Bitcoin

https://iuk.one/1033-1321

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock, Germany
clemens.cap@uni-rostock.de

Version 2

Overview

1. Befassung mit dem Thema
2. Was ist Geld?
3. High Level Perspektive
4. Was ist Bitcoin?
5. Smart Contracts und weitere Entwicklungen

1. Befassung mit dem Thema

Bereits sehr früh in der Entwicklung dabei gewesen...

Eurobit-Tagung

Clemens Cap about electronic bitcoin wallet at EuroBit

bitgroups | Subscribe | 13 videos

Wissenschaftliche Arbeiten

HMD 283, 49. Jahrgang, Februar 2012

Open Source - Konzepte, Risiken, Trends

Herausgeber: Susanne Strahringer

Bitcoin - das Open-Source-Geld

Clemens H. Cap

Cebit

CeBIT

About the Trade Show

Topics & Trends | Program | Facts & Figures

Information for

Visitors | Exhibitors | Journalists

Homepage >

Product: Print | Save

Bitcoin – Digital Open Source Money of the Internet Age

Product

It is astonishing that in the Internet age we still settle our bills with physical objects (bills or coins), But also account-based money has its problems, since the user must trust the bank and its governance....

Read more

Exhibitor

Uni Rostock

Universitätsplatz 1
18055 Rostock
Germany

Phone: +49 381 498 0
Fax: +49 381 498 1216

Exhibition stand

Hall 26, Stand A34

Topic: Mecklenburg-Vorpommern Pavilion

Footer

Workshop


Erstes akademisches Workshop & Tutorial
GMDS 2012/INFORMATIK 2012 · 16. bis 21. SEPTEMBER 2012
57. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GM
42. Jahrestagung der Gesellschaft für Informatik e.V. (GI)
Informatik 2012 > Workshop "Bitcoin"
.: Workshop & Tutorial Bitcoin :.
Call for Papers
The English version of the call for papers can be found here.
Halbägiges Tutorial und halbtägiger Workshop an der Jahrestagung der Gesellschaft für Informatik (GI), 20. September 2012, Braunschweig
Verlängerte Deadline zur Einreichung: 30.04.2012
Koordinator: Clemens Cap (Universität Rostock), clemens.cap@uni-rostock.de

Situation heute

Bitcoin und Blockchain sind weiterhin eine sehr interessante Technologie.

Aber: Jede gute Idee findet rasch ihre Mißbrauchs-Täter.

Stromverbrauch

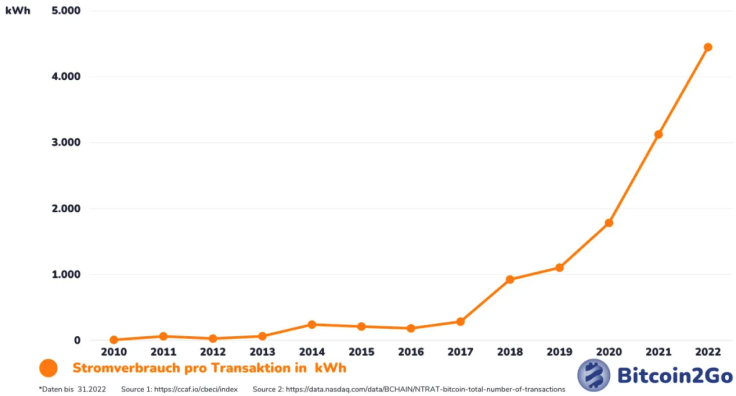

Fig. 5: Stromverbrauch: Bitcoin 2024: 172 TWh, Deutschland 2020: 418 TWh. In der Abbildung Stromverbrauch pro Transaktion. Quelle: https://bitcoin-2go.de/statistiken/bitcoin-energieverbrauch/.

Rezentralisierung

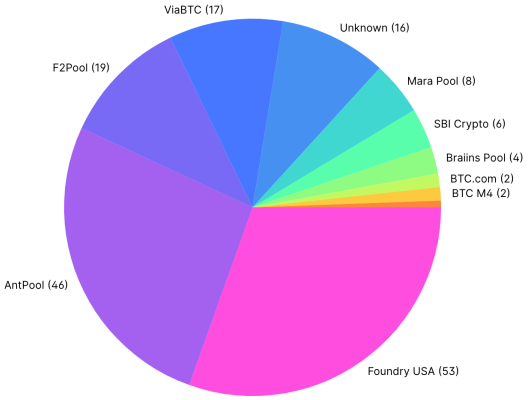

Fig. 6: Ursprünglich war die Blockchain als hochverteiltes System geplant. Jetzt geschieht durch die Mining Pools eine Rezentralisierung. Quelle: https://www.blockchain.com/explorer/charts/pools

Absurde Entwicklung bei Transaktions-Kosten

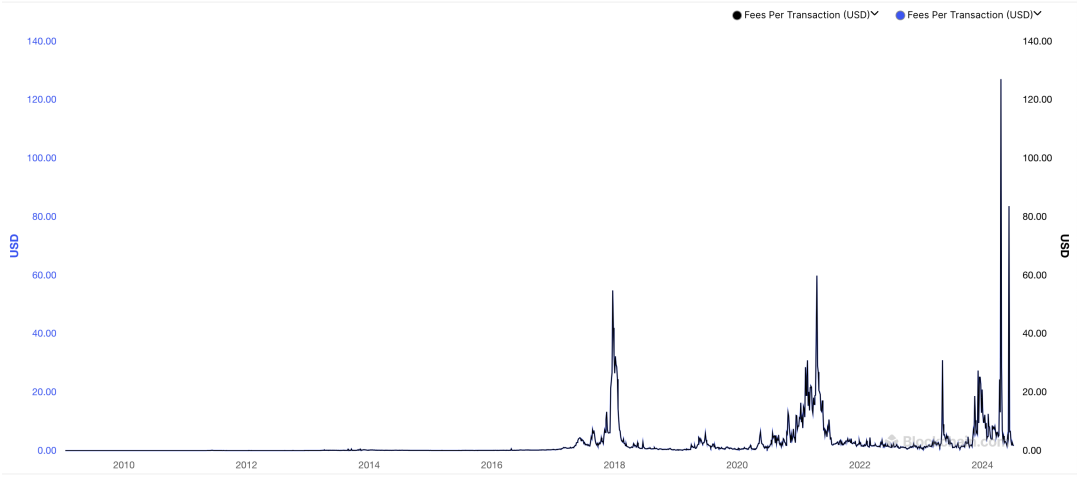

Fig. 7: Die Transaktionskosten entwickeln sich absurd und machen C2C Anwendungen unwahrscheinlicher: Quelle: https://www.blockchain.com/explorer/charts/fees-usd-per-transaction

Verdrehung der ursprünglichen Idee

We are working with the national central banks of the euro area to look into the possible issuance of a digital euro. It would be a central bank digital currency, an electronic equivalent to cash. And it would complement banknotes and coins, giving people an additional choice about how to pay.

Fig. 8: Das erklärte Ziel der europäischen Zentralbank. Quelle: https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html Ursprünglich war der Bitcoin als Befreiung des Geldsystems von den Zentralbanken geplant.

2. Was ist Geld?

Welchen Datentyp müssen wir implementieren?

Was ist Geld?

Mögliche Definitionen

- Wertmaßstab
- Tauschmittel
- Wertaufbewahrung

Wertmaßstab

Problem: Wie viel ist eine Stunde "Vorlesung Cap" wert?

Fragen:

- Gibt es den objektiven Wertmaßstab?
- Wie entsteht er?
- Wie wird stabiles Vertrauen darin etabliert?

Tauschmittel

Problem:

- Lehrer bietet Unterricht und will ein Steak
- Schüler will Unterricht, hat aber nur eine ganze Kuh.

Konzepte:

- Geld vereinfacht mehrfache Tauschketten.
- Geld ermöglicht die Aufteilung von Werten in kleinere Einheiten.

Fig. 9:

Wertaufbewahrung

Aufgeschobener Tausch:

- Tausch jetzt – Rücktausch später
- Heute Unterricht, Morgen Opernbesuch, In 20 Jahren in die Rente

Was sind geeignete Tauschmittel?

Fig. 11: Goldbarren: Aufwendiges Mining.

Fig. 12: Kauri-Muscheln. Nur an besonderem Strand zu finden.

Fig. 13: Diamanten: Aufwendiges Gewinnen.

Was sind ungeeignete Tauschmittel?

Fig. 14: Was gibt dem Geld seinen Wert?

Fig. 15: Was gibt dem Geld seinen Wert?

Kernfragen

Frage:

- Wodurch entsteht die (möglichst universelle Akzeptanz)?
- Wodurch bleibt diese Akzeptanz persistent?

Wertverlust durch Inflation

Fig. 16: Mesing-Münze zu 50 Millionen Mark

Fig. 17: Bahngutschein über 5000000000 Mark

Wertverlust durch System-Crash

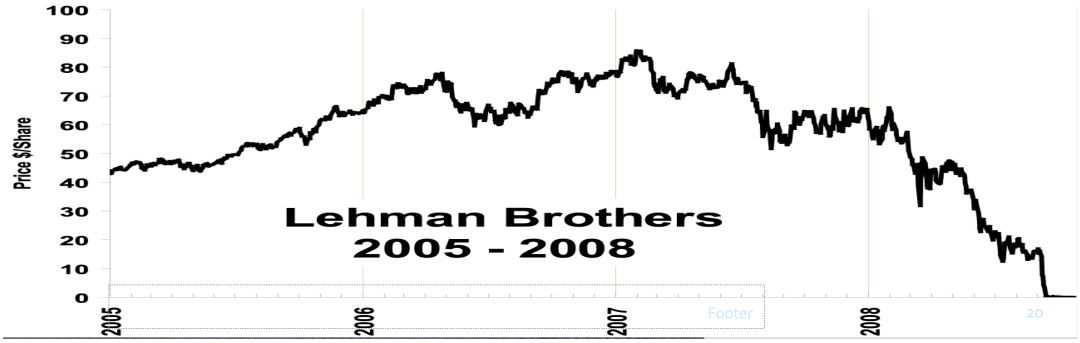

Fig. 18: Zusammenbruch der Lehman Brothers Bank

Wertverlust durch Denial-of-Service

Kreditkartenfirmen

Ku-Klux-Klan ja, Wikileaks nein

(Headline der Süddeutschen Zeitung)

Fig. 19:

3. High Level Perspektive

Nochmals, aber in abstrakten Begrifflichkeiten, die sich implementieren lassen.

Nochmals: Was ist Geld?

- Ein **Recht** zur Ausführung einer bestimmten Transaktion,
- das von seinem **Träger**
- **genau einmal** ausgeübt werden kann und
- **nur** durch die Ausübung des Rechts auf **andere übergeht**.

Nochmals: Was ist Geld?

- Ein **Recht** zur Ausführung einer bestimmten Transaktion,
- das von seinem **Träger**
- **genau einmal** ausgeübt werden kann und
- **nur** durch die Ausübung des Rechts auf **andere übergeht**.

Träger:

An Name gebunden	Konto ad personam
An Kenntnis gebunden	Nummernkonto, PIN, TAN
An Pseudonym gebunden	Public / Private Key Paar
An Objekt gebunden	Münze, Goldbarren
An Körper gebunden	Biometrie, Fingerabdruck

Nochmals: Was ist Geld?

- Ein **Recht** zur Ausführung einer bestimmten Transaktion,
- das von seinem **Träger**
- **genau einmal** ausgeübt werden kann und
- **nur** durch die Ausübung des Rechts auf **andere übergeht**.

Genau einmal ... von seinem Träger:

- Anti-Beispiel: Digitale Informatioon
- Problem: Double Spending
- Aber: Weitergabe möglich für Übergang des Rechts
- Aber: Backup möglich

Nochmals: Was ist Geld?

- Ein **Recht** zur Ausführung einer bestimmten Transaktion,
- das von seinem **Träger**
- **genau einmal** ausgeübt werden kann und
- **nur** durch die Ausübung des Rechts auf **andere übergeht**.

Nur durch:

- Anti-Beispiel: Geld selber fertigen
- Challenge: Kein Erzeugen von Geld-Einheiten ohne:
  - Wert-Deckung: Gegenleistung in Zeit oder Energie
  - Regelungs-Deckung: Legitimität und rechtliche Befugnis
  - De-Facto Deckung: Tatsächliche gesellschaftliche Akzeptanz

Nochmals: Was ist Geld?

- Ein **Recht** zur Ausführung einer bestimmten Transaktion,
- das von seinem **Träger**
- **genau einmal** ausgeübt werden kann und
- **nur** durch die Ausübung des Rechts auf **andere übergeht**.

Auf andere übergeht:

- Einer verliert das Recht, ein anderer bekommt das Recht
- Übertragung kann mit Zwischen-Instanz geschehen (Bank)
  Buchgeld und Kontostand
- Übertragung kann ohne Zwischen-Instanz geschehen (Peer 2 Peer)
  Bargeld, Edelmetalle

Woher kommt im Geld der Wert?

Langandauernde Konvertierbarkeit in Waren und Dienstleistungen

Unmittelbare Konvertierbarkeit:

- Energieträger: universelle physikalische Eigenschaft
- Nahrungsmittel: universelle Nachfrage

Akzeptanz und Nachfrage: Was nimmt / was will der Tauschpartner?

- Brot, Wasser, Gold, Waffen, Zigaretten

Konvention und Gesetz: Was muß der Tauschpartner nehmen?

- Weil es das Gesetz so vorschreibt: Recht in Euro / Dollar zu zahlen
- Früher: Goldstandard: Dollar als Schuldschein für Gold

4. Was ist Bitcoin?

Ein erste Einführung

Was ist Bitcoin=

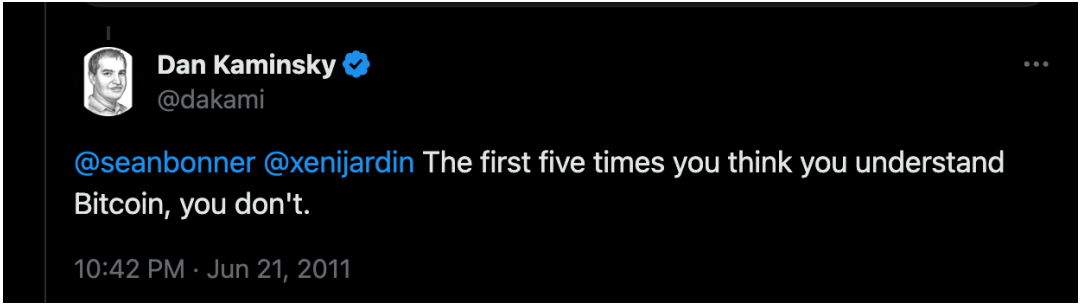

Fig. 20: Quelle: https://x.com/dakami/status/83273542501810176

Was ist bei Bitcoin der Träger?

- Bindung an ein Pseudonym ("Bitcoin Adresse")
- Nachweis der Befugnis durch (Public, Private) Key Paar mit ECC
- Bitcoin Adresse ist hash des public key
- Private Key verlieren = Geld verlieren

Was ist bei Bitcoin die Übertragung?

- Völlig Peer-to-Peer, ohne irgendeine Zentralinstanz
- Jeder Teilnehmer betreibt einen Bitcoin Knoten
- Jeder Knoten speichert Konto-Stände zu allen Adressen
- Transaktionen werden an alle Knoten gesandt
- Berechtigung wird durch Signatur überprüft
- Neue Konto-Stände werden an alle Knoten gesandt

Zentrale Idee

- Hochreplizierte Datenbank
- Nach einer gewissen Zeit mit hoher Wahrscheinlichkeit konsistent
- Probabilistischer Konsistenz-Begriff
- Probabilistischer Wert-Begriff

Was ist die Blockkette?

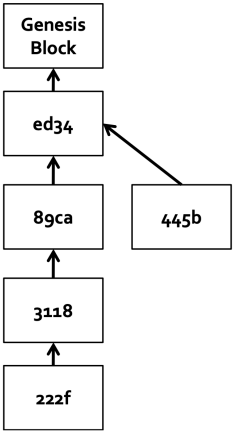

Fig. 21: Beispiel einer Blockkette

Explorer

Die Daten der Blockchains sind öffentlich einsehbar:

- In jeder Wallet
- Auf geeigneten Sites. Bsp: https://explorer.btc.com/btc

Blockketten-Algorithmus: Grundidee

- Jeder Block versiegelt via Hash Funktion eine Welt-Sicht (d.h. Kontostände)
- Wird durch seinen Hash-Wert addressiert
- Verweist via Hash-Wert auf genau einen Vorgänger
- Es gibt einen öffentlichen bekannten Genesis-Block als Wurzel
- Daraus entsteht ein Baum mit mehreren Ästen
- Unklar bleibt im Fall einer Verzweigung welche Weltsicht die richtige ist.
- Jeder neue Block muss an frühere ankoppeln und ein Proof of Work enthalten.
- Rate Zufallszahl so, dass hash mit großer Anzahl 0 beginnt – das kostet Rechenzeit.
- Wer einen neuen Block findet & verteilt – bekommt 50 BTC (25 BTC, ...)

Ökonomischer Ansporn

- **Bitcoins generieren**
  - Im Mittel alle 10 Minuten 50 neue BTC für jeden Block
  - Parameter 50 wird immer wieder mal reduziert, sodass maximale Menge Bitcoins nach oben limitiert ist
- **Grund 1:** Mining Bounty
  - Wer einen Block versiegelt, erhält 50 BTC
  - Alle 4 Jahre wird der Wert halbiert
  - Asymptotisch: Maximal 21 Millionen BTC hergestellt
  - Eingebauter Inflations-Schutz
- **Grund 2:** Fees
  - Überweisung wird nur durchgeführt, wenn eine kleine Fee gezahlt wird
  - Größe der Fee derzeit unklar
  - Schrittweise Ablöse der Mining Bounty durch die Fees

Ist Bitcoin anonym?

Beispiel:

- Alice an Bob via anonymer Mail: Sende bitte 10 BTC an Konto 33.
- Bob: Überweist
- Alice: Sieht Überweisung, sendet Ware per anonymer Mail
- Aber: Wenn Alice an Carol von Konto 33 überweist, dann sieht Bob das
- Daher legt Alice 10 neue Konti an: 20, 56, 88 usw. und überweist Geld quer durch die Gegend

Aussage:

- Problem der Weiterüberweisung
- Kontrolle an der Grenze in Euro möglich

Probleme mit Bitcoin

- Bezahlung illegaler Transaktionen (Bsp: Drogenhandel auf Silk Road)
- Erpressung (Bsp: Vorfall um die Steuererklärung von Mitt Romney)

Bitcoin verbieten?

- Wie? So, wie auch Peer-2-Peer Filesharing von Filmen unter © verboten ist?

Bitcoin nutzen

- Weltweite Überweisung innerhalb von Sekunden
- Nach 1 Stunde relativ sicherer Status
- Frei von zentralen Instanzen
- Kann nicht gesperrt werden
- Absolutes "Bank"geheimnis möglich, da keine Bank
- Geld im Backup halten
- Jeder kann Teil der Infrastruktur sein
- Radikale Konkurrenz bei den Transaktionsgebühren
- Immun gegen politische Versuche, Geld zu drucken
- Völlig unter der Kontrolle der Mehrheit

Kursentwicklung

Bitcoin Difficulty

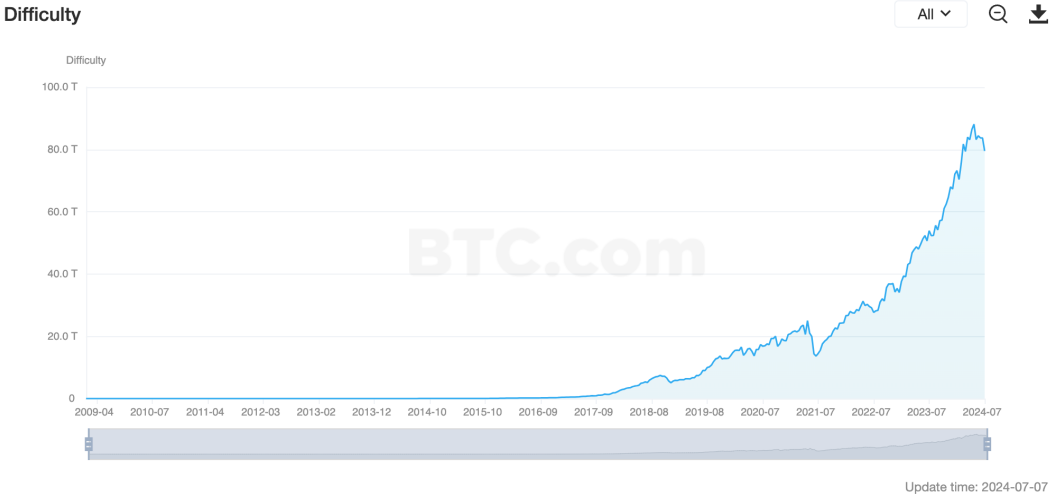

Fig. 23: Entwicklung der Difficulty des Bitcoin

Hashrate

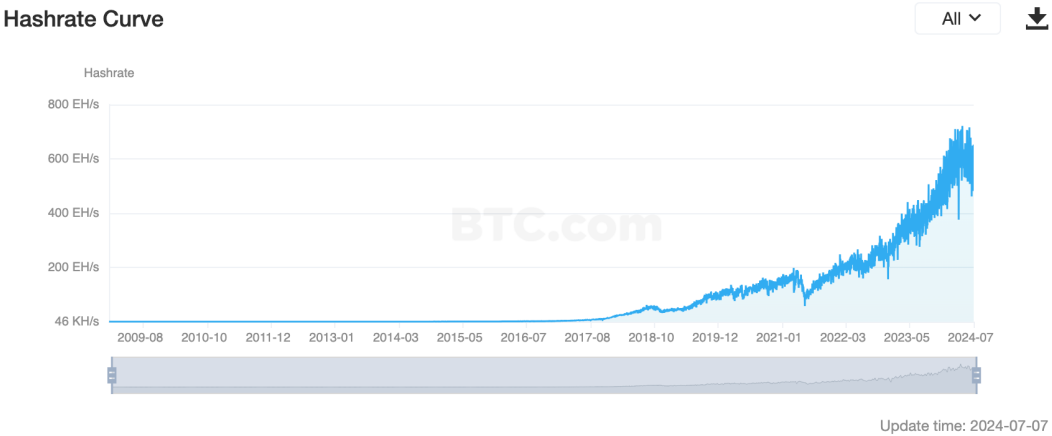

Fig. 24: Entwicklung der Hashrate des Bitcoin

5. Smart Contracts und weitere Entwicklungen

Was kommt nach dem Bitcoin?

Alternative Crypto Währungen

Fig. 25: Enorme Zahl von Krypto-Währungen mit sehr hoher Gesamtkapitalisierung

Weitere Datenbanken, Beispiel Namecoin

Grundidee:

- DNS-artige Datenbank
- Zuständig für Top Level Domain `.bit`
- Nicht in das normale BIND / DNS angebunden, benötigt Porxy Dienst
- Ermöglicht Nachweis des Eigentums an einer `.bit` Domäne

Smart Contract

Bitcoin:

- Bestimmte Anforderungen an Korrektheit
- Summen der Einzahlungen und Abhebungen ergeben Wert
- Signaturen sind vorhanden und lassen sich verifizieren
- Difficulty Werte in der Blockchain stimmen

Verallgemeinerung: Smart Contract

- Verallgemeinerung des Bitcoin-Konzepts
- Beliebige Bedingungen (Turing vollständig)
- Anbindung an Außenwelt (Ereignisse)
- Weitere Incentives für Miner

Beispiel: Wohnungsmiete

- Mieter bekommt Quittung und Zugangsschlüssel
- Vermieter bekommt Geld
- Bestimmte Zeiten und Übergänge sind vereinbart
- Garantien darüber werden eingehalten & überwacht
- Blockchain basierte Kontostände passen sich automagisch an

Weitere Beispiele

- Altcoins
- Crowdfunding Schemata
- Prediction Markets
- Lotterien
- Überwachte Wahlen
- Zugangskontrollen
- Spiele
- Verteilte Organisationen

Ethereum

- Eigene Programmiersprache für Smart Contracts (Solidity)
- Ähnlich wie Javascript; Anbindung an UI und Crypto
- Berechnungen einer Transaktion kosten Zeit
- Wird in entsprechendes "gas" / Geld umgerechnet
- Eigene Blockchain als erweitertes Bitcoin

Anwendung

On top of Ethereum

- Funktioniert out of the box
- Skalierbarkeit, Sicherheit (viele Miner), Community
- Fokus auf eigenen Geschäftsprozess
- Kostet gas.

Eigene Blockchain mit Ethereum Technologie

- Unabhängigkeit von Schicksal & Entscheidungen bei Ethereum
- Eigene Wahl von gas-Preis und weiteren Parametern
- Auch private Chain möglich (nur bestimmte, authentisierte Teilnehmer)

Beispiel für Smart Contract (1)

```
1  // SPDX-License-Identifier: MIT
2  pragma solidity ^0.8.0;
3
4  contract MyToken {
5    string public name = "MyToken";
6    string public symbol = "MTK";
7    uint8 public decimals = 18;
8    uint256 public totalSupply;
9
10   mapping(address => uint256) public balanceOf;
11   mapping(address => mapping(address => uint256)) public allowance;
12
13   event Transfer(address indexed from, address indexed to, uint256 value);
14   event Approval(address indexed owner, address indexed spender, uint256 value);
15
16   constructor(uint256 _initialSupply) {
17     totalSupply = _initialSupply * (10 ** uint256(decimals));
18     balanceOf[msg.sender] = totalSupply;}
```

Beispiel für Smart Contract (1)

```
  function transfer(address _to, uint256 _value) public returns (bool success) {
    require(balanceOf[msg.sender] >= _value, "Insufficient balance");
    balanceOf[msg.sender] -= _value;
    balanceOf[_to] += _value;
    emit Transfer(msg.sender, _to, _value);
    return true;}
  function approve(address _spender, uint256 _value) public returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    emit Approval(msg.sender, _spender, _value);
    return true;}
  function transferFrom(address _from, address _to, uint256 _value) public returns (bool
    require(_value <= balanceOf[_from], "Insufficient balance");
    require(_value <= allowance[_from][msg.sender], "Allowance exceeded");
    balanceOf[_from] -= _value;
    balanceOf[_to] += _value;
    allowance[_from][msg.sender] -= _value;
    emit Transfer(_from, _to, _value);
    return true;}
}
```

Proof of Work

Mechanismus

- Validator ist, wer ein PoW löst
- PoW ist ein Hash Rätsel, das nur durch Probieren gelöst werden kann
- Probieren braucht Zeit oder Performanz
- Wer das Rätsel als erster löst hat statistisch die besten Chancen, dass sein Block in der globalen Blockchain verbleibt und damit sein Eigentum an der Bounty wahr bleibt

Probleme:

- Stromverbrauch, CO2 Footprint
- 51% Attacke
- hop-on-hop-off Attacke von Minern
- Absicherbar durch private Blockchain
- Zeitbedarf

Proof of Stake

Mechanismus:

- Validator wird, wer einen hohen Stake nachweisen kann
- Stake: Einsatz, ev. auch in Tokens
- Auswahl durch Zufallsmechanismus
- Wahrscheinlichkeit der Auswahl steigt mit Stake
- Validator, der sich nicht an Regeln halt, verliert später Stake u/o Bounty

DAG Verifikation

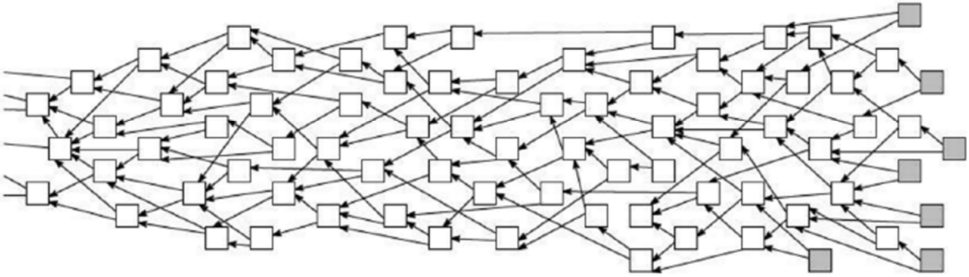

Fig. 26: Das Tangle System von IOTA

DAG Verifikation

Mechanismus:

- Wer Ledger nutzen will muss auch validieren
- Validator unterschreibt mit private Key
- Jeweils 2 vorangegangene Blöcke einbinden
- Auswahl der nächsten 2 Kandidaten nach Random Walk
- Kleine PoW als Spam und Sybil Schutz

Bewertung:

- Skaliert besser, leichtgewichtig
- Keine Fees nötig sondern eigene Mitarbeit
- Auch offline Transaktionen
- Für IoT Anwendungen gut geeignet

Appendix

Contents of Appendix

List of Figures (1/4)

List of Rights

Terms of Use (1)

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das Zitatrecht in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise Par 60a UrhG ermöglichen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Use of Logos and Trademark Symbols: The logos and trademark symbols used here are the property of their respective owners. The YouTube logo is used according to brand request 2-9753000030769 granted on November 30, 2020. The GitHub logo is property of GitHub Inc. and is used in accordance to the GitHub logo usage conditions https://github.com/logos to link to a GitHub account. The Tweedback logo is property of Tweedback GmbH and here is used in accordance to a cooperation contract.

Terms of Use (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status nicht oder nur mit unverhältnismäßig hohem Aufwand abzuklären ist. Ebenso kann den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen, obwohl deren Leistungen genutzt werden.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 (Pressemitteilung, Blog-Beitrag, Urteilstext). ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungs- und Anreizsystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungs- und Anreizsysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Citing This Document

If you use contents from this document or want to cite it,
please do so in the following manner:

Clemens H. Cap: Bitcoin. Electronic document. https://iuk.one/1033-1321 7. 7. 2024.

Bibtex Information: https://iuk.one/1033-1321.bib

```
@misc{doc:1033-1321,
   author       = {Clemens H. Cap},
   title        = {Bitcoin},
   year         = {2024},
   month        = {7},
   howpublished = {Electronic document},
   url          = {https://iuk.one/1033-1321}
}
```

Typographic Information:
Typeset on ?today?
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

List of Slides

5. Smart Contracts und weitere Entwicklungen

Legend:
- continuation slide
- slide without title header
- image slide