Disruptive Technologien - Blockchain, Umfeld und Grundlagen
Teil 2: Blockchain Prinzip

Peter Heinzmann, Prof. Dr. sc. techn.
HSR Hochschule für Technik Rapperswil / cnlab information technology research ag
www.cnlab.ch peter.heinzmann@cnlab.ch

Gesellschaftliche Bedeutung (Heinzmann)

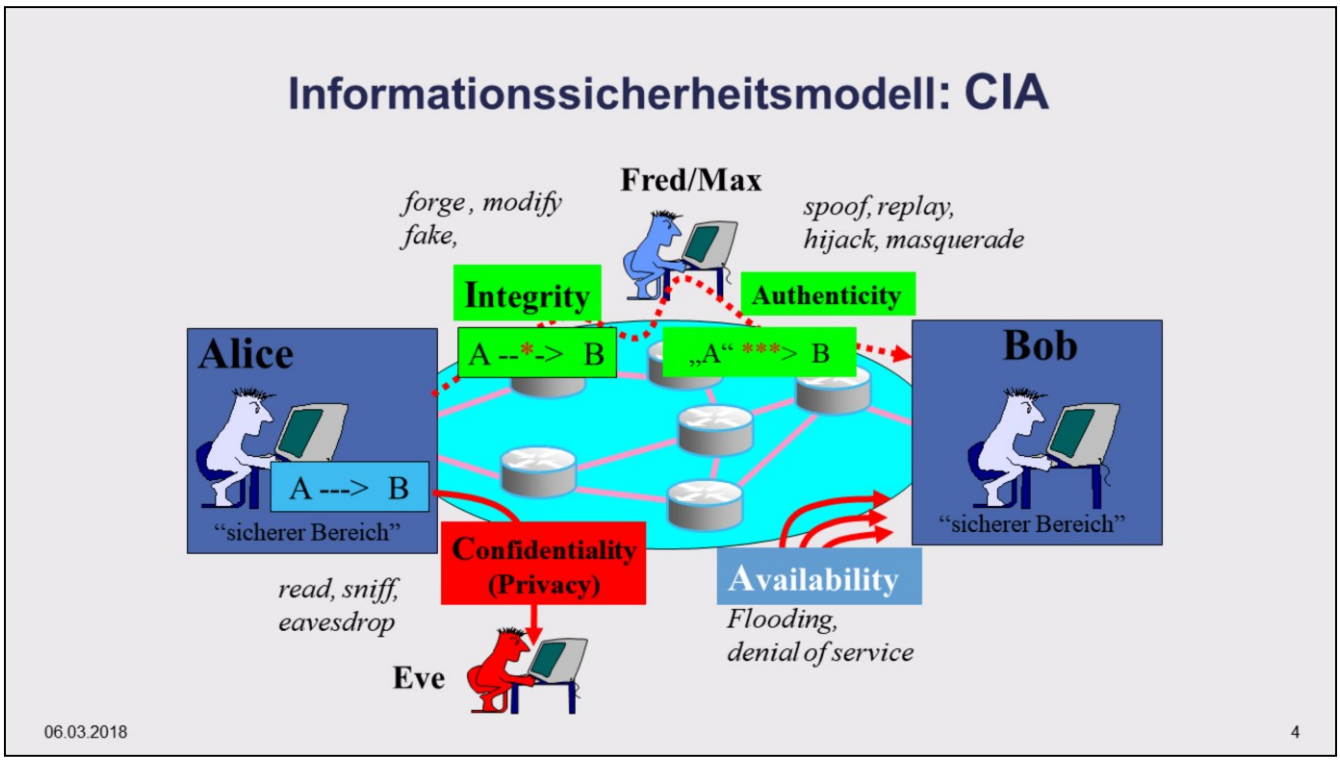
08.45 – 10.15

- Decentralized Society
- Verteilte Datenbanken

10.45 – 12.00

- Kryptologische Grundlagen
- Blockchain Grundlagen
- Demo

2.1 Krypto Grundlagen



Confidentiality, Secrecy, Privacy: Vertraulichkeit bzw. Geheimhaltung der Information, d.h. Information ist nur dem Sender und Empfänger bzw. einem definierten Personenkreis bekannt. Privacy meint eher die Vertraulichkeit in Zusammenhang mit Privatsphärenschutz bzw. Schutz vor dem Missbrauch der Personendaten.

Integrity: Integrität (Echtheit) der Information ist gewährleistet, wenn die Information nicht unerkannt durch einen nicht-autorisierten Dritten geändert werden kann. In Zusammenhang mit der Integrität (Echtheit) von Sender und Empfänger spricht man auch von Authenticity (Authentizität).

- Sender (Server) -Authentisierung: Der Empfänger kann überprüfen, ob die übermittelten Daten vom richtigen Sender gesandt wurden.
- Empfänger (Client) –Authentisierung: Der Sender kann überprüfen, dass er mit dem richtigen Empfänger kommuniziert.
- Meldungs-Authentisierung: Überprüfen, ob die Daten nicht verändert wurden (entspricht der Integritätsüberprüfung).
- Zertifizierung: Beglaubigung von Authentisierungsdaten durch eine vertrauenswürdige Partei.
- Validieren: Methode um die Echtheit und die Gültigkeit einer Autorisierung zu überprüfen.
- Revozieren: Methode zum widerrufen (unsicherer) Authentisierungs- oder Autorisierungsdaten.
- Zeitstempel: Liefert die beglaubigte Aufzeichnung des Datums eines Ereignisses (z. B. zuverlässige Angabe von Erzeugung, Versand, Empfang der übermittelten Daten)
- Spoofing (englisch für Manipulation, Verschleierung oder Vortäuschung) nennt man Täuschungsversuche zur Verschleierung der eigenen Identität. Früher stand Spoofing ausschließlich für den Versuch des Angreifers, IP-Pakete so zu fälschen, dass sie die Absenderadresse eines anderen (manchmal vertrauenswürdigen) Hosts trugen. Später wurde diese Methode jedoch auch auf andere Datenpakete angewendet. Heutzutage umfasst Spoofing alle Methoden, mit denen sich Authentifizierungs- und Identifikationsverfahren untergraben lassen, welche auf der Verwendung vertrauenswürdiger Adressen oder Hostnamen in Netzwerkprotokollen beruhen

Availability: Verfügbarkeit eines Systems oder einer Anwendung ist gewährleistet (keine Leistungsverminderung und kein Leistungsausfall). Reliability beschreibt die Zuverlässigkeit (Ausfallsicherheit) von Systemen.

Ferner: **Verbindlichkeit** fasst die Sicherheitsziele Authentizität und Nichtabstreitbarkeit (Non repudiation) zusammen. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Die **Central Intelligence Agency (CIA)** ist der zivile Auslandsnachrichtendienst der USA. Dieser umfasste 2012 rund 16’500 Mitarbeiter und hatte ein Budget von 750 MUSD. Die **National Security Agency (NSA)** der USA ist für die weltweite Überwachung und Auswertung von elektronischer Kommunikation zuständig. Sieist auch für die Festlegung von staatlich eingesetzten Kryptoverfahren zuständig. Die NSA hatte 2013 rund 24’000 Mitarbeiter und ein Budget von 1’200 MUSD. Zum Vergleich: Die Schweizer Armee hatte 2012 noch 150’000 aktive Soldaten und ein Budget von 3’900 MCHF (2010).

2.1.1 Digital Signatures (Integrität, Authentizität)

06.03.2018 5

Digitale Signaturen sind dazu da, die Integrität und Authentizität zu gewährleisten.

Integrität www.enzyklo.de/Begriff/Integrit%C3%A4t

Nachrichten (Informationen, Datensätze) können nach der Erstellung nicht (von Unbefugten) unerkannt verändert werden. Falls auch nur ein einziges Bit (bei der Übermittlung oder Abspeicherung) verändert wird, so kann dies der Nutzer der Daten (anhand einer Checksumme, Signatur) erkennen. Falls jemand eine völlig neue Nachricht erstellt, d.h. alles inklusive Checksumme/Signatur verändert, so ist das nicht zu erkennen. Synonyme von Integrität sind Echtheit, nicht Veränderbarkeit, Ehrlichkeit, Loyalität, Makellosigkeit, Pflichtbewusstsein, Rechtschaffenheit, Redlichkeit, Unbescholtenheit, Vertrauenswürdigkeit, Zuverlässigkeit

Die Integrität einer Nachricht versichert deren Vollständigkeit und Unversehrtheit, d.h. der Empfänger kann davon ausgehen, dass die Nachricht so vom Absender erstellt wurde. Es ist aber nicht klar, wer wirklich der Absender der Nachricht war.

Bei ITSEC wird Integrität als „Verhinderung unautorisierter Modifikation von Information“ definiert.

Laut Glossar des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bezeichnet Integrität die „Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen“.

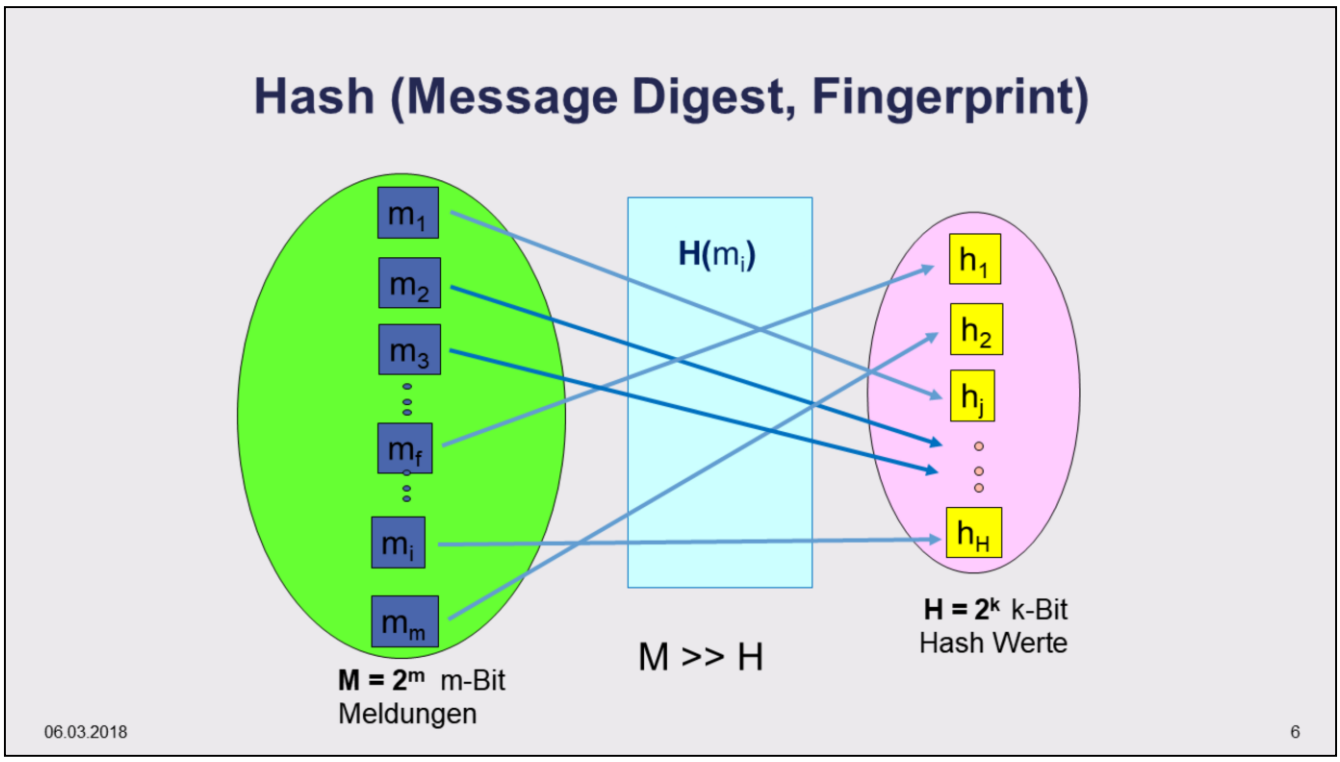
Authentizität www.enzyklo.de/Begriff/Authentizit%C3%A4t

Authentifizierung (oder Authentifikation) bezeichnet den Identitätsbeweis des Erstellers einer Nachricht (Information, Datensatz) gegenüber dem Nutzer bzw. Empfänger der Nachricht. Der Empfänger kann sicher sein, dass die Nachricht nicht von einem anderen (unbefugten) Absender stammt. Synonyme von Authentizität sind Echtheit, Gesichertheit, Glaubwürdigkeit, Rechtsgültigkeit, Sicherheit, Verbürgtheit, Zuverlässigkeit.

Mit Hilfe der Authentizität wird sichergestellt, dass eine Nachricht tatsächlich von derjenigen Person oder Institution stammt, welche sich als Absender ausgibt.

Eine Nachricht ist authentisch, wenn ihr Ursprung unzweifelhaft ist.

Beachte: Die Veränderung der gesamten Nachricht ist gleichbedeutend wie Generierung einer neuen Nachricht durch einen anderen Absender.



Eine Hash-Funktion (engl. hash = dt. das Gehackte, klein hacken, zerhacken, verkleinern) bildet einen beliebig langen Datensatz (Meldung, Input) auf einen kurzen Datensatz (Hash, Output) ab. Anstelle des Begriffs "Hash" wird auch Message Digest (engl. digest = dt. Auszug, Abriss, verdauen, verarbeiten) oder Fingerabdruck (Fingerprint, Thumbprint) verwendet.

Hash-Funktionen bilden Objekte aus einem „Originalbereich" (Quellelement, Pre-image, m Bit) auf einen Bildbereich (Zielelement, k Bit) ab. Die Anzahl der Objekte im Originalbereich ist in der Regel wesentlich grösser, als die Anzahl der Objekte im Bildbereich.

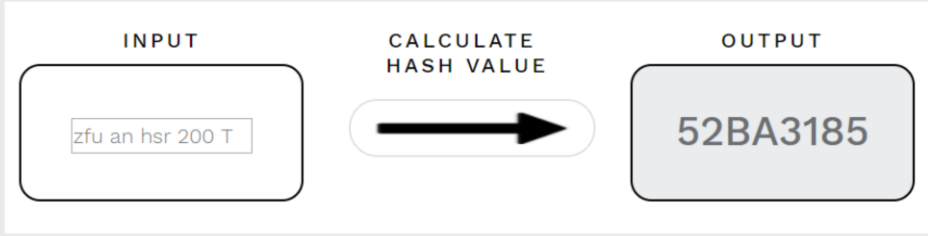
Bei Hash-Funktionen sind folgende Eigenschaften wichtig:

- Datenreduktion: Der Speicherbedarf des Hash-Wertes soll deutlich kleiner sein als der Speicherbedarf der Nachricht. (Kryptologen sprechen in diesem Zusammenhang manchmal auch von Kompression.)
- Zufälligkeit: Ähnliche Quellelemente sollen zu völlig verschiedenen Hash-Werten führen. Im Idealfall verändert das Umkippen eines Bits in der Eingabe die Hälfte aller Bits im resultierenden Hash-Wert.
- Eindeutigkeit: Die Funktion muss deterministisch von der Quellmenge auf die Zielmenge abbilden. Wiederholtes Berechnen des Hash-Wertes desselben Quellelements muss jedes Mal das selbe Ergebnis liefern.
- Effizienz: Die Funktion muss schnell berechenbar sein. (Diese Anforderung kann je nach Hash-Anwendungsbereich unterschiedlich lauten. Beispielsweise bei Passwort Hashes will man nicht allzu schnelle Berechnungsmöglichkeit.)
- Kollisionsfreiheit: Verschiedene Meldungen sollen nicht auf gleiche Hashes führen.

Die Hash-Funktion H(m) selbst muss öffentlich sein, d.h. jeder ist in der Lage, zu einer gegebenen Eingabe den Hashwert zu berechnen. Es soll jedoch rechnerisch unmöglich sein, zu einem vorgegebenen Hashwert eine Eingabe zu finden, die genau diesen Hashwert ergibt (Einweg-Eigenschaft, Einweg-Hash-Funktion, engl.: one-way or pre-image resistant hash function). Ähnlich wie bei Verschlüsselungsfunktionen, wo es Dritten rechnerisch unmöglich sein soll, zu einem vorgegebenen Ciphertextwert den zugehörigen Klartextwert zu bestimmen, soll das Auffinden eines passenden Originalwertes nur mittels „Exhaustive Search" bzw. „Brute Force Attacke" möglich sein.

Blockchain Basics: Hashing

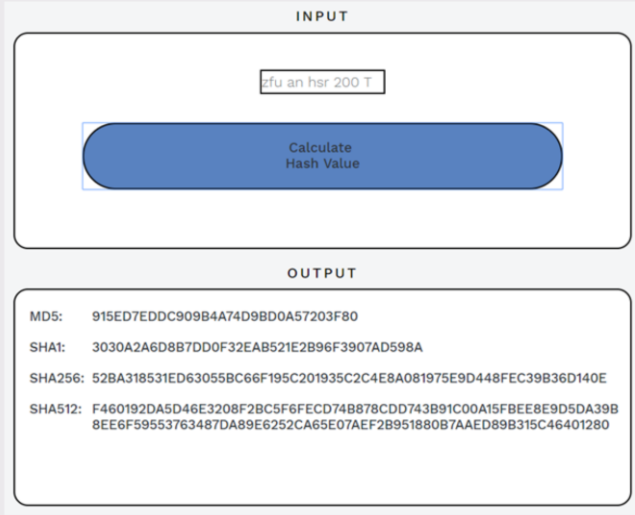
http://www.blockchain-basics.com/Hashing.html



Bei diesem Beispiel wird der SHA256 Hash Algorithmus verwendet. SHA256 liefert total 256 Bit bzw. 256/4 = 64 HEX-Zeichen, aber es werden nur die ersten 8 HEX-Zeichen angezeigt.

Blockchain Basics: Hash Functions

http://www.blockchain-basics.com/HashFunctions.html



Es gibt verschiedene Hash-Funktionen. Die bekanntesten sind Message Digest (MD) und Secure Hash Algorithm (SHA). Die Länge des produzierten Hash in Bit ist meist bei der Hash-Bezeichnung angegeben. In diesem Beispiel werden für den angegebenen Text drei verschiedene Hashes angezeigt:

MD5:

915E D7ED DC90 9B4A 74D9BD0A57203F80

SHA1:

3030 A2A6 D8B7 DD0F 32EA B521 E2B9 6F39 07AD 598A

SHA2 mit 256 Bit Hashlänge, SHA256:

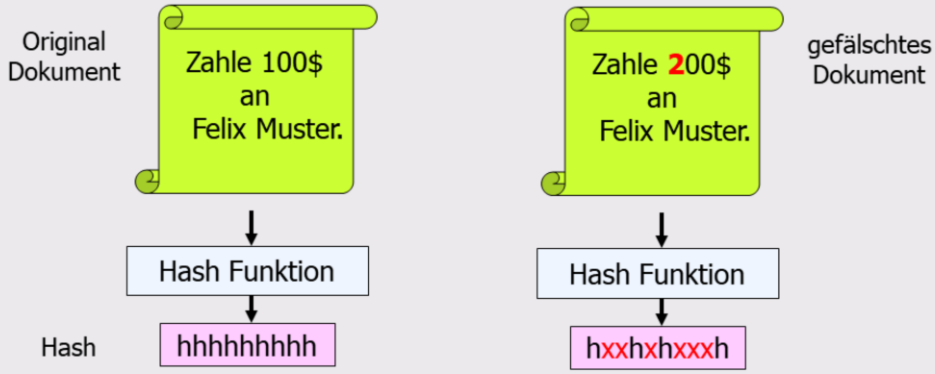
52BA 3185 31ED 6305 5BC6 6F19 5C20 1935

C2C4 E8A0 8197 5E9D 448F EC39 B36D 140E

SHA2 mit 512 Bit Hashlänge, SHA512:

F460192DA5D46E3208F2BC5F6FECD74B878CDD743B91C00A15FBEE8E9D5DA39B
8EE6F59553763487DA89E6252CA65E07AEF2B951880B7AAED89B315C46401280

Erkennung von Veränderungen (kryptologische Hashes)



Bei kryptologischen Hashes ist es das Ziel, anhand des Hash-Wertes die Echtheit des Dokuments sicherstellen zu können.

Der Dokumentersteller berechnet zum Dokument den Hash-Wert, welchen er zusammen mit dem Dokument abspeichert bzw. den Empfängern des Dokuments zustellt. Die Empfänger berechnen beim erhaltenen Dokument ebenfalls den Hash-Wert. Sollte im Dokument auch nur ein einziges Bit geändert worden sein, so wird ein völlig anderer Hash-Wert resultieren.

Recap: Hashing Algorithms and Security – Computerphile

https://www.youtube.com/watch?v=b4b8ktEV4Bg 7m22s

Hashing Algorithms and Security – Computerphile, Veröffentlicht am 08.11.2013

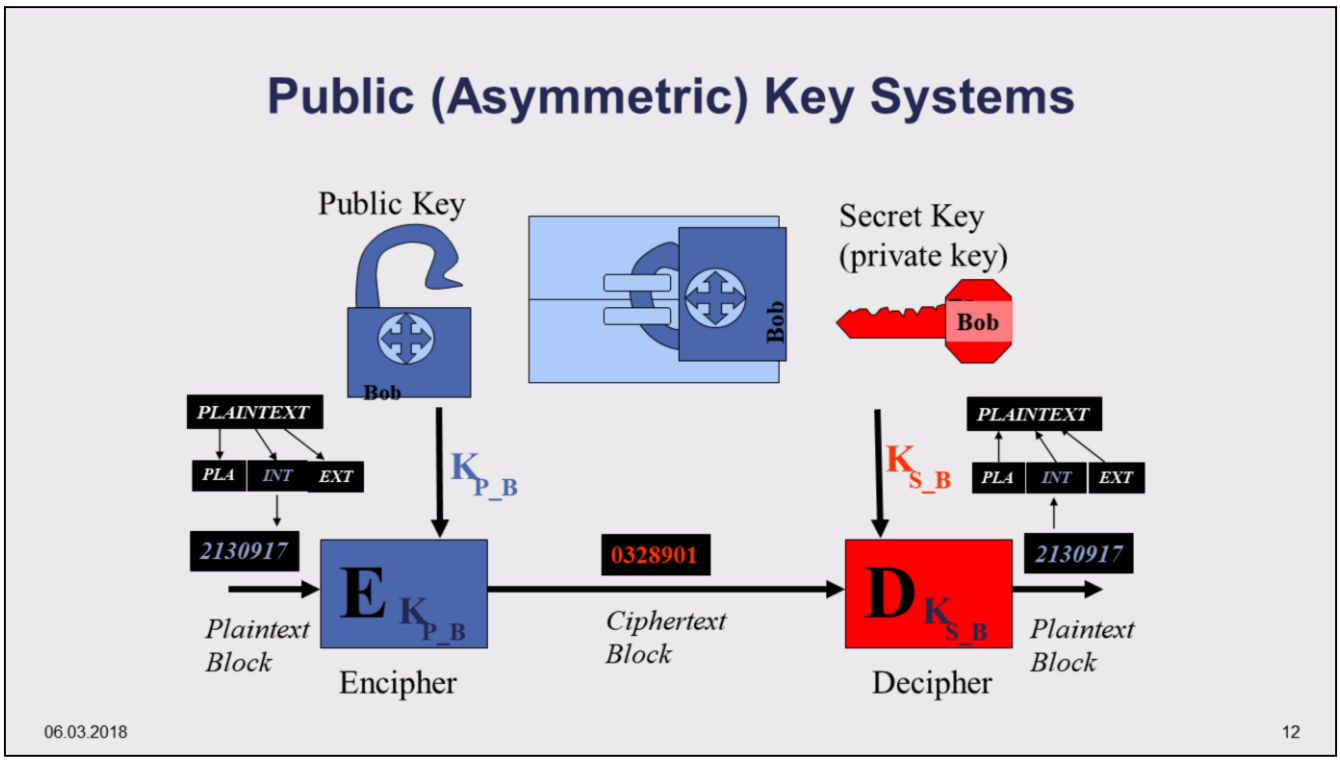
Hashing Algorithms are used to ensure file authenticity, but how secure are they and why do they keep changing? Tom Scott hashes it out.

2.1.2 (Public Key) Digital Signature

A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). These assurances may be obtained whether the data was received in a transmission or retrieved from storage.

For both the signature generation and verification processes, the message (i.e., the signed data) is converted to a fixed-length representation of the message by means of an approved hash function. Both the original message and the digital signature are made available to a verifier.

A digital signature algorithm includes a signature generation process and a signature verification process. A signatory uses the generation process to generate a digital signature on data; a verifier uses the verification process to verify the authenticity of the signature.



Bei den asymmetrischen Verfahren unterscheiden sich die Verschlüsselungsoperation beim Sender und die Entschlüsselungsoperation beim Empfänger. Verschlüsselung und Entschlüsselung werden durch unterschiedliche Schlüssel bzw. Schlüsselteile gesteuert. Die Verschlüsselung wird durch den „öffentlichen Schlüssel“, die Entschlüsselung durch den «geheimen Schlüssel» gesteuert.

Beispiel:

Wer Bob eine verschlüsselte Meldung senden will, besorgt sich Bob‘s öffentlichen Schlüssel und verschlüsselt die Meldung mit diesem Schlüssel. Man geht davon aus, dass Bob der einzige ist, der den passenden geheimen Schlüssel hat und damit die Meldung wieder entschlüsseln kann.

Die zu verschlüsselnden Informationen bzw. der Klartext wird auf (Klartext-) Zahlen abgebildet, welche dann gesteuert durch den öffentlichen Schlüssel in (Chiffrat-) Zahlen umgewandelt werden. Gesteuert durch den geheimen Schlüssel kann der Empfänger aus den (Chiffrat-) Zahlen wieder die (Klartext-) Zahlen und daraus den Klartext zurückgewinnen. Die Klartextinformationen müssen in Blöcke unterteilt werden.

Einwegfunktionen (One-Way Function)

- Y = f(x) ist einfach zu berechnen
  $x = f^{-1}(Y)$ schwierig zu berechnen

- Beispiel: Faktorisieren

Bestimmen Sie Faktoren von: 397'915'121'138'603 = a b

4'221'571 * 94'257'593 = 397'915'121'138'603

- Beispiel: Logarithmieren Modulo p

$$y = b^x \Leftrightarrow x = log_b y \qquad 81 = 3^4 \Leftrightarrow 4 = \log_3 81$$

$$y = b^x \, mod(p) \Leftrightarrow x = log_b y \; mod(p) \qquad 13 = 3^4 \, mod(17) \Leftrightarrow 4 = \log_3 13 \; mod(17)$$

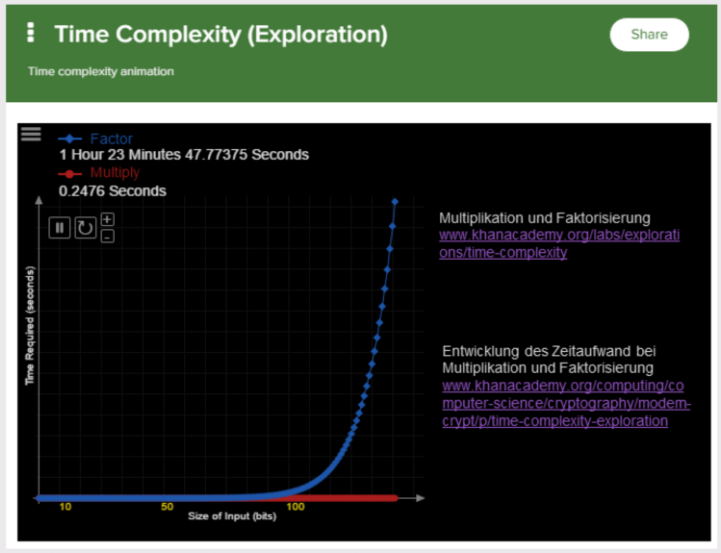
Mathematisch gesehen basieren öffentliche Schlüsselsysteme auf so genannten “Einwegfunktionen”. Dies sind Funktionen, welche nicht einfach umkehrbar sind. Sie lassen sich in die eine Richtung einfach berechnen, in die andere Richtung aber nicht oder nur mit sehr grossem Aufwand.

Ein Beispiel für eine solche Funktion ist die Multiplikation von zwei großen Primzahlen, da man annimmt, dass eine Primfaktorzerlegung ein "schwieriges" Problem darstellt. Eine weiteres Beispiel ist die modulare Exponentiation. Die inverse Funktion, d.h. die Bildung des diskreten Logarithmus ist schwierig zu berechnen. Eine Variante der Einwegfunktionen sind Trapdoor-Einwegfunktionen (auch Falltürfunktionen genannt). Diese lassen sich effizient umkehren, wenn man eine gewisse Zusatzinformation (eine Geheimtür, engl. trap door) kennt.

Andere “Einweg-Funktion” wären das “Mischen von Farben” oder das “Zerbrechen einer Platte”. Allerdings ist hier kein Rückwandlungsfunktionstrick bekannt.

Falls die beiden Zahlen keine Primzahlen sind, so lässt sich die Faktorisierung schneller durchführen. Man kann dies beispielsweise mit 712’569’131 * 457’821 = 326’229’112’123’551 überprüfen.

Rechenaufwand zur Multiplikation und zur Faktorisierung



https://www.youtube.com/watch?v=vgTtHV04xRI (16m36s)

Gambling with Secrets: Part 2/8 (Prime Factorization) www.youtube.com/watch?v=HkM6dj-qR4E **(7m04s)**

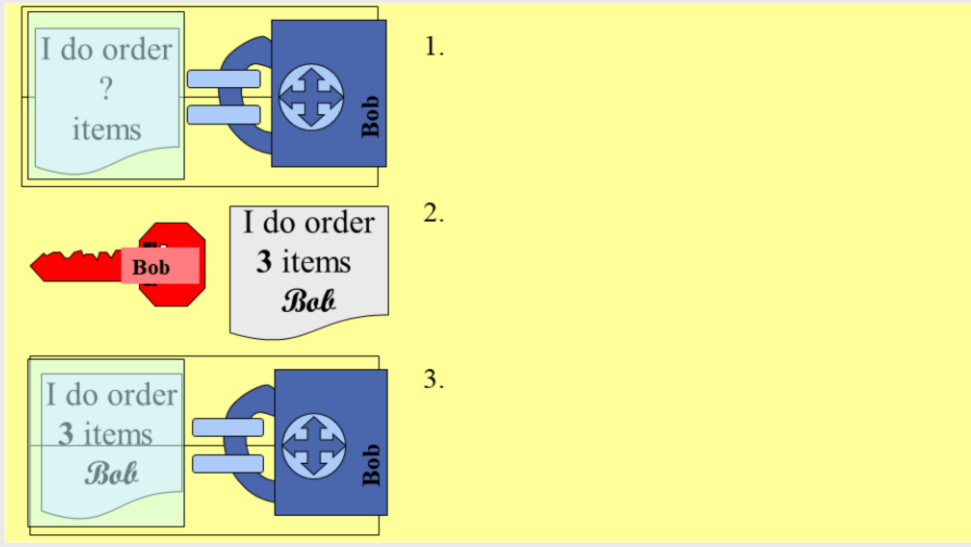
This chapter explores numerals, divisibility & Euclid's fundamental theorem of arithmetic (prime factorization) from a Caveman's perspective.

- Pime numbers are unbreakable.
- 4:11 Write down the prime numbers in a spiral leading to a pattern.
- 4:48 Euklid
- Every number can be constructed from a group of smaller primes.
- Factorization gives the prime factors of a number.

Gambling with Secrets: 8/8 (RSA Encryption) https://www.youtube.com/watch?v=vgTtHV04xRI (16m36s)
Links to time complexity graph:

- www.khanacademy.org/labs/explorations/time-complexity
- www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/p/time-complexity-exploration

Chat: Digital signature analogon: Bob signs a message and somebody checks Bob‘s signature

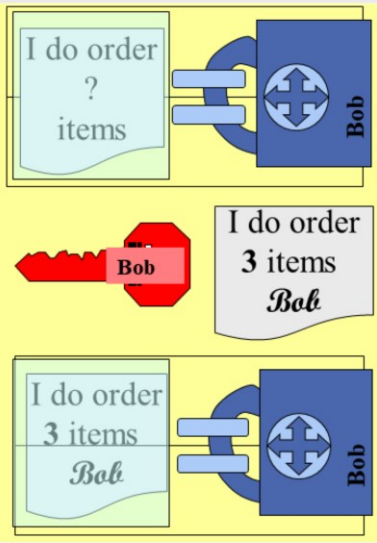


Erklären Sie anhand des “Digital Signature Analogons” wie mit der verschliessbaren Kiste die Grundprinzipien der digitalen Signatur erklärt werden können:

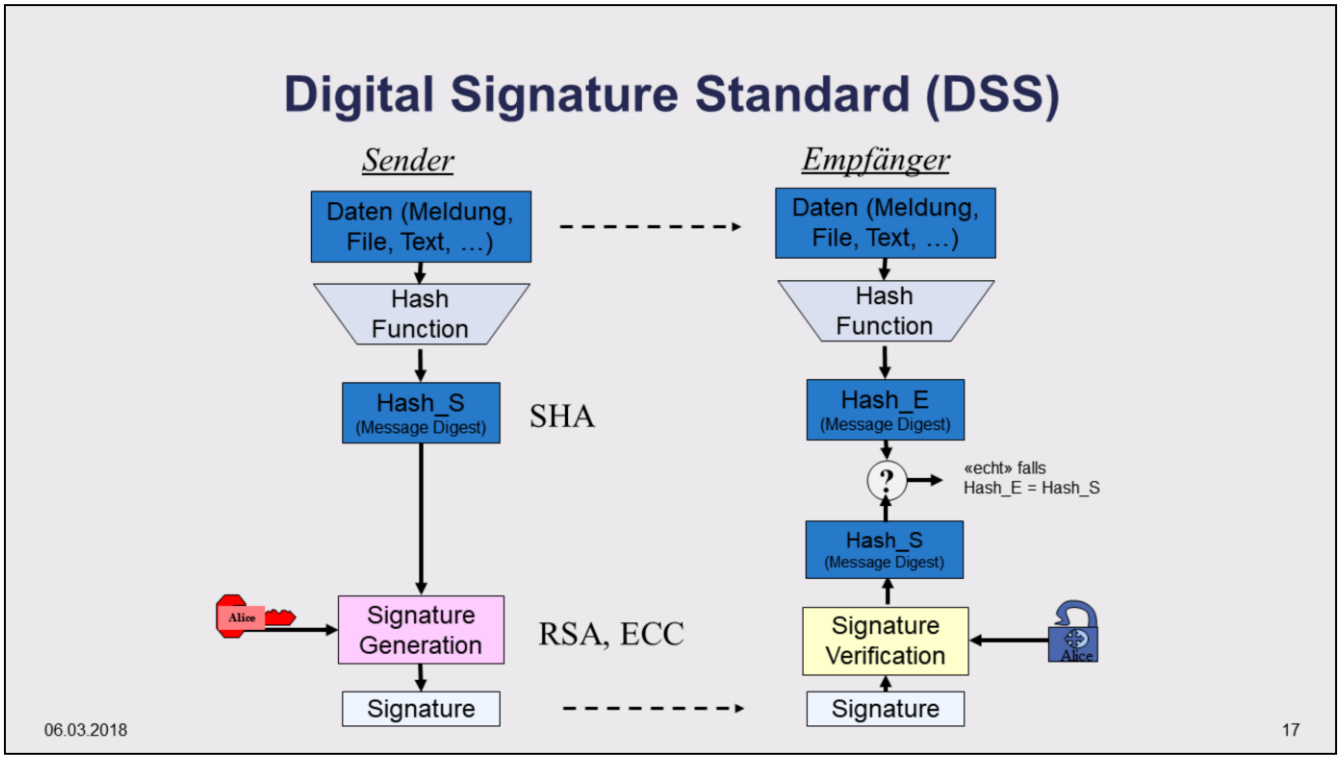
Wie stellt der Unterzeichner sicher, dass nur er unterzeichnen kann?

Wie überprüft der Empfänger, dass nur er der Unterzeichner der Verfasser der Meldung sein kann?

Solution: Digital signature analogon: Bob signs a message and somebody checks Bob‘s signature



1. The order which shall be signed by Bob is placed in a transparent box and *locked with the signer's i.e. Bob's public key*
2. Bob opens the box using his *private key* and writes the order (this proves that it must be Bob who places the order since he is the only one who can open Bob's lock)
3. Bob put the message back into the box, locks it again with his public key and sends the box back to the person who want to check his signature



Der Digital Signature Standard (DSS) wurde 2000 vom U.S. Dept. Of Commerce (DOC) und vom National Institute of Standards and Technology (NIST) als Standard für elektronische Unterschriften festgelegt. (FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, FIPS PUB 186-2, 2000 January 27.) http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

Die Originalmeldung wird mit Hilfe des Secure Hash Algorithmus (SHA) auf eine 160 Bit Folge reduziert. Als Alternative hat DSS auch eine Reduktion mittels DES vorgesehen.

Im DSS (Digital Signature Standard) Version 1991 war der Digital Signature Algorithm (DSA) als Unterschriftsalgorithmus festgelegt. Der DSA basiert auf die Schnorr / ElGamal Public Key Algorithmen. Er wurde vom NIST vorgeschlagen, wobei auch die National Security Agency (NSA) involviert war. Der DSA arbeitet mit Schlüssellängen von 512 bis 4096 Bit. Später – nachdem 2000 das RSA-Patent erloschen war - wurden auch der Rivest Shamir Adleman Algorithmus (RSA, ANSI X9.31) und der Elliptic Curve Algorithmus (ECDSA, ANSI X9.62) als Unterschriftsalgorithmen im DSS zugelassen.

The Digital Signature Standard (DSS) defines methods for digital signature generation that can be used for the protection of binary data (commonly called a message), and for the verification and validation of those digital signatures. Three techniques are approved.

(1) The Digital Signature Algorithm (DSA) is specified in this Standard. The specification includes criteria for the generation of domain parameters, for the generation of public and private key pairs, and for the generation and verification of digital signatures.

(2) The RSA digital signature algorithm is specified in American National Standard (ANS) X9.31 and Public Key Cryptography Standard (PKCS) #1. FIPS 186-3 approves the use of implementations of either or both of these standards, but specifies additional requirements.

(3) The Elliptic Curve Digital Signature Algorithm (ECDSA) is specified in ANS X9.62. FIPS 186-3 approves the use of ECDSA, but specifies additional requirements. Recommended elliptic curves for Federal Government use are provided herein.

Taher Elgamal arbeitete von 1995 bis 1998 als Chef-Wissenschaftler für für Netscape und war in dieser Position auch an der Entwicklung des Web Verschlüsselungsverfahrens Secure Socket Layer (SSL) beteiligt.

2.2 Blockchain

The Blockchain and Us (2017)

www.youtube.com/watch?v=2iF73cybTBs&t=837s 31m26s

06.03.2018 19

04.04.2017, The Blockchain and Us, A film by Manuel Stagars www.blockchain-documentary.com

The goal of this film is to encourage the conversation about the economic and social impacts of blockchain technology. Participate in the comments and subscribe to the channel to stay in the loop.

https://www.youtube.com/watch?v=2iF73cybTBs&t=837s 31m26s

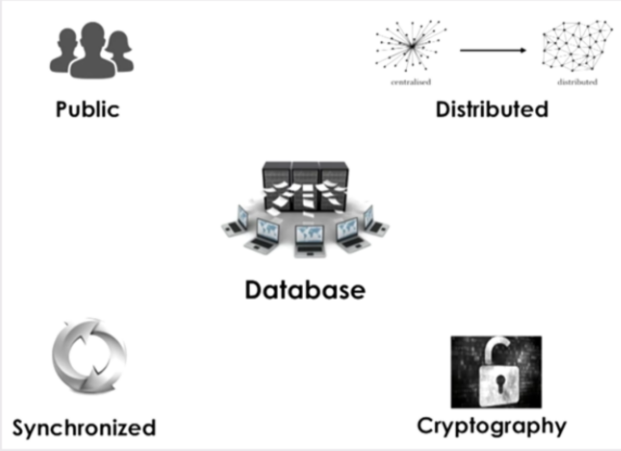
In 2008, Satoshi Nakamoto invented bitcoin and the blockchain. For the first time in history, his invention made it possible to send money around the globe without banks, governments or any other intermediaries. The concept of the blockchain isn't very intuitive. But still, many people believe it is a game changer. Economist and filmmaker Manuel Stagars portrays this exciting technology in interviews with software developers, cryptologists, researchers, entrepreneurs, consultants, VCs, authors, politicians, and futurists from the United States, Canada; , the UK, and Australia. The Blockchain and Us is no explainer video of the technology. It gives a view on the topic, makes it accessible and starts a conversation about its potential wider implications in a non-technical way. The film deliberately poses more questions than it answers.

For a deep dive, see all full-length interviews from the film here: http://blockchain-documentary.com/interview

Auszug aus Credits zu Beitragenden aus der Schweiz:

Christian Decker Core Tech Engineer, Blockstream Zurich; Taylor Gerring Co-Founder, Ethereum Zug; Marco Carlo Grossi Director Audit & Risk Advisory, Deloitte Switzerland; Paul Meeusen Head Finance and Treasury Services, Swiss Re Zurich; Dolfi Müller Mayor of the City of Zug Zug; Matthew Roszak Co-Founder & Chairman, Bloq Chicago, USA; Guido Rudolphi Founder, Cryptocash Uster; Jan Seffinga Partner, Deloitte Switzerland Zurich; Lars Thomsen Chief Futurist & Founder, Future Matters Zurich; Roger Wattenhofer Professor, Distributed Computing Group, Swiss Federal Institute of Technology (ETH) Zurich;

Blockchain Grundkonzepte



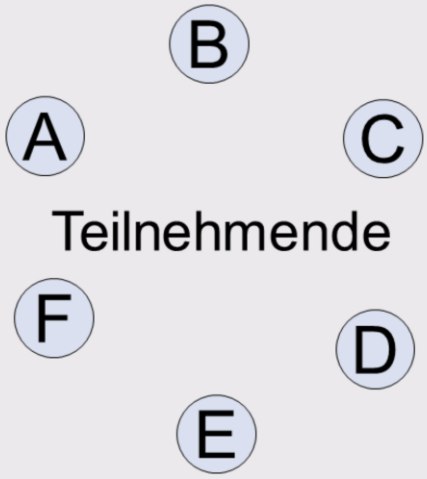
- Verteilte Systeme
  - Peer-to-Peer
- Transaktionen
  - Jeder kennt alle Transaktionsdaten
  - Transaktionsgeschichte ist nachvollziehbar
  - Transaktionen sind signiert
- Integrität (Echtheit)
  - Digitale Signatur
  - Hashing (Mining)
- Consensus Bildung
  - Verteilte Konsensus Bildung (Erzielung von Einigkeit)
  - Rechnaufwand (proof of work)
  - Tokenbesitz (proof of stake)

Die wichtigsten Eigenschaften einer Blockchain sind:

- dezentrale Organisation
- kryptographische Sicherheitsverfahren
- direktes Versenden von Werten mittels Peer-to-Peer-Verfahren
- Transparenz und Nachverfolgbarkeit der Transaktionen
- Manipulationssicherheit von Transaktionen und Daten
- Entscheidungen auf Basis von Konsens-Mechanismen

2.2.1 Blockchain Prinzip

Zentrale Transaktionsliste (ledger dt. Kontenblatt, Journal): Initialisierung (Initial Coin bzw. Token Offering, ICO)

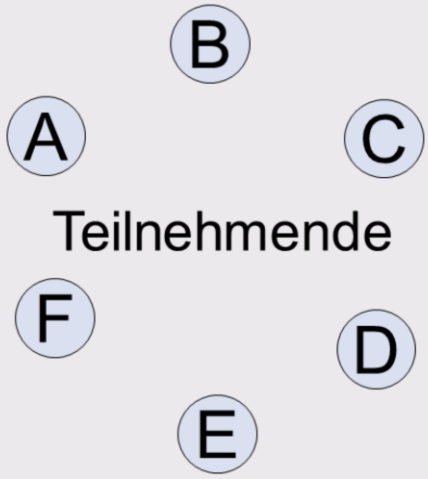


ID	Transaktionstext				
1.	A	erhält		100 T	
2.	B	erhält		100 T	
3.	C	erhält		100 T	
4.	D	erhält		100 T	
5.	E	erhält		100 T	
6.	F	erhält		100 T	
7.					
…					

Ein wichtiges Element der Blockchain ist eine Liste mit Einträgen, englisch als Ledger (Kontenblatt) bezeichnet. Es handelt sich aber nicht um ein Buchhaltungsblatt, weshalb man besser von Transaktionsliste oder Journal spricht. Die Liste enthält Einträge, welche mit einer Identifikationsnummer (ID) versehen sind. Die Einträge betreffen normalerweise einen oder mehrere Blockchain Teilnehmer. Je nach Anwendungsfall ist der Text des Eintrags eine Angabe zu einer Transaktion von einer Anzahl «Tokens», ein Vertragstext oder sogar ein Programm.

Zur Initialisierung der Blockchain werden verschiedenen Teilnehmern eine gewisse Anzahl Tokens zugesprochen. Bei Cryptocurrency Blockchains spricht man von einem «Initial Coin Offering, ICO)». Interessierte kaufen Tokens, denen ein echter Geldbetrag entspricht. Bei der Cryptocurrency Bitcoin gab es kein ICO, alle Bitcoins wurden mittels Mining generiert.

Zentrale Transaktionsliste (ledger dt. Kontenblatt, Journal): Transaktionen eintragen



ID	Transaktionstext				Signatur
…					
11.	A	gibt	B	80 T	*Sig_A*
12.	F	gibt	A	30 T	*Sig_F*
13.	B	gibt	F	20 T	*Sig_B*
14.	A	gibt	E	60 T	*Sig_A*
15.	B	gibt	A	40 T	*Sig_B*
16.	C	gibt	A	20 T	*Sig_C*
17.	C	gibt	A	20 T	*Sig_B*
…					

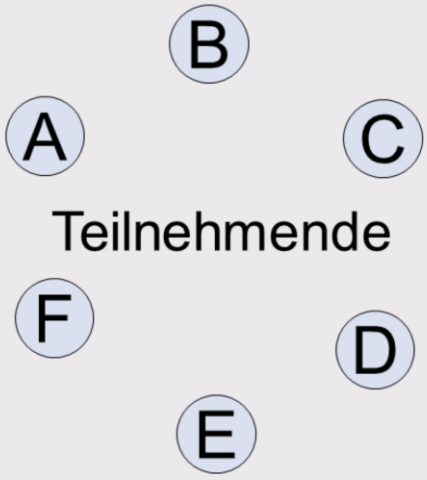
(z.B. Zahlungsliste einer Kartenspielrunde)

A = 40
B = -10
C = -20
D = 0
E = 10
F = -10

Protokoll

- Jeder kann Transaktionen in die Liste schreiben
- Jeder kann seine eigenen Transaktionen unterschreiben, alle können die Echtheit von Unterschriften überprüfen
- Alle Transaktionen haben eine eindeutige Identifikationsnummer
- Die effektiven Zahlungen werden erste Ende der Abrechnungsperiode (z.B. Ende Monat) ausgelöst

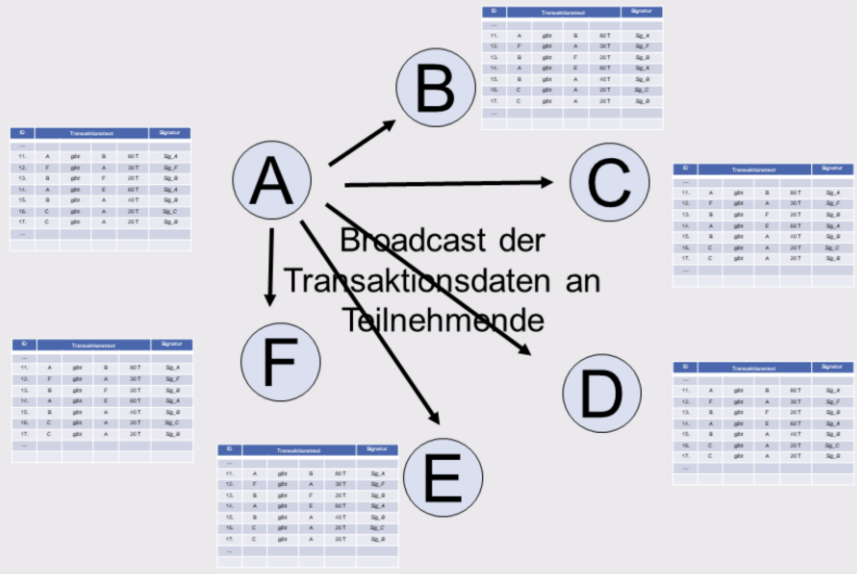
Zentrale Transaktionsliste (ledger dt. Kontenblatt, Journal): Token-Kontostand überprüfen



ID	Transaktionstext				Signatur	gültig
…						
11.	A	gibt	B	80 T	*Sig_A*	*ja*
12.	F	gibt	A	30 T	*Sig_F*	*ja*
13.	B	gibt	F	20 T	*Sig_B*	*ja*
14.	A	gibt	E	60 T	*Sig_A*	*nein*
15.	B	gibt	A	40 T	*Sig_B*	
16.	C	gibt	A	20 T	*Sig_C*	
17.	C	gibt	A	20 T	*Sig_B*	
…						

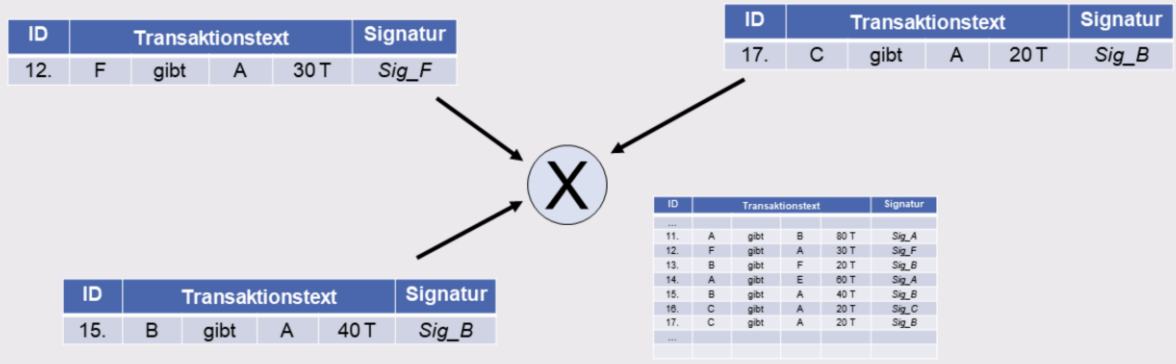
Es wird vor jeder Transaktion überprüft, wie der Kontostand des Zahlenden ist. Falls jemand zu wenig Geld hat, wird die Transaktion als ungültig bezeichnet, genau so, wie wenn die Signatur nicht stimmen würde.

Verteilte Transaktionslisten (ledger dt. Kontenblatt): «Broadcasting» der Transaktionen



Transaktionen werden an alle geschickt, so dass sich jeder seine eigene Transaktionsliste aufbauen kann.

Verteilte Transaktionsliste (ledger dt. Kontenblatt, Journal): Jeder Teilnehmer notiert empfangene Transaktionen und überprüft deren Gültigkeit



Jeder Teilnehmer kann selbst überprüfen, ob eine Transaktion gültig ist. Gültig ist eine Transaktion, wenn

1. die Signatur stimmt (kann mit dem öffentlichen Schlüssel des Absenders überprüft werden)
2. der Absender noch über genügend Tokens verfügt

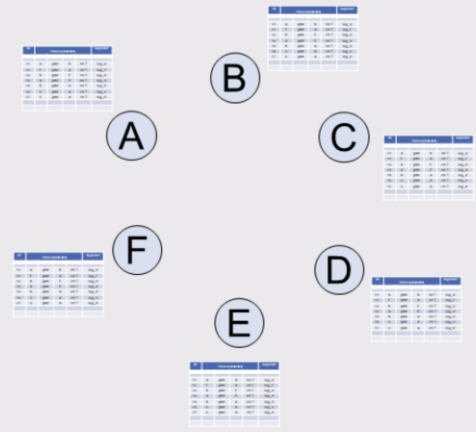
Beispiel: Entwicklung der Anzahl Bitcoin Transaktionen pro Tag blockchain.info/de/charts/n-transactions

Verteilte Block Bilder (Block Creator, Miner): Sammlung/Zusammenfassung von Transaktionen

Block

Initial Number

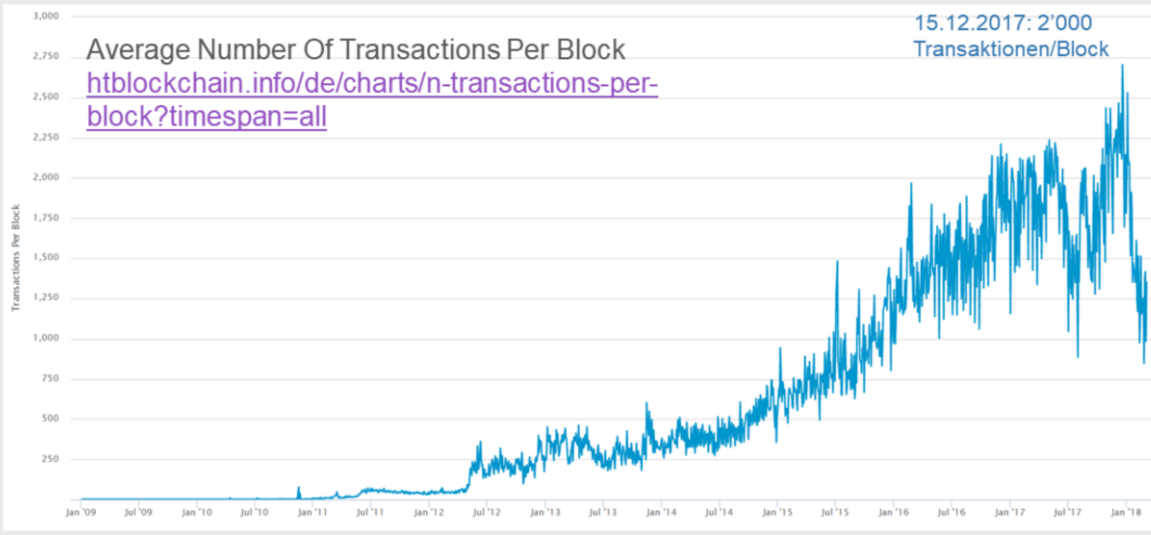
ID	Transaktionstext				Signatur
…					
11.	A	gibt	B	80 T	*Sig_A*
12.	F	gibt	A	30 T	*Sig_F*
13.	B	gibt	F	20 T	*Sig_B*
14.	A	gibt	E	60 T	*Sig_A*
15.	B	gibt	A	40 T	*Sig_B*
16.	C	gibt	A	20 T	*Sig_C*
17.	C	gibt	A	20 T	*Sig_B*
…					



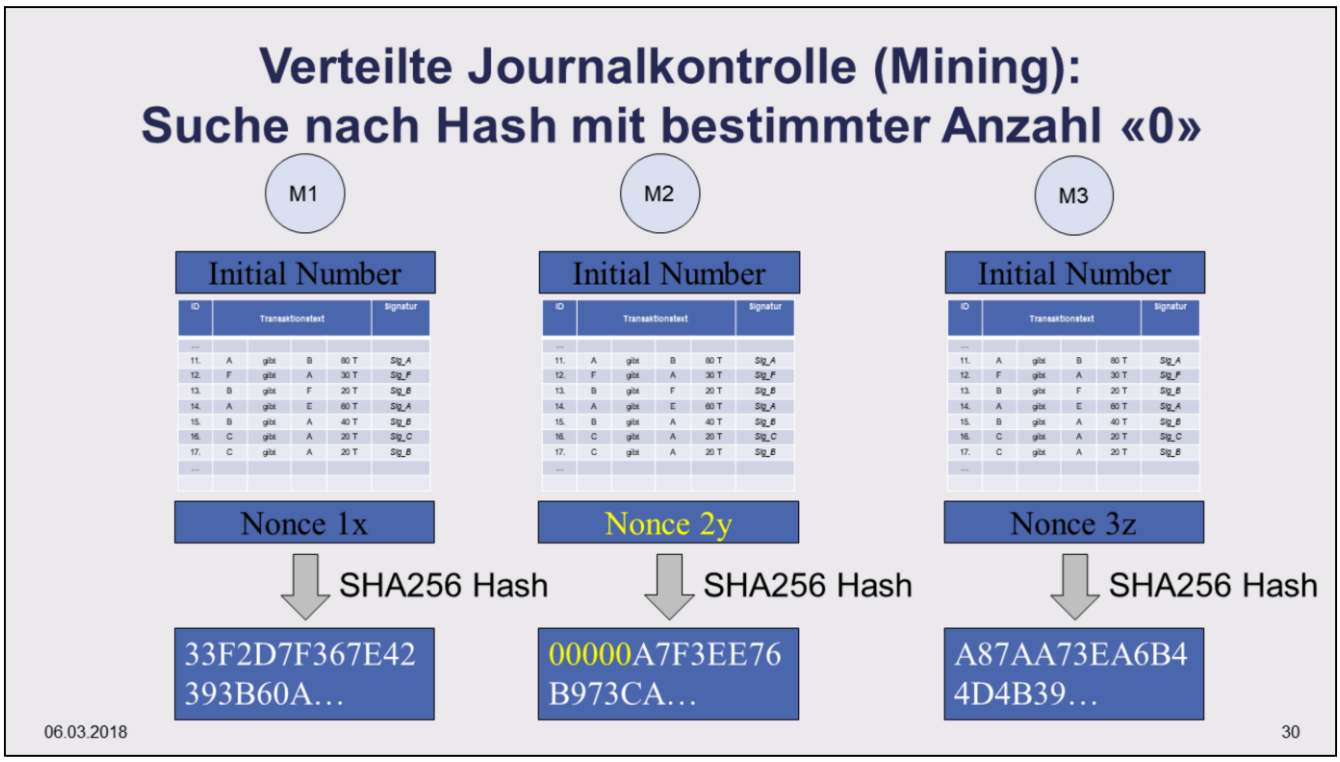
06.03.2018

Teilnehmer des Netzes fassen Transaktionen in Blöcken zusammen. Jeder Block enthält neben der Auflistung der kürzlich erfolgten Transaktionen auch eine Referenznummer und einen Zeitstempel. Die Referenznummer des ersten Blocks ist hier „Initalnummer“ genannt. In einen Block werden nur „gültige“ Transaktionen aufgenommen, d.h. die Signatur der Transaktion muss stimmen und für die jeweils angegebenen Transaktionen müssen noch ausreichend Token vorhanden sein. Es darf keine negativen „Kontostände“ geben.

Beispiel: Entwicklung der Anzahl Bitcoin Transaktionen pro Block



Bei Bitcoin enthält ein Block mittlerweile etwa 2'000 Transaktionen und die einzelnen Blöcke haben eine Grösse von etwa 1 MB. Damit umfasst eine einzelne Transaktion etwa 500 B.



Transkationen werden von sogenannten «Minern» in Blöcken zusammengefasst und auf die Gültigkeit überprüft. Der erste erhaltene Block erhält eine Initialnummer. (Weitere Blöcke erhalten eine Nummer, welche vom vorangehenden Block übernommen wurde.)

Beim Mining fügt der Miner dem Block einen Nonce-Wert hinzu und bildet den Hash über den Block. Er führt die Hash-Operation mit unterschiedlichen Nonce-Werten durch, bis der Hash mit einer vorgegebenen Anzahl «0» beginnt. Je mehr «0» verlangt sind, desto schwieriger ist es, einen passenden Nonce-Wert zu finden, d.h. desto grösser wird der Rechenaufwand für den Miner.

Beispiel: Block #511280 bei Bitcoin

https://blockchain.info/block/00000000000000000030b12ee5a31aaf553f49cdafa52698f70f0f0706f46d3d

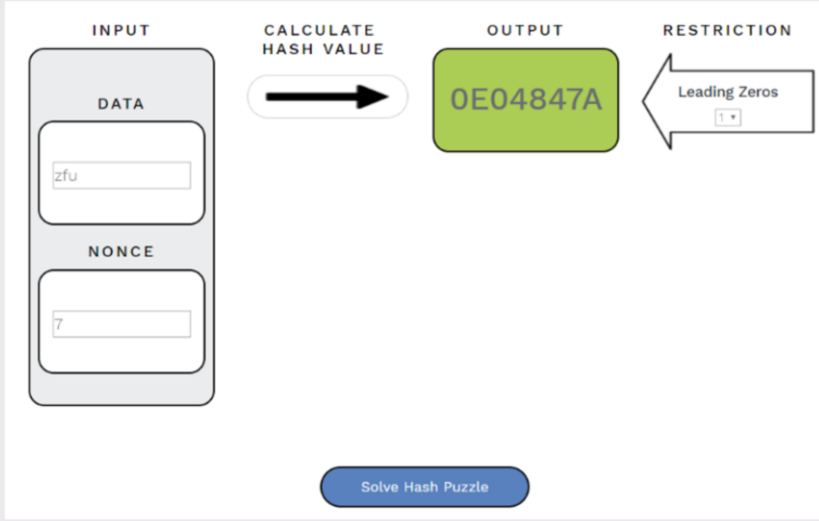
Anzahl der Transaktionen	3117
Ausgang insgesamt	18,461.59248097 BTC
Geschätztes Transaktionsvolumen	1,516.11624847 BTC
Transaktions Gebühren	0.76245969 BTC
Height	511280 (Hauptchain)
Zeitstempel	2018-02-28 06:08:42
Empfangene Zeit	2018-02-28 06:08:42
Weitergeleitet von	BTC.TOP
Schwierigkeit	3,007,383,866,429.73
Bits	392009692
Größe	1374.924 kB
Gewicht	3992.559 kWU
Version	0x20000000
Nonce	2607597846
Block Reward	12.5 BTC

Hash	00000000000000000030b12ee5a31aaf553f49cdafa52698f70f0f0706f46d3d
Vorheriger Block	00000000000000000004d59b7367d8900118b6c0f219b665e236735e96d87719b
Nächster Block	
Merkle Root	8a4e544a5111ad06b732f28f6efb8e9e2702401e99ad467e8ed2ef49c301f95d

Bei Bitcoin wird die Anzahl der geforderten Nullen beim Hash so eingestellt, dass etwa alle 10 Minuten ein Nonce gefunden bzw. ein Bock abgeschlossen werden kann.

Demo: Finde Hash, welcher mit einer «0» beginnt

www.blockchain-basics.com/HashPuzzle.html?nonce=2

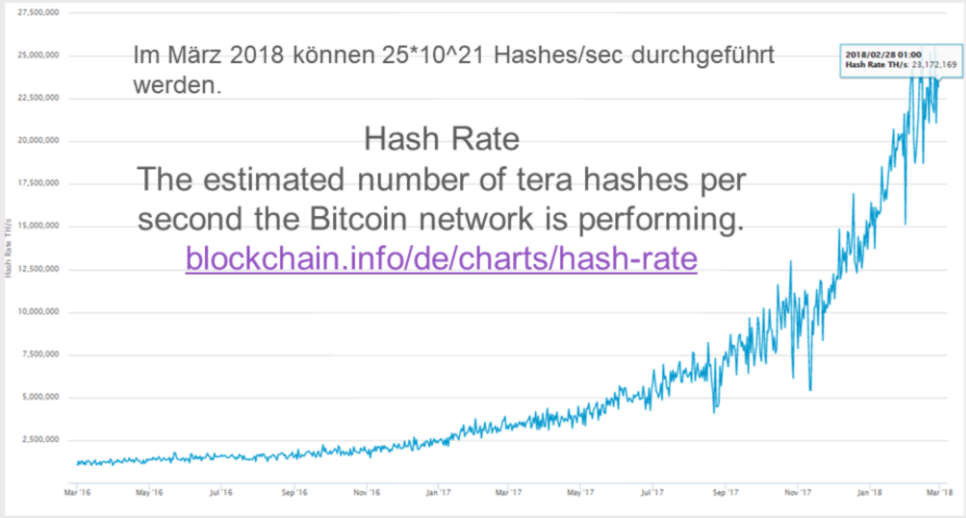


cnlab + 2 = 0FBE…

cnlab + 59 = 0C27…

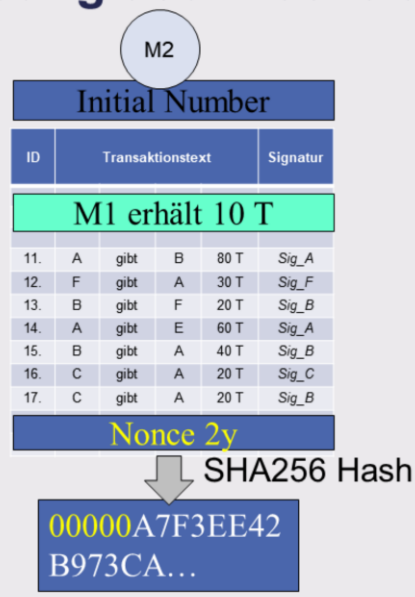
Ufu + 7 = 0E048…

Beispiel: Entwicklung der Hash Rate im Bitcoin Netz



https://blockchain.info/de/charts/hash-rate?timespan=all

Mining: Reward für Finder von Hash mit n Nullen, Broadcasting des Blocks an Alle



Miner, die einen Nonce-Wert finden, welcher auf einen mit einer bestimmten Anzahl Nullen beginnenden Hash führt, erhalten für ihre Leistung eine bestimmte Anzahl Tokens (Reward). Dazu tragen sie in der Transaktionsliste die ihre Adresse ein. Die Höhe des Rewards kann sich mit der Zeit ändern. Bei Bitcoin ist festgelegt, dass sich der Reward etwa alle zweieinhalb Jahre halbiert. Aktuell beträgt der Reward 12.5 Bitcoin pro Block.

Mining Maschinen und Plattformen

youtu.be/4pyRW8YpQMM 10m03s
16.5.2017, Bitcoin-Mine in Island, Galileo ProSieben
coincentral.com/asic-gpu-cpu-mining

- Mining mit
  - «normalen» Rechnern
  - Spezieller Hardware
    - Grafikkarten
    - Avalon Miner (6 TH/s)
  - Fremden Rechnern
- Cloud Mining
  - Genesis GPU Mining Farm
    www.genesis-mining.com

Spezielle Hardware für das Mining kann mit «normalen» Grafik Processing Units (CPU) oder speziellen Chips (Field Programmable Gate Array, FPGA; Application Specific Integrated Circuits, ASIC) realisiert werden. Das Bitcoin Wiki liefert bei Mining hardware comparison

https://en.bitcoin.it/wiki/Mining_hardware_comparison einen Vergleich von verschiedenen Mining Systemen.

Bitcoin Miner Avalon 721 6TH Asic Miner 6000GH

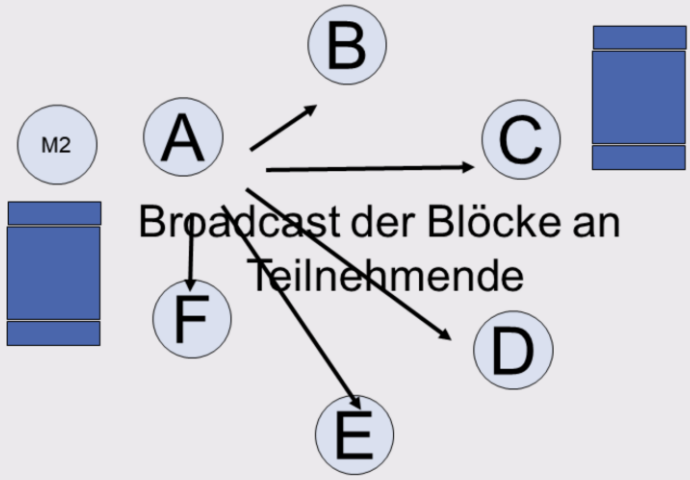
- Hashrate: 6 TH/s
  Power Consumption: ≈ 850-1000 Watts (with assumption of 90% power conversion ratio).
  PSU output pins: 8 x 6PIN PCIe power connectors.
  Controller: AvalonMiner Controller
  Gross Dimensions: 400 mm x 210 mm x 220 mm
  Operating Temperature: -5 °C to 40°C
  Gross weight: 4.7 kg
  https://asicminermarket.com/product/bitcoin-miner-avalon-721-6th-asic-miner-6000gh

Es gibt Firmen, welche spezielle «Mining Farms» aufgebaut haben, welche sie selbst nutzen oder Kunden gegen entsprechende Gebühren anbieten.

Genesis Mining wurde Ende 2013 gegründet. Genesis bietet Mining Computer für Kunden an. Als die Kundenbasis wuchs, wurden neue Mining-Farmen gebaut und Spezialisten in den Bereichen Programmierung und Steuerung eingestellt.

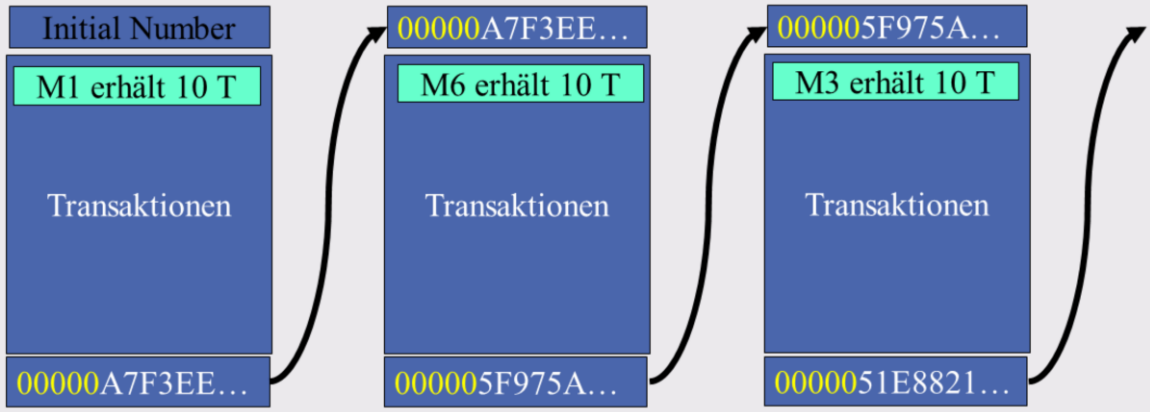
- Genesis Mining has facilities on every continent www.genesis-mining.com/datacenters
- 11.7.2017 A look inside iceland largest bitcoin mining farm: Genesis Mining youtu.be/TeA8h0X8uG0 5m49
- 22.08.2017 visit Inside Genesis Mining (GPU Mining Farm) youtu.be/2Jqf_wZKFCc 6m07s

Blockchain:
Empfang von Blöcken der Miner

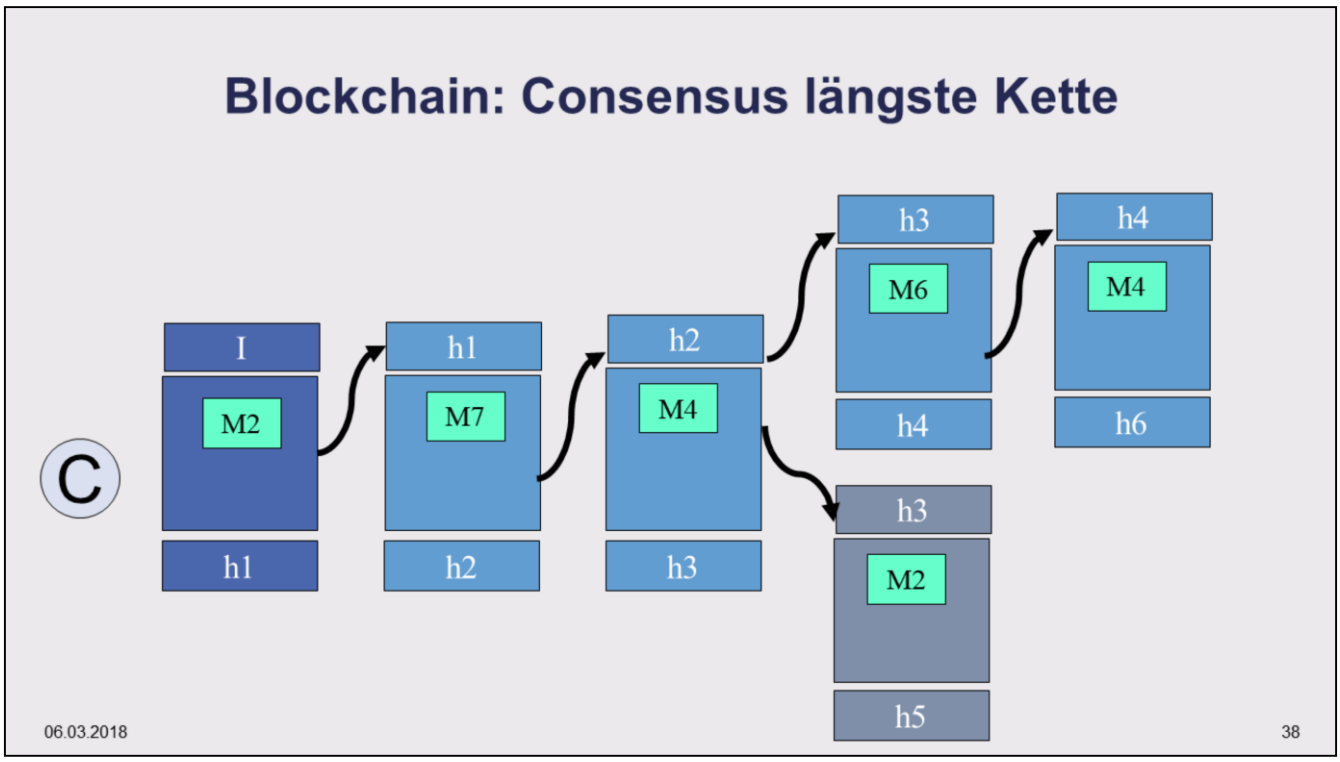


Die Miner schicken den gefundenen Block an alle Teilnehmenden.

Blockchain: Verkettung der empfangenen Blöcke mit weiteren empfangenen Blöcken



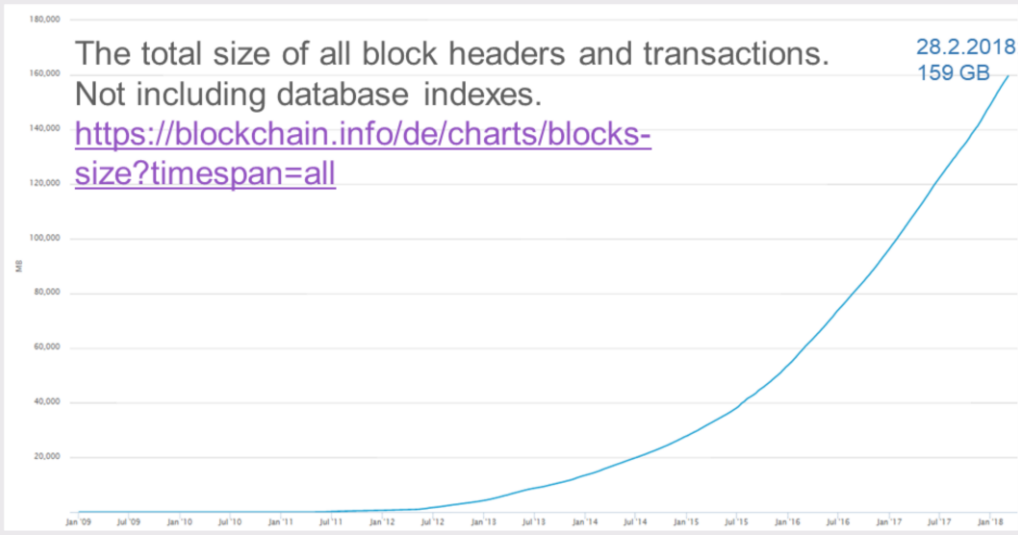
Miner verketten weitere Blöcke mit den vorangehenden Blöcken, indem der vorangehende Hash als «Blocknummer» verwendet wird.



Die Miner arbeiten unabhängig voneinander und man weiss nicht, wie viele Teilnehmer bzw. Minder mitmachen. Zu einem Block können mehrere verkettete Blöcke eintreffen, weil mehrere Miner etwa gleichzeitig einen Hash gefunden haben. In den von verschiedenen Minern ankommenden Blöcken können unterschiedliche Transaktionen enthalten sein. Die Entscheidung, welchen Block bzw. welche Transaktionen nun «als gültig» erklärt werden sollen, fällt man in diesem «verteilten Transaktionsjournal» über ein Consensus Verfahren. Bei diesem lässt man temporär Abzweigungen in der Kette der Blöcke zu. Nach weiteren eintreffenden Blöcken werden die verzweigten Ketten weiter verlängert. Das Consensus Verfahren erklärt diejenige Kette als die «gültige Kette», welche länger ist bzw. welche mit einem höheren Aufwand berechnet wurde. Man spricht in diesem Zusammenhang von «Proof of Work». Die Transaktionen und Mining Rewards in der nicht weiter geführten Kette sind ungültig.

Bei Bitcoin wird gesagt, dass eine Transaktion erst nach 6 weiteren eingetroffenen Blöcken als «gültig» angesehen werden sollte. Da etwa alle 10 Minuten ein neuer Block eintrifft, sind somit Transaktionen nach etwa einer Stunde abgeschlossen.

Beispiel: Entwicklung der Grösse der Bitcoin Blockchain



2.2.2 Blockchain Anwendungen

Transaktionsarten

- Besitzerangaben
  - Land-, Immobilienbesitz
  - Diamantenbesitz
  - Besitz von Internet Domainnamen (DNS)
- Geldüberweisungen
  - Crypto Currency

Blockchain Anwendungsbeispiele

coinmarketcap.com/coins/views/all

Die Liste der Blockchain Anwendungsbeispiele zeigt enorm viele Projekte. Falls man diese mit den Listen vergangener Jahre vergleicht, so ist offensichtlich, dass jeweils sehr viele Projekte wieder verschwinden.

Blockchain Wallets

- **Web Browser** (Cooinapult, Green Address, BitGo, Coin.Space)
- **Android** (breadwallet, Electrum, Green Address, GreenBits, Mycelium, Airbitz, ArcBit, Coin.Space, Simple Bitcoin, Bitcoin Wallet, Bither)
- **Desktop Client Windows** (ArcBit, Armory, Bitcoin Core, Bitcoin Knots, Bither, Electrum, Green Address, mSIGNA)
- **Hardware-Wallets** (USB-Sticks Ledger Nano S, KeepKey, Trezor)

Für die Nutzung von Cryptocurrency Blockchains wurden Blockchain Wallets (Brieftasche für Coins) eingeführt. Diese sind in der Regel keine vollwertige Blockchain Nodes, d.h. sie laden nicht die ganze Bockchain zu sich herunter. Ein Wallet ist ein Software Programm in dem Coins (vor allem Bitcoins) gespeichert werden. Es gibt verschiedene Wallet-Anbieter, die miteinander kompatibel sind. Es gibt Wallets als Desktop-, Mobile-, Online-, Hardware- und Papier-Version.

Das Wallet ist durch den Public Key des Inhabers eindeutig identifiziert. Der Public Key stellt eine Art Cryptocurrency (Bitcoin) Adresse dar, an welche Coins überwiesen werden können. Der Besitzer des Wallets ist nicht immer namentlich bekannt. In der Regel wird keine „Know Your Customer (KYC)“ Legitimationsprüfung durchgeführt, wie sie bei Banken, Kreditinstituten oder Versicherungen regulatorisch verlangt ist.

Für den Zugriff auf sein Wallet muss man seinen privaten Schlüssel bzw. einen Geheimcode kennen. Falls man diesen verliert, kann man nicht mehr auf seine Token bzw. Cryptocurrency zugreifen.
https://de.yeeply.com/blog/was-ist-ein-blockchain-wallet

Wallet Formen https://www.buybitcoinworldwide.com/de/bitcoin-wallets :

- Hardware Wallets
  - Das Ledger Nano S ist die Günstigste der drei Hardware-Wallets mit einem Bildschirm; sie kostet rund 95 $. Ledger, eine der bekanntesten Bitcoin-Security-Firmen, hat das Gerät im August 2016 rausgebracht.
  - TREZOR wurde im August 2014 als die erste Bitcoin-Hardware-Wallet eingeführt und bietet sichere Bitcoin-Speicherung und die Fähigkeit, mit dem Komfort einer Hot Wallet auszugeben. TREZOR ist ein kleines, daumengroßes Gerät.
  - KeepKey wurde im September 2015 rausgebracht und war die zweite Hardware-Bitcoin-Wallet mit einem Bildschirm. Der größere Bildschirm bietet ihr einige zusätzliche Sicherheitsfunktionen, die dem Nano S und Trezor fehlen.
- Papier-Wallets sind reine Papierdokumente mit den Schlüsselinformationen in Form von QR-Codes auf Papier: Einen Code mit einer öffentliche Adresse, um die Bitcoins zu empfangen und einen zweiten QR-Code mit dem privaten Schlüssel für das Verwahren und Versenden von Bitcoins.

Beispiel: Private Key Backup mit Cryptosteel

cryptosteel.com

Cryptosteel HEX

- One set contains 285+ letter tiles and numbers.
- Unit can be used as an “eternal backup” for:
  - any Cryptocurrency RAW Private Key
  - Ethereum Private Key Backup
  - Token Key Backup
- USD 79 (includes $68 Lifetime Warranty)

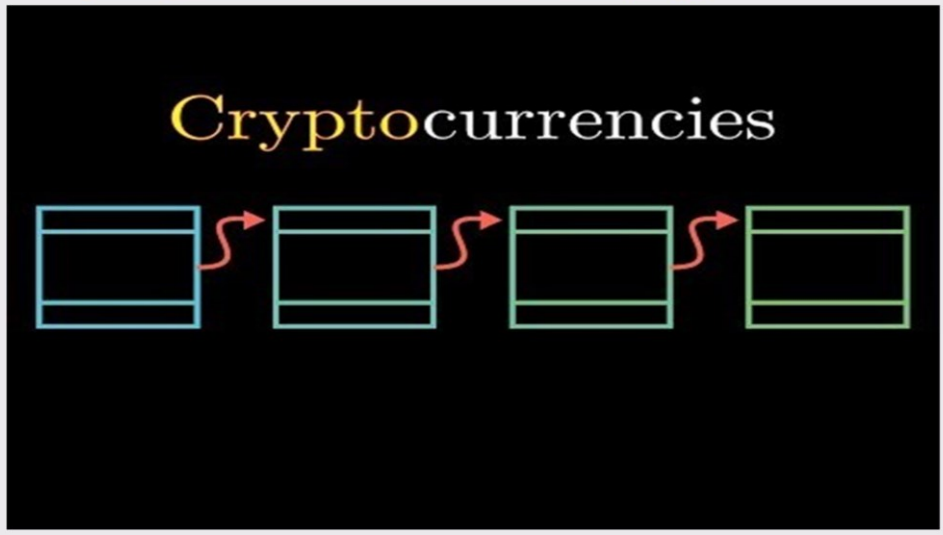
Cryptosteel is the premier indestructible backup tool for optimal offline storage of private keys, passwords and wallet recovery seeds without any third-party involvement. You can think of Cryptosteel as the master of all backups. A safe deposit box for your virtual valuables. The one artifact you can hold in your hand that actually protects your digital assets. The DIY equivalent of engraving—which is the most proven and reliable method of storing information invented to date.

Cryptosteel comes with more than 250 stainless steel letter tiles engraved on each side. Codes and passwords are assembled manually from the supplied part-randomized set of tiles. Users are able to store up to 96 characters worth of confidential information in minutes, guaranteeing safety of the data with no need for specialized tools or third-party involvement. Once a desired sequence is locked into the Cryptosteel unit, it essentially gains the status of offline permanence, featuring resistance to physical damage, including fire, flooding, corrosive conditions and impact from accidents.

2.3 Zusammenfassung

Ever wonder how Bitcoin (and other cryptocurrencies) actually work?

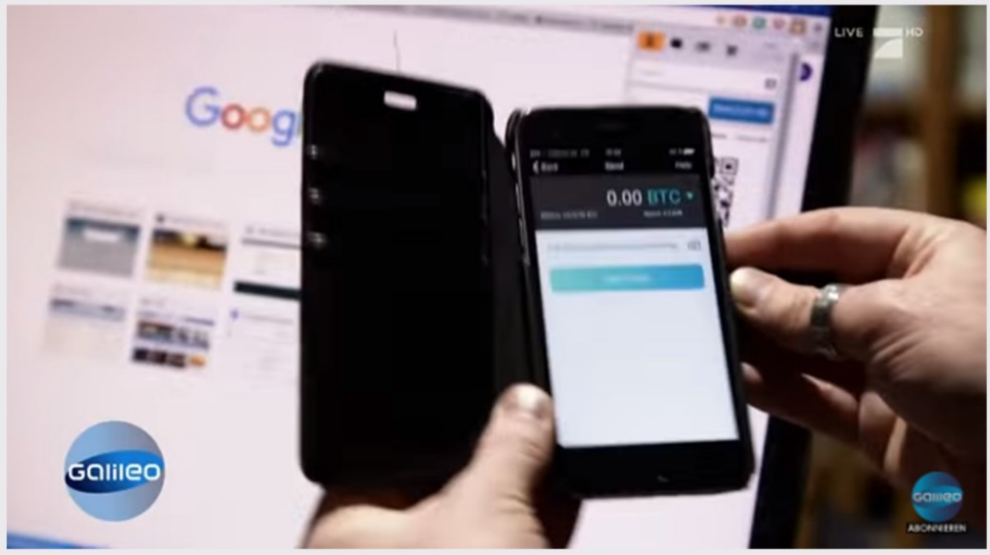
www.youtube.com/watch?v=bBC-nXj3Ng4 26m20s



07.07.2017 Bitcoin explained from the viewpoint of inventing your own cryptocurrency.
https://youtu.be/bBC-nXj3Ng4 26m20s
Patreon: https://patreon.com/3blue1brown Protocol Labs: https://protocol.ai/

For contributions in cryptocurrency to Patreon use the following addresses.
ETH: 0x88Fd7a2e9e0E616a5610B8BE5d5090DC6Bd55c25
BTC: 1DV4dhXEVhGELmDnRppADyMcyZgGHnCNJ
LTC: LNPY2HEWv8igGckwKrYPbh9yD28XH3sm32

Bitcoins: Wie zuverlässig funktioniert die Internetwährung? Galileo, ProSieben, 22.11.2017 www.youtube.com/watch?v=53wwrkRTNbw 10m34s



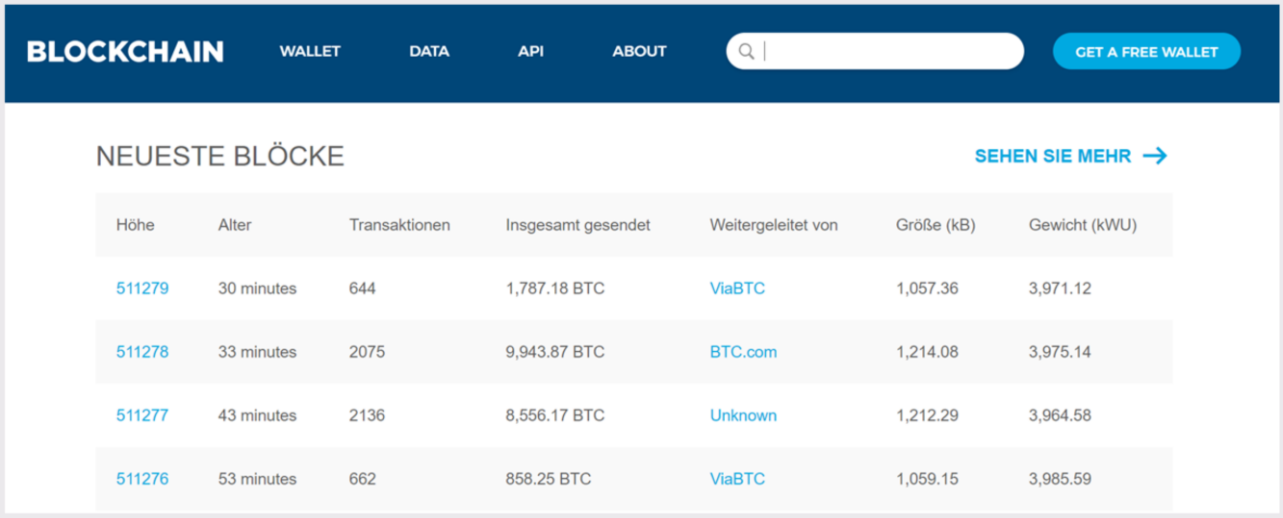
22.11.2017 Galileo **Bitcoins: Wie zuverlässig funktioniert die Internetwährung?**

Ob beim Supermarkt oder im Bekleidungsgeschäft: Immer mehr Menschen zahlen inzwischen mit Bitcoins. Aber wie sicher ist diese Bezahlungsmethode wirklich?

https://www.prosieben.ch/tv/galileo/themen/thema-u-a-selbstexperiment-leben-mit-bitcoins 10m34s

Demo: Blockchain Luxembourg

https://blockchain.info



Höhe	Alter	Transaktionen	Insgesamt gesendet	Weitergeleitet von	Größe (kB)	Gewicht (kWU)
511279	30 minutes	644	1,787.18 BTC	ViaBTC	1,057.36	3,971.12
511278	33 minutes	2075	9,943.87 BTC	BTC.com	1,214.08	3,975.14
511277	43 minutes	2136	8,556.17 BTC	Unknown	1,212.29	3,964.58
511276	53 minutes	662	858.25 BTC	ViaBTC	1,059.15	3,985.59

Die von Nicolas Cary und Peter Smith 2011 gegründete Firma Blockchain blockchainl.com hat den Firmensitz in Luxembourg. Blockchain bietet Bitcoin Wallets mit Übergängen zu «normalem Geld» an.

Die Firma Firma Blockchain stellt mit Blockchain.info auch eine Webanwendungen zur Untersuchung und Analyse der Bitcoin Blockchain zu Verfügung. Damit kann man Details zur Blöcken, Transaktionen oder Minern anzeigen, wobei die historischen Daten bis zu den Bitcoin Anfängen (2011) zurückgehen.

How the blockchain is changing money and business | Don Tapscott, TED Banff Alberta, June 2016

youtu.be/PI8OlkkwRpc 18m49s

- Internet social inequelity is
- 70% of people who have land do not have a serious proff
- Sharing economy
  - B-airbnb, B-uber
  - Big sharing economy disrupters could be disrupted
  - Global diastra 600 Billion $ per year - send money back to manila > abra
  - Data asset: virtual you – is not owned by you > privacy protection
  - Content creators, intellectual property system is broken > Imogen Heap

16.09.2016 How the blockchain is changing money and business, Don Tapscott, https://youtu.be/PI8OlkkwRpc 18m49s

What is the blockchain? If you don't know, you should; if you do, chances are you still need some clarification on how it actually works. Don Tapscott is here to help, demystifying this world-changing, trust-building technology which, he says, represents nothing less than the second generation of the internet and holds the potential to transform money, business, government and society.

www.youtube.com/watch?v=PI8OlkkwRpc&index=3&list=PLY3awliEftl25xPLpRfzsCr9NkhbFZzPh&t=47s

TED TEDTalks is a daily video podcast of the best talks and performances from the TED Conference, where the world's leading thinkers and doers give the talk of their lives in 18 minutes (or less). Look for talks on Technology, Entertainment and Design -- plus science, business, global issues, the arts and much more.

Referenzen, weitere Informationen zur Vertiefung

- TED Präsentationen www.ted.com/search?q=blockchain
- BoxMining boxmining.com YouTube Channel youtu.be/dw4INCPven4 https://www.btc-echo.de
- Julian Hosp YouTube Channel, Blockchain, Kryptowährungen, Bitcoin, Ethereum, ICOs, TokenSales, etc. https://www.youtube.com/user/julianhosp/featured
- IEEE Spectrum, Blockchain World, spectrum.ieee.org/static/special-report-blockchain-world
- Daniel Drescher, Blockchain Basics, A Non-Technical Introduction in 25 Steps, Apress, eBook ISBN 978-1-4842-2604-9, 201, 244p. www.apress.com/de/book/9781484226032

- BoxMining: YouTube channel breaking down the most important topics into easy-to-stand videos, covering Bitcoin, DASH, Ethereum, Decred, etc. www.btc-echo.de

- Galileo TV Thema Bitcoin ch.galileo.tv/themen/bitcoin
  Erik Finman ging mit seinen Eltern eine Wette ein: Wenn er es schaffen würde, mit 18 Jahren ein Millionär zu sein, dann dürfen sie ihn nicht dazu zwingen, aufs College gehen zu müssen. Jetzt ist er 18. Und Millionär. „Ich kann mit Stolz sagen, dass ich es geschafft habe, und ich gehe nicht aufs College“, so Finman. Ziemlich abgefahren, oder? Das hat er geschafft, indem er 1.000 Dollar – die ihm seine Oma 2011 vermacht hatte – in die Kryptowährung Bitcoin investierte. Einfach ausgedrückt handelt es sich bei Bitcoin um eine digitale Geldeinheit. Wie genau das Bitcoin-System funktioniert, erklären wir euch hier:
- 7.7.2017, Ever wonder how Bitcoin (and other cryptocurrencies) actually work? Bitcoin explained from the viewpoint of inventing your own cryptocurrency. https://youtu.be/bBC-nXj3Ng4 26m20s
- Michael Nielsen, How the Bitcoin protocol actually works, 6.12.2013 http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/
- 14.7.2013, Video by CuriousInventor, A somewhat technical explanation of how Bitcoin works. https://youtu.be/Lx9zgZCMqXE 22m24s
- In-depth course “Introduction to Bitcoin and Decentralized Technology” on the latest in Bitcoin, Blockchain, and a survey of the most exciting projects coming out (Ethereum, etc). Lots of demos on how to buy, send, store (hardware, paper wallet). how to use javascript to send bitcoin. How to create Ethereum Smart Contract, much more. https://www.pluralsight.com/courses/bitcoin-decentralized-technology
- 5.11.2016, Video by Anders Brownworth, Very basic visual introduction to the concepts behind a blockchain, introduces the idea of an immutable ledger with an interactive web demo. youtu.be/_160oMzblY8 17m49s
- Original Bitcoin paper: bitcoin.org/bitcoin.pdf
- Ethereum white paper: goo.gl/XXZddT
- 8.7.2017 Supplement to the cryptocurrency video: How hard is it to find a 256-bit hash just by guessing and checking? What kind of computer would that take? youtu.be/S9JGmA5_unY 5m05s

Blockchain Informations- und Analysesysteme

- **Block Explorer** blockexplorer.com offers open source web tools that allow you to view information about blocks, addresses, and transactions on the Bitcoin, Bitcoin Cash, and Zcash blockchain.
- **Blockchain** blockchain.com is the world's leading software platform for digital assets. Blockchain offers with blockchain.info real time and historical Blockchain transaction data.
- **Coinmarketcap** coinmarketcap.com offers various tools illustrating the evolution of crypto currencies.

Block Explorer blockexplorer.com is the longest running source of Bitcoin blockchain information and a leader in the financial technology media industry. Block Explorer offers open source web tools that allow you to view information about blocks, addresses, and transactions on the Bitcoin, Bitcoin Cash, and Zcash blockchain.

Blockchain www.blockchain.com is the world's leading software platform for digital assets. Offering the largest production blockchain platform in the world. The Blockchain software has powered over 100M transactions and empowered users in 140 countries across the globe to transact quickly and without costly intermediaries. Blockchain www.blockchain.info offers tools for developers and real time transaction data for users to analyze the burgeoning digital economy.

Coinmarketcap coinmarketcap.com offers various tools illustrating the evolution of crypto currencies.