Veronika Kütt

bitcoin. math. ultramarathon. yoga.

Veronika Kütt
bitcoin. math. ultramarathon. yoga.

- Frankfurt School Blockchain Center
  - PC & PM for Blockpool.eu
- Cashlink
  - Consulting & PM: tokenised securities
- Hansecoin o.Ü.
  - Tokenised securities - hard assets
- Unchain Convention – Bitcoin Conference, Berlin

Today

- Expectations
- (Payments): Public vs. Private ledgers
- Bitcoin + Co.
- Hands-on
- What else? Smart Contracts & Autonomy

What is…

… Bitcoin?

What is…

… Blockchain?

Quote

> Blockchain will do to the financial system
>
> what the internet did to information

What is it the internet did to information?

Quote +

Blockchain will do to … what the internet did to information

Definition

A **blockchain**,[1][2][3] originally **block chain**,[4][5] is a growing list of records, called *blocks*, that are linked using cryptography.[1][6] Each block contains a cryptographic hash of the previous block,[6] a timestamp, and transaction data (generally represented as a Merkle tree). - Wikipedia

Definition

A **blockchain**,[1][2][3] originally **block chain**,[4][5] is a growing list of records, called *blocks*, that are linked using cryptography.[1][6] Each block contains a cryptographic hash of the previous block,[6] a timestamp, and transaction data (generally represented as a Merkle tree). - Wikipedia

Blockchain builds on the idea of P2P networks and provides a **universal data set** that every actor can trust, even though they **might not know or trust each other**. It provides a shared and trusted ledger of transactions, where **immutable** and encrypted copies of **information** are **stored on every node in the network**. **Economic incentives** in the form of native network tokens are applied to make the network **fault tolerant,** and **attack and collusion resistant**. – Shermin Voshmgir, Token Economy

Definition

A **blockchain**,[1][2][3] originally **block chain**,[4][5] is a growing list of records, called *blocks*, that are linked using cryptography.[1][6] Each block contains a cryptographic hash of the previous block,[6] a timestamp, and transaction data (generally represented as a Merkle tree). - Wikipedia

Blockchain builds on the idea of P2P networks and provides a **universal data set** that every actor can trust, even though they **might not know or trust each other**. It provides a shared and trusted ledger of transactions, where **immutable** and encrypted copies of **information** are **stored on every node in the network**. **Economic incentives** in the form of native network tokens are applied to make the network **fault tolerant,** and **attack and collusion resistant**. – Shermin Voshmgir, Token Economy

Blockchain is a protocol for **digital value exchange**. – Igor Gramatikovski

Only hype?

What are public blockchains all about?

Leo Weese 獅 草地
@LeoAW

Follow

Amazing how people suddenly realize they don’t own their data on Facebook. Let’s see how they react when they find out they dont own the money in their bank accounts either!

2:35 AM - 13 Apr 2018

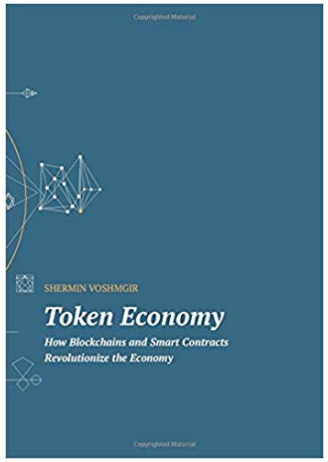
3,284 Retweets **7,156** Likes

Zwei paar Schuhe: public vs. private ledgers

	Public permissionless	Private permitted
Access	Read & Write Public to anyone	Read & Write Upon invitation only
Network Actors	Don‘t know each other	Know each other
Native Token	Yes	No
Security	Economic incentives (PoW, PoS, …)	Legal Contracts (PoA)
Speed	Slow	Fast
Examples	Bitcoin, Ethereum, Monero, Zcash, Steemit, …	R3 (Banks), B3i (Insurance), Corda, Facebook
Effects	Potential to disrupt current business models through disintermediation. Lower infrastructure cost: no need to maintain servers os system admins radically reduces the costs of creating and running decentralized applications (dApps)	Reduces transaction costs and data redundancies and replaces legacy systems, simplifying document handling and getting rid of semi manual compliance mechanisms. In that sense it can be seen as equivalent to SAP in the 1990‘s: reduces costs, but not disruptive

Zwei paar Schuhe: public vs. private ledgers

	Public permissionless	Private permitted
Access	Read & Write	Read & Write Upon invitation only
		Know each other
		No
		Legal Contracts (PoA)
		Fast
		R3 (Banks), B3i (Insurance), Corda, Facebook
		Reduces transaction costs and data redundancies and replaces legacy systems, simplifying document handling and getting rid of semi manual compliance mechanisms. In that sense it can be seen as equivalent to SAP in the 1990‘s: reduces costs, but not disruptive



Shermin Voshmgir, director of the Research Institute for Cryptoeconomics at the Vienna University of Economics and the founder of BlockchainHub Berlin

Zwei paar Schuhe: public vs. private ledgers – i.e. Bitcoin & Libra

Which problem has been solved through Bitcoin?

Double-spending problem

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.

The building blocks of bitcoin

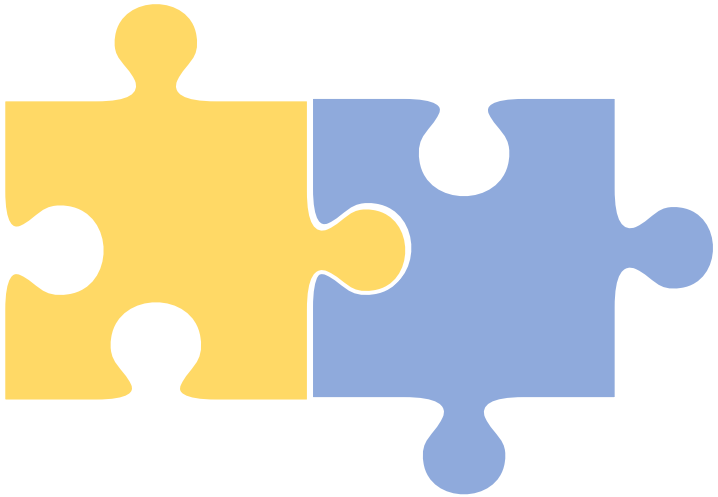
Game theory

Strategic interaction between rational decision-makers

The building blocks of bitcoin

Game theory

Strategic interaction between rational decision-makers



Consensus mechanism

How do we make sure everyone is writing down the same data?

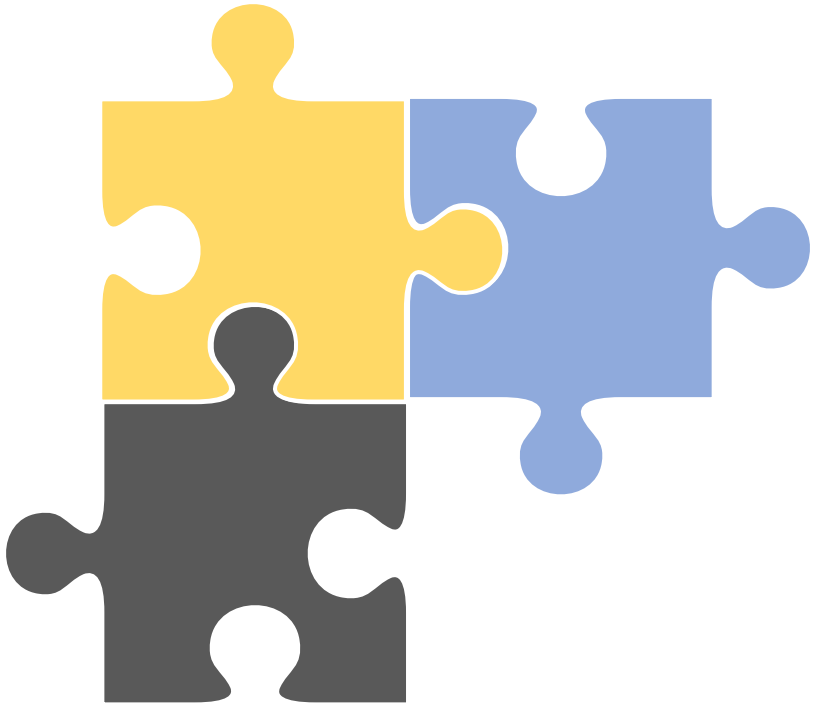
The building blocks of bitcoin

Game theory

Strategic interaction between rational decision-makers

Decentralization

Data is written down by everyone



Consensus mechanism

How do we make sure everyone is writing down the same data?

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed May 22 2019 11:58:01 GMT+0200 (Central European Summer Time).

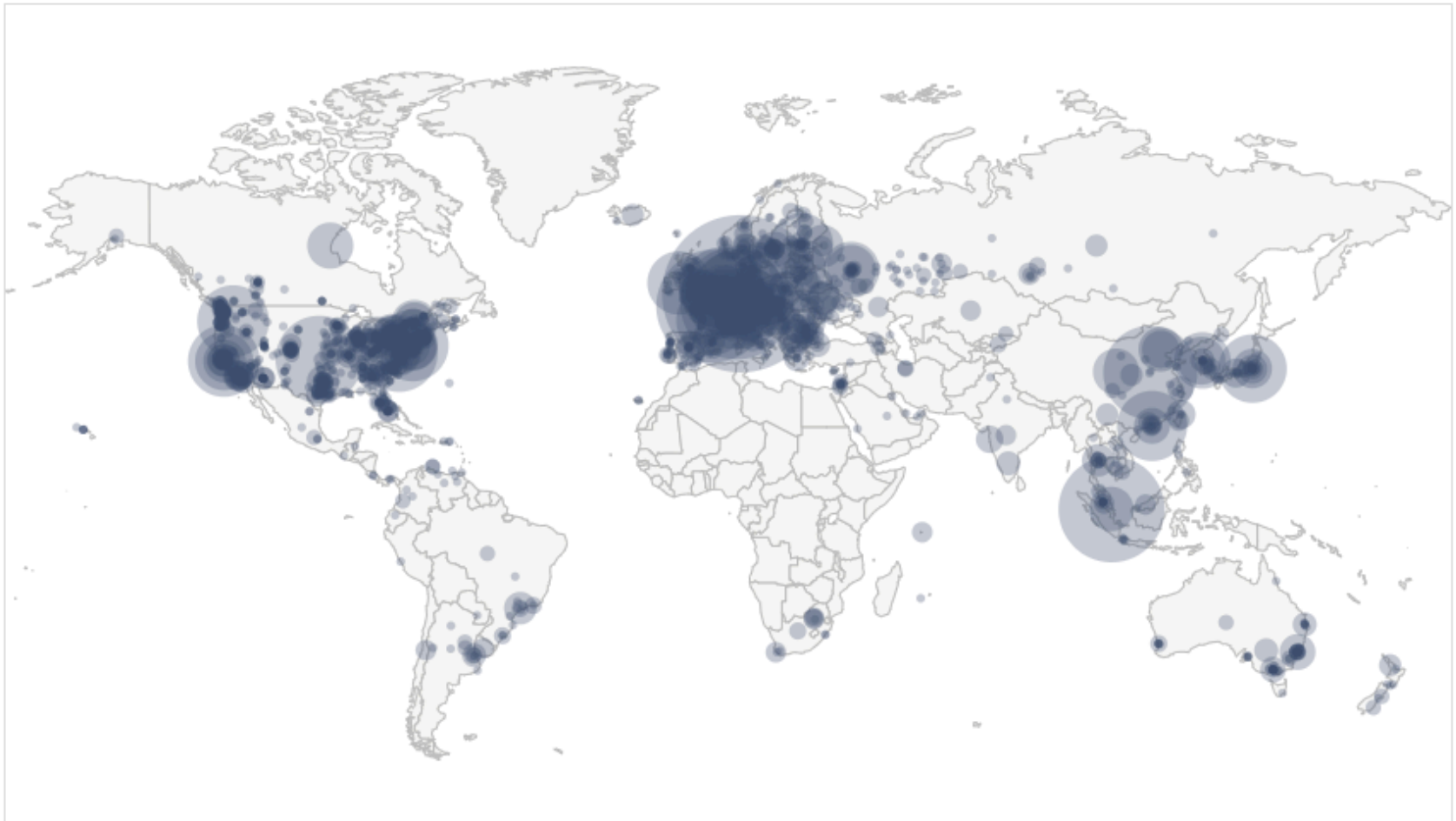
9466 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2379 (25.13%)
2	Germany	1899 (20.06%)
3	France	614 (6.49%)
4	Netherlands	516 (5.45%)
5	Canada	348 (3.68%)
6	China	312 (3.30%)
7	United Kingdom	311 (3.29%)
8	Singapore	301 (3.18%)
9	Russian Federation	244 (2.58%)
10	n/a	220 (2.32%)

More (98) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Source: https://bitnodes.earn.com/

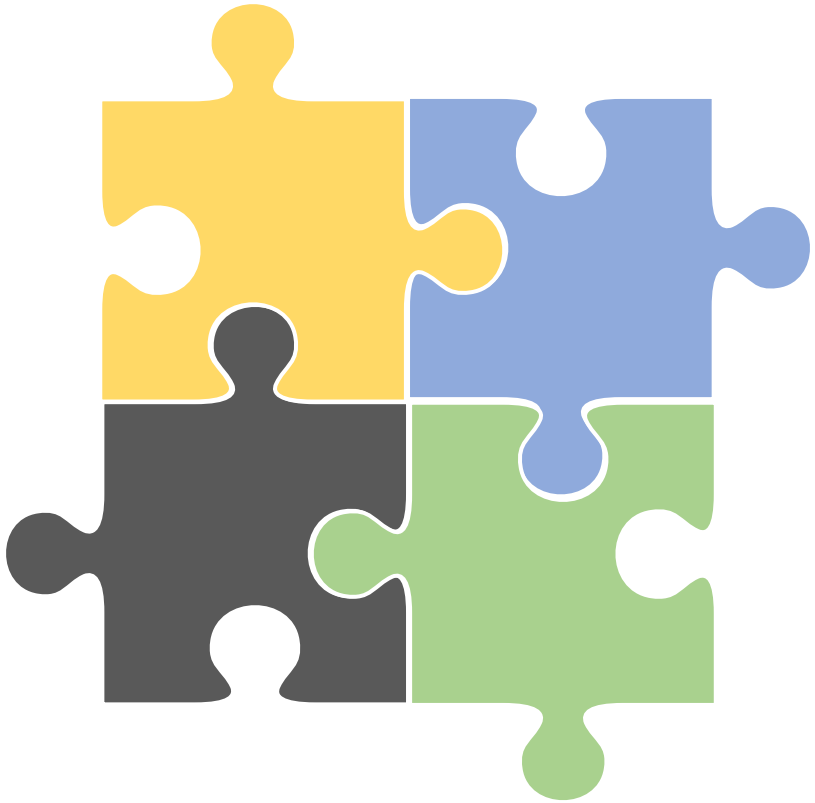
The building blocks of bitcoin

Game theory

Strategic interaction between rational decision-makers

Decentralization

Data is written down by everyone



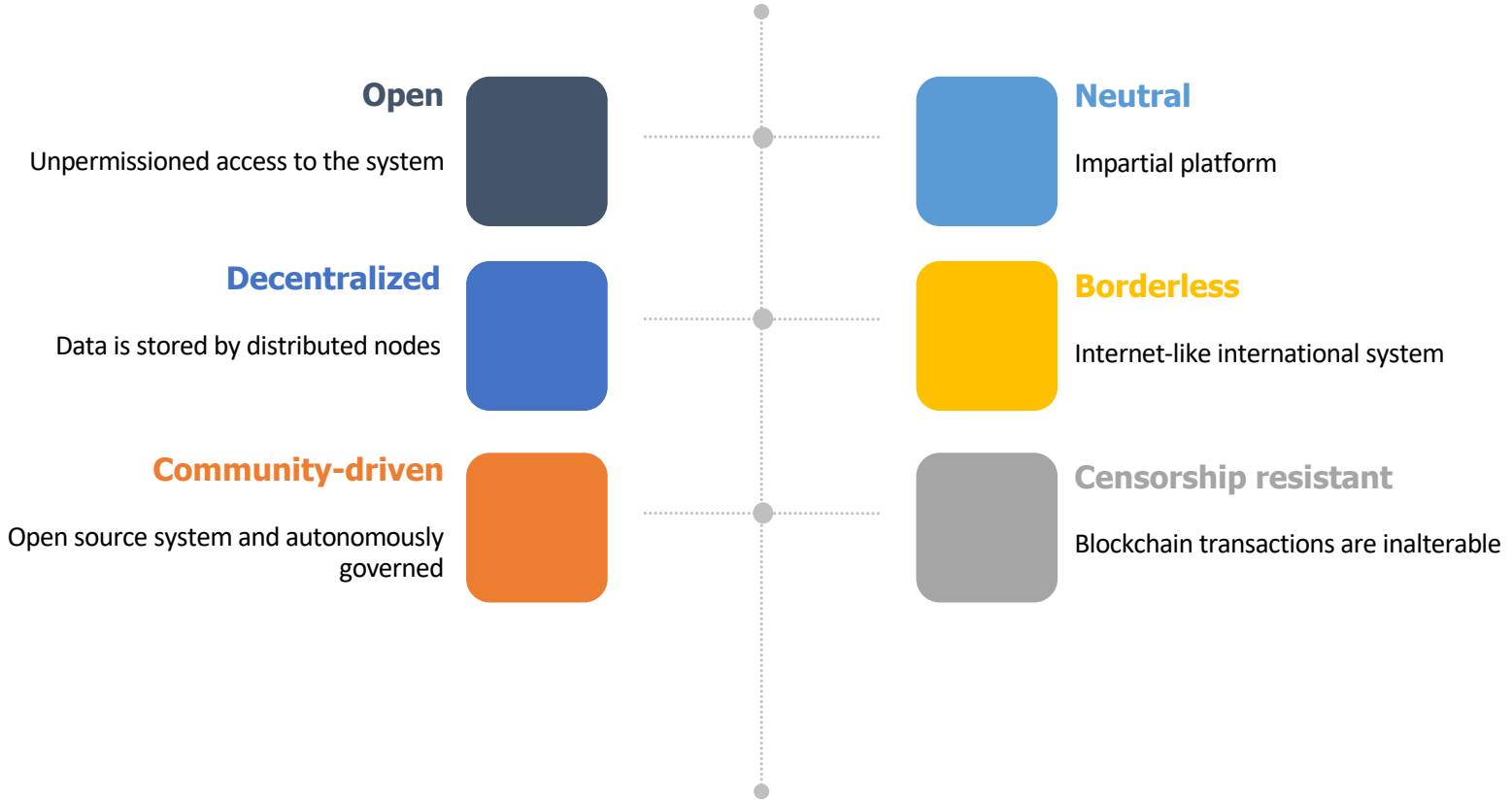
Consensus mechanism

How do we make sure everyone is writing down the same data?

Economic incentives

Reward for securing the network

Properties of open blockchains



The result

(Financial) Sovereignty

Now…

Hands-on

Zwei paar Schuhe: public vs. private ledgers

Blockchain…

…what else can we do with it?

Would you…

… enter into a contract with someone you never met before and haven‘t talked to?

… lend money to a stranger, say, a farmer in Guatemala, a young girl in China or a cashier in the UK?

… set up a contract for a 1€ purchase?

SMART CONTRACTS

on the Blockchain

A smart contract is a computer code with a predefined set of rules. It runs on a blockchain and sets the conditions under which all parties to the smart contract agree to interact with each other. It auto executes if and when all conditions are met.

"Like a cryptographic box that contains value & only unlocks if certain conditions are met"

Smart contracts eliminate the need for trusted third parties

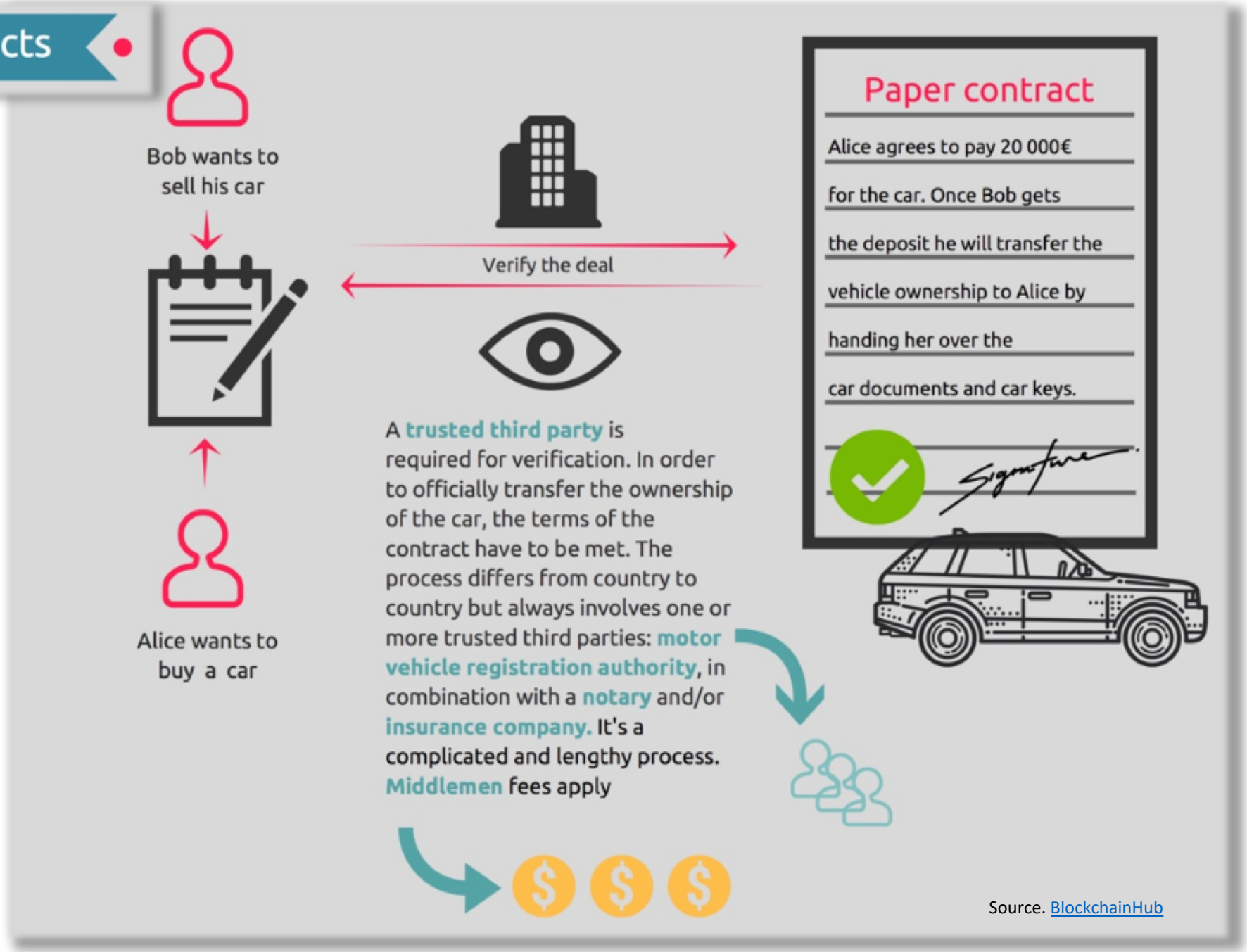
Source. BlockchainHub

Smart Contracts

Ein **Smart Contract** ist ein Computercode, der eine Reihe von Regeln enthält. Wenn und sobald diese vordefinierten Regeln erfüllt sind, wird die Vereinbarung automatisch durchgesetzt.

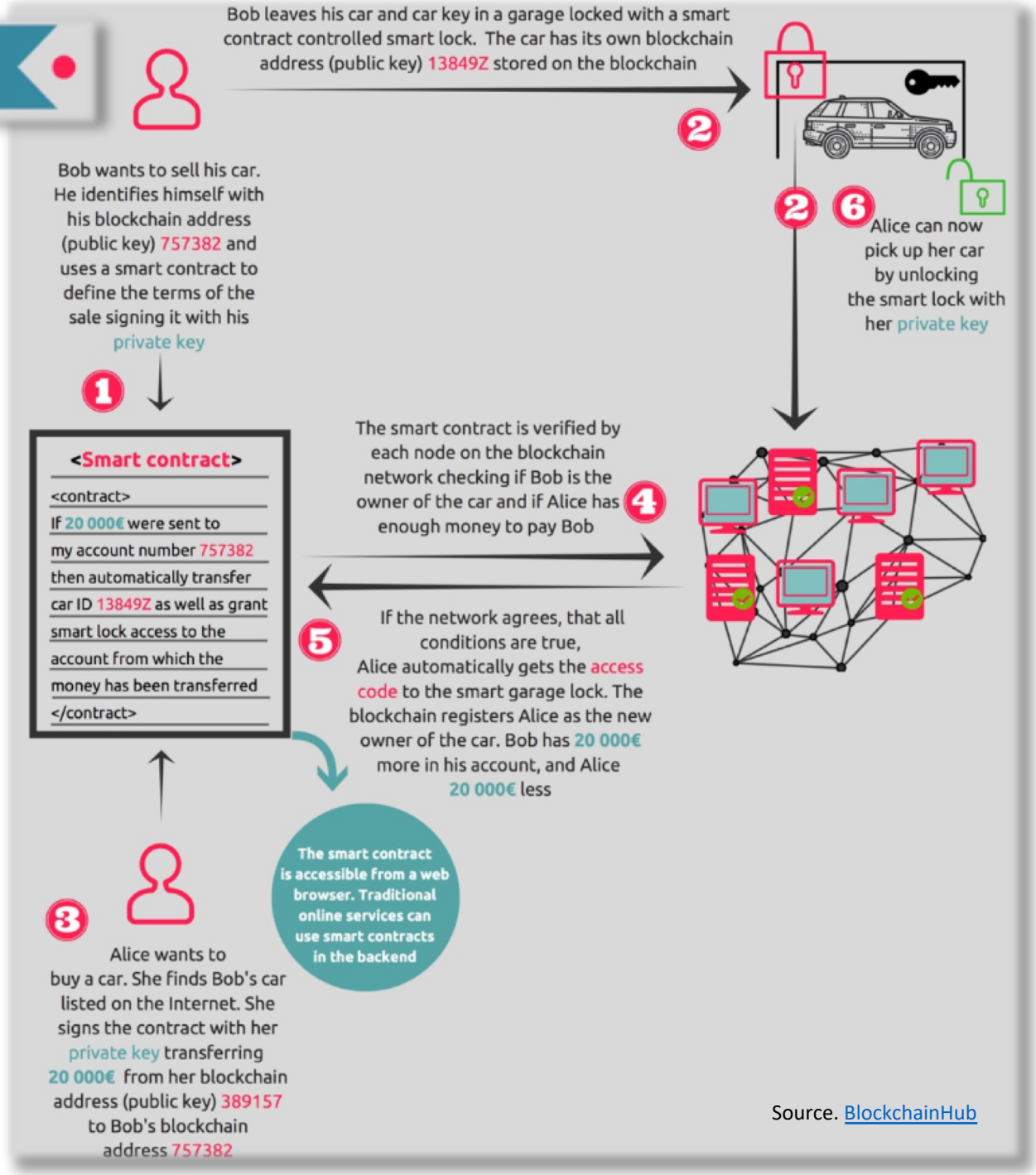
1. Arbeitet mit **WENN-DANN-Bedingungen**
2. Bedingungen werden **automatisch** ausgewertet und ausgeführt – daher **trustless**
3. Vom **Netzwerk überwacht**, daher (fast) unmöglich zu manipulieren
4. Vertrauenswürdige Ausführung impliziert **zeitnahe und objektive Transaktionen**

Traditional Contracts

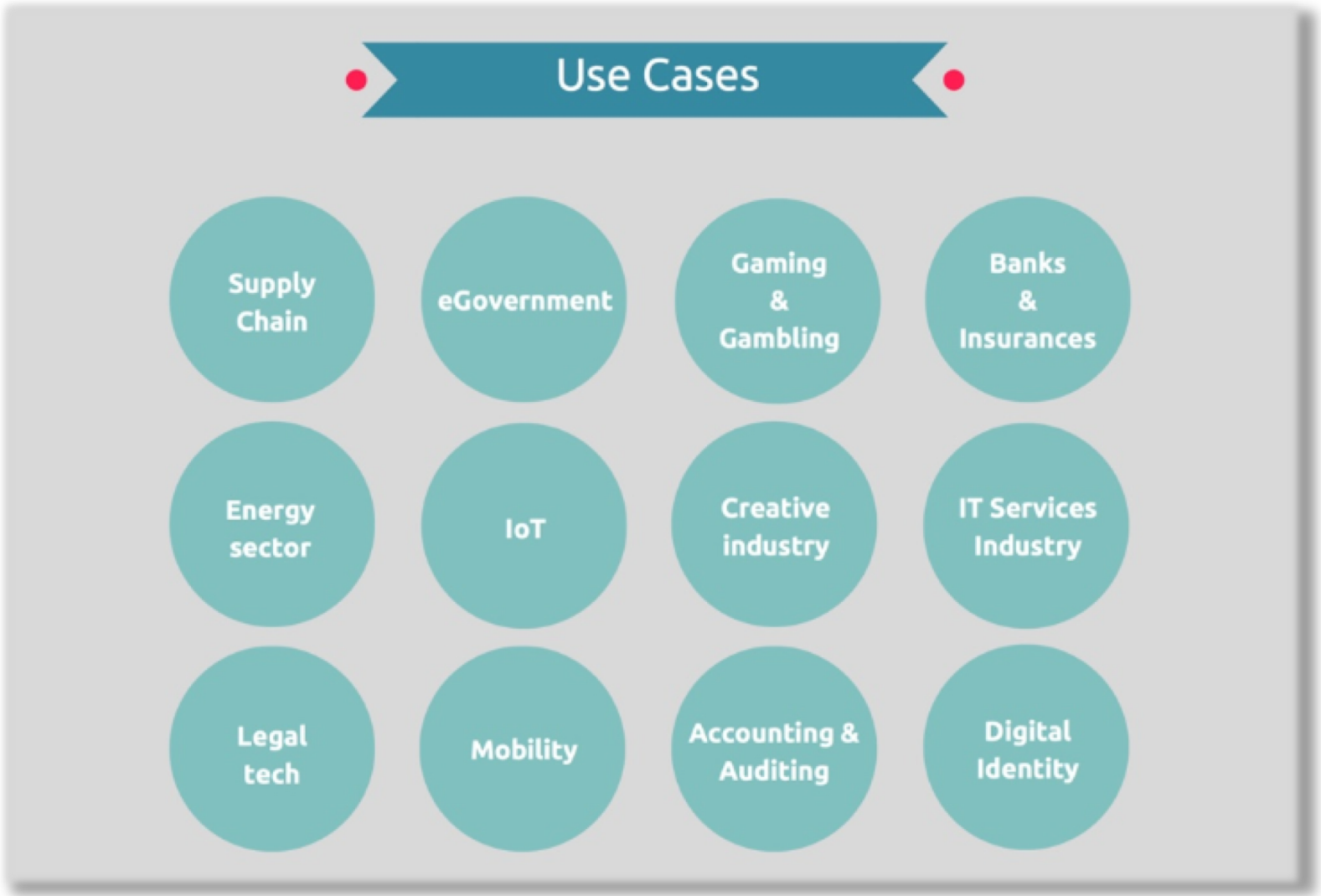


Source. BlockchainHub

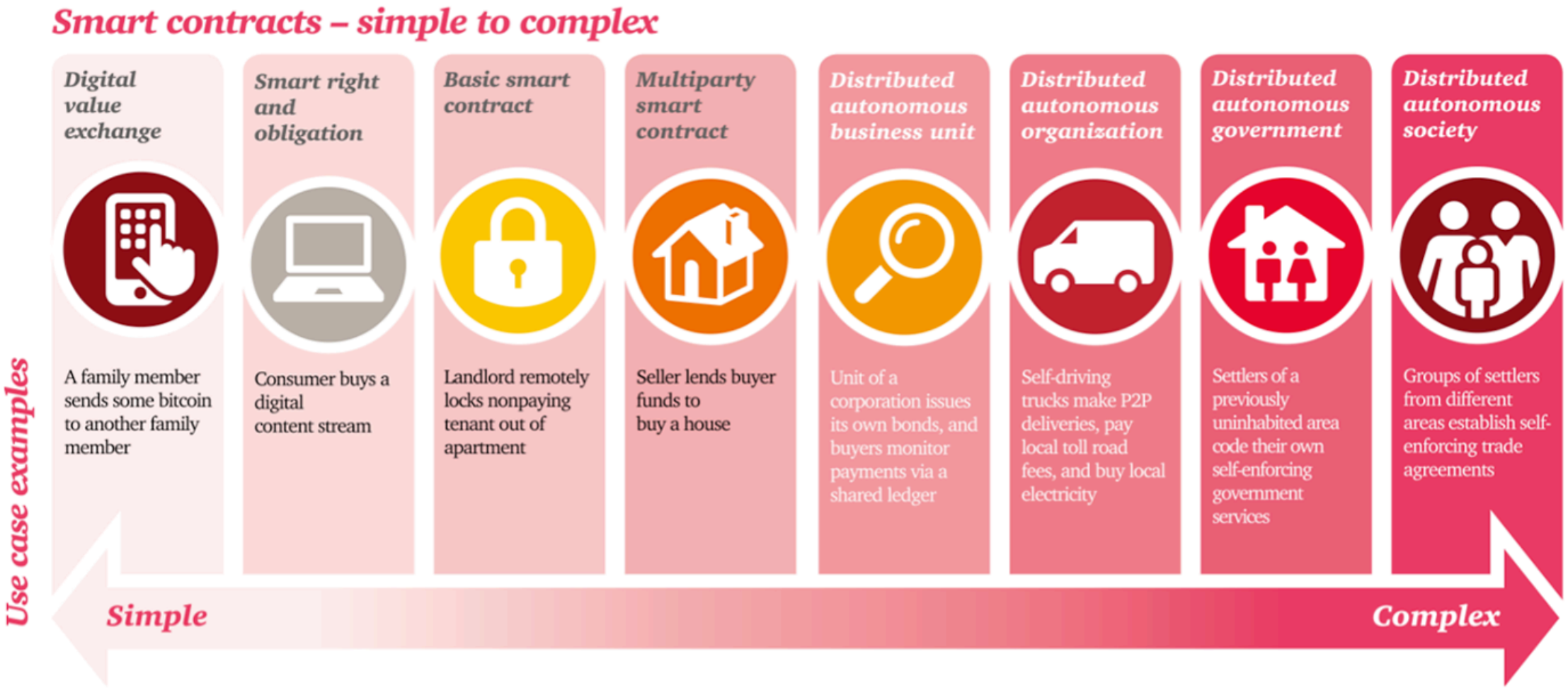
Smart Contracts



Source. [BlockchainHub]



Source. BlockchainHub


Smart contracts – simple to complex
Digital value exchange
A family member sends some bitcoin to another family member
Smart right and obligation
Consumer buys a digital content stream
Basic smart contract
Landlord remotely locks nonpaying tenant out of apartment
Multiparty smart contract
Seller lends buyer funds to buy a house
Distributed autonomous business unit
Unit of a corporation issues its own bonds, and buyers monitor payments via a shared ledger
Distributed autonomous organization
Self-driving trucks make P2P deliveries, pay local toll road fees, and buy local electricity
Distributed autonomous government
Settlers of a previously uninhabited area code their own self-enforcing government services
Distributed autonomous society
Groups of settlers from different areas establish self-enforcing trade agreements
Use case examples
Simple
Complex

Source. PwC

ZDF (1996) – Was ist das Internet?

Source. Youtube

Veronika Kütt
bitcoin. math. ultramarathon. yoga.

- Frankfurt School Blockchain Center
  - PC & PM for Blockpool.eu
- Cashlink
  - Consulting & PM: tokenised securities
- Hansecoin o.Ü.
  - Tokenised securities - hard assets
- Unchain Convention – Bitcoin Conference, Berlin

- veronika.kuett@gmail.com
- 015141641548
- Linkedin: /veronikakuett
- Twitter: veronikakuett