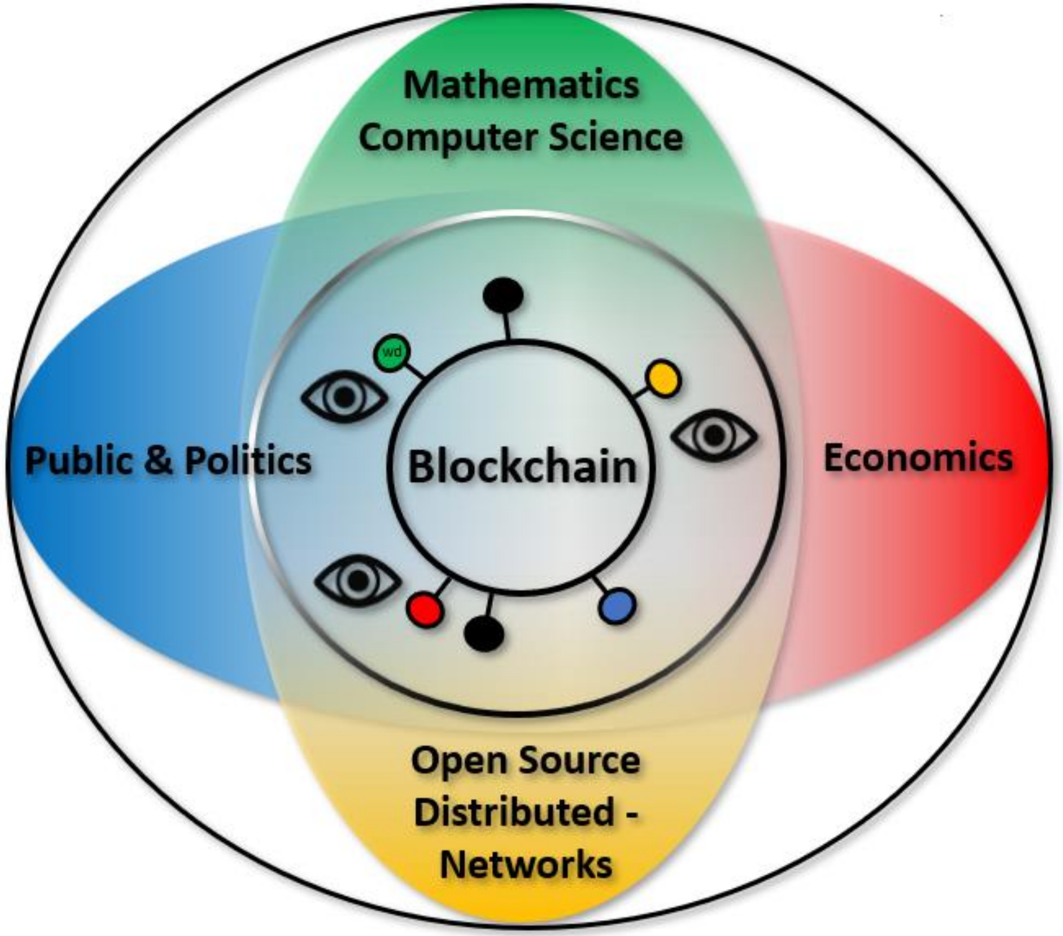
Rules and controls of the system are connected to human behaviour and economic principles and organized with algorithms and game theory.



The main principles of a Blockchain Algorithm

Secure Identities and transactions with

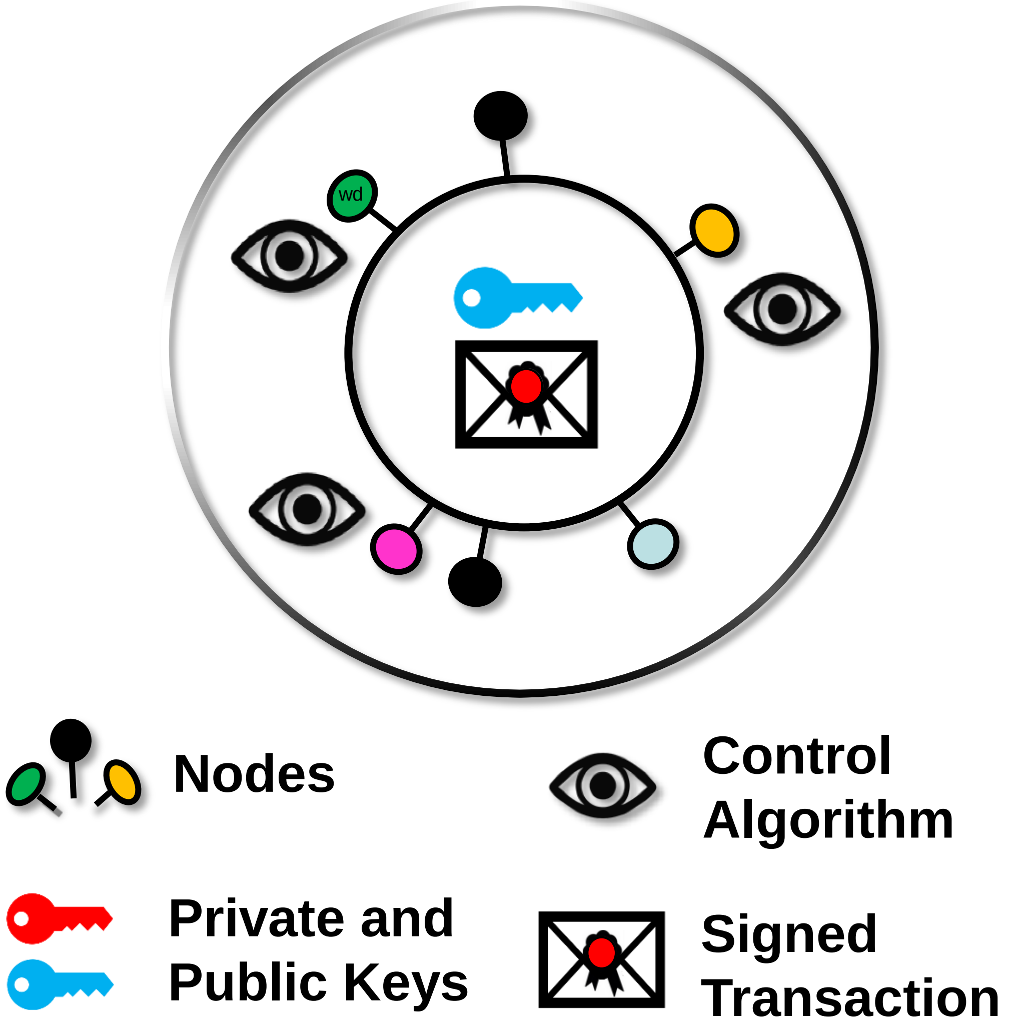
- **Cryptography**
- **Distributed multilayer consensus**
- **Economic incentives**
- **Randomized execution**



How Blockchains work

Blockchains check and perform transactions from any source and store them in a public database (also called public ledger) on all participating nodes.

Transactions are identified by a public key, the owner of the transaction is identified by a private key.



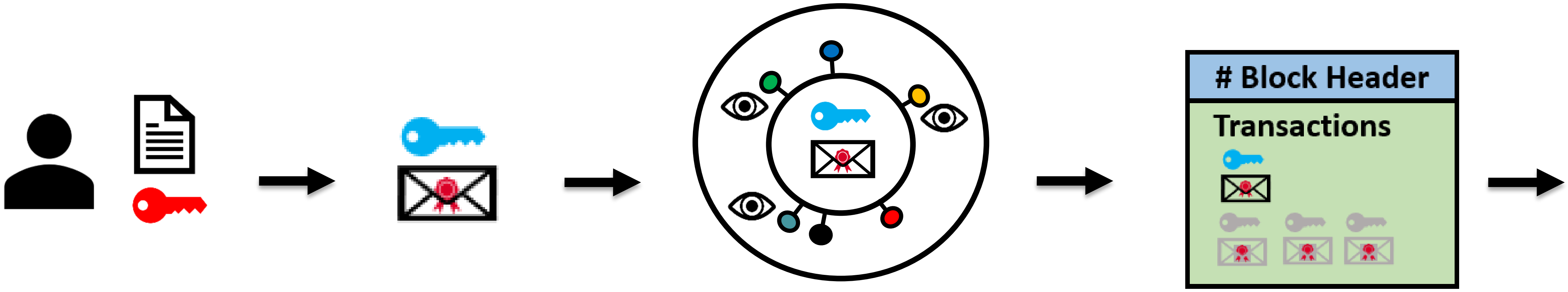
Nodes

Control Algorithm

Private and Public Keys

Signed Transaction

How a transaction gets into the blockchain I



1

Sender signs a transaction with private key

2

Sender sends signed transaction and his public key

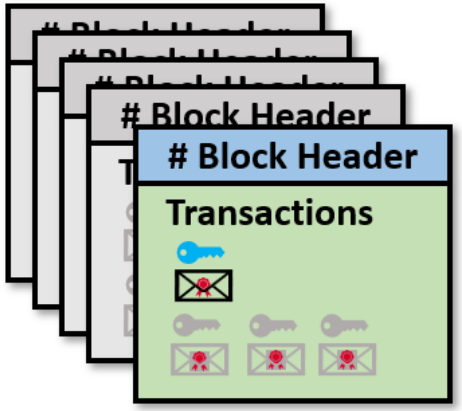
3

Active nodes check the transaction and the signature

4

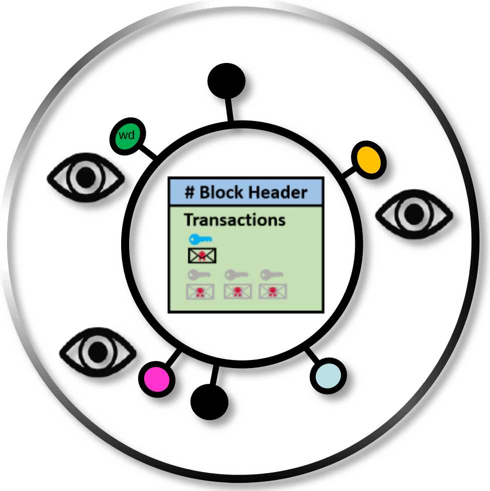
Valid transactions are put in a block

How a transaction gets into the blockchain II



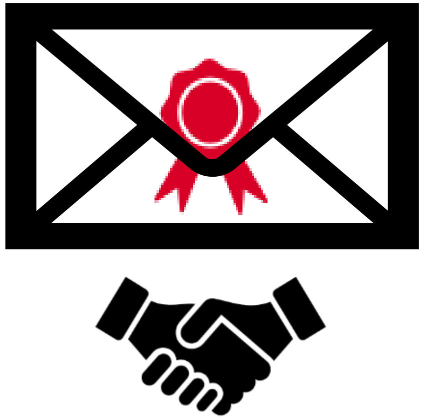
4

The new block is added to the existing blocks by one node..



5

.. and checked again by all other nodes

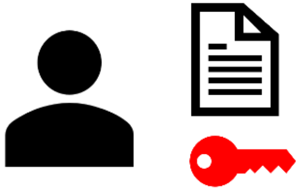


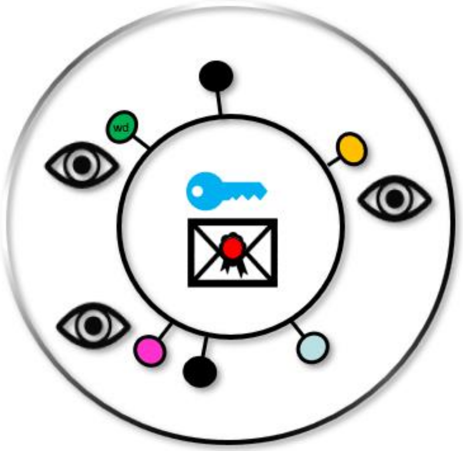
6

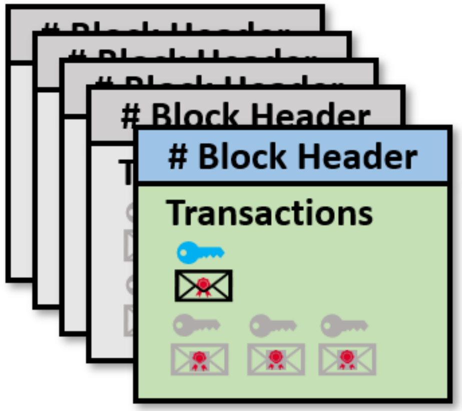
Now the transaction is part of the blockchain and can not be changed or deleted anymore

Some important characteristics of Blockchains

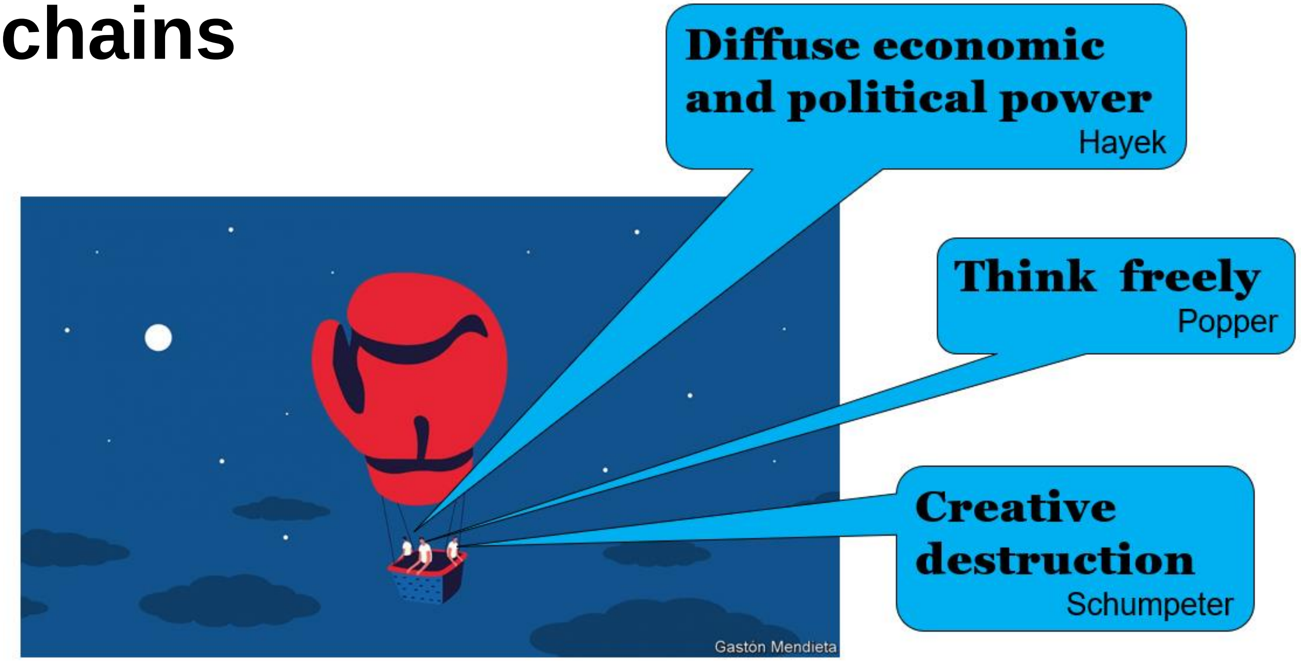
- Each block has a timestamp.
- Transactions are stored visibly for everybody.
- There is no centralised server which stores or controls the network, the transactions, the nodes or the users.
- It is impossible to change or delete any transaction when it is stored in the blockchain.







The potential of Blockchains



Diffuse economic and political power
Hayek

Think freely
Popper

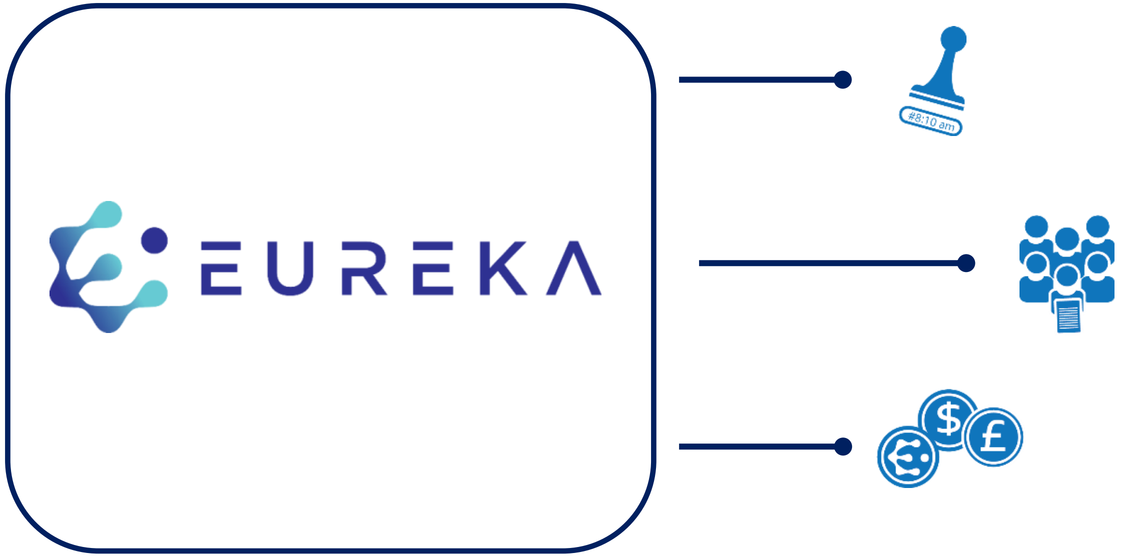
Creative destruction
Schumpeter

Source: Economist, Aug 23rd 2018

- **Blockchains diffuse the role of centralized organizations and systems like banks, government, companies**
- **Blockchains give the control over identity and data to the single user**
- **Blockchains are a seed for new structures in communication and business processes**

Example: Scientific publishing, a 25 Billion $ market

EUREKA Platform, a token-operated science publishing ecosystem on a blockchain



Immediate timestamping, ownership and archiving of observations including negative and replication studies

Crowdsourced open review

Smart contract-based payment of authors, peer-reviewers and editors

Source: https://eurekatoken.io/

Relevance of Blockchains for the individual

- **Self-sovereignty**, i.e. for users to identify themselves while at the same time maintaining control over the storage and management of their personal data;
- **Trust**, i.e. for a technical infrastructure that gives people enough confidence in its operations to carry through with transactions such as payments or the issue of certificates;
- **Transparency & Provenance**, i.e. for users to conduct transactions in knowledge that each party has the capacity to enter into that transaction;
- **Immutability**, i.e. for records to be written and stored permanently, without the possibility of modification;
- **Disintermediation**, i.e. the removal of the need for a central controlling authority to manage transactions or keep records;
- **Collaboration**, i.e. the ability of parties to transact directly with each other without the need for mediating third parties.

Source: JRC Science for Policy Report: Blockchain in Education, 2017, p. 8
https://ec.europa.eu/jrc/en/open-education

Relevance in Education

Blockchain is a technology that clearly has applications in the world of learning at the individual, institutional, group, national and international levels. It is relevant in all sorts of contexts: schools, colleges, universities, MOOCs, CPD, corporates, apprenticeships, and knowledge bases. Rather than the old hierarchical structures, the technology becomes the focus, with trust migrating towards the technology, not the institutions. It really is a disintermediation technology

Donald Clark

Source: JRC Science for Policy Report: Blockchain in Education, 2017, p.51
https://ec.europa.eu/jrc/en/open-education

Blockchains are a challenge for us!

https://www.pinterest.de/pin/392658279706351114/dbd9

Blockchains are complex systems. We do not know what the outcome of their existence and application will bring.

It is important that we do not delegate decisions where and how to use them to technocrats or political and business lobbyists.

Thank you!