What role does the blockchain have on trust in smart cities?

Martin Walker

Luzern, Switzerland

January 14th 2020

Blockchain?

Smart City

a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business.

Blockchain ?

Sharing

Ordinary residents can help each other and the city as a whole.

Sharing, cooperation, and contribution to the common good to create lives and a world worth having.

Sharing

Anthropologist David Graeber describes models or resource sharing in various societies.

"Exchange allows us to cancel our debts. It gives us a way to call it even: hence to end a relationship. With vendors, one is usually only pretending to have a relationship at all. With neighbours, one might for this very reason prefer *not* to pay one's debts."

He then goes to describe an endless cycle of giving and receiving gifts in the Tiv Community of Nigeria.

According to Graeber what is essentially "sharing", is a fundamental nature of smaller human communities.

Reference - David Graeber "Debt: The First 5000 Years"

Cheating

"Reciprocal altruism led to cheating, that led to defence against cheating, and that led to the evolution of a sense of fairness, friendship, and trust,"

Robert Trivers (Evolutionary Biologist)

Human beings are social creatures, utterly dependent on each other to survive but also uniquely evolved to deceive each other.

Reference – Robert Trivers "*The Folly of Fools: The Logic of Deceit and Self-Deception in Human Life*"

Incentivising Trustworthy Behaviour

Bruce Schneier – (Cryptographer and IT Security Expert) Identified four systems our species uses to incentivize trustworthy behaviour.

1&2. *Morals and reputation*. The problem is that they scale only to a certain population size. Primitive systems were good enough for small communities, but larger communities required delegation, and more formalism
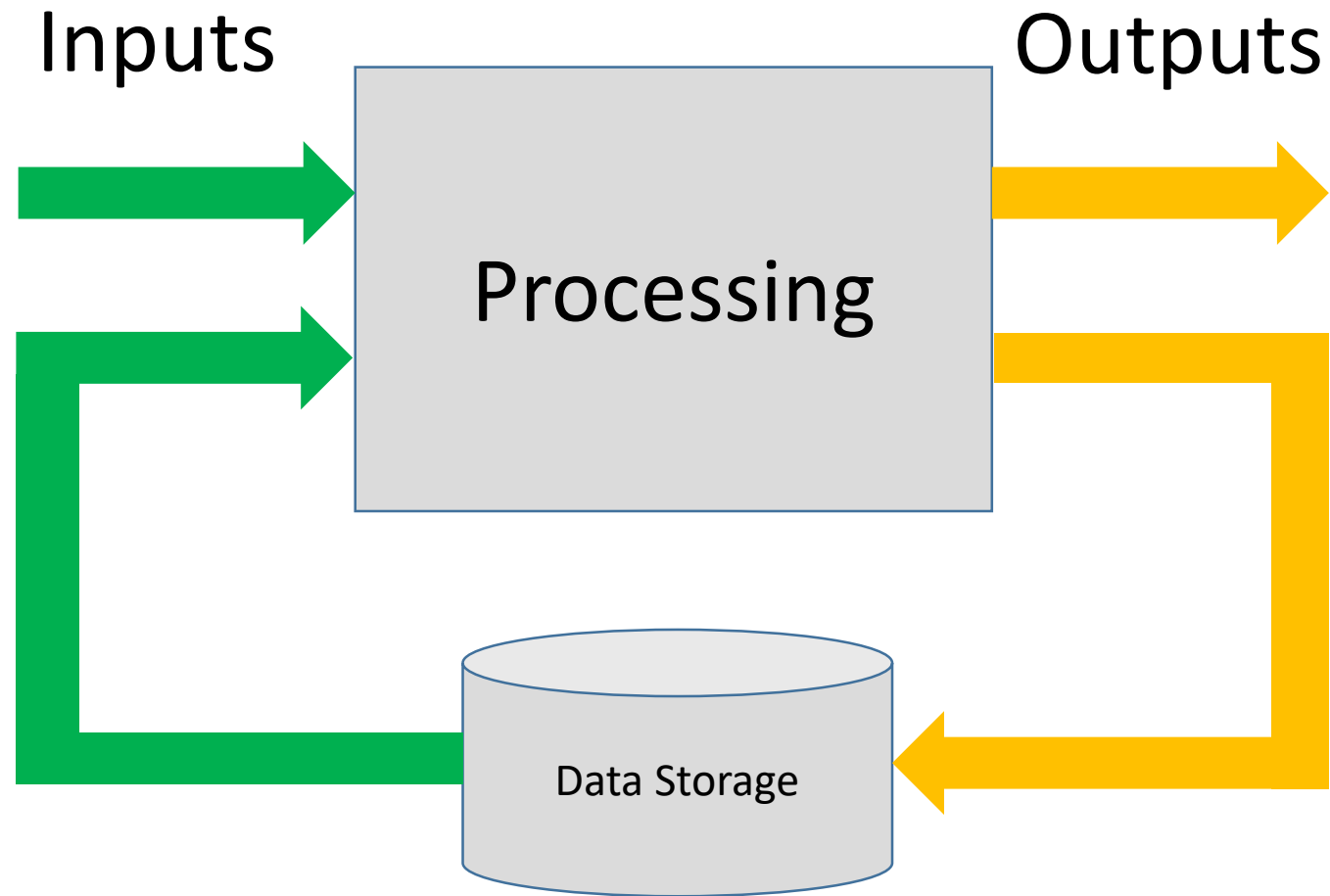3. *Institutions*. Institutions have rules and laws that induce people to behave according to the group norm, imposing sanctions on those who do not. In a sense, laws formalize reputation
4. *Security systems*. These are the wide varieties of security technologies we employ: door locks and tall fences, alarm systems and guards, forensics and audit systems, and so on

Reference – "There's No Good Reason to Trust Blockchain Technology" (2019) & "Liars and Outliers" (2012)
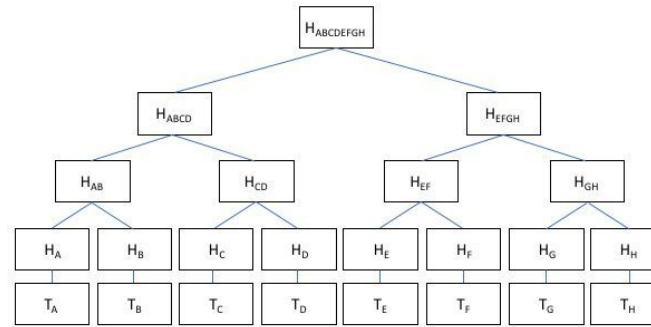
https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/
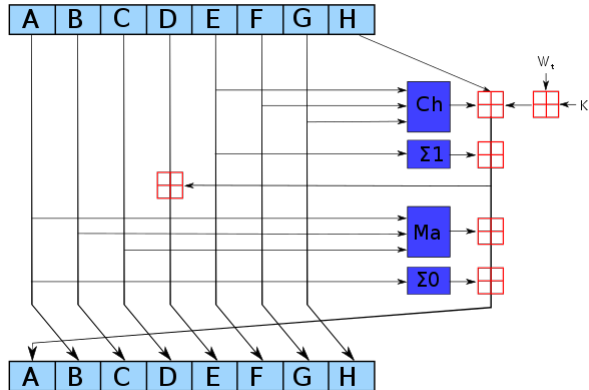
IT Systems – Made Simple

Inputs

Outputs

Processing

Data Storage

www.cebma.org

Blockchain - Predecessors
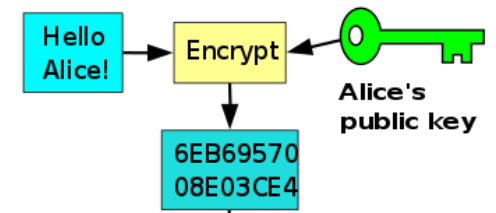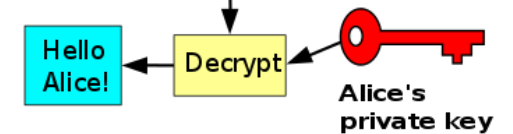
Merkle tree (1979)

SHA-2 (2001)

Blockchain uses three key technologies invented long before Bitcoin. They continue to be used independently of blockchain.

Using these technologies does not mean you are using blockchain

Bob

Hello Alice! → Encrypt ← Alice's public key

6EB69570 08E03CE4

Alice

Hello Alice! ← Decrypt ← Alice's private key

Public-key Cryptography (1970s)

Blockchain Basics (Bitcoin Version)

- A list of transactions
- Stored in blocks
- No central control of the code running on the system
- No central control of the processing of transactions
- Anyone can participate
- All transactions visible
- Identity of the parties to transactions hidden
- All transactions in a private currency
- Private currency is created in the process of validating transactions
- Create of currency incentivises people to process transactions
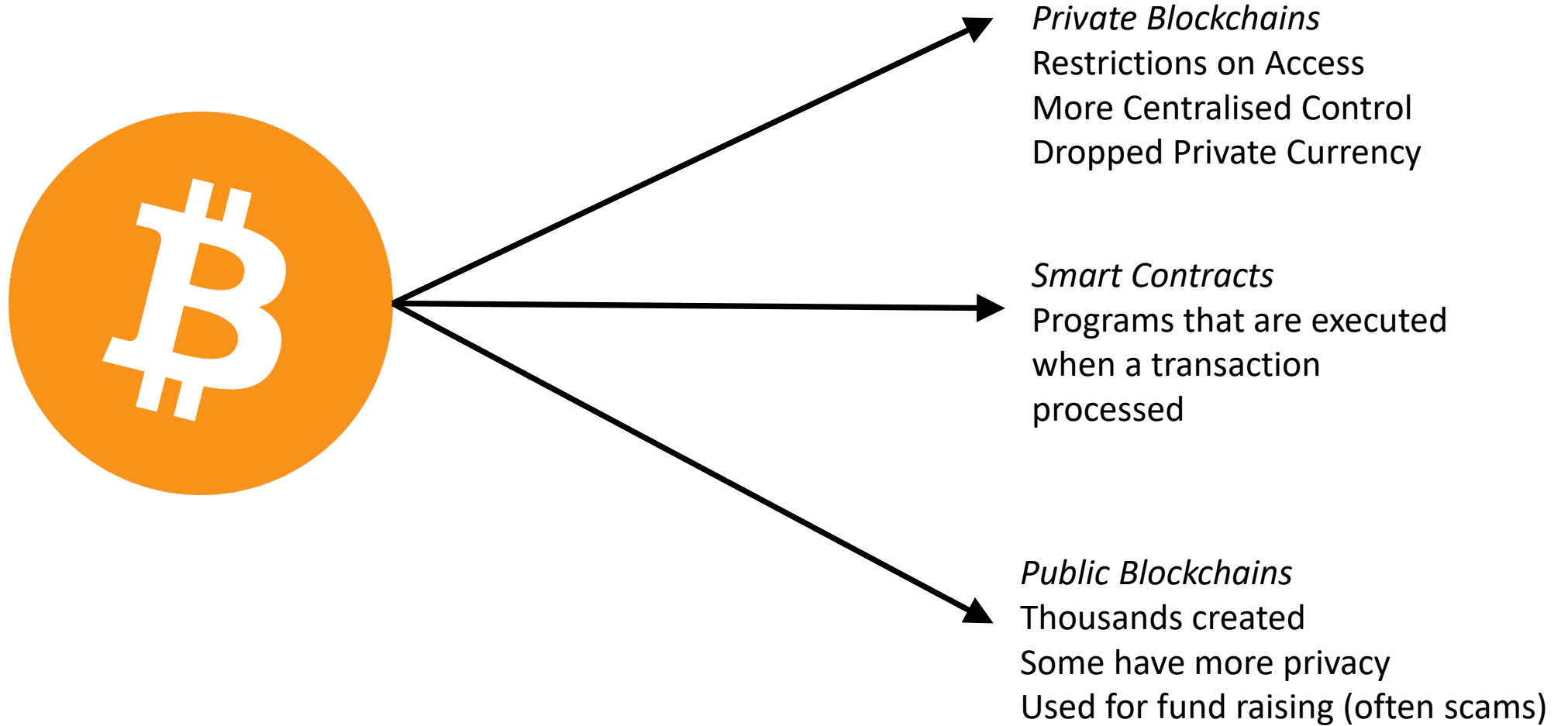
2009 Bitcoin Whitepaper

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA

The Economist

Our guide to America's best colleges
Myanmar's free-ish election
Those ever-creative accountants
America takes the fight to IS
Ceywolves: the new superpredator

The trust machine
How the technology behind bitcoin could change the world

2015 Wide Scale Excitement

Doing business with people you do not trust?

Blockchain Divergence

Private Blockchains
Restrictions on Access
More Centralised Control
Dropped Private Currency

Smart Contracts
Programs that are executed
when a transaction
processed

Public Blockchains
Thousands created
Some have more privacy
Used for fund raising (often scams)

IT Systems – The Trust Problems

Garbage In – Garbage Out
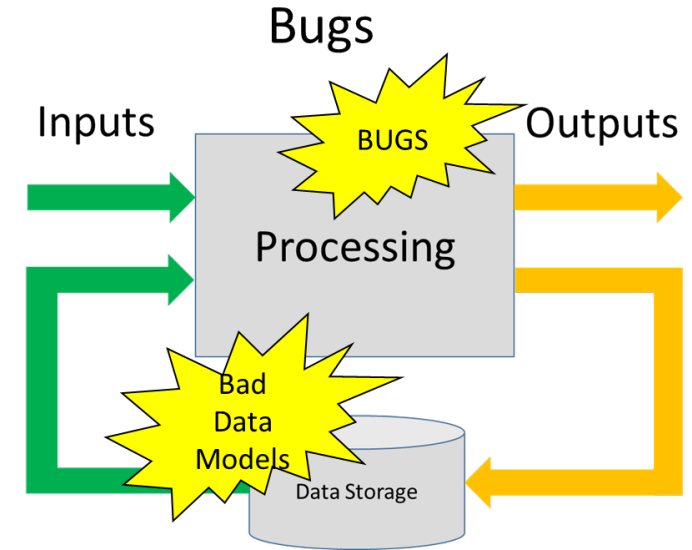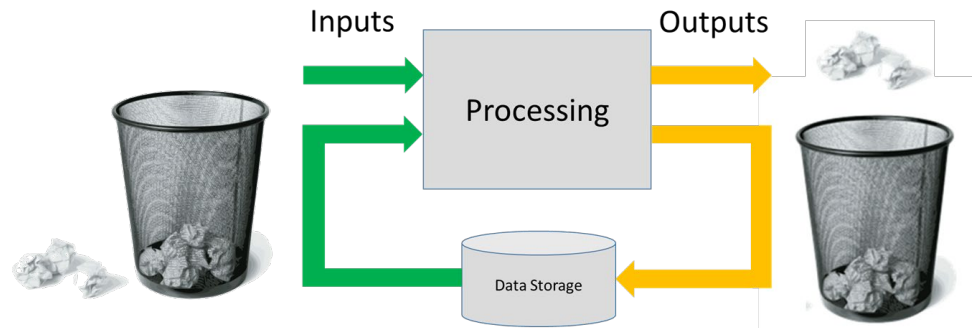
Accurate Representation of the Real World

ID	233301223
DataTime	05/05/2019 12:03
InputUser	Martin
Type	Floribunda
Color	Yellow
Origin	UK
Supplier	English Roses Ltd

Bugs
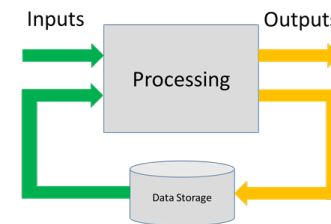
Security

Access To Use System
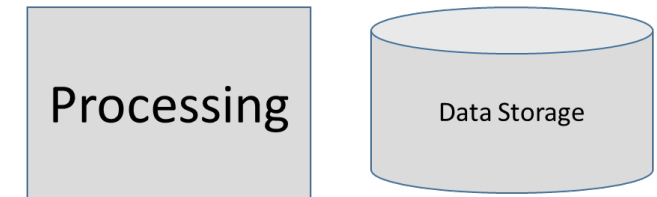
Ability to change code

Access to Data

IT Systems – More Trust Problems

Any system will have one or more parties:

- Writing and maintaining the system

- Operating/Supporting the system

- Owning the software

- Managing the Hardware

- Owning the Hardware

- Auditors/Regulators

Can you trust them to:

- Keep your data safe and secure

- Not use the data to commit fraud or theft

- Ensure the system is performant

- Ensure the system functions correctly

- Does not exploit its users

- Correct mistakes (including users)

Blockchain Lessons

The DAO - Decentralized Autonomous Organization

Big Blocks versus Small Blocks

ICOs and the Democratisation of Finance

Provenance

General Lessons

Smart Cities, models for Sharing economy are "systems", we can learn from the great cryptocurrency/blockchain experiment some key lessons about how to design those systems

A system is not just code and hardware it is the people who operate it, build it, own it, govern it and use it

Human factors are the major problem in why systems go wrong

Lack of a governance framework can lead to paralysis or chaos

A system open to all which allows anonymous actors that can be exploited for financial gain – will be exploited

Final Thought

- A smart city or a sharing city is a system

- The Internet has demonstrated the Earth is not quite a village yet

- Millions have been exploited, manipulated or just plain defrauded because an anonymous global network (even one with as many benefits as the internet) allows humans to act in ever more inhuman ways

- Even the largest city has the benefit that people can be truly people because they can make human connections to each other. A great enabler of trust.

- Technology can become an enabler for the Sharing Movement but it needs to do so by helping people to be more human not less

- If you hear great claims made for blockchain based systems, I recommend you use the "Key Concepts for Informed Choices Framework" for evaluating those claims
https://thatsaclaim.org/management/