Blockchain

1. The hype
2. The technical background
3. What does a blockchain guarantee?
4. Pro‘s & Con‘s

UN/CEFACT whitepaper on Blockchain for trade facilitation open for comments until 21 July

How could blockchain technology be used to facilitate trade? What do government decision-makers who deal with information technology need to be aware of? And how could UNECE contribute to the development of this technology as a trade facilitation tool?

UNECE's United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) is at the forefront of these discussions and needs your input for the development of a new whitepaper.

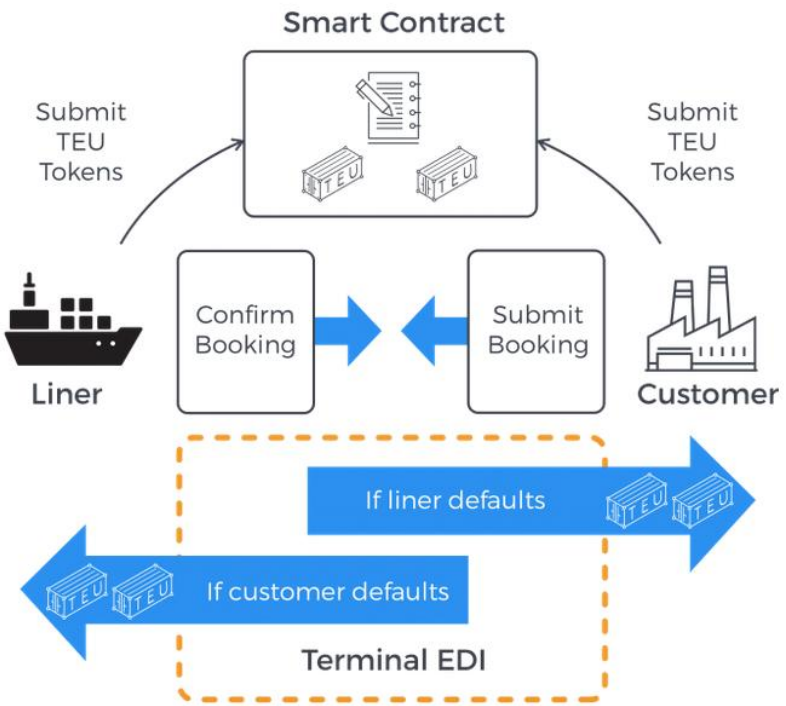
The international supply chain can be characterised as a set of three flows - of goods, funds and data. Goods flow from exporter to importer in return for funds that flow in the reverse direction. The flow of goods and funds is supported by a bidirectional flow of data such as invoices, shipping notices, bills of lading, certificates of origin and import/export declarations lodged with regulatory authorities.

https://www.unece.org/info/media/news/trade/2018/uncefact-whitepaper-on-blockchain-for-trade-facilitation-open-for-comments-until-21-july/doc.html

Blockchain initiatives in the container shipping industry

Companies	Blockchain application	Date announced	Product roll out plan
300cubits	Digital currency for use as booking deposit in container shipping transactions.	1 Aug 2017	15 Jun 2018
PIL, PSA & IBM	MOU to trial blockchain-based supply chain business network innovations chain and trade finance.	15 Aug 2017	not available
MOL, NYK, K-line with 11 Japanese companies	Consortium to develop trade data sharing platform using blockchain technology.	15 Aug 2017	not available
EY, Guardtime with Maersk & 5 partners	Blockchain platform for marine insurance industry.	6 Sep 2017	2018 onwards
HMM & Samsung SDS	Pilot testing systems for encrypted sharing of data in shipping transactions.	7 Sep 2017	not available
Maersk & IBM JV	Blockchain applications to digitize global trade processes with initial focus on paperless trade and shipping information pipeline.	16 Jan 2018	within 6 months

Alphaliner, Weekly Newsletter, Issue 05, Volume 2018, 24.1.-30.1.2018



„300cubits ist eine Blockchain-Lösung für die Containerschifffahrt, die durch die Ausgabe einer digitalen Währung namens TEU-Token realisiert wurde. …
Phase 1 des Projekts ist die Einführung vom TEU-Token als Anzahlung für die Reservierungsbuchung, die über ein Buchungskautionsmodul ausgeführt wird, um die branchenspezifischen Probleme von No Show und Verspätungen zu lösen. No Show bezieht sich auf den Fall, dass Kunden einen Frachtplatz buchen, aber nicht mit Fracht erscheinen, während Verspätungen passieren, wenn Linienschiffe eine Buchung akzeptieren, aber die Ladung nicht entsprechend beladen. Zusammen kosten diese Schmerzpunkte die Containerschifffahrtindustrie jährlich 23 Mrd. Dollar an Verlusten.“

“300cubits is a blockchain solution for the container shipping industry, realized through the issuance of a digital currency called TEU Tokens. …
Phase 1 of the project is to introduce TEU Tokens as a shipping booking deposit executed through a Booking Deposit Module to tackle the industry pain points of No Show and Rolling. No Show refers to the case where customers book a shipping slot but do not show up with cargo while Rolling occurs where liners accept a booking but fail to load the cargo accordingly. Together, these pain points cost the container shipping industry $23bn of losses annually.”

https://300cubits.tech/pdf/whitepaper_2.0_german.pdf
https://300cubits.tech/pdf/whitepaper_2.0.pdf

DNV·GL

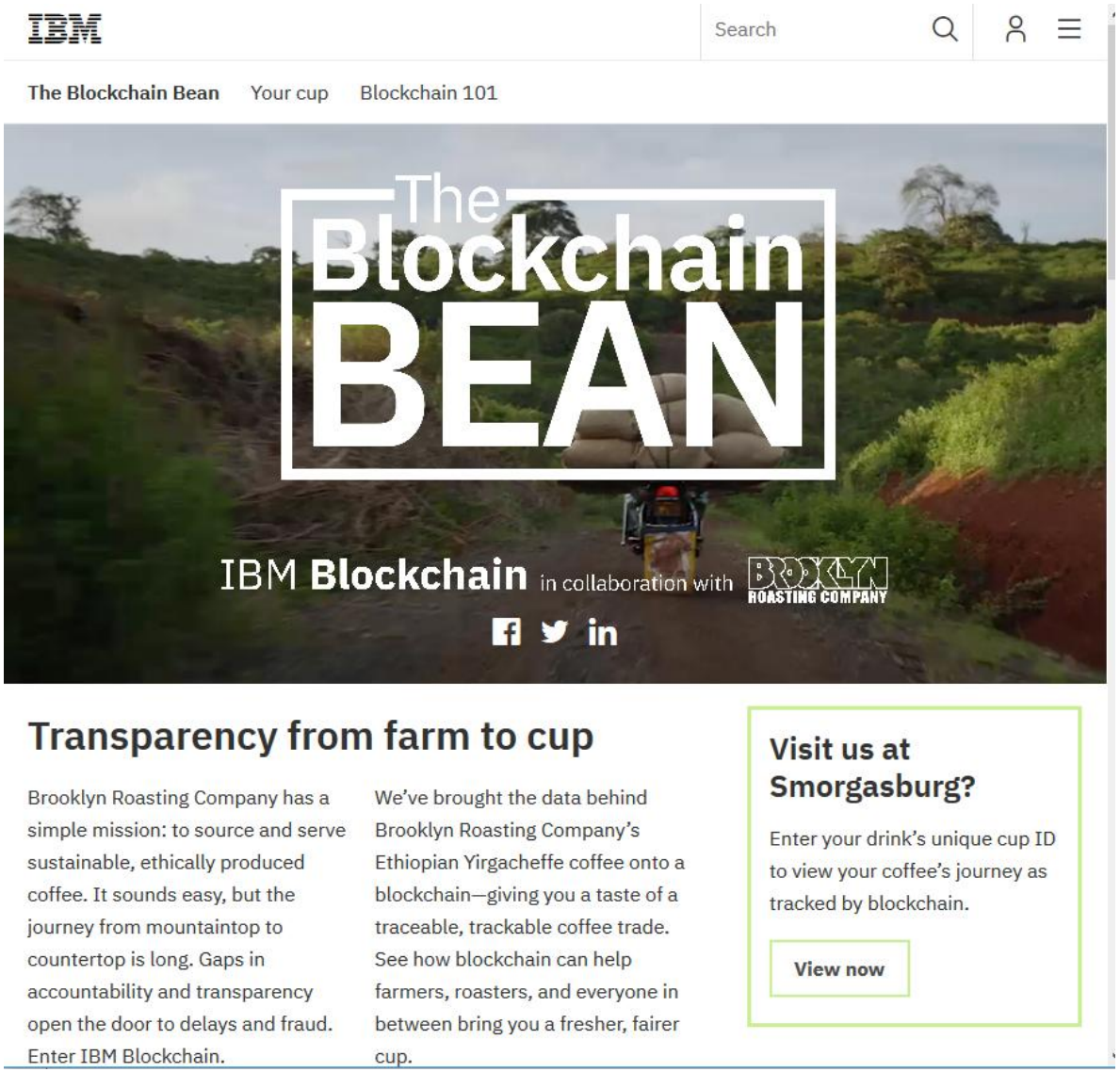
Sehr geehrter Herr Stern,

anbei übersenden wir Ihnen die finale PDF-Version Ihres neuen elektronischen Zertifikates, inklusive des neuen QR Codes.

Wie Sie unserer **Kundeninformation vom 28.09.2017** entnehmen konnten, sind seit September 2017 alle DNV GL Zertifikate in unserer ersten Blockchain-Anwendung gespeichert. Ihr Zertifikat ist damit eindeutig identifizierbar, rückverfolgbar und wird sicher aufbewahrt - dank einer Technologie, die Fälschungen und unsachgemäßen Gebrauch verhindert und leicht erkennbar macht.

Mittels des QR-Code können ab sofort die Daten Ihres Zertifikats in der Blockchain von Interessierten Parteien über einen einfachen Scan mit dem Smartphone überprüft werden.

Our ISO 9001 certificate



https://www.ibm.com/thought-leadership/blockchainbean/

The „coffee blockchain“

Industriekonsortium testet erfolgreich Blockchain-Lösung

CONTAINERSCHIFFFAHRT | Ein Konsortium aus AB InBev, Accenture, APL, Kühne + Nagel sowie einer europäischen Zollbehörde hat den Testeinsatz einer Blockchain-Lösung für die Containerschifffahrt erfolgreich abgeschlossen – das teilt das an dem Test beteiligte Unternehmen Accenture mit. Die Lösung ersetzt gedruckte Frachtdokumente und könnte den Angaben zufolge dazu beitragen, mehrere hundert Millionen Euro jährlich in der Transport- und Logistikindustrie zu sparen.

Die vom Konsortium getestete Lösung macht den bisher gängigen physischen oder digitalen Austausch von Dokumenten überflüssig, so Accenture. Stattdessen werden die Frachtdaten über die Blockchain verbreitet und den beteiligten Akteuren zugänglich gemacht. Nach dem Single-Ownership-Prinzip sind die jeweiligen Informationen klar einem bestimmten Besitzer innerhalb der Frachtkette zugeordnet. Für die Lösung wurden zunächst die heutigen Dokumentationsprozesse analysiert, um anschließend festzulegen, wie sich der Besitz von Informationen sowie Verantwortlichkeiten und Risiken neu ordnen lassen. Die Blockchain würde dabei den Vorteil bieten, dass sie nicht manipulierbar sei und höchsten Sicherheitsanforderungen entspreche.

Accenture zufolge sind für das internationale Verfrachten von Waren, wie etwa Fahrzeugen oder Konsumgütern, nicht selten mehr als zwanzig unterschiedliche und zumeist papierbasierte Dokumente nötig; zusammengenommen würden sich jedoch etwa 70 Prozent der Informationen aus diesen Dokumenten elektronisch abbilden lassen. Große Nachteile der heute genutzten Dokumentationsverfahren seien die geringe Qualität sowie der fehlende Echtzeitzugriff auf diese Daten. Dieses Problem würde alle am Warenaustausch beteiligten Akteure gleichermaßen betreffen und vor allem zu Verzögerungen bei der finanziellen Abwicklung im Warenverkehr führen.

Mithilfe der neuen Lösung soll sich der Austausch von Frachtdokumenten zukünftig erheblich beschleunigen lassen. So würden bis zu 80 Prozent der heute nötigen manuellen Dateneingaben entfallen und Änderungen an den Daten könnten über den gesamten Transportprozess hinweg deutlich einfacher vorgenommen werden. Weiterhin würde die Überprüfung des Frachtguts durch den Zoll vereinfacht werden und somit die Gefahr von Strafzahlungen aufgrund falscher Angaben deutlich verringert. Der Test zeigte, dass der Einsatz der Blockchain nicht nur Kosten im Containerschiffsverkehr reduziert, sondern auch die Transparenz über die gesamte Supply Chain hinweg steigert.

Im Rahmen des Testeinsatzes der Blockchain-Lösung wurden zwölf Containertransporte per Schiff in verschiedene Zielhäfen geschickt, die jeweils in Ländern mit unterschiedlichen regulatorischen Bestimmungen lagen. Die am Konsortium beteiligten Firmen stehen dabei repräsentativ für die einzelnen Abläufe während eines typischen Verschiffungsvorgangs von Waren: AB InBev als Exporteur von Waren, APL als Reederei, Kühne + Nagel als Speditionsunternehmen sowie eine europäische Zollbehörde und die damit verbundenen Dokumentationspflichten bei der Ein- und Ausfuhr von Waren.

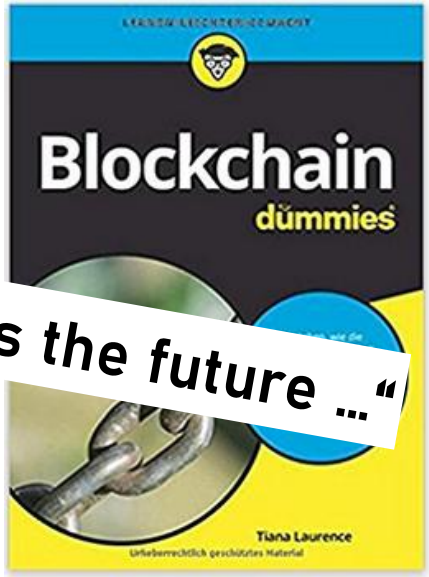
Accenture brachte seine Technologie- und Beratungsexpertise rund um die Blockchain mit ein und entwickelte die technische Architektur, auf der die getestete Blockchain-Lösung aufbaut. Dafür zeichnete dem Unternehmen zufolge vor allem das „Internet of Things"-Kompetenzzentrum von Accenture in Singapur verantwortlich, wo innerhalb kürzester Zeit der entsprechende Prototyp entwickelt wurde.

64 Schiff&Hafen | Mai 2018 | Nr. 5

1. The hype
2. The technical background
3. What does a blockchain guarantee?
4. Pro‘s & Con‘s

„Blockchain is important …“

„Blockchain is the future …“



„Blockchain is safe …“

???

Who explains it to me??

Eine Blockchain… ist eine **kontinuierlich erweiterbare Liste von Datensätzen**, genannt „Blöcke“, welche mittels kryptographischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptographisch sicheren Hash (Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten.

Der Begriff Blockchain wird allgemeiner für ein Konzept genutzt, mit dem ein Buchführungssystem **dezentral** geführt werden kann und dennoch ein Konsens über den richtigen Zustand der Buchführung erzielt wird, auch wenn viele Teilnehmer an der Buchführung beteiligt sind. …

Worüber in dem Buchführungssystem Buch geführt wird, ist für den Begriff der Blockchain unerheblich. Entscheidend ist, dass spätere Transaktionen auf früheren Transaktionen aufbauen und diese als richtig bestätigen, indem sie die Kenntnis der früheren Transaktionen beweisen. Damit wird es **unmöglich** gemacht, Existenz oder Inhalt der früheren Transaktionen **zu manipulieren** oder zu tilgen, ohne gleichzeitig alle späteren Transaktionen ebenfalls zu zerstören, die die früheren bestätigt haben. Andere Teilnehmer der dezentralen Buchführung, die noch Kenntnis der späteren Transaktionen haben, würden eine manipulierte Kopie der Blockchain ganz einfach daran erkennen, dass sie Inkonsistenzen in den Berechnungen aufweist.

Quelle: https://de.wikipedia.org/wiki/Blockchain

A blockchain… is a **continuously growing list of records**, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data.

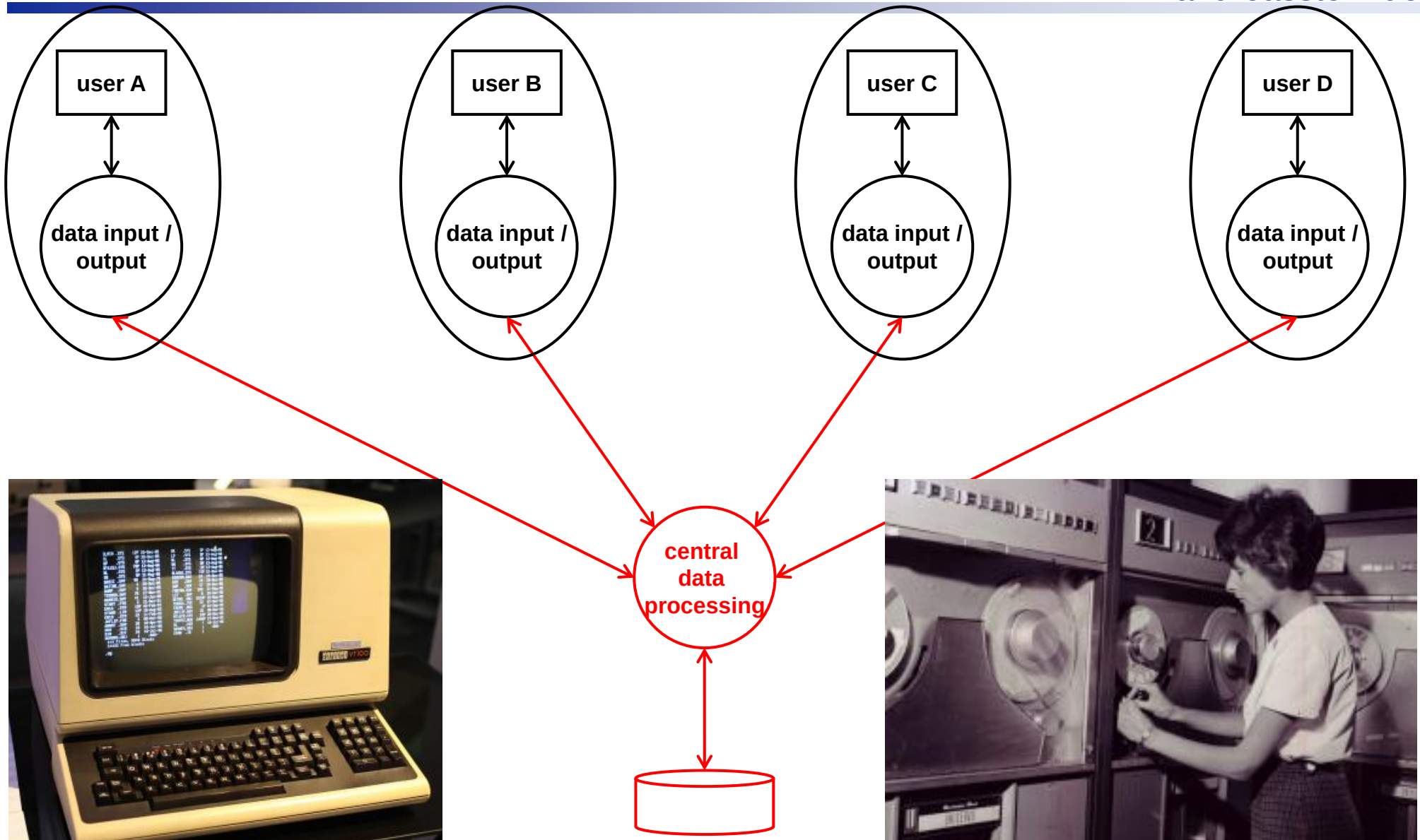
By design, a blockchain is inherently resistant to modification of the data. It is "an open, **distributed** ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block **cannot be altered** retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

… This makes blockchains potentially suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, food traceability or voting.

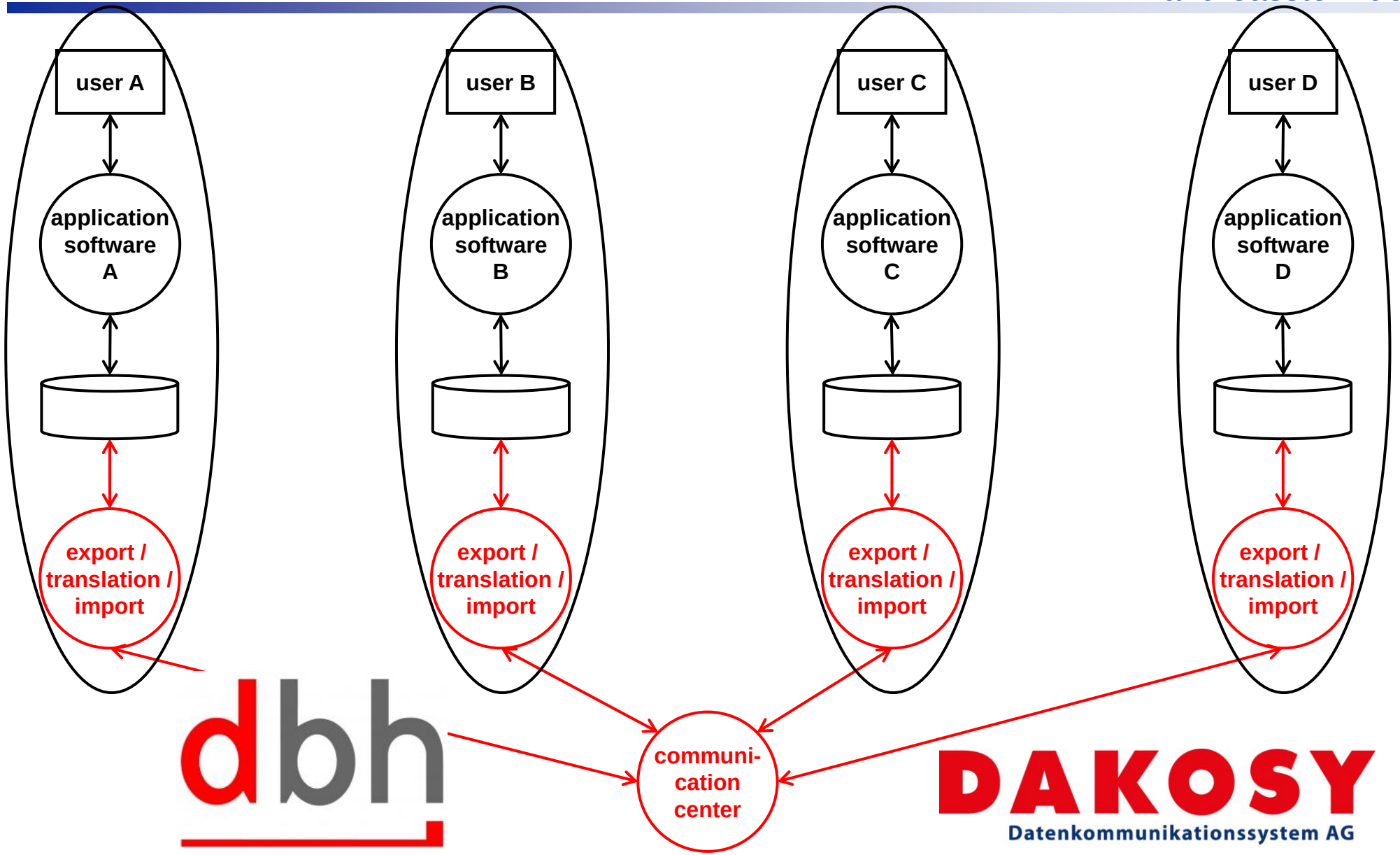
Blockchain was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server.

Source: https://en.wikipedia.org/wiki/Blockchain

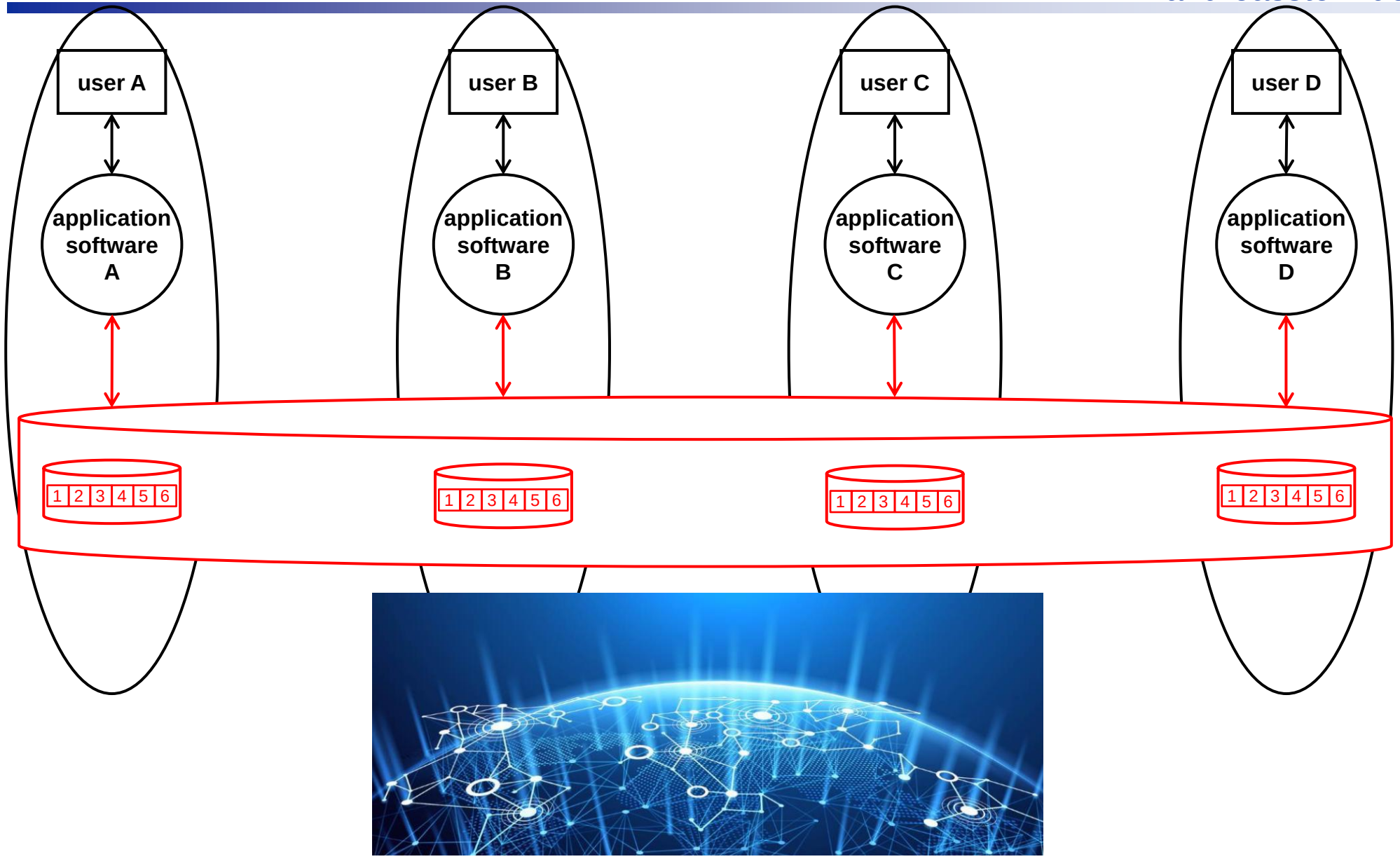
Let‘s go some decades back in time …



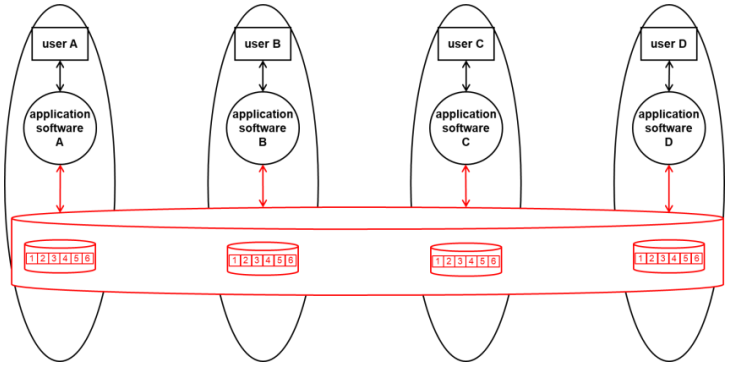
In ealier times: The data processing center



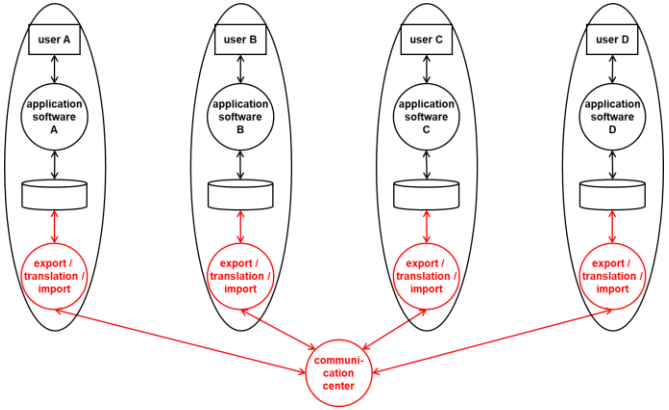
Nowadays: The communication center



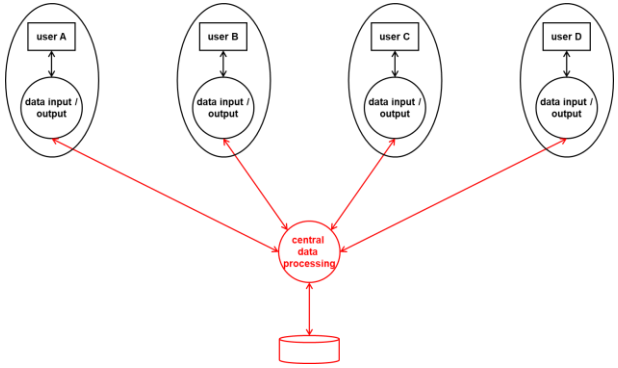
In future: The blockchain



virtually central data storage
decentral data processing

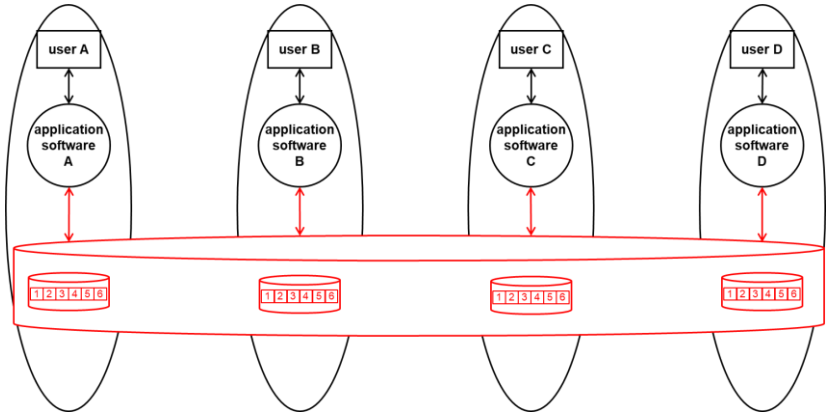


decentral data storage
decentral data processing
message exchange



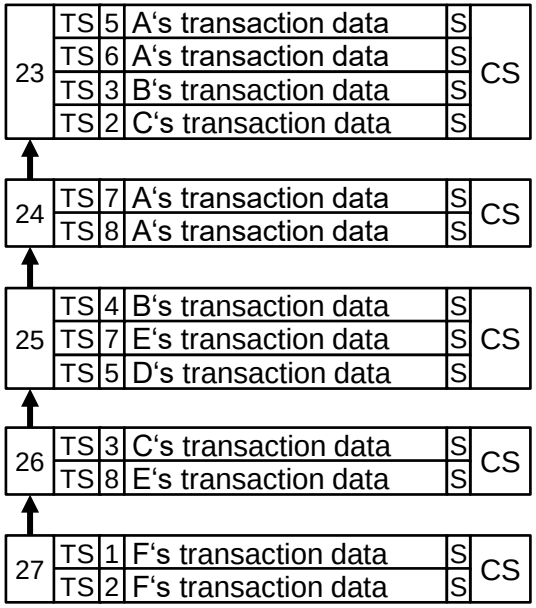
central data storage
central data processing

„Back to the future“



There is no center. All data are stored decentralized in form of identical copies at all nodes of the blockchain.

Each node has all data and can always look at them. Everybody can track all transactions, which have ever been made in the system.



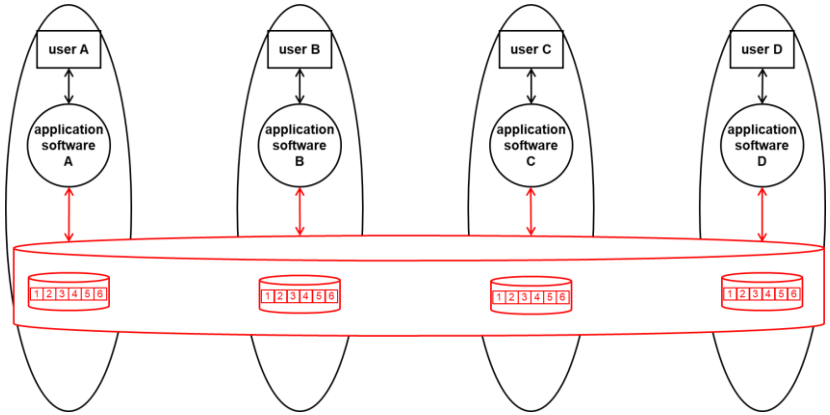
The data are stored in blocks which form a chain.

Each block has a serial number, which points to the preceeding block.

One block may contain several transactions of different users.

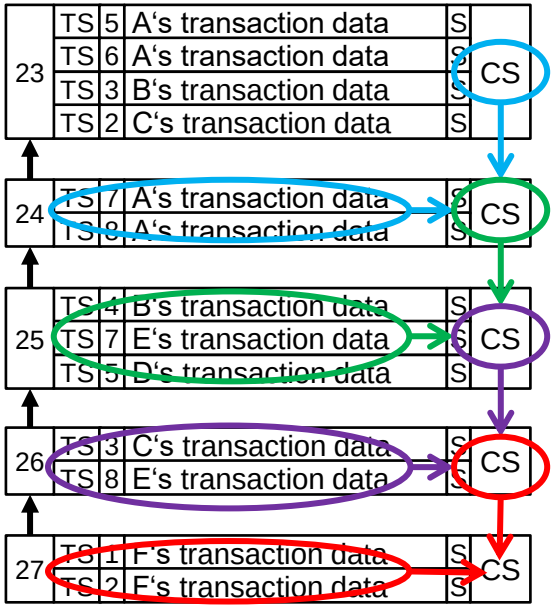
Each transaction contains a user specific serial number, a time stamp (TS) and a digital signature (S).

„transaction“ = sell or buy something, send or receive something, …



There is no center. All data are stored decentralized in form of identical copies at all nodes of the blockchain.

Each node has all data and can always look at them. Everybody can track all transactions, which have ever been made in the system.



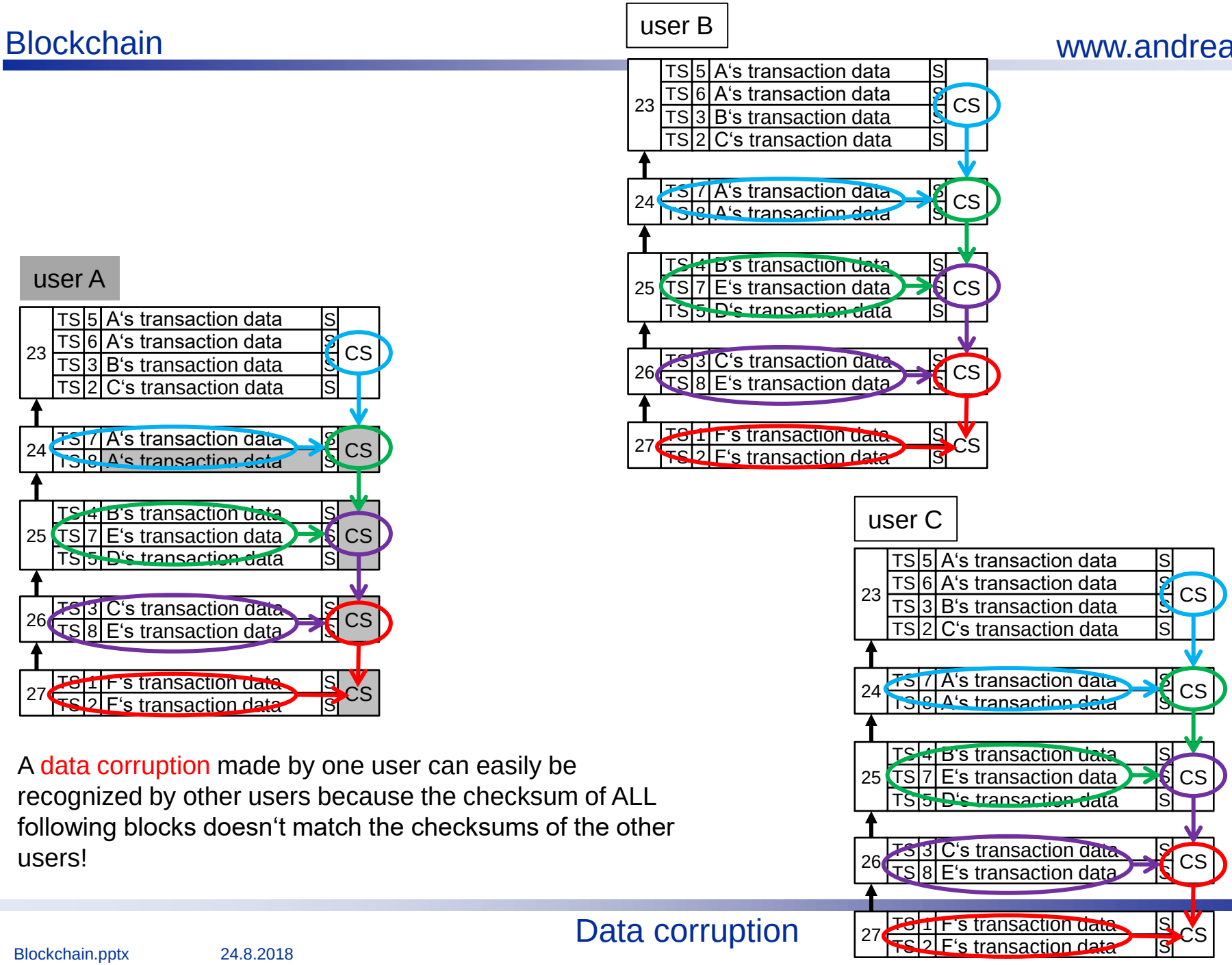
The data are stored in blocks which form a chain.

Each block has a serial number, which points to the preceeding block.

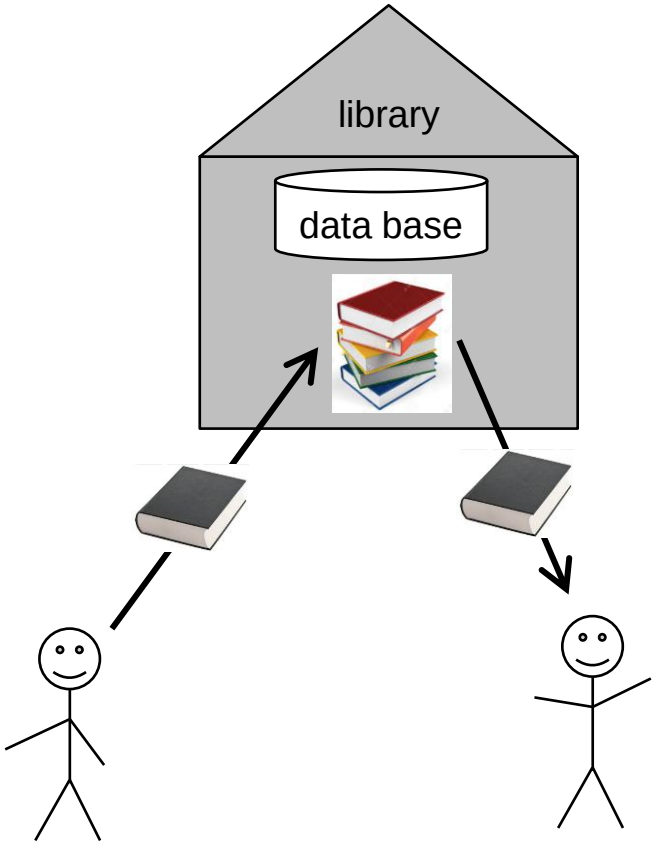
One block may contain several transactions of different users.

Each transaction contains a user specific serial number, a time stamp (TS) and a digital signature (S).

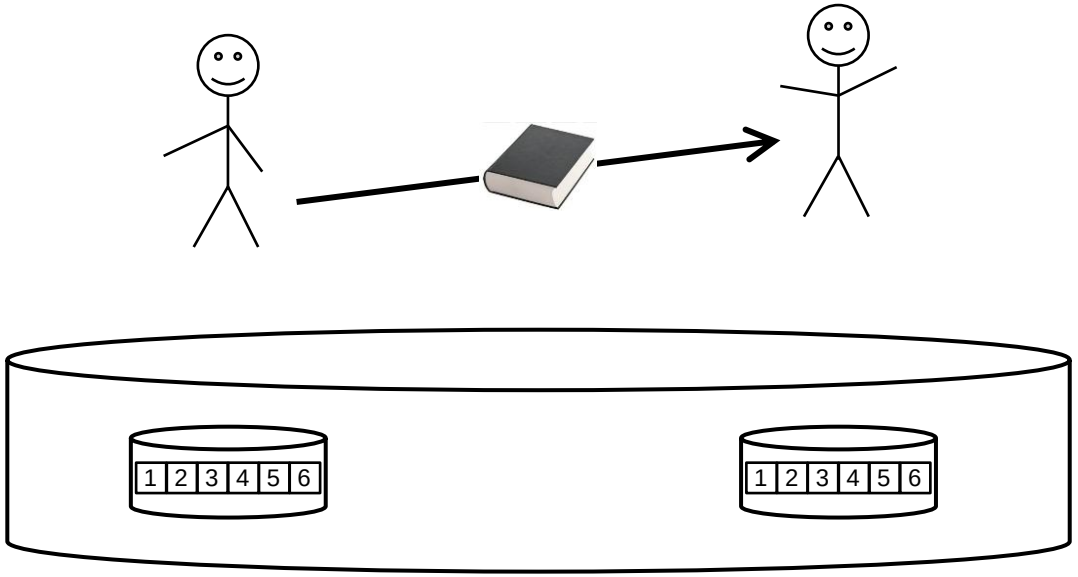
Each block contains a checksum (CS), which is calculated from the transaction data and the checksum of the preceeding block.



A data corruption made by one user can easily be recognized by other users because the checksum of ALL following blocks doesn‘t match the checksums of the other users!



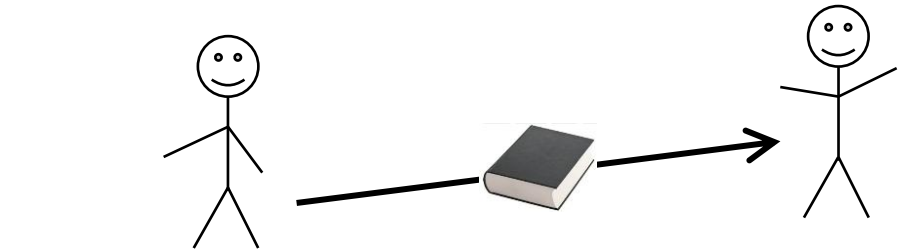
The transaction („to loan a book“) needs a broker (the library) and is recorded in a centralised data base.

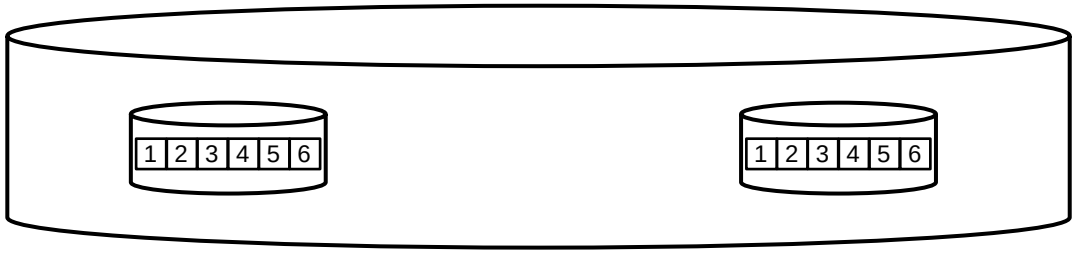


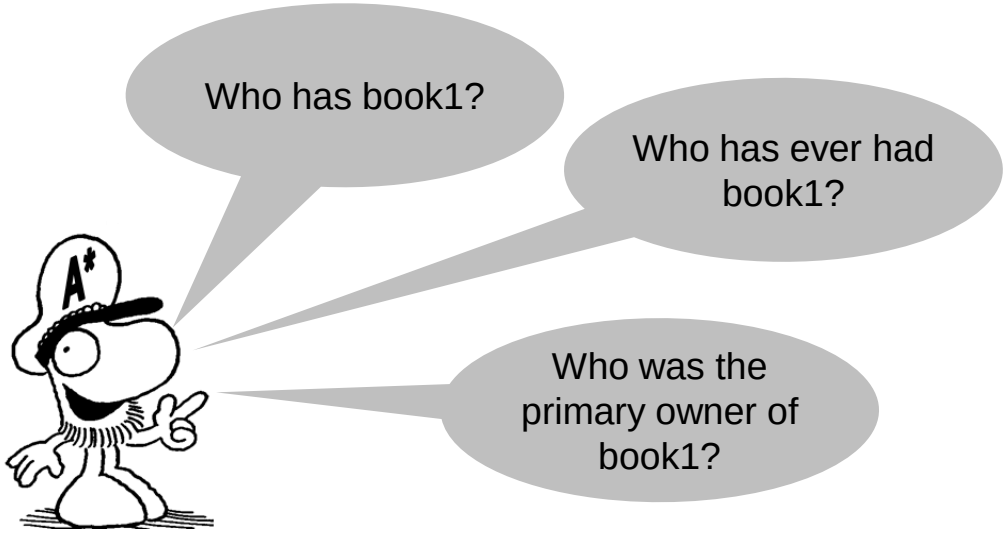
The transaction („to loan a book“) is executed directly without a broker (the library) and is recorded in a distributed blockchain.

Everybody can see at any time, who has loaned which book from whom!

23	TS	5	A has loaned book1 to B	S	CS
	TS	6	A has loaned book2 to B	S	
	TS	3	B has loaned book1 to C	S	
	TS	2	C has loaned book1 to D	S	
24	TS	7	A has loaned book3 to D	S	CS
	TS	8	A has loaned book4 to C	S	
25	TS	4	B has loaned book2 to E	S	CS
	TS	7	E has loaned book2 to F	S	
	TS	5	D has loaned book1 to E	S	
26	TS	3	C has loaned book4 to F	S	CS
	TS	8	E has loaned book1 to G	S	
27	TS	1	F has loaned book2 to G	S	CS
	TS	2	F has loaned book4 to H	S	



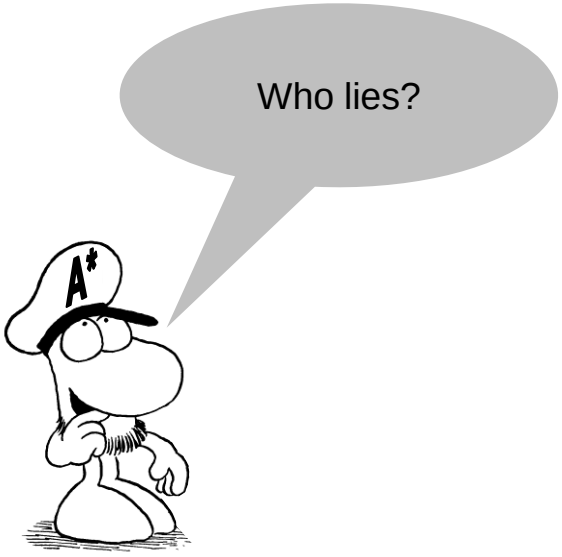


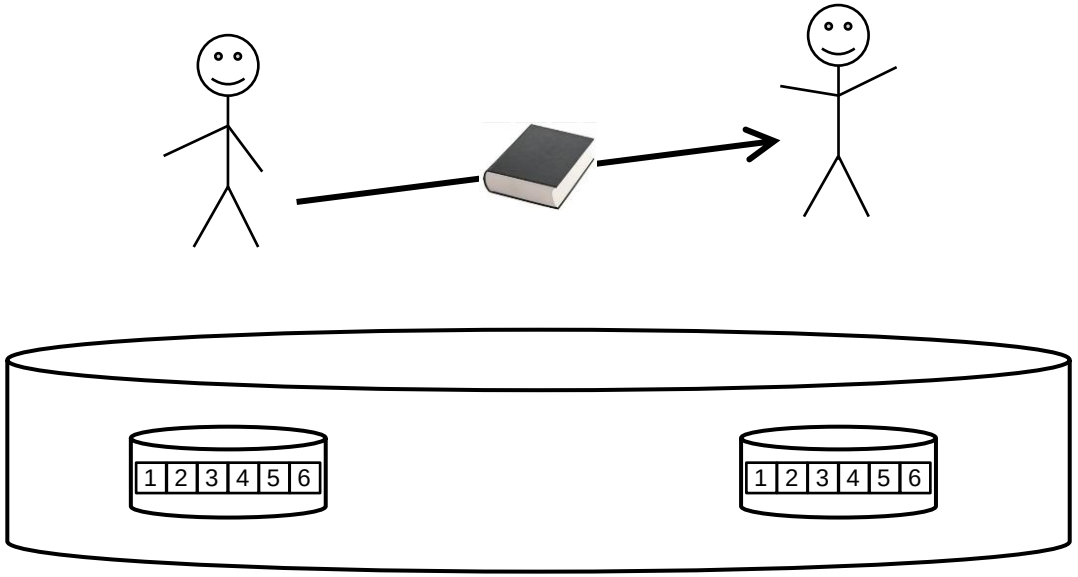


The transaction („to loan a book“) is executed directly without a broker (the library) and is recorded in a distributed blockchain.

Everybody can see at any time, who has loaned which book from whom!

23	TS	5	A has loaned book1 to B	S	CS
	TS	6	A has loaned book2 to B	S	
	TS	3	B has loaned book1 to C	S	
	TS	2	C has loaned book1 to D	S	
24	TS	7	A has loaned book3 to D	S	CS
	TS	8	A has loaned book4 to C	S	
25	TS	4	B has loaned book2 to E	S	CS
	TS	7	E has loaned book3 to F	S	
	TS	5	D has loaned book1 to E	S	
26	TS	3	C has loaned book4 to F	S	CS
	TS	8	E has loaned book1 to G	S	
27	TS	1	F has loaned book2 to G	S	CS
	TS	2	F has loaned book4 to H	S	



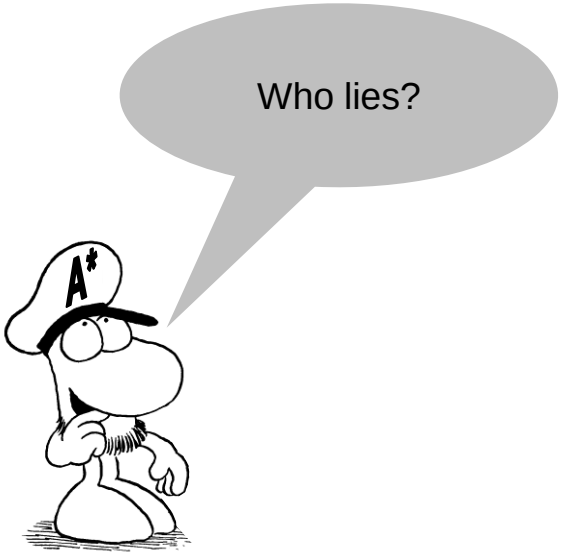


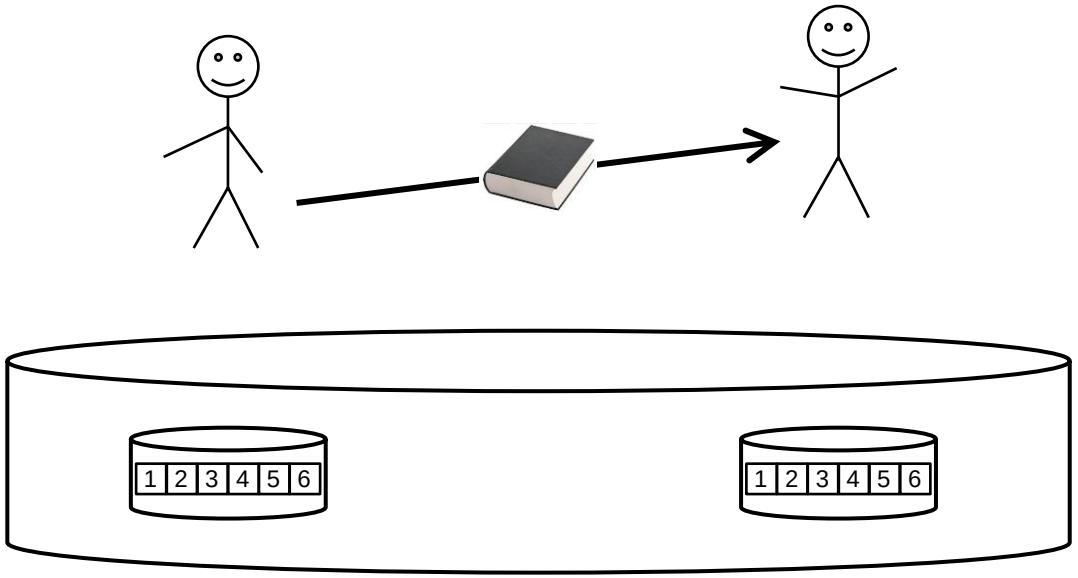
The transaction („to loan a book“) is executed directly without a broker (the library) and is recorded in a distributed blockchain.

Everybody can see at any time, who has loaned which book from whom!

Data corruption can easily be detected

23	TS	5	A has loaned book1 to B	S	CS
	TS	6	A has loaned book2 to B	S	
	TS	3	B has loaned book1 to C	S	
	TS	2	C has loaned book1 to D	S	
24	TS	7	A has loaned book3 to D	S	CS
	TS	8	A has loaned book4 to C	S	
25	TS	4	B has loaned book2 to E	S	CS
	TS	7	E has loaned book3 to F	S	
	TS	5	D has loaned book1 to E	S	
26	TS	3	C has loaned book4 to F	S	CS
	TS	8	E has loaned book1 to G	S	
27	TS	1	F has loaned book2 to G	S	CS
	TS	2	F has loaned book4 to H	S	

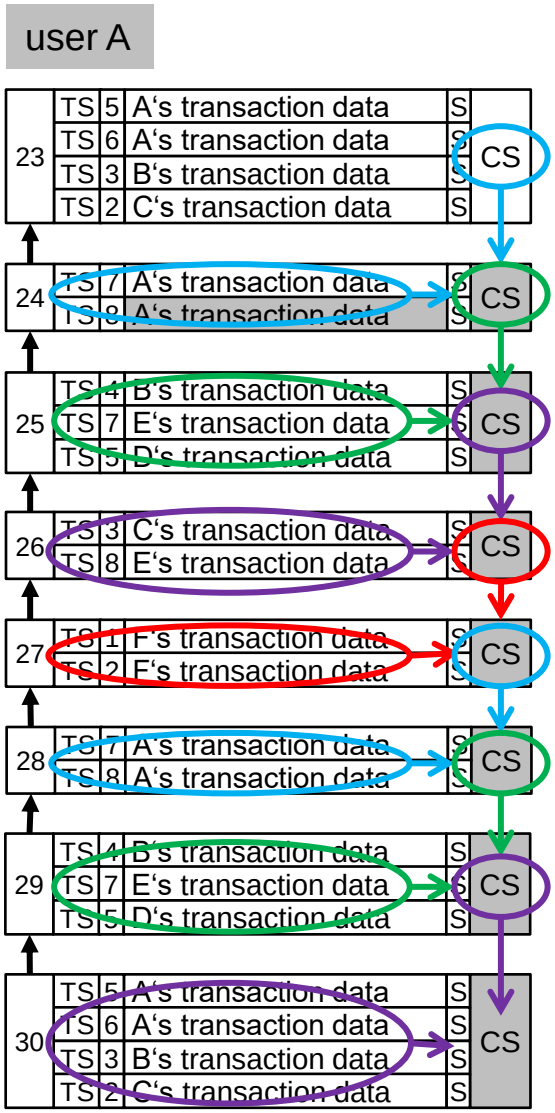




The transaction („to loan a book“) is executed directly without a broker (the library) and is recorded in a distributed blockchain.

Everybody can see at any time, who has loaned which book from whom!

Data corruption can easily be detected

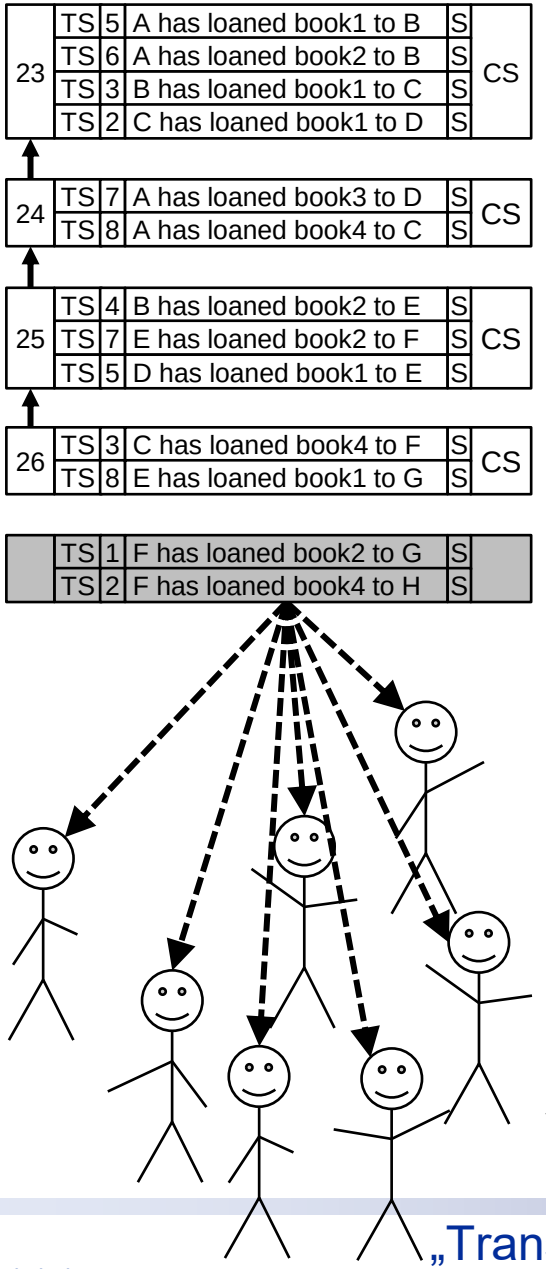


The technical effort to add a block to a blockchain is very large (solution of the riddle and calculation of the checksum)

For a corruption of a data block all checksums of all the following blocks must be re-calculated.

„The Bitcoin network estimates, that it is impossible to change a transaction after six new blocks have been added, because the IT efford would be too large… Some companies wait for six confirmations (=new blocks) before they can be sure, that a transaction can not be changed after it has been added to the blockchain.“

(Mark Gates: „Blockchain“)



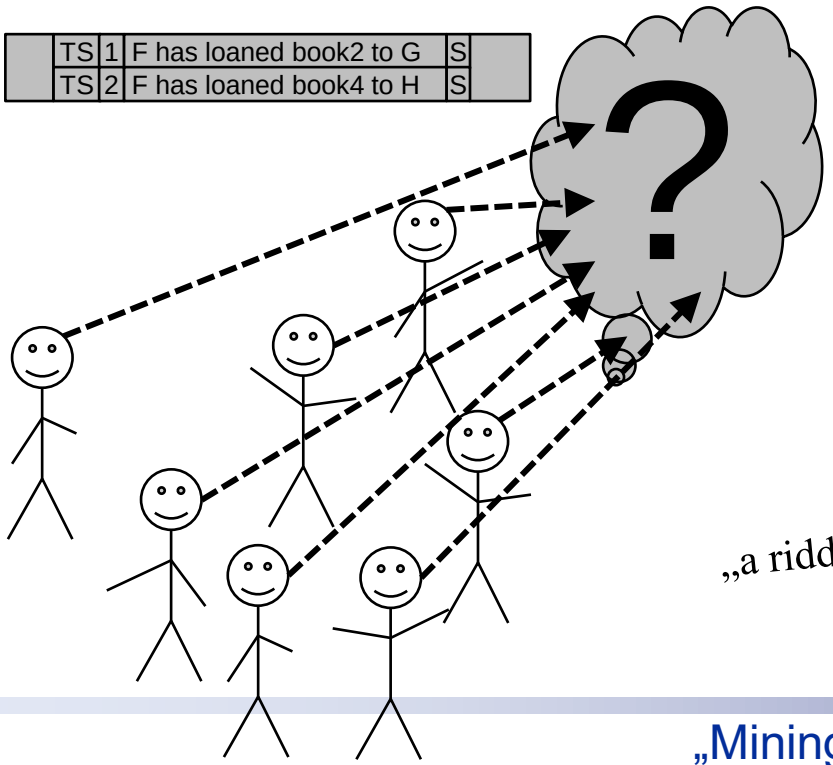
51% = OK

A „candidate block“ (a ledger) can be added to a blockchain – if …

… the majority of the blockchain nodes (=51%) agree, that the transactions are valid. To this end the following properties are checked

1. Plausability
   - Valid time tamp?
2. Identity
   - Was the signature really made by the sender of the transaction? (public/private key procedure)
3. Authenticity
   - Valid user counter?
4. Liquidity
   - Is there a contradiction to earlier transactions? (Can the user have the object / the money / the book / …?)

23	TS	5	A has loaned book1 to B	S	CS
	TS	6	A has loaned book2 to B	S	
	TS	3	B has loaned book1 to C	S	
	TS	2	C has loaned book1 to D	S	
24	TS	7	A has loaned book3 to D	S	CS
	TS	8	A has loaned book4 to C	S	
25	TS	4	B has loaned book2 to E	S	CS
	TS	7	E has loaned book2 to F	S	
	TS	5	D has loaned book1 to E	S	
26	TS	3	C has loaned book4 to F	S	CS
	TS	8	E has loaned book1 to G	S	
	TS	1	F has loaned book2 to G	S	
	TS	2	F has loaned book4 to H	S	



A „candidate block“ (a ledger) can be added to a blockchain – if …

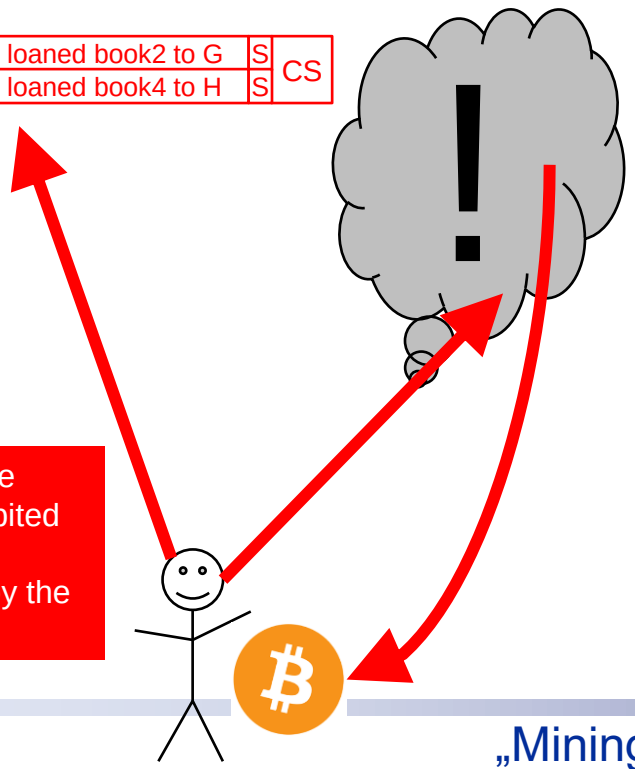
… the majority of the blockchain nodes (=51%) agree, that the transactions are valid.

„To validate a transaction and to add it to a blockchain the computers of the users in the blockchain network must solve a riddle… The computer which solves the riddle first can add the block of transactions to the blockchain.“

(Mark Gates: „Blockchain“)

„a riddle“ = a complex and expensive mathematical operation

23	TS	5	A has loaned book1 to B	S	CS
	TS	6	A has loaned book2 to B	S	
	TS	3	B has loaned book1 to C	S	
	TS	2	C has loaned book1 to D	S	
24	TS	7	A has loaned book3 to D	S	CS
	TS	8	A has loaned book4 to C	S	
25	TS	4	B has loaned book2 to E	S	CS
	TS	7	E has loaned book2 to F	S	
	TS	5	D has loaned book1 to E	S	
26	TS	3	C has loaned book4 to F	S	CS
	TS	8	E has loaned book1 to G	S	
27	TS	1	F has loaned book2 to G	S	CS
	TS	2	F has loaned book4 to H	S	



ATTENTION: The coins are not debited somewhere, but **created newly** by the mining process!!

A „candidate block“ (a ledger) can be added to a blockchain – if …

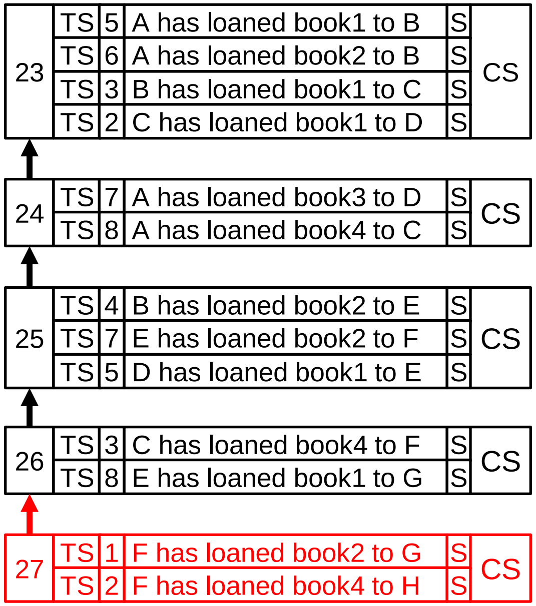
… the majority of the blockchain nodes (=51%) agree, that the transactions are valid.

„To validate a transaction and to add it to a blockchain the computers of the users in the blockchain network must solve a riddle… The computer which solves the riddle first can add the block of transactions to the blockchain.“

„Who solves the riddle first, gets a reward, which is payed normally with the digital currency (e.g. „Bitcoin“)“, which is used in the blockchain (=„mining“).

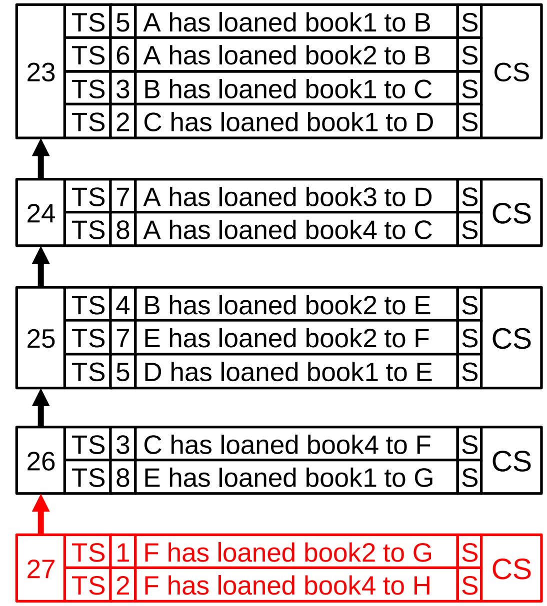
Who adds new blocks to the blockchain gets this reward, because he has invested computing power, energy and resources into the network, which keeps the network running („proof of work“).“

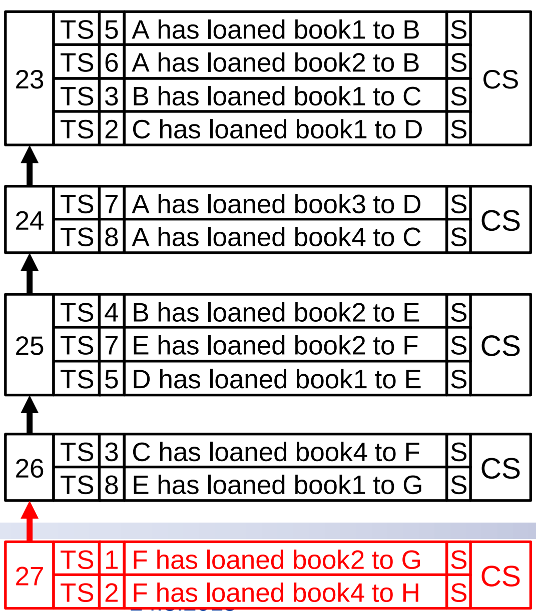
(Mark Gates: „Blockchain“)

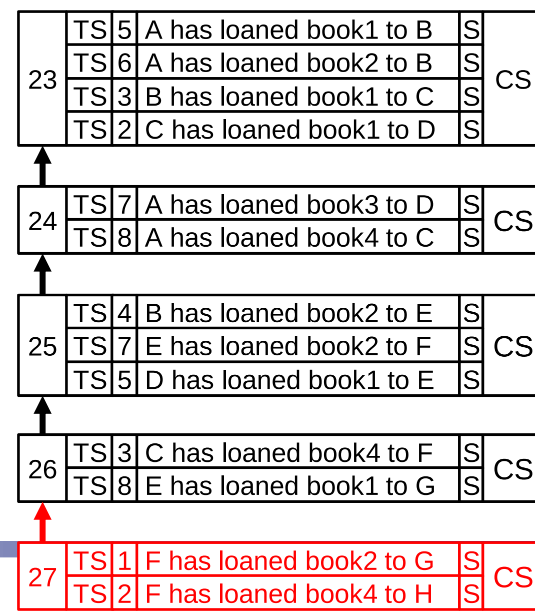


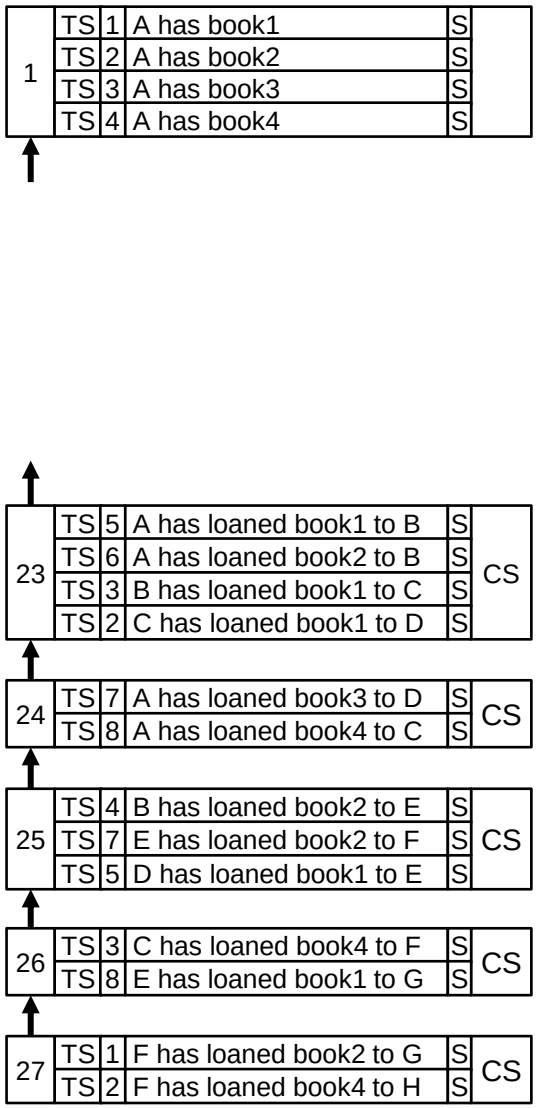
All other nodes of the blockchain receive the new block, check its checksum and add it to their own copy of the blockchain.

If a node was offline, it gets the current copy of the blockchain, if it is online again.









If A loans book1 to B, he must have it.

If he didn‘t get it from someone else, he must have had it right from the start of the block chain.

The first block is initialized manually – all the succeeding blocks are managed by the network.

For the first block an agreement between the members of the blockchain is necessary.

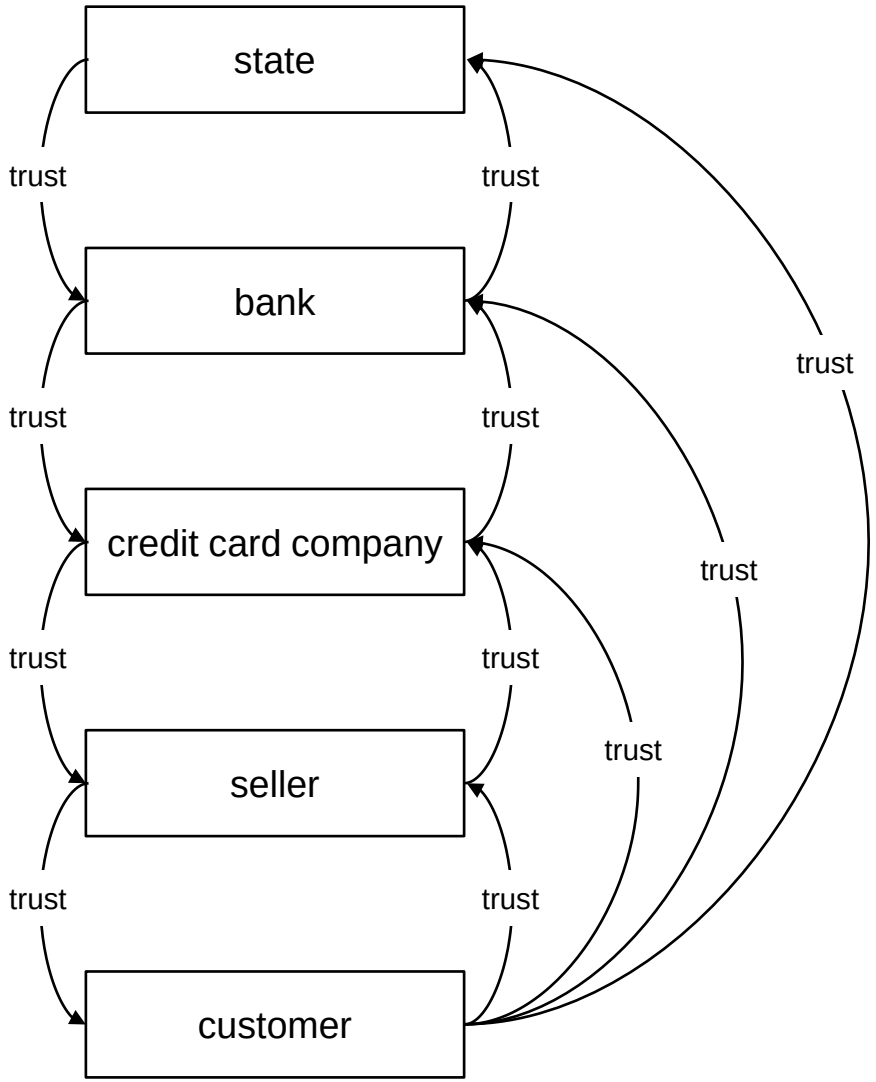
Normally not books but coins are the most important objects in blockchains.

Therefore this procedure is called „Initial Coin Offering“ (ICO).

Members can get coins

- either by buying existing coins for real money
- or by creating new ones by executing the mining

1. The hype
2. The technical background
3. What does a blockchain guarantee?
4. Pro‘s & Con‘s



Normally:

We trust in institutions (=brokers for transactions) and centralised data bases.

Money is based on trust.

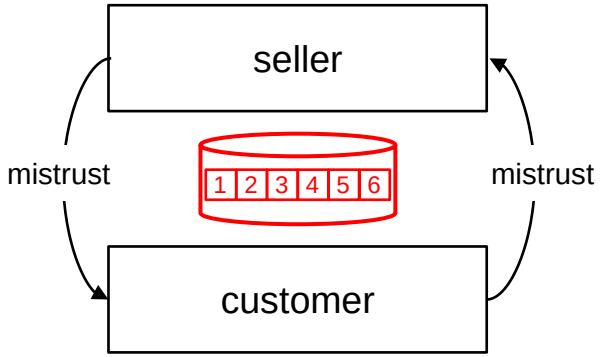
Transactions are based on trust.

But:

There are many opportunities not to trust each other!

Then:

A blockchain may help!



Everything is based on trust!

A blockchain can not prevent the users from lying and cheating.

It can not be varyfied, that „A has sold a house for 500.000€ to B“ is true.

BUT:

1. This statement is documented in the blockchain and can never be changed or removed.
2. It can be checked, if there is a contradiction to other transactions (Has A sold the same house already before to C?)

A blockchain does not guarantee the truth of the transactions but their internal consistency!

-> comparable with the objective of the ISO 9001 standard:

It does not say, that a company produces quality – but it confirms, that the company applies a quality management system.

1. The hype
2. The technical background
3. What does a blockchain guarantee?
4. Pro‘s & Con‘s

+ Transparency

All data and all of their changes are always visible for everybody. The status of a transaction can be followed in real time.

+ Elimination of brokers

Transactions can be processed directly between the involved partners without including a third party.

+ Decentralisation

There is no central institution which manages and controls the data. The blockchain is less vulnerable for hacking, data loss and data corruption than a central data base.

+ Trust

It is no more necessary to trust a central broker (e.g. a bank).

+ Security

Data in a blockchain can not be changed after their storage. All changes of data can be tracked. Transactions can not be changed without leaving a trace behind. Everybody can reveal a data corruption.

+ Many applications

Everything that has any kind of value can be recorded in a blockchain (ownership, identity, copyright, …). Any kind of information can be communicated using a blockchain.

+ Easily accessible technology

The necessary software is free of charge. No significant investment in infrastructure is necessary.

+ Cost reduction

It is no longer necessary to pay brokers.

+ Increased transaction speed

Because of the elimination of brokers transactions can be processed directly between the involved partners.

(Mark Gates: „Blockchain“)

- **Insufficient privacy**
  All information is accessible always for everybody.
- **Security problems**
  If somebody looses his login code he will never again have access to his data (including coins!!) because there is no center which can recover the login. Transfers to the wrong account are irreversibly lost!
- **No central control**
  Extensive and may be impossible processes for agreements among the partners about changes in the network, because 50 … 60 … 70% of them must agree.
- **Risk of the „51% attack“**
  Who controls at least 51% of the network nodes has all transactions under his control (Mining farms in Russia and China!!)
- **Untested new technology**
  Except Bitcoin there is no really working application until now (mid 2018).
- **Costs**
  For the solution of the riddle („mining“ / „proof of work“) enormous IT power is necessary. Half an hour of the Bitcoin network consumes as much energy as one household per year!!
- **Missing scalability**
  The Bitcoin network processes 3 transactions per second. In the same time Visa processes 20.000 transactions.
- **Poor reputation**
  For many people „blockchain“ means „bitcoin“ means „crime“. Instead of trusting a central broker one must trust an anonymous network. There is no mass acceptance for blockchains.
- **Hype**
  Many promises of blockchains are sugarcoated and exaggerated. The time and effort for implementation is often underestimated. Many startups in this field will not survive.
  „Blockchain“ is not the answer for all problems of the world! Don‘t believe in the hype!

(Mark Gates: „Blockchain“)

+ Transparenz

Alle Daten und alle ihre Änderungen sind jederzeit für jedermann sichtbar. Der Status einer Transaktion kann in Echtzeit verfolgt werden.

+ Eliminierung von Vermittlern

Transaktionen können direkt zwischen den Beteiligten abgewickelt werden, ohne eine dritte Partei mit einzubeziehen.

+ Dezentralisierung

Es gibt keine zentrale Institution, die die Daten verwaltet und sie damit kontrolliert. Die Blockchain ist nicht so anfällig für Hacking, Verlust und Korruption wie eine zentrale Datenbank.

+ Vertrauen

Es ist nicht mehr notwendig, zentralen Vermittlern (z.B. Banken) zu vertrauen.

+ Sicherheit

In der Blockchain gespeicherte Daten sind unveränderbar. Die Änderung der Daten ist nachvollziehbar. Transaktionen können nicht geändert werden, ohne Spuren zu hinterlassen. Jeder kann eine Fälschung entlarven.

+ Viele Anwendungen

Alles, was „irgendwie von Wert ist“, kann in einer Blockchain aufgezeichnet werden (Eigentumsrechte, Identitäten, Urheberrechte, …). Über die Blockchain können beliebige Informationen kommuniziert werden.

+ Leicht zugängliche Technologie

Die erforderliche Software ist frei verfügbar. Es ist keine signifikante Investition in die Infrastruktur notwendig.

+ Kostenreduzierung

Die Bezahlung der Dienste von Vermittlern entfällt.

+ Erhöhte Transaktionsgeschwindigkeit

Durch die Eliminierung von Vermittlern können die Nutzer Transaktionen direkt zwischen sich abwickeln.

(Mark Gates: „Blockchain“)

- **Mangelnde Privatsphäre**
  Alle Informationen sind jederzeit jedem zugänglich.
- **Sicherheitsprobleme**
  Wer seinen Zugangscode vergisst, kommt nicht mehr an seine Daten und ggf. sein Geld heran, denn es gibt keine Zentrale, die es ihm wieder herstellt! Überweisungen auf das falsche Konto sind unwiderruflich weg!
- **Keine zentrale Kontrolle**
  Aufwändige und z.T. unmögliche Einigungsprozesse bezüglich Änderungen im Netzwerk (mehr als 50 … 60 … 70% müssen zustimmen).
- **Risiko des „51%-Angriffs“**
  Wer über 51% der Computer des Blockchain-Netzwerkes kontrolliert, hat alle Transaktionen unter Kontrolle (Mining-Farmen in Russland und China!!)
- **Unerprobte neue Technologie**
  Es gibt außer Bitcoin noch keine realen Anwendungen, die wirklich funktionieren.
- **Kosten**
  Für das Lösen des „Rätsels“ (-> Mining / Proof of work) sind enorme Rechenleistungen notwendig. Eine halbe Stunde Bitcoin-Netzwerk verbraucht so viel Energie wie ein Haushalt in einem Jahr!
- **Fehlende Skalierbarkeit**
  Das Bitcoin-Netzwerk bearbeitet etwas 3 Transaktionen pro Sekunde. Visa bearbeitet in derselben Zeit 20.000 Transaktionen.
- **Angeschlagener Ruf**
  Für viele Menschen ist „Blockchain“ = „Bitcoin“ = „Kriminalität“. Statt einer Zentrale muss man einem anonymen „Netzwerk“ vertrauen. Es gibt keine Massenakzeptanz für Blockchains.
- **Hype**
  Viele Versprechungen der Blockchain sind geschönt und aufgebauscht. Die Zeitspanne bis zur Einführung wird oft dramatisch unterschätzt. Startups werden möglicherweise nicht lange überleben.
  „Blockchain“ ist nicht die Antwort auf alle Probleme der Welt. Glaube nicht dem Hype!

(Mark Gates: „Blockchain“)