BLOCKCHAIN: TECHNICAL FOUNDATION

LUZIUS MEISSER, COMPUTER SCIENTIST AND ECONOMIST
BITCOIN ASSOCIATION SWITZERLAND

OVERVIEW

- Setting the Stage
- Bitcoin: Electronic Cash
- Ethereum: Smart Contracts
- Arbitration Opportunity
- Questions & Answers

THE SLAYING OF BEARWHALE, OCTOBER 6, 2014

«Crypto Valley»

GDI Impuls 2 . 2016

Blockchain

Eine Chance für den Finanzplatz

Gastkommentar
von LUZIUS MEISSER

Ein kleiner Schritt des Gesetzgebers könnte dem Finanzplatz einen grossen Schritt vorwärts erlauben. Gemessen an der Marktkapitalisierung liegen unsere Grossbanken zurzeit am Boden, zermürbt von Jahren der Krise und rechtlicher Querelen. Die Situation in Gesamteuropa sieht nicht besser aus. So sah sich die Deutsche Bank unlängst veranlasst, auf ihre Solvenz hinzuweisen, und es wird auch wieder laut über milliardenschwere Rettungspakete nachgedacht. In diesem unsicheren Umfeld bietet die vielbeschworene Blockchain-Technologie die Chance, ein neues, dezentral organisiertes und damit robusteres Finanzsystem aufzubauen.

Die weltweit bekannteste Anwendung der Blockchain-Technologie ist die Internetwährung Bitcoin. Auf Rang zwei folgt das jüngere und technisch überlegene Ethereum, das in Zug entwickelt wird. Zug ist es gelungen, zu einem Kristallisationskeim der Szene zu werden. Das Erfolgsgeheimnis ist einfach: Blockchain-Startups werden mit offenen Armen empfangen und rechtlich-steuerliche Fragen rasch und unkompliziert beantwortet, während andernorts die Behörden behäbiger agieren.

Dass manchmal kleine regulatorische Unterschiede über die Zukunft einer ganzen Region entscheiden können, zeigt das Beispiel Hollywood. Gemäss Harvardprofessor Lawrence Lessig ist Hollywood heute deshalb in Hollywood und nicht etwa an der Ostküste der USA beheimatet, weil das kalifornische Bezirksgericht die Filmpa- automatisch durchgesetzt werden können. Die erste solche Organisation wurde diesen Frühling mit umgerechnet 150 Millionen Franken Kapital im Ethereum-System lanciert. Kurz darauf gelang es einem Hacker unter Ausnützung eines Programmierfehlers, in den Statuten einen Drittel des Kapitals auf ein eigenes Konto abzuzweigen, bevor ihm das meiste davon auf abenteuerliche Weise wieder abgenommen werden konnte. Der vernünftigere Ansatz wäre wohl der Verzicht auf die vollständige Automatisierung und die Schaffung von Schnittstellen für Schiedsstellen, die im Ernstfall schlichtend eingreifen könnten. So oder so entsteht die Nachfrage nach Spezialisten in Finanzen, Recht und Informatik sowie nach neutralen und stabilen Standorten, die eine Verknüpfung von Einträgen in einer Blockchain mit der übrigen Realität rechtswirksam zulassen.

Die Schweiz ist dank Neutralität und Stabilität gut positioniert, um ein solcher Standort zu werden. Zudem sind unsere Gesetze allgemein formuliert, was den zuständigen Behörden erlaubt, diese mit Augenmass auf neue Gegebenheiten anzuwenden. Zum Beispiel hat die Eidgenössische Steuerverwaltung früh Bitcoin als Zahlungsmittel im Sinn des Mehrwertsteuergesetzes anerkannt, während die Steuerbehörden anderer europäischer Länder erst durch den Europäischen Gerichtshof an diese Einsicht herangeführt werden mussten. Eine Hürde besteht aber noch darin, dass das Schweizer Gesetz die Schriftform bei der Übertragung von Forderungen und Wertrechten vorschreibt.

Im papiernen Alltag ist dies durchaus im Interesse der involvierten Parteien, doch in einer digi-

ECOSYSTEM

Banks

MME
Legal | Tax | Compliance

Lawyers

Crypto-Startups

SINGULAR

Issue tokens to fund themselves

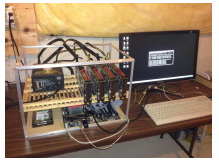
Bitcoin Suisse

satoshiDICE

Merchants, Gambling, etc.

Exchanges, Broker

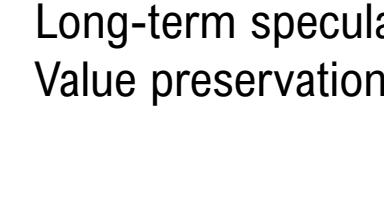
Miner

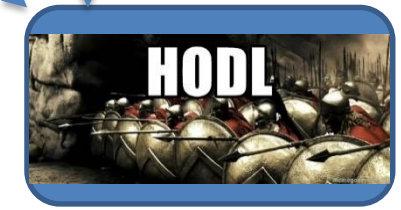


“mine” new coins,
Operate infrastructure

Users

Traders





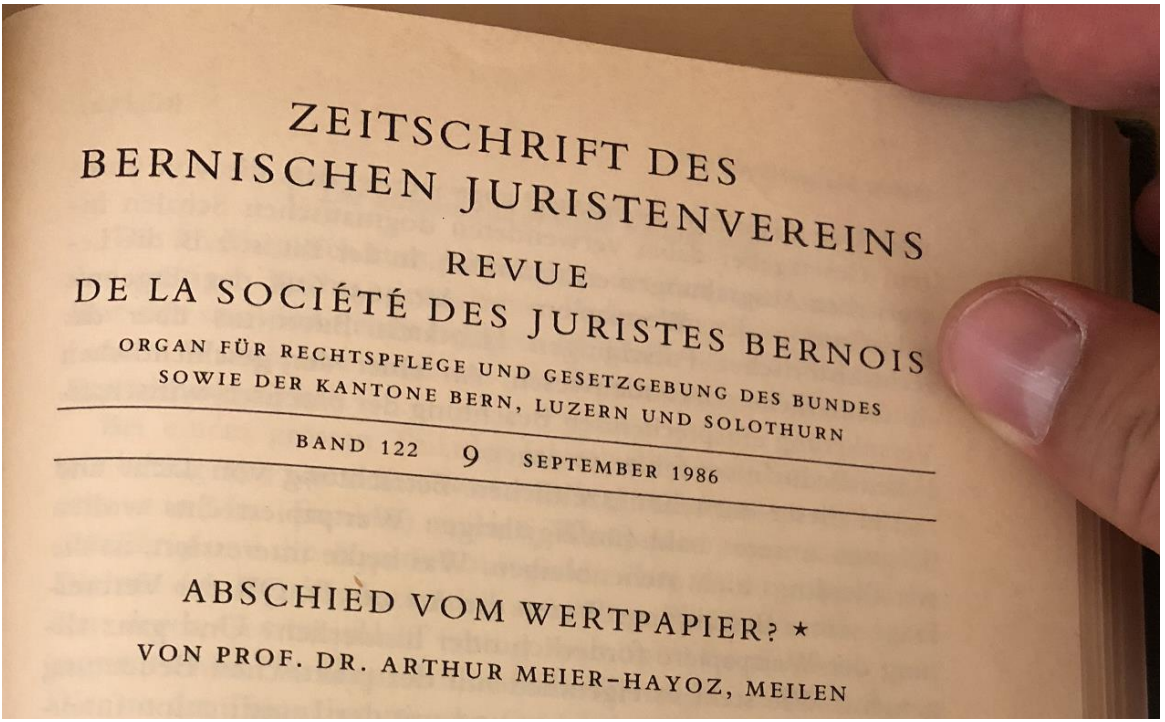
Long-term speculation,
Value preservation.

Regulators

DYNAMIC EQUILIBRIA ARE MORE STABLE

- The health of a forrest is determined by the young trees
- Making old trees support each other makes the system as a whole more fragile
- Tree line: small incremental differences in the surrounding conditions can have a huge impact

A DECLINING "TREE LINE" IN FINANCE?



ZEITSCHRIFT DES
BERNISCHEN JURISTENVEREINS

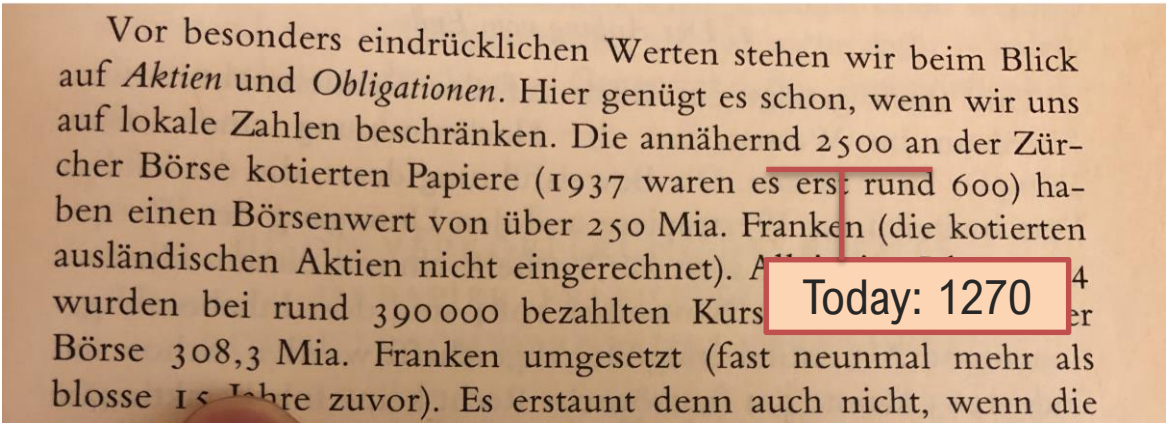
REVUE
DE LA SOCIÉTÉ DES JURISTES BERNOIS

ORGAN FÜR RECHTSPFLEGE UND GESETZGEBUNG DES BUNDES
SOWIE DER KANTONE BERN, LUZERN UND SOLOTHURN

BAND 122 9 SEPTEMBER 1986

ABSCHIED VOM WERTPAPIER? *

VON PROF. DR. ARTHUR MEIER-HAYOZ, MEILEN



Vor besonders eindrücklichen Werten stehen wir beim Blick auf *Aktien* und *Obligationen*. Hier genügt es schon, wenn wir uns auf lokale Zahlen beschränken. Die annähernd 2500 an der Zürcher Börse kotierten Papiere (1937 waren es erst rund 600) haben einen Börsenwert von über 250 Mia. Franken (die kotierten ausländischen Aktien nicht eingerechnet). A 4 wurden bei rund 390 000 bezahlten Kurs er Börse 308,3 Mia. Franken umgesetzt (fast neunmal mehr als blosse 15 Jahre zuvor). Es erstaunt denn auch nicht, wenn die

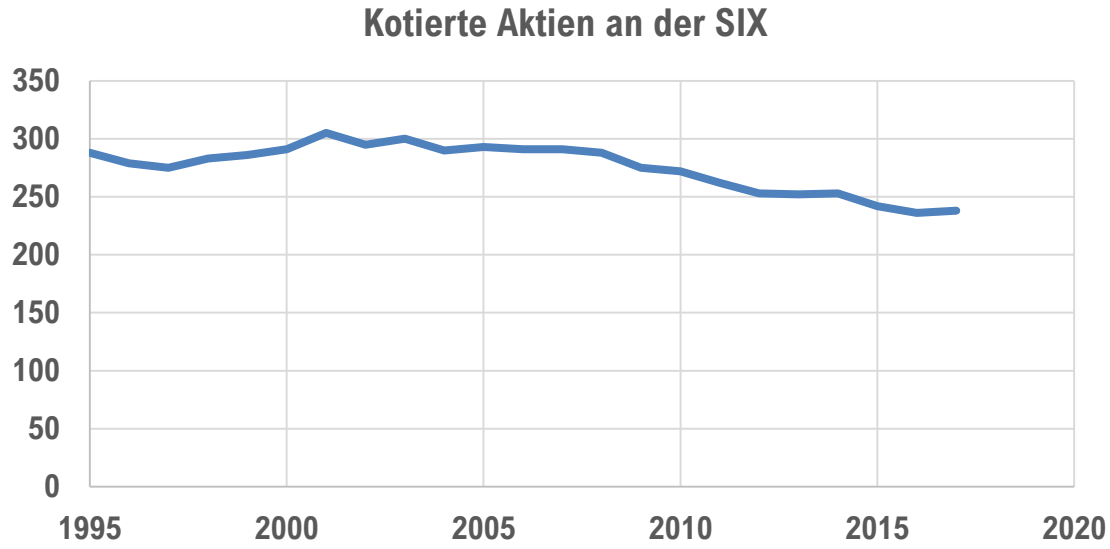
Today: 1270

Tabelle 1

Wertschöpfung, in Mio. Franken

	2007	2012	2017
Finanzdienstleistungen	47 068	34 581	30 787
Versicherungsdienstleistungen	26 777	28 429	29 951
Total Finanzstandort	**73 845**	**63 010**	**60 738**
in % des BIP	**12,8**	**10,1**	**9,1**
BIP Schweiz	576 088	626 414	668 149

Daten: BFS / SECO, Jahresaggregate des BIP, Produktionsansatz (Jahreswerte).

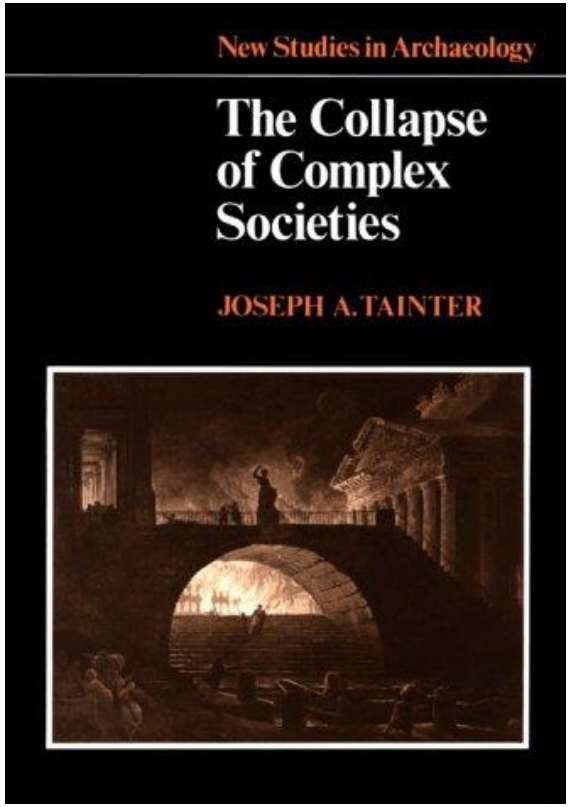


RISK: RISK-AVERSION

Google Books Ngram Viewer

Graph these comma-separated phrases: opportunity,risk case-insensitive

between 1800 and 2008 from the corpus English with smoothing of 5 . Search lots of books



«Compliance is not a product.» - Daniel Aegerter, Fintech-Investor
«Die grösste Sorge bereitet mir, dass wir als Gesellschaft keine Risiken mehr eingehen. Darunter leidet unsere Wirtschaft und unsere Bildung. Angst tötet die besten Ideen.» - Patrick Aebischer, EPFL

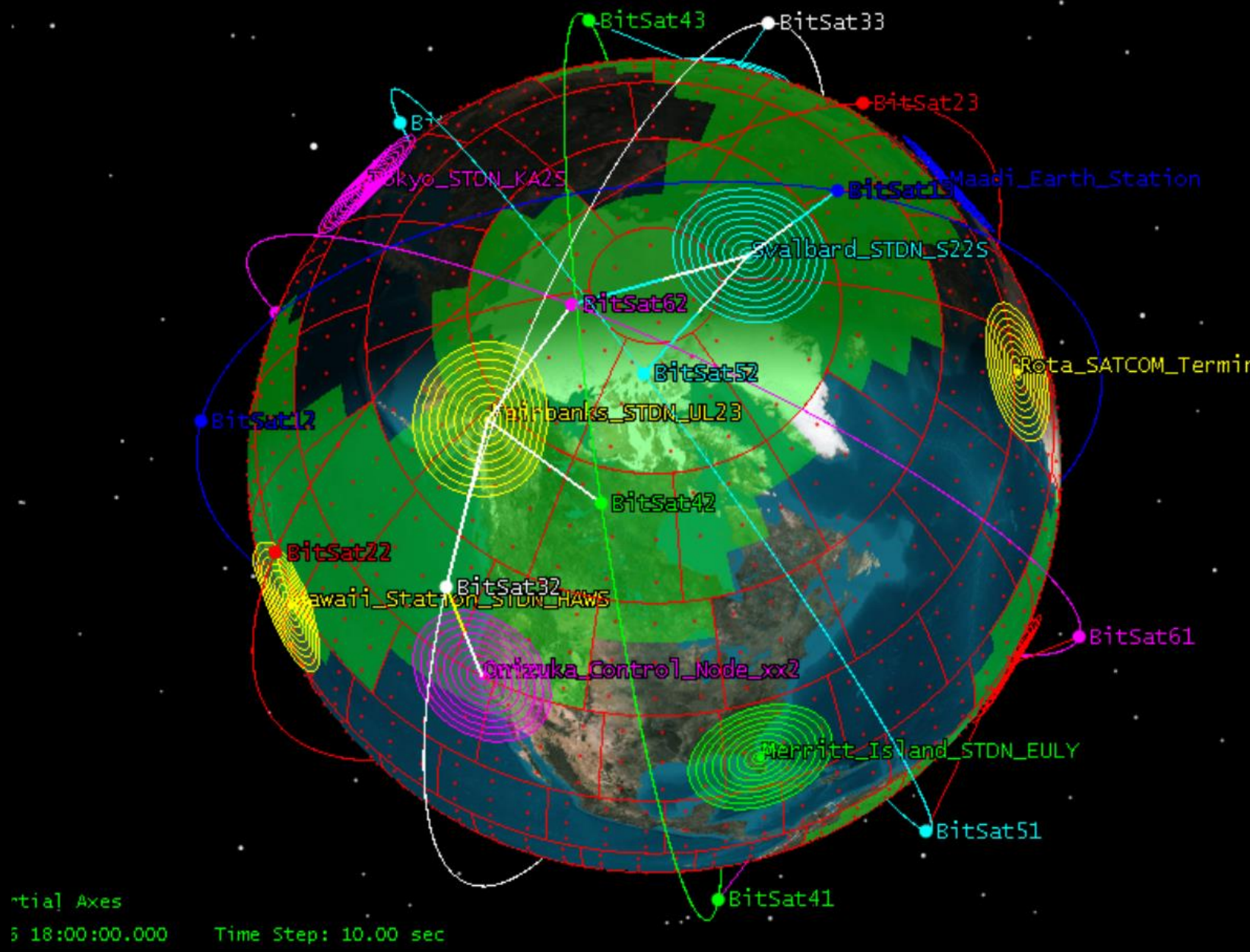
BITCOIN VISION

A decentralized, world-wide and free financial system.

An Internet of Finance.

Anyone can transact with anyone else at any time.

(But who resolves disputes?)



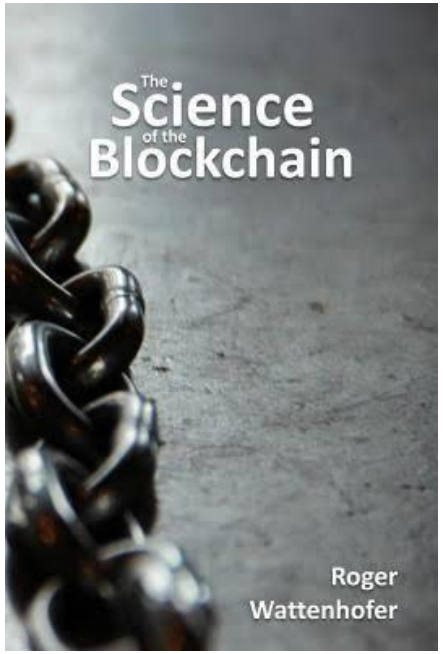
WHAT IS BITCOIN?

Bitcoin is digital cash.

Bitcoin enables the transfer of digital assets directly from person to person, without intermediary.

The underlying innovation is the blockchain, a very inefficient but also very robust way to reach distributed consensus.

I the blockchain unregulated? No, but regulation that is attached to the financial intermediary does not apply, as there is none.



A BITCOIN IS NOT DATA

Bitcoin and other crypto tokens are NOT “data”, at least not according to the definitions of Computer Science. (Common misconception in the legal literature.)

In Computer Science, data is a string of characters. Its length is measured in Bits. Information is data with an interpretation. Data is objective, information is subjective. Information is also measured in Bits, but depends on the context, as the same data can have different meanings in different contexts.

In the Bitcoin system, data is used to keep track of the balances, but there is no string of characters that can be associated with a particular Bitcoin or fraction thereof.

WHAT IS BITCOIN?

What is Bitcoin in legal terms?

- Vermögenswert, Geld im weiteren Sinn
- Keine Forderung, kein Wertrecht, kein Guthaben
- Can be transferred directly from person to person
- Use the blockchain instead of paper to transfer possession.

-> Much more similar to physical cash than to bank deposits.

Gabriela Hauser, Luzius Meisser, Eigenschaften der Kryptowährung Bitcoin, Digma 1/2018

Eigenschaften der Kryptowährung Bitc

Geld, aber ohne Sachqualität – wem «gehört» ein Bitcoin be Verfügungsmacht?

Gabriela Hauser-Spühler, Rechtsanwältin und Urkundsperson des Kantons Zug, Lachen SZ ghauser@hauser-law.ch

Luzius Meisser, Informatik-Ingenieur und Mitgründer der Bitcoin Association Switzerland, Erlenbach ZH luzius@meisser economics.com

Nach einer allgemeinen Betrachtung der Internetwährung wird erstmals zur Möglichkeit des Mitgewahrsams am Vermögenswert Stellung genommen.

Der Wechselkurs des Bitcoins brach in den Wochen vor dem Jahreswechsel einen Rekord nach dem anderen. Anfang 2017 kostete ein Bitcoin noch USD 1000. Ende Jahr waren es bereits USD 14 000. Der Gesamtwert aller Bitcoins erreichte über 200 Milliarden. Bitcoin gehört damit – an der Geldmenge gemessen – zu den grössten 20 Währungen der Welt, noch vor der norwegischen Krone, aber ein Stück hinter dem Schweizer Franken, bei dem die Geldmenge dreimal so gross ist[1,2].

Der Vizepräsident der Europäischen Zentralbank, Vítor Constâncio, verglich Bitcoin in Anspielung auf die Spekulationsblase des 17. Jahrhunderts in den Niederlanden mit einer «Tulpe»[3]. Doch darf Bitcoin nicht einzig als spekulative Gier abgetan werden. Die dem Bitcoin zugrunde liegende Technologie, die Blockchain, ist mehr als eine Tulpe. Sie könnte das Fundament sein für ein «Internet of Finance», einem weltweiten, freien und digitalen Finanzsystem.

Die Schweiz ist ein Kristallisationskeim dieser Entwicklung, die eine enorme Chance für den Finanzplatz darstellt. Bundesrat Johann Schneider Ammann hat unlängst die Vision einer «Crypto Nation Switzerland» geäussert und das Staatssekretariat für Internationale Finanzfragen eine Arbeitsgruppe zur Klärung des recht-

Ist Bitcoin Geld?

Funktionale Betrachtung

Bitcoin ist eine dezentral org
netwährung mit einem zugehör
system, das auf der Innovation
beruht. Der Wechselkurs entste
deren Währungen durch Angebo
ge auf dem freien Markt. Der
coins wird von niemandem gara
Aufhebung des Goldstandards
gilt dies übrigens auch für den S
ken[6]. Die Menge an Bitcoins ist
auf 21 Millionen Bitcoins begr
dieser Verknappung des Angebo
oft auch als «digitales Gold» b
ders als in allen zuvor geschaff
schen Zahlungssystemen finden
im Bitcoin-System direkt von Pe
statt. Der Finanzintermediär – wi
se ein zwischengeschalteter Z
leister – entfällt.

Bitcoins oder Bruchteile dav
unkörperliche und vertretbare
die stets genau einer Adresse i
tem zugeordnet sind, betrachte
die Adresse ist definiert, wie d
Bitcoins auf eine neue Adres
werden können. Bei den meiste
mittels eines geheimen kryptogra
sels – eines langen Codes beste
Abfolge von Zahlen und Zeich
Werteinheiten verfügt, analog e
terschrift. Es können aber auch
tigungsmechanismen im Zusa
einer bestimmten Adresse konfi
Am Beispiel «Unterschrift zu zw
sen werden oft auch als Konte

HOW DOES THE BLOCKCHAIN WORK?

Just like the stone money of Yap, but without the stones.

On the pacific Island Yap, stones act as money for large denominations.
Problem: the large stones are too heavy to carry around.
Solution: don’t carry the stone around, but tell everyone who it belongs to.

Luzius Meisser *

Kryptowährungen: Geschichte, Funktionsweise, Potential

Beitrag zum Tagungsband «**Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme**»

Rolf H. Weber / Florent Thouvenin (Hrsg.), Schulthess 2015, 217 Seiten, broschiert, ISBN 978-3-7255-7217-5, CHF 82.00

Bestellen Sie Ihr Exemplar bei Schulthess

(More detailed technical article, link at the end.)

The blockchain works similarly: transactions become official by letting everyone know about them.

DEMO OF A BITCOIN TRANSACTION

1. Bitcoins are assigned to addresses
2. Anyone can generate as many addresses as she wants
3. The balance of every address is public
4. The power to dispose (Verfügungsmacht) over an address is exercised with one or more private key that are generated along with the address.
5. To send Bitcoins, generate an according transaction and sign it. E.g. “I hereby send 0.1 Bitcoin to address X, signed Y”
6. Announce the transaction publicly in the Bitcoin network and add a transaction fee.
7. If the transaction is formally valid and the fee high enough, it will be integrated into the blockchain, a chain of blocks that serves as an archive for all transactions that ever happened. The miners who integrated the transaction into the block serve as witnesses and archivers.

Address	1K4t2vSBSS2xFjZ6PofYnbgZewjeqbG1TM
Transactions	
No. Transactions	257
Total Received	16.39490321 BTC
Final Balance	16.39490321 BTC

ROLE OF PRIVATE KEYS

While a private key or a set of private key defines the power to dispose (Verfügungsmacht), the contractual situation needs to be considered when deciding who a Bitcoin belongs to (i.e. who has the right to dispose (Verfügungsrecht)).

This becomes clear when considering how the funds of the Tezos foundation are managed.

→ This distinction could be key in arbitration cases.

Bitcoin Suisse Foundation Funds Tezos

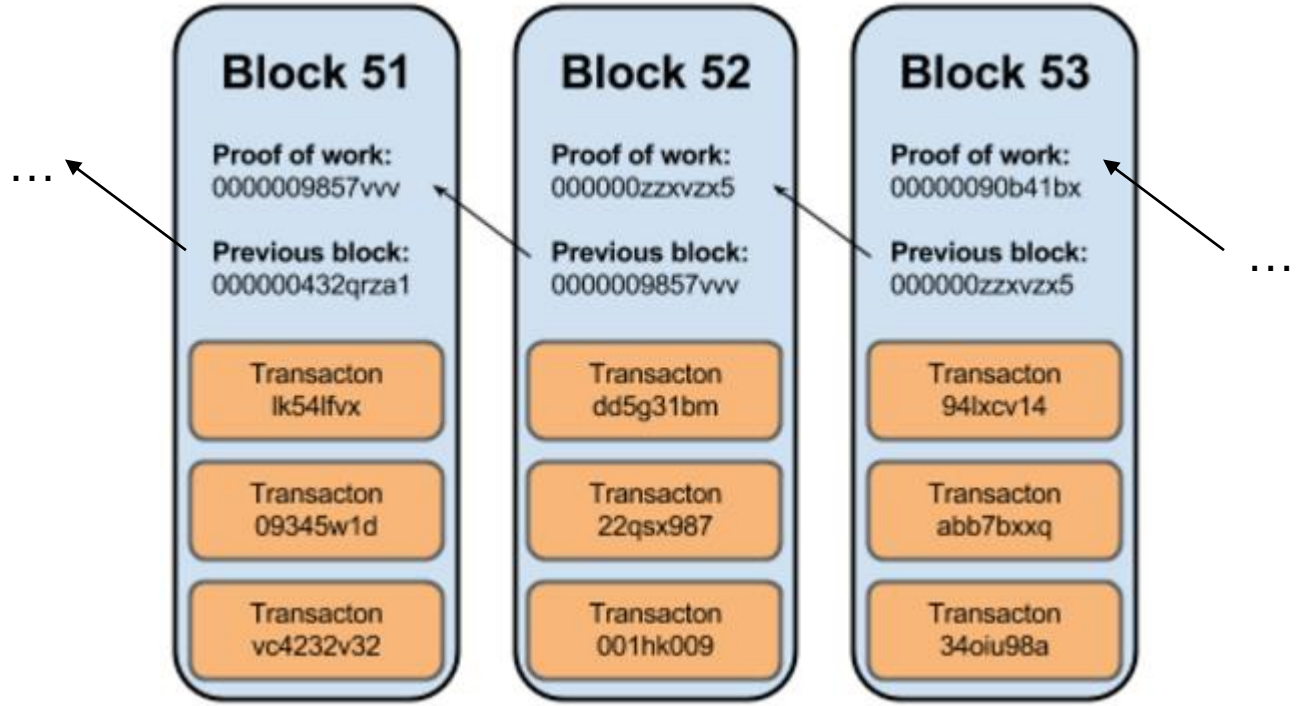
Vgl.: Christian Meisser / Luzius Meisser / Ronald Kogens, Verfügungsmacht und Verfügungsrecht an Bitcoins im Konkurs, in: Jusletter IT 24. Mai 2018

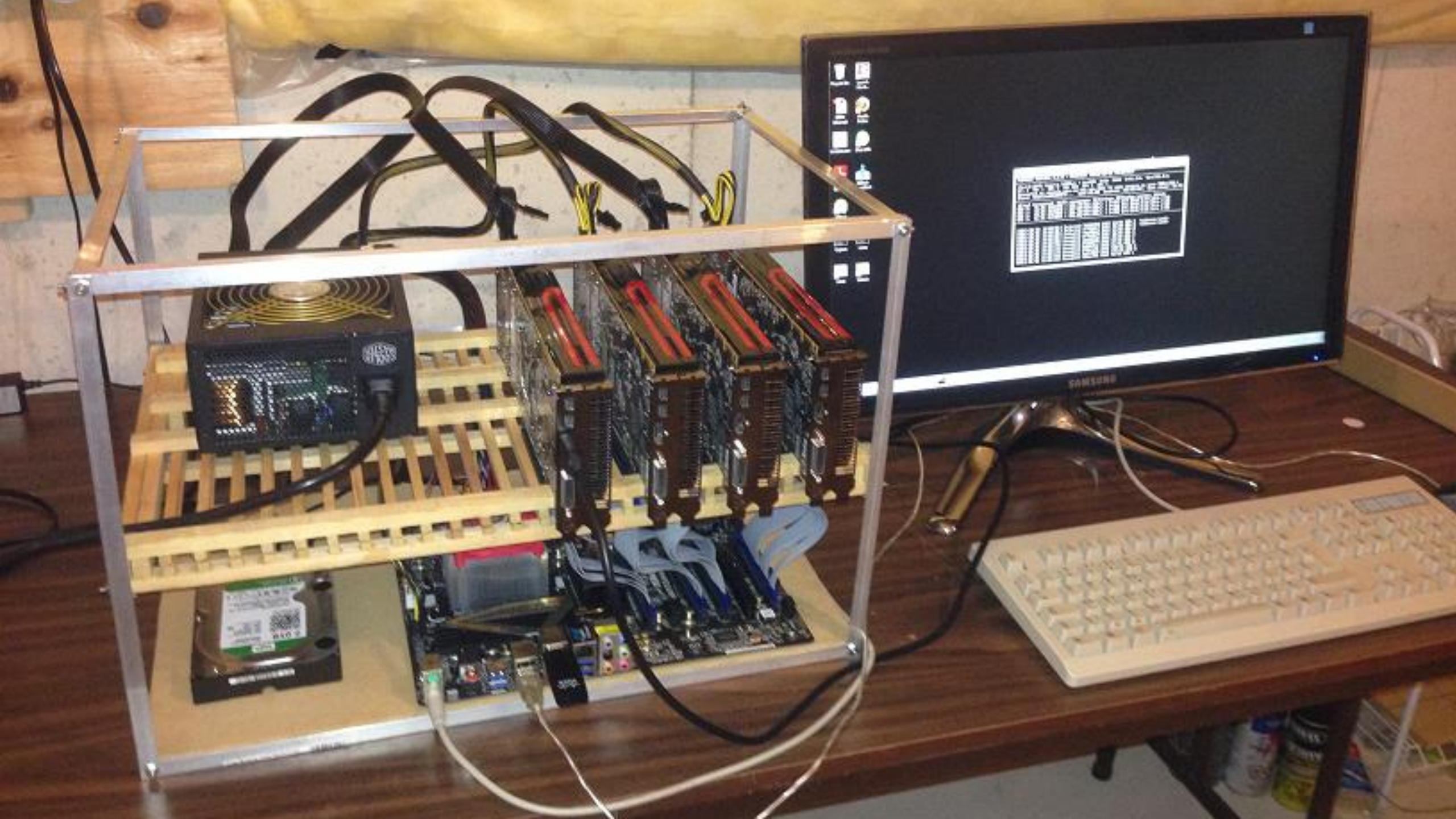
HOW TO BUILD A BLOCKCHAIN

1. Ingredient: electronic signatures to securely sign transactions
2. Ingredient : a distributed database, ensure that everyone knows everything
3. Ingredient : consensus mechanism to resolve conflicts

Consensus mechanisms:

- Traditional ones like Paxos that only works for closed systems (fixed number of participants)
- Proof-of-Work: most common. Democracy with voting weights proportional to computing power
- Proof-of-Stake: voting weights proportional to wealth





COUNTLESS CRYPTOCURRENCIES

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$110,801,367,935	$6,419.99	$3,654,215,127	17,258,812 BTC	3.26%	
2	Ethereum	$20,518,993,545	$201.45	$1,662,061,115	101,857,228 ETH	2.12%	
3	XRP	$11,321,104,634	$0.285525	$165,043,142	39,650,153,121 XRP *	3.33%	
4	Bitcoin Cash	$8,477,489,408	$488.91	$285,398,235	17,339,575 BCH	3.55%	
5	EOS	$4,631,994,473	$5.11	$594,272,868	906,245,118 EOS *	8.33%	
6	Stellar	$3,683,226,204	$0.196091	$54,177,719	18,783,274,341 XLM *	0.78%	
7	Litecoin	$3,265,913,064	$56.10	$256,676,504	58,219,828 LTC	6.15%	
8	Tether	$2,764,753,209	$1.00	$2,433,452,950	2,756,421,736 USDT *	-0.13%	

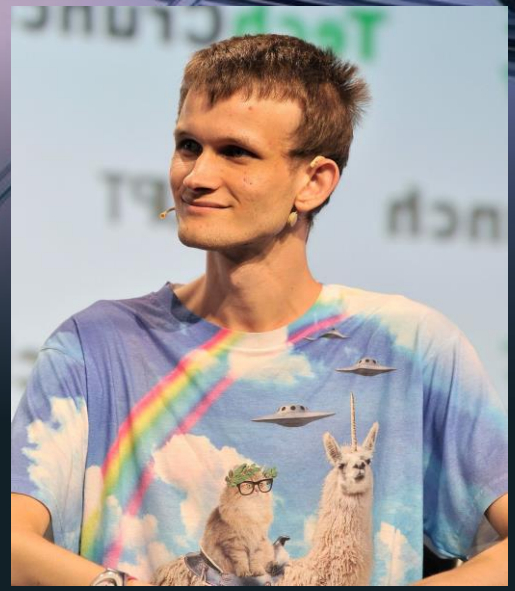
ethereum

HOMESTEAD RELEASE

BLOCKCHAIN APP PLATFORM

Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts:** applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.



BLOCKCHAIN VOCABULARY

- Cryptocurrency: an abstract value that serves as a means of payment within its own blockchain
- Token: an abstract value whose possession is tracked through a smart contract
- Ethereum: the most popular platform for smart contracts and the issuance of tokens
- ERC-20 Token: the most popular token standard within Ethereum
- Smart contract: A small, public program that lives on a blockchain and that everyone can interact with. Once it is deployed, it cannot be stopped or changed anymore unless it is designed to be so.
- Solidity: programming language to formulate Smart Contracts for the Ethereum system
- Address: an identifier to which tokens are assigned. Addresses can represent persons, groups of persons, or smart contracts.
- Private key: a cryptographic key that belongs to a particular address and that is needed to transact in the “name” of that address.
- Multi-signature address or wallet: requires signatures from multiple private keys to transact (e.g. two out of five)
- Wallet: a software or service to manage addresses

A real-world “smart contract”.

SELF-EXECUTING CONTRACTS

- Execute automatically within their system, allow system participants and other smart contracts to interact with it
- Can only refer to objects that are adequately represented in the system
- Most important use-case: securities on the blockchain

Die Blockchain als Standortvorteil

Schweizer Recht verlangt für das Übertragen von Forderungen und Wertrechten Schriftform. Das behindert digitales Abwickeln von Geschäften und die Entwicklung hier ansässiger Technologieunternehmen. **LUZIUS MEISSER**

Eine kleine Gesetzesänderung könnte in einer Zeit, in der gute Nachrichten über den Finanzplatz selten sind, einer digitalen Erneuerung den Weg bereiten. Das Obligationenrecht verlangt heute für die Übertragung von Forderungen und Wertrechten die Schriftform, was eine Hürde für die digitale Abwicklung solcher Geschäfte darstellt. Die Technologie dazu, nämlich die Blockchain, stünde bereit. Dank ihrer robusten, dezentralen Architektur könnte sie eine Schlüsselrolle in der globalen Finanzinfrastruktur der Zukunft spielen.

Sie ermöglicht nicht nur die Beschleu-

über den international berichtet wurde.

Die Internetwährung Bitcoin ist die älteste und bekannteste Anwendung der Blockchain-Technologie. Ethereum, das zweitgrösste Blockchain-basierte System nach Bitcoin, wird in Zug entwickelt. Ethereum hat gute Chancen, mittelfristig das etwas ältere und technisch weniger fortgeschrittene Bitcoin-System vom Thron zu stossen. Das wäre auch ein Erfolg für Zug und die Schweiz.

«In der Pionierphase einer

mit wenigen Zeilen Programmcode erstellen. Dass viele darin grosses Potenzial sehen, zeigt sich zum Beispiel daran, dass Elevence, ein aus der ETH hervorgegangenes Start-up, das eine eigene Programmiersprache zur Formulierung von selbstausführenden Verträgen entwickelt hat, bereits weniger als ein Jahr nach seiner Gründung von der New Yorker Finanzkoryphäe Blythe Masters aufgekauft wurde.

Doch so einig sich die Experten sind, dass es sich bei der Blockchain um eine revolutionäre Technologie handelt, so unklar ist es noch, welche Unternehmen sich

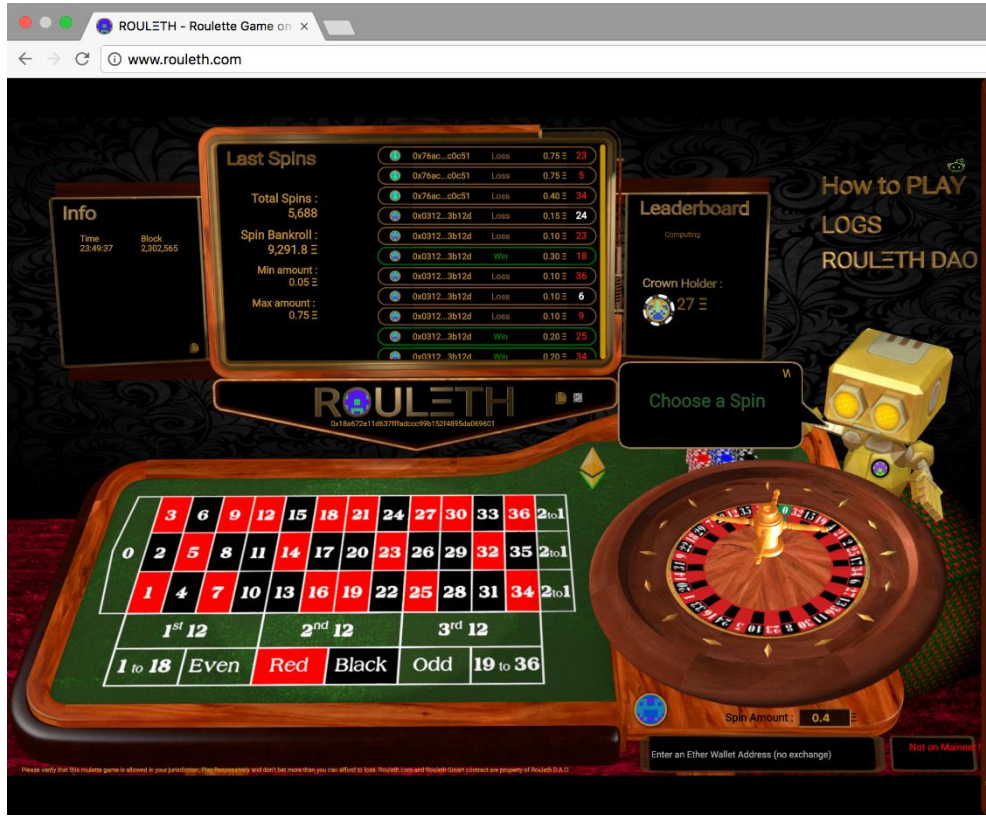
mit der Materie beschäftigen muss. Eine Hürde für die Digitalisierung besteht aber noch darin, dass das Obligationenrecht die Schriftform für die Übertragung von Forderungen (Art. 165) und von Wertrechten (Art. 973c) vorschreibt. Deshalb muss eine rechtsgültige Abtretung einer auf einer Blockchain festgehaltenen Forderung nach Schweizer Recht heute stets von einer manuellen Unterschrift begleitet werden. Dieses Erfordernis besteht anderswo (z.B. in Deutschland) nicht.

Manuelle Unterschrift weg

EXAMPLE: ROULETH

```
//  ROULETH
//
//  Play the Roulette on ethereum blockchain !
//  (or become a member of Rouleth's Decentralized Organisation and contribute to the bankroll)

contract Rouleth
{
  //Game and Global Variables, Structure of gambles
  address developer;
  Gamble[] gambles;
.....
  //bet on Number
  function betOnNumber(uint8 numberChosen) {
     //check that number chosen is valid and record bet
     if (numberChosen>36) throw;
        placeBet(BetTypes.number, numberChosen);
     }
  }
.....
}
```

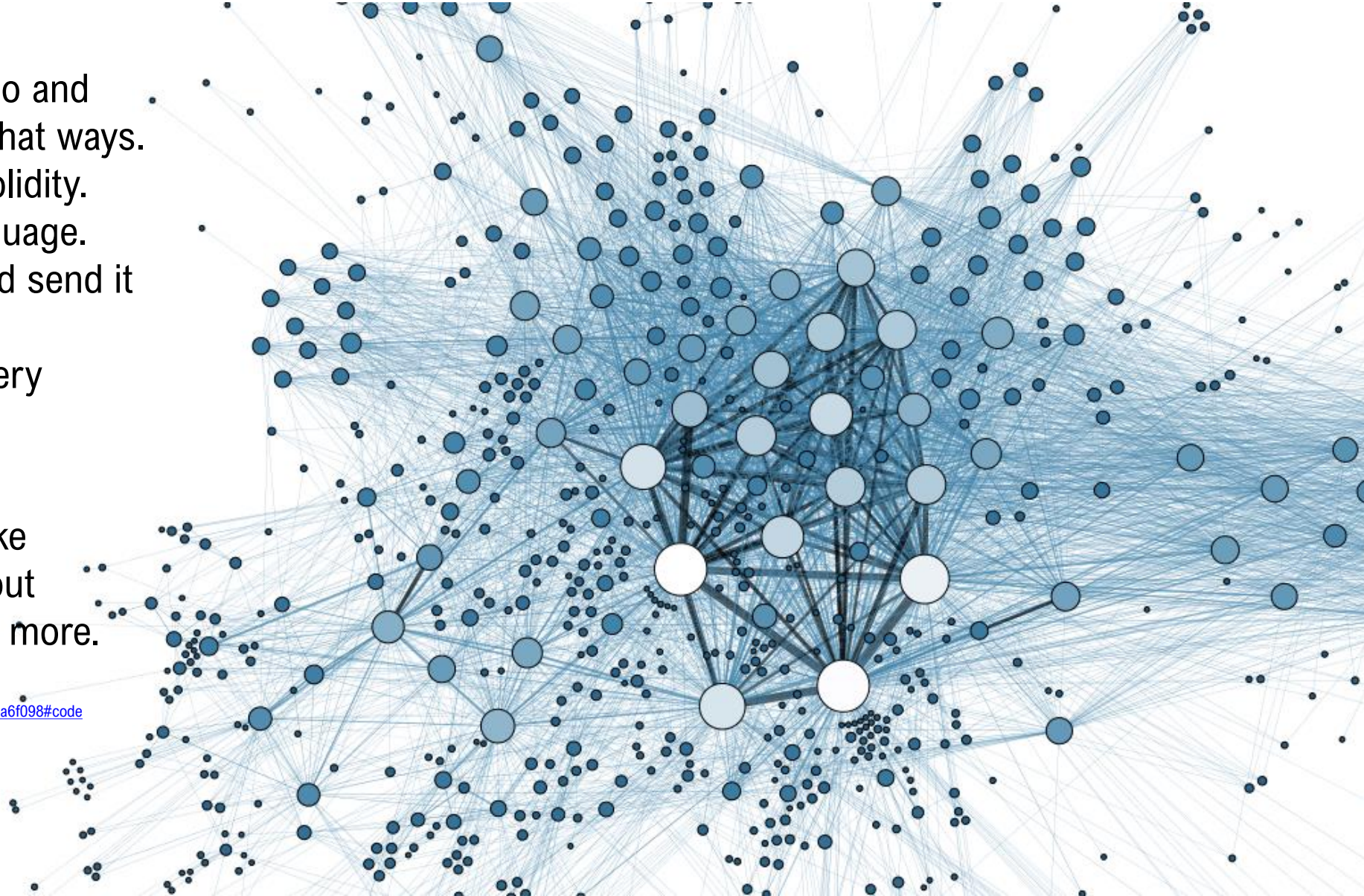


CREATING A SMART CONTRACT

1. Think about what it should do and who can interact with it in what ways.
2. Formulate the program in Solidity.
3. Compile it into machine language.
4. Wrap it into a transaction and send it to the Ethereum network.
5. It is now addressable for every participant in the network.

Deploying a smart contract is like launching a satellite: once it is out there, it cannot be changed any more.

Demo: https://etherscan.io/address/0x656038e97cee7c095673f7b9fad695b323a6f098#code



EXAMPLE: SHARES ON THE BLOCKCHAIN

- Immediately tradable world-wide
- Atomically exchangeable for other assets on the same blockchain
  → Enables «Share Dispenser» to sell shares directly to website vistors, bypassing the banking system
- Continuous dividends
- Provably correct votes
- Self-enforcing shareholder agreements
- Automatic market making
  (Liquidity premium for shares is 25%)

→ We have the technology to make all firms in the world 25% more valuable!

ARBITRATION OPPORTUNITY

- Smart contract allows to define arbitrary roles with arbitrary powers, including a predefined role with predefined powers for arbitration
- Main problem of smart contracts is the same as with real contracts: it’s almost impossible to make them perfect and to foresee every possible eventuality.
  → Need for trusted third parties to interfere with the smart contract.
- Example: If a physical share certificate gets lost, a judge can declare it invalid and the company can issue a new one. What should a company do when a blockchain-based share gets lost?
  → Give an arbiter a «backdoor» to declare tokens invalid so the company can issue new ones.
- Related: an oracle is a trusted source the puts data onto the blockchain that smart contracts can act on (exchange rates, stock prices, credit defaults, etc.)

ARBITRATION EXAMPLE: KLEROS

- Authors of smart contracts can give Kleros the power to resolve disputes.
- In case of a dispute, a group of “jurors” decide

BITNATION

BECOME A WORLD CITIZEN

INSTALL THE PANGEA JURISDICTION

Download on the App Store

GET IT ON Google Play

P2P AGREEMENTS

Pangea is a decentralised market for legal services. Create and execute peer-to-peer agreements seamlessly across the world, resolve disputes fairly and efficiently. Choose an arbitrator, or become an arbitrator in your field of expertise.

FRONTIER TECHNOLOGY

Pangea is a secure mesh network forming a distributed web, accessed through a smartphone-chat user-friendly interface. Blockchain agnostic smart contract functionality powers the Pangea Jurisdiction, currently implemented with Ethereum.

YOUR OWN NATIONS

On Pangea you can create your own Decentralised Borderless Voluntary Nation (DBVN). Choose your Code of Law and Decision Making Mechanism, write a Constitution and provide Governance Services to Citizens.

QUESTIONS?

Events: bitcoinassociation.ch

Contact: luzius@meissereconomics.com

Download the mentioned articles from:
https://github.com/meisserecon/www/raw/gh-pages/2018-04-04%20Hauser%20und%20Meisser%20-%20Digma.pdf
https://github.com/meisserecon/www/raw/gh-pages/2018-05-24%20Meisser%20Meisser%20und%20Kogens%20-%20Jusletter-IT.pdf
https://github.com/meisserecon/www/raw/gh-pages/freedom.pdf
https://github.com/meisserecon/www/raw/gh-pages/tagungsbeitrag.pdf