IOTA

The revolution of Blockchain

Bernd KLAUS (51807077)
FernFH Wiener Neustadt
Bachekir Wirtcshaftsinformatik
Wien, Österreich
bernd.klaus@mail.fernfh.ac.at

***Abstract* — IOTA ist eine neuartige Kryptowährung, welche ihren Fokus auf den Zahlungsverkehr zwischen Internet of Things (IoT) Geräten legt. Im Fokus dieser 3rd Generation Blockchain liegen hohe Skalierbarkeit sowie gebührenfreie Transaktionen zwischen den Teilnehmern.**

Keywords — IOTA, MIOTA, Tangle, Micropayment

I. Introduction

Die Anzahl an internetfähigen Geräten nimmt rasant zu [2], diese Entwicklung stellt die vorherrschenden Protokolle sowie auch darunter liegenden Technologien vor neue Herausforderungen. Im speziellen müssen Methoden gefunden werden um den Skalierungsanforderungen gerecht zu werden. Beispielsweise wurde schon vor geraumer Zeit IPv6 eingeführt um den vorherrschenden IP-Adressen Mangel entgegen zu wirken [3]. IOTA bietet dabei technologische Raffinessen um eine enorm hohe Skalierbarkeit im IoT Zahlungsverkehr zu erreichen [4]. Zusätzlich bietet IOTA, aufgrund des neuartigen Technologieansatzes, eine kostenfreie Transaktionsmöglichkeit. Dieser Sachverhalt ermöglicht es minimale Kleinstbeträge, sogenannte Micropayments, zu überweisen, welche in anderen Netzten schlicht nicht rentabel bzw. möglich wären [5].

In Folge der neuartigen und innovativen Ansätze des IOTA Netzwerkes haben auch bereits einige namhafte Unternehmer ein Auge auf diese Technologie geworfen bzw. unterstützen diese bereits. Darunter befindet sich Microsoft, Volkswagen, DNB, Bosch sowie Fujitsu um die fünf größten hervorzuheben.

In den folgenden Absätzen dieses Whitepapers soll die genauere Funktionsweise von IOTA beleuchtet werden. Eine Übersicht der Themen in chronologischer Folge findet sich nachfolgend:

- **Tanlge**: Was ist die Tangle und welche Vorteile hat diese gegenüber eine herkömmlichen Blockchain
- **Miner**: Wieso auf Miner verzichtet werden kann und damit eine hohe Skalierbarkeit erreicht wird.
- **Gebührenfrei**: Micropayments, ein absolutes Muss für IoT Netzwerke.
- **Quanten-Resistent**: Zukunftsorientiert und Sicherheit gegen Quantencomputing.
- **Conclusio:** Aussichten und Resümee.

Grundsätzlich zu erwähnen ist, dass sich IOTA noch in einem frühen Entwicklungsstatus befindet und es stetig zu Weiterentwicklungen sowie Änderungen innerhalb des Netzwerkes kommen kann. Eine wichtige Eigenschaft ist demnach die Aktualität, welcher im Whitepaper besonders nachgegangen wird.

II. Die Tangle

Ist die logische Weiterentwicklung der Blockchain. Das erste Mal bekannt wurde die Blockchain-Technologie durch den Bitcoin Ende 2013 [6]. Man könnte den Bitcoin also als Ursprung aller Kryptowährungen bezeichnen. Die Blockchain brachte eine dezentrale „Datenbank-Ähnliche“ Struktur, welche Transaktionen aufzeichnet. Zur Veranschaulichung im Folgenden eine grafische Darstellung der Blockchain.

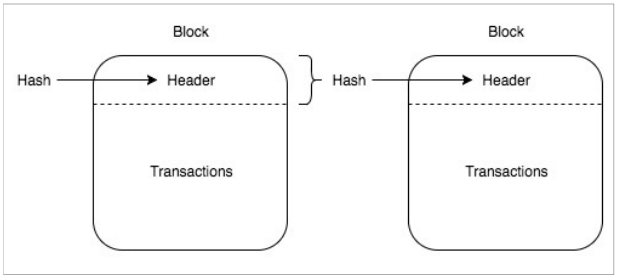

Abbildung 1: Blockchain - Quelle: http://bit.do/eMhUT

Die Blockchain wächst also stetig und schon jetzt kommt es auf einigen Geräten zu Speicherproblemen, wenn der gesamte Datenbestand benötigt wird. Limitiert ist diese Technologie außerdem damit, dass pro Block, je nach Blockgröße, nur eine begrenzte Anzahl an Überweisungen getätigt werden können. Beide dieser Probleme löst die Tangle indem sie in Form eines „directed acyclic graph“ (DAG) aufgebaut ist. Dies ist in folgender Grafik veranschaulicht.

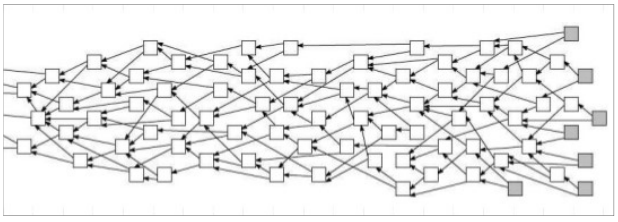

Abbildung 2: Tangle - Quelle: http://bit.do/eMhPT

Es wird keiner „Block für Block“ Mythologie gefolgt, sondern können mehrere Blocks parallel abgearbeitet werden. Jeder Block stellt dabei nur eine einzige Transaktion dar und verifiziert gleichzeitig zwei vorherige Transaktionen. Je mehr Überweisungen stattfinden, desto schneller wird demnach das Netzwerk. Das dabei entstehende Bild gleicht einem wirren

Geflecht, weshalb sich auch der Name „Tangle“ entwickelt hat [1]. Wie eingangs erwähnt wird dadurch, dass eine Transkation zwei vorherige bestätigt, die Skalierbarkeit enorm erhöht. Um dem Problem der gesamten Datenmenge der Transaktionen entgegen zu wirken hat IOTA Snapshots eingeführt [7]. Dabei wird immer nur ein bestimmter Zeithorizont betrachte und ältere Strukturen ausgeblendet. Wichtig dabei ist, dass diese alten Transaktionen nicht „vergessen“ werden, Sie sind für den aktuellen Stand jedoch nicht mehr von Relevanz.

Eine Live-Visualisierung der Tangle kann auf folgender Site eingesehen werden: http://tangle.glumb.de/ - Dort besteht ebenso die Möglichkeit Transaktionen zu suchen und aufzulisten.

III. Miner

Eine Fundamentale Änderung ist auch der vollständige Verzicht auf Miner. In anderen Netzwerken werden diese Zwingend benötigt um die Echtheit der einzelnen Blöcke, siehe Abbildung 1, zu bestätigen [8]. Dabei wird eine Art Rätsel in vorm eines Hashwertes berechnet, sind sich die Mehrheit der Miner über das Ergebnis einig, so wird der Block für echt gehalten und damit bestätigt. Hingegen ist im IOTA Netzwerke jeder aktive Teilnehmer automatisch auch „Miner“ bzw. bestätigt er Transaktionen. Wie in Abbildung 2 ersichtlich bestätigt jede einzelne Transaktion zwei vorherige. Je „Tiefer“, also je weiter Links, sich die Transaktion befindet desto „stärker“ ist die Bestätigung da diese von umso mehr nachfolgenden Transaktionen referenziert wird. Das Teilnehmer gleichzeitig zu Miner werden hat einige Vorteile, so kann eine Transaktionsgebühr vollkommen weggelassen werden, die den Miner zustehen würde. Die einzigen „Kosten“ welche zu tragen sind, ist die Berechnungsleistung der Bestätigung der beiden vorherigen Transaktionen. Zusätzlich kann es niemals es zu einem Interessenkonflikt zwischen den beiden Parteien kommen.

Aber auch bei IOTA ist ein „Proof-of-Work“, wie die Berechnung eines Hashwertes in auf Blockchain basierenden Systemen, erforderlich. Verfügbar sind zwei unterschiedliche Varianten:

- **WebGL 2** Implementierung (Deprecated)
- **CCurl** Implementierung

Insofern es von Geräten unterstützt wird, sollte man auf die CCurl Variante setzen. Das Ergebnis ist der sogenannte „Nonce“ welcher der Transaktion beigefügt wird. Hauptziel dieser Funktion ist es einen Spam Schutz des Netzwerkes zu bewirken, da die Berechnung mit einem gewissen Aufwand verbunden ist. Da einige IoT Geräte nicht die nötige Rechenleistung dazu verfügen, besteht auch die Möglichkeit den PoW auf einer Remote-Instanz zu delegieren [9].

IV. Gebührenfrei

Wie im Kapitel „Miner“ bereits erläutert so sind keinerlei Transaktionsgebühren zu entrichten [7]. Diese Tatsache ist nicht nur eine angenehme Nebenerscheinung, sondern vielmehr ein absolutes muss Kriterium für ein funktionierendes IoT Payment System [10]. Denn wenn Geräte andere Geräte bezahlen, so können minimale Kleinstbeträge entstehen, welche nicht von Gebühren „aufgefressen“ werden dürfen. In Netzwerken, in welchen Gebühren zu entrichten sind, würden sich solche kleinen Überweisungen schlicht nicht mehr rentieren. Um Micropayments zu veranschaulichen sind im Weiteren einige Beispiele angeführt:

- Ein Smartes Elektro-Auto bezahlt die Ladestation im Sekundentakt.
- Der Boardcomputer Ihres Fahrzeuges bezahlt die Wetterstation für das letzte Wetterupdate.
- Ihre Waschmaschine sendet ein Micropayment an einen Mobilfunkbetreiber damit Sie Ihnen eine SMS mit dem Status der Wäsche übermitteln kann.

Weitere Real-World use cases hat IOTA gemeinsam mit Volkswagen im folgenden Video veröffentlicht: https://www.youtube.com/watch?v=-r6G3XVJTSI

Um diese minimalen Überweisungen zu ermöglichen bedarf es außerdem einer sehr kleinen Währungseinheit. Deshalb wird als Währungseinheit mIOTA verwendet, welche für Millionen IOTA steht. 1 mIOTA stehen also für 1.000.000 IOTA. Aktuell bewegt sich der Kurs von einem mIOTA um die 1,2$ [11]. Es ist leicht erkennbar, dass Aufgrund der geringen Wertigkeit winzige Bruchteile unserer kleinesten Währungseinheit gesendet werden können ohne ein Komma zu benötigen.

V. Quanten Resistent

IOTA setzt auf Signaturen welche auf dem Winternitz Algorithmus basieren. Dabei werden Witernitz One Time Signatures (WTOS) generiert, welche auf einem Private und Public Key-Pair basieren. Der Winternitz Algorithmus gilt als Quantum-Computer sicher [12]. Er kann also auch nicht von Supercomputer der Zukunft geknackt werden. Ein kleiner Nachteil dabei ist, dass mit jedem Schlüssel der erstellt wird auch ein kleiner Teil des Privaten Schlüssel preisgegeben wird, weshalb man immer nur eine einzige Transaktion von einer Adresse senden sollte. Dies wird aber bereits von allen gängigen Wallet‘s automatisch erledigt, indem der Restbetrag einer Transaktion auf eine neue Adresse gesendet wird. Weist Ihre aktuelle Adresse also ein Guthaben von 100 mIOTA auf und Sie möchten 40 mIOTA versenden, so werden bei der Transaktion immer die kompletten 100 mIOTA versendet. 40 mIOTA dieser Überweisung gehen an die angegebene Adresse, die restlichen 60 mIOTA werden ebenfalls an eine neu generierte Adresse versendet, die nur Sie innehaben. Dieser Vorgang ist vollkommen Transparent.

VI. Conclusion

IOTA ist ein neuartiger und revolutionärer Ansatz um die Blockchain-Technologie auf den nächsten Level zu bringen und Zukunftsorientiert zu gestallten.

Abbildung 3: IOTA Logo - Quelle: https://www.iota.org

Für viele Probleme, wie sie in einem riesigen Netz an IoT Geräten entstehen können, scheint IOTA die Lösung zu sein. Sei es Miropayments, Quantum-Resistent oder Skalierbarkeit für all diese Hürden hat IOTA Antworten und Lösungen parat. Jedenfalls zu beachten ist, dass sich das IOTA Netzwerk noch in einem sehr frühen Entwicklungs-Status befindet und es noch weiterer Forschung bedarf. Einige der offenen Thematiken möchte ich im Zuge des Resümees kurz erläutern:

- **Koordinator und Zentralisierung**

Aktuell wird das Gesamte IOTA Netzwerk noch durch eine sogenannte Koordinator Instanz gesteuert. Diese Rolle soll „Side-Tanlge“ Attacken vorbeugen und ist im weiteren Zwingend für den Start eines solchen Netzes erforderlich. Solange eine zentrale Instanz entscheidet welche Transaktion als gültig angesehen wird ist von einer starken Zentralisierung auszugehen. Die IOTA Foundation hat jedoch bereits Pläne dieses zentrale Node zu entfernen [13].

- **Proof-of-Work**

Es ist anzunehmen, dass nicht alle IoT Geräte die Fähigkeit besitzen werden den PoW selbstständig berechnen zu können. Das delegieren des PoW auf eine Remote-Instanz führt ebenso zu einer Zentralisierung. Diese Zentralisierungen sollen in einem Liberalen Netzwerk jedoch vermieden werden. Als Lösungs-Ansatz könnten eigene Chips dienen welche lediglich den PoW berechnen können. Dazu gibt es bereits ein Konzept Namens „Jinn“.

- **Quantum-Resistent**

Zwar wird auf der IOTA Homepage erwähnt, dass IOTA Quantum-Sicher sei, jedoch ist dies nicht im White-Paper von IOTA angeführt [14]. Man könnte also annehmen die Beurteilung, IOTA sei Quantum-Sicher, sei voreilig geschehen. Wie kann Beurteilt werden ob Sicherheit gegeben ist, gegenüber einem System, wovon noch nicht einmal alle Möglichkeiten bekannt sind. Kurzum, die Möglichkeiten die uns Quantum-Computing bieten werden stehen noch gar nicht alle fest. Demnach kann auch nicht mit Sicherheit bestätigt werden ob Sicherheit demgegenüber geboten werden kann. Positiv ist, dass zumindest zum aktuellen Zeitpunkt von einer theoretischen Sicherheit ausgegangen werden kann.

Zusammenfassend finde ich IOTA eine sehr spannende und Zukunftsträchtige Technologie und die kommenden Jahre werden uns zeigen ob ein realer Einsatz, außerhalb des Labors, machbar ist. Auch der IoT Markt steht erst am Beginn und es ist stark davon auszugehen, dass diese Themen immer mehr Beachtung finden werden. Entscheidend wird außerdem, ob die einzelnen Hersteller das IOTA Netzwerk annehmen um ein Globales Netzwerk zu schaffen, oder Ihr eigenes Netzwerk in Form eines Forkes betreiben wollen. Aus Benutzersicht ist selbstverständlich ein globales und dezentrales Netzwerk von Vorteil.

VII. BIBLIOGRAPHY

[1] S. Popov, "The Tangle," 2018.

[2] S. Duraisamy, "A Case Study Review: Future of Internet of Things (IoT)," in *ASCENT International Conference Proceedings*, 2017.

[3] e. a. Sébastien Ziegler, "IoT6 – Moving to an IPv6-Based Future IoT," 2013.

[4] D. N. Ramachandran, "The IOTA Distributed Ledger," UCL Centre for Blockchain Technologies, 2011.

[5] G. Holst, "Micropayments Between IoT," Stockholm, 2018.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[7] B. Breier, "Technical Analysis of the Tangle in the IOTA-Environment," Technical University of Munich, München, 2017.

[8] D. R. Sterry, "Introduction to Bitcoin Mining," 2012.

[9] Phani. [Online]. Available: https://medium.com/bytes-io/iota-proof-of-work-remote-vs-local-explained-1cbd89392a79. [Accessed 20 03 2019].

[10] e. a. Thomas Lundqvist, "Thing-to-Thing Electricity Micro Payments Using Blockchain Technology," University West, Trollhättan, Sweden, 2018.

[11] "CoinMarketCap," [Online]. Available: https://coinmarketcap.com/currencies/iota/. [Accessed 20 03 2019].

[12] e. a. Johannes Buchmann, "On the Security of the Winternitz One-Time Signature Scheme," Technische Universit¨at Darmstadt, 2011.

[13] "IOTA Blog," [Online]. Available: https://blog.iota.org/coordinator-part-1-the-path-to-coordicide-ee4148a8db08. [Accessed 20 03 2019].

[14] CleanApp, "Altcoin Magazine," 5 10 2018. [Online]. Available: https://medium.com/altcoin-magazine/is-iotas-tangle-really-quantum-proof-e08550387b96. [Accessed 20 03 2019].