# Blockchain, smart contracts, Internet of Things: Land registration and the data economy

*Sjef van Erp*

Maastricht University

# Blockchain, smart contracts

- 1. Introduction
- 2. What are ‘smart contracts’?
- 3. What is ‘distributed ledger technology’(‘DLT’, or ‘blockchain’)?
- 4. What/who are ‘oracles’?
- 5. Who are ‘trusted third parties’ (‘TTP’)?
- 6. Does Artificial Intelligence (‘AI’) play a role?
- 7. What is the ‘Internet of Things’ (‘IoT’)?
- 8. Legal framework
- 9. Do we still need ‘trusted third parties’?
- 10. Object/subject: a diffuse world
- 11. Summary and conclusions

# Blockchain, smart contracts

- Digitalisation of information
- Interconnectivity (Internet)
- Collecting data: big data and databases
- Connecting databases
- Connecting “nodes”
- Self-executing software
- Artificial intelligence

# Blockchain, smart contracts

- What do you think of these statements?

  - You are no longer a person, you are your data
  - You no longer exist when you stop adding data to Google’s servers
  - Objects and subjects can no longer be clearly separated

# Blockchain, smart contracts

*“The data they collect includes tracking where you are, what applications you have installed, when you use them, what you use them for, access to your webcam and microphone at any time, your contacts, your emails, your calendar, your call history, the messages you send and receive, the files you download, the games you play, your photos and videos, your music, your search history, your browsing history, even what radio stations you listen to.”*

Dylan Curran: Are you ready? Here is all the data Facebook and Google have on you (The Guardian)

# Blockchain, smart contracts

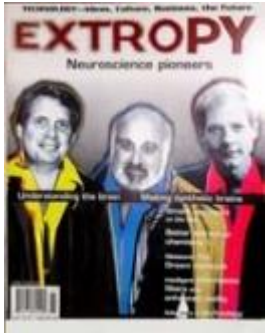
# Blockchain, smart contracts

- Two (or more?) worlds:
  - IT and law (Lawrence Lessig ‘code is law’)
  - Standardised (form based, and yes/no) thinking  v. reflexive thinking
  - Younger v. older generation
  - Yes or no access to the Internet

# Blockchain, smart contracts

- New developments build upon existing architecture:
  - Internet protocols: TCP/IP
  - Blockchain: Examples are Bitcoin, Ethereum
  - ‘Decentralised app’ (‘Dapp’) framework (cf. more traditional apps, such as Gmail or Uber)
  - ‘Dapp’ applications by using these apps

# Blockchain, smart contracts



TECHNOLOGY—Ideas, Culture, Business, the Future

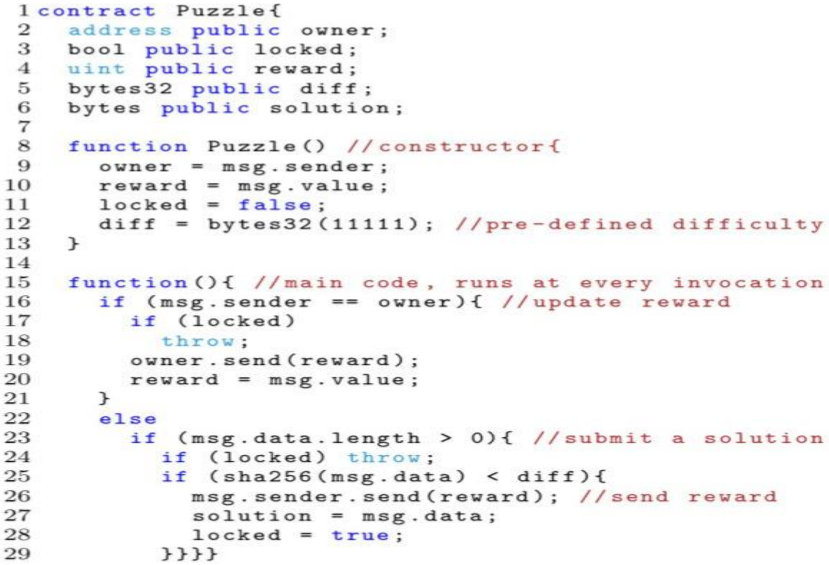
EXTROPY

Neuroscience pioneers

Understanding the brain

Making synthetic brains

# Blockchain, smart contracts



```
contract Puzzle{
  address public owner;
  bool public locked;
  uint public reward;
  bytes32 public diff;
  bytes public solution;

  function Puzzle() //constructor{
    owner = msg.sender;
    reward = msg.value;
    locked = false;
    diff = bytes32(11111); //pre-defined difficulty
  }

  function(){ //main code, runs at every invocation
    if (msg.sender == owner){ //update reward
      if (locked)
        throw;
      owner.send(reward);
      reward = msg.value;
    }
    else
      if (msg.data.length > 0){ //submit a solution
        if (locked) throw;
        if (sha256(msg.data) < diff){
          msg.sender.send(reward); //send reward
          solution = msg.data;
          locked = true;
        }}}}
```

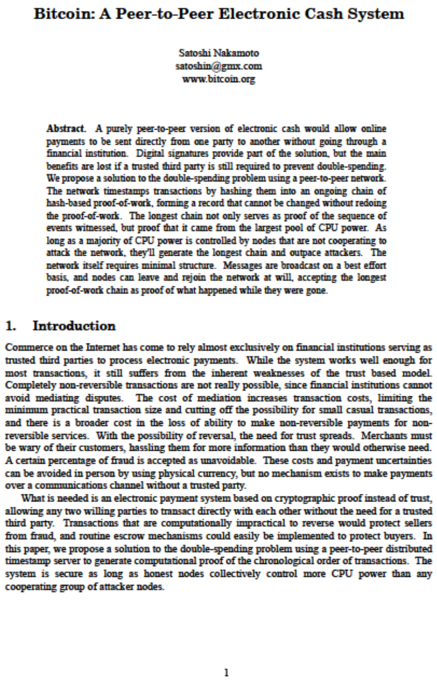
Figure 3: A contract that rewards users who solve a computational puzzle.

# Blockchain, smart contracts

- 2. Smart contracts: Nick Szabo

  - Self-executing programmes
  - Example: insurance against flight delays

# Blockchain, smart contracts



## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

### 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

# Blockchain, smart contracts

- 3. DLT: Satoshi Nakamoto (?)

  - The name is meant to hide the real person(s)
  - Block chain technology is far more than “just” ‘bitcoins’ = cryptocurrency

# Blockchain, smart contracts

- 3. DLT (continued)

    - Several technologies (example: Ethereum)
    - Public and private block chains
    - ‘On chain’ and ‘Off chain’

# Blockchain, smart contracts

- A ‘smart contract’ adds information to a block and by doing so creates a new block and thus a ‘block chain’.

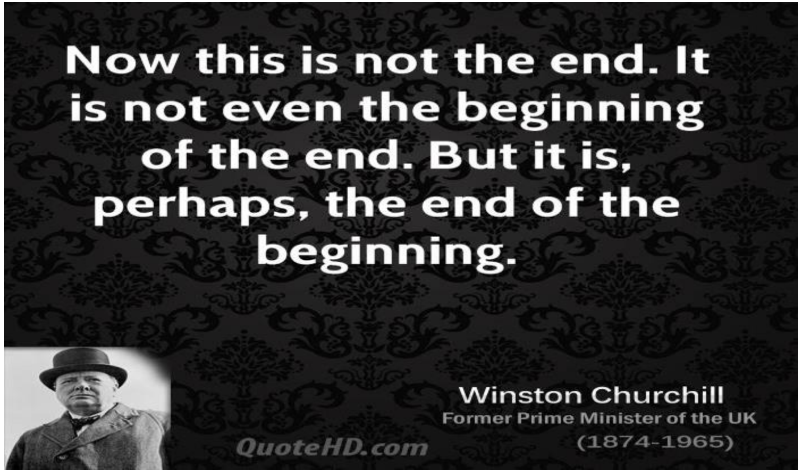
# Blockchain, smart contracts

- Information in the block cannot be changed and – for the time being? – not be hacked.

  - Question: What does this mean for the ‘right to be forgotten’ under the new GDPR?

# Blockchain, smart contracts

- ‘Blockchain and Property in 2018: At the End of the Beginning’: Is this exaggerated?



Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.

Winston Churchill
Former Prime Minister of the UK
(1874-1965)

QuoteHD.com

# Blockchain, smart contracts

- Public blockchains are not supervised by a central authority, such as governments
  - ‘Initial coin offerings’ (‘ICO’s’)
- At the same time: A government can use blockchain technology to control its citizens
  - Privacy!

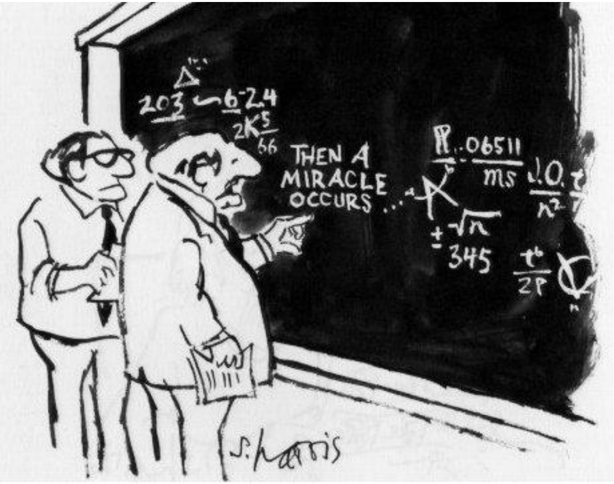
# Blockchain, smart contracts

# Blockchain, smart contracts

- 4. ‘Oracles’

  - Third parties (human persons, but especially also computer systems: ‘agencies’)
  - Judges, mediators, notaries, land registrars

# Blockchain, smart contracts



“I think you should be more explicit here in step two.”

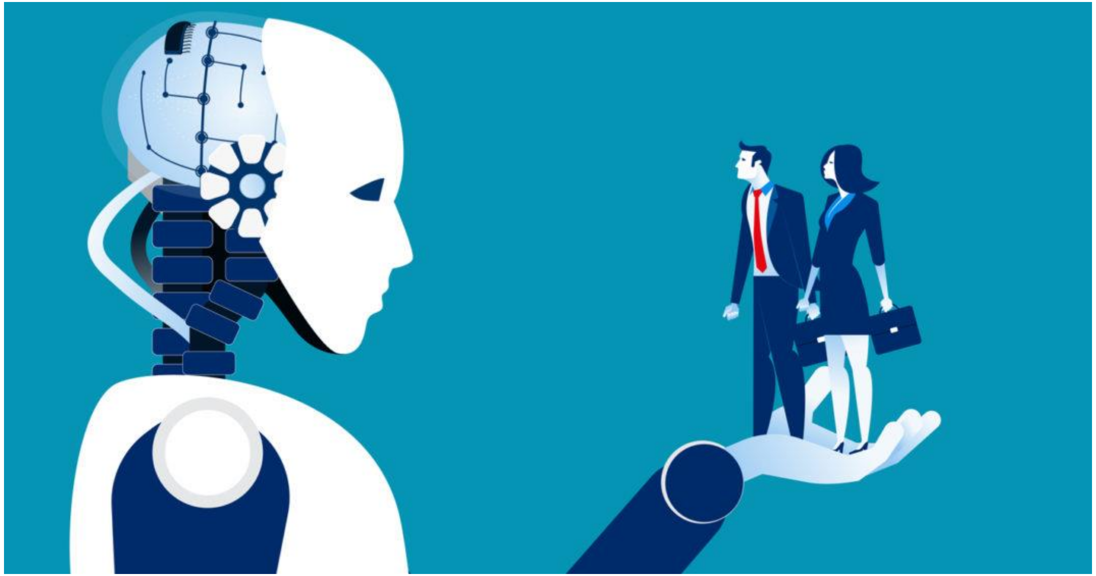
from *What's so Funny about Science?* by Sidney Harris (1977)

# Blockchain, smart contracts

- 5. Trusted third parties

  - A third person, necessary to verify that a particular transaction is correctly performed
  - Is there a role left for land registrars?

# Blockchain, smart contracts

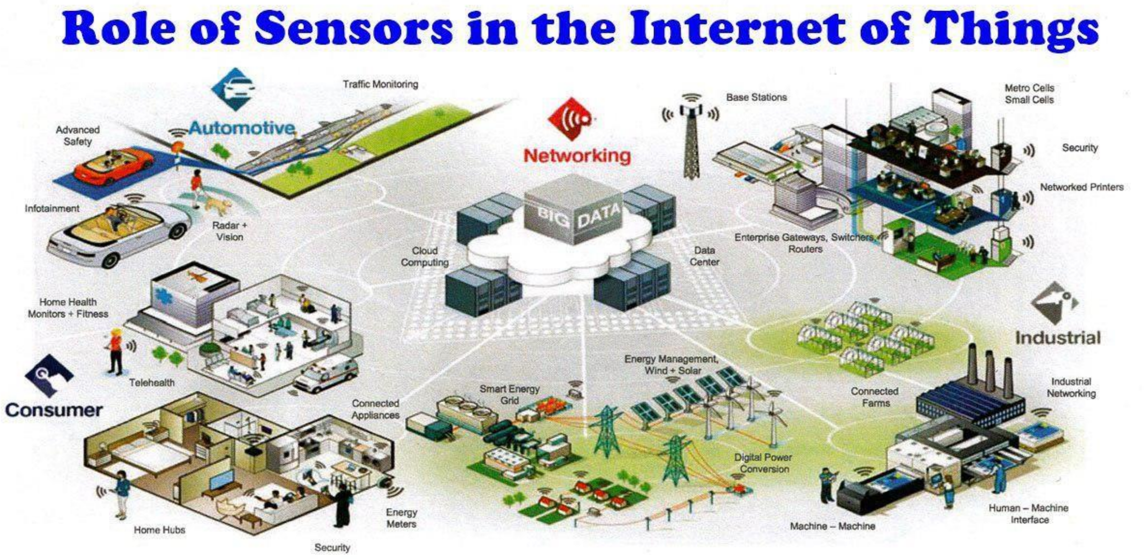


# Blockchain, smart contracts

- 6. Does Artificial Intelligence (‘AI’) play a role?

    - Developments go further and faster than we perceive
    - Google’s ‘Deepmind’: www.deepmind.com

# Blockchain, smart contracts



# Blockchain, smart contracts

- 7. ‘IoT’

  - Collecting data: ‘big data’
  - Sensors collect data, but for which purpose?
    - To better describe an object?
    - Data analysis (targeting, customer specific)?
    - To check whether a person is acting within the limits of the law?

# Blockchain, smart contracts

- 8. Legal framework

    - Why is a ‘smart contract’ binding?
    - Who is liable for mistakes in a ‘block’?
    - Who is liable in a diffuse real/virtual world (e.g. for measuring mistakes made by sensors)?

# Blockchain, smart contracts

- 9. Do we still need ‘trusted third parties’?

  - Yes, in any case for complicated transactions and as ‘gate keeper’ for what is happening ‘off chain’

# Blockchain, smart contracts

- 10. Object/subject: a diffuse world

  - Are data part of a parcel or do they belong to the parcel's "owner"?
  - What is the "object", who is the "subject"?
  - Can we separate the real object from the digital data?
  - Which IoT data should be registered in a land registry?
  - Should we accept different types and degrees of ownership?

# Blockchain, smart contracts

- 11. Summary and concusions:

  - Block chain, smart contracts, IoT
  - Which data “belong” to a parcel (object) or to the owner (subject)?

# Blockchain, smart contracts, Internet of Things: Land registration and the data economy

*Prof. dr. J.H.M. (Sjef) van Erp*

*Maastricht University*

*s.vanerp@maastrichtuniversity.nl*

*European Law Institute*

*vice-president.eli@univie.ac.at*

Maastricht University