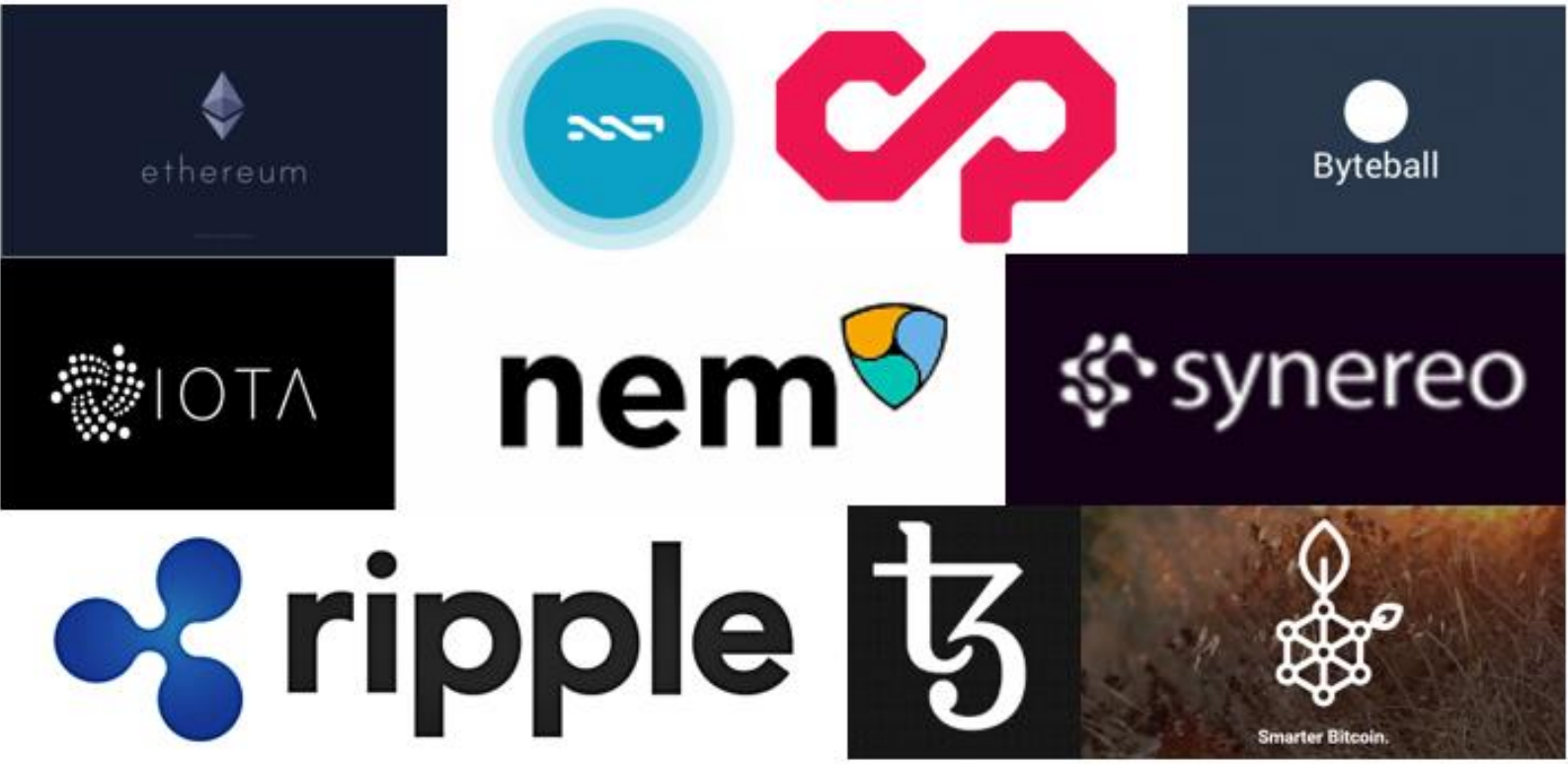
:get know howww
UBIT Steiermark

BlockchainHub Graz

Das Internet der Werte – Blockchain Technologie & Kryptowährungen als Basis einer neuen Wirtschaft

Kapitel 3: Neue Plattformen und Anwendungsgebiete



Von DI Thomas Zeinzinger

BlockchainHub Graz (https://blockchainhub.net/graz/)

Meetup jeden letzten Montag im Monat
http://www.meetup.com/de-DE/BlockchainHub-Graz/

Inhaltsverzeichnis

Die Entwicklung von Blockchain-Plattformen eröffnen neue Möglichkeiten 1
Ethereum 2
Entwickler und Organisation 4
Whitepaper, Yellowpaper und technische Informationen 7
1. Accounts (Konten) 7
2. Ethereum Virtual Machine („EVM“) 7
3. Gas 8
4. DApp 9
5. Mining und Konsens 9
6. Uncle-Block (Onkel-Block) 9
Ethereum, Swarm & Whisper 10
1. Swarm 10
2. Whisper 11
Rootstock 12
Entwickler und Organisation 12
Whitepaper und technische Informationen 12
Counterparty 14
Eigene Tokens kreieren 14
Smart Contracts 14
Asset Exchange ("DEX") 14
Payment Channels 15
Entwickler und Organisation 15
Weitere Informationen 15
IOTA 16
Entwickler und Organisation 16

Whitepaper und technische Informationen 18
Byteball 19
Entwickler und Organisation 19
Verteilung der Währung 20
Whitepaper und technische Informationen 20
NEM 21
Weitere Projekte der Hauptentwickler 22
Eine Auswahl weiterer Plattformen: 23

Die Entwicklung von Blockchain-Plattformen eröffnen neue Möglichkeiten

Dezentral, nicht veränderbar, transparent, das Internet der Werte – die Grundkonzepte hinter Bitcoin und Altcoins führten zur Entwicklung unterschiedlicher Plattformen, auf denen verschiedene Anwendungen laufen können und die so grundsätzlich das Potenzial haben, zentrale Lösungen zu ersetzen.

So wurde die Möglichkeit geschaffen, Verträge in der Blockchain zu speichern, was – aufgrund der Unmanipulierbarkeit der Blockchain – in Folge automatisierte Treuhänder denkbar macht. Oder die Entwicklung einer Plattform, die sich als Grundlage für das Internet of Things sieht und gebührenfreien Daten- und Werttransfer für die unterschiedlichsten IoT-Devices ermöglicht.

Die Plattformen befinden sich noch in den Baby- oder Kinderschuhen, trotzdem ist es spannend zu sehen, wie sich diese weiterentwickeln werden und auf welche weiterführende Anwendungsmöglichkeiten sich auf Basis der Plattformen entwickeln werden.

Ich möchte Ihnen hier einige der Plattformen mit ihren Einsatzmöglichkeiten, Besonderheiten und dem aktuellen Entwicklungsstand vorstellen. Einen besonderen Fokus lege ich hier auf Ethereum, einer Plattform, die interessante Anwendungsmöglichkeiten eröffnet und eine treue Entwicklergemeinde hinter sich hat. Außerdem kam diese Plattform aufgrund der Aufregung rund um „The DAO“ in die Schlagzeilen.

Lassen Sie uns in diese turbulente Welt eintauchen.

Ethereum

Ethereum stellt eine der revolutionärsten und ambitioniertesten Weiterentwicklungen der Blockchain Technologie dar und erfreut sich einer sehr treuen und aktiven Entwicklergemeinde. Es handelt sich um eine öffentliche, also für jeden zugängliche Blockchain-Lösung. Viele der einzelnen Weiterentwicklungen rund um Bitcoin wurden von Vitalik Buterin aufgegriffen und in ein komplett neues System verpackt. So sind Ideen eingeflossen, um die Entwicklung von Spezialhardware für das Mining zu verhindern, die Blockzeit wurde auf niedrige 15 Sekunden reduziert und die Anzahl der Transaktionen pro Sekunde gegenüber Bitcoin verdreifacht.

Das Besondere ist die relativ einfache Möglichkeit, sogenannte „Smart Contracts“ in die Blockchain zu speichern und diese von einer im Softwareclient laufenden virtuellen Maschine (Ethereum Virtual Machine oder kurz EVM) ausführen zu lassen. Damit die für die Ausführung benötigte Rechenleistung auch bezahlt wird, gibt es das sogenannte „Gas“ welches mit Ether (Ethereum’s eigene Kryptowährung) bezahlt wird. Auch die alle 15 Sekunden berechneten Blöcke werden nicht über eine definierte Blockgröße wie bei Bitcoin gesteuert, sondern über ein Gaslimit. Das Konzept von Gas[1] ist auch notwendig für die Absicherung des Netzwerks vor Attacken, da ja ansonsten jemand die EVM über einen Smart Contract dauerhaft blockieren könnte.

Diese Möglichkeit des Angriffs hat auch zu deutlichen Beeinträchtigungen im September und Oktober 2016 geführt und ist als DDoS Attacke[2] in die Medienberichterstattung eingegangen. Bei den eher konservativ eingestellten Krypto-Entwicklern wird genau deshalb die Möglichkeit einfach programmierbarer Smart Contracts als zu gefährlich angesehen. Andere sehen es als die spannendste Blockchain-Weiterentwicklung des Jahrzehnts und einen wichtigen Schritt eine breitere Entwicklergemeinde für die Technologie zu begeistern.

[1] Weiterführende Informationen zu Gas: https://ethereum.gitbooks.io/frontier-guide/content/costs.html
[2] https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/

Smart Contracts können aktuell mit vier Programmiersprachen geschrieben werden – Solididy[3], Serpent[4], Mutan[5] und LLL[6] – wobei die hauptsächlich verwendete Sprache Solidity ist, welche wieder sehr viele Ähnlichkeiten mit Javascript teilt. Das erleichtert den Einstieg in die Smart Contract Programmierung und erweitert damit den Teilnehmerkreis potentieller Entwickler.

In diesem Zusammenhang ist es auch wichtig die bisher größte Kontroverse in der Ethereum-Fangemeinde zu besprechen – „The DAO“[7]. DAO steht für Decentralized Autonomous Organization, also eine Organisation, die dezentral ohne klassische Firmenstruktur und autonom agieren kann. Auch wenn es sich im ersten Moment etwas eigenartig anhört, so ist es durchaus machbar, derartige Strukturen zu bauen, wo die verfügbaren Gelder in einem dezentralen System (z.B. Ethereum) gespeichert sind und von den über den gesamten Globus verstreuten Eigentümern durch einen Wahlmechanismus vergeben werden. „The DAO“ war ein erster Versuch einen dezentralen Investmentfond zu installieren und die darin gespeicherten Gelder für Startups zur Verfügung zu stellen, welche wieder automatisch deren Profite mit „The DAO“ teilen sollten. Am 30. April 2016 startete der Verkauf der Anteile und nach nur 28 Tagen waren mehr als 11,5 Mill. Ether (ca. 150 Mill. €) eingesammelt. Am 9. und 14. Juni wurde auf mehrere Sicherheitsprobleme hingewiesen – unter anderem auf eine Möglichkeit von „recursive calls“. Genau diese Schwäche im Smart Contract code von „The DAO“ wurde am 17. Juni 2016 durch Hacker ausgenützt um ca. 1/3 der eingesammelten Ether in eine neue DAO[8] zu transferieren. Damit hatte man 28 Tage Zeit an einer Lösung des Problems zu arbeiten und nachdem ein Versuch das „Geld“ zurück zu stehlen fehlgeschlagen war, hat man sich für einen „Hard Fork“ entschieden. Dabei wurden alle gestohlen Ether in einen Multisig Account verschoben, wo sich die bestohlenen ursprünglichen Eigentümer ihr

[3] http://solidity.readthedocs.io/en/latest/
[4] https://github.com/ethereum/wiki/wiki/Serpent
[5] https://github.com/ethereum/go-ethereum/wiki/Mutan
[6] The Ressurection of LLL: http://blog.syrinx.net/the-resurrection-of-lll-part-1/
[7] https://en.wikipedia.org/wiki/The_DAO_(organization)
[8] Details zum DAO Hack: http://vessenes.com/deconstructing-thedao-attack-a-brief-code-tour/

Geld wieder abholen konnten. Ende Dezember 2016 waren auf diesem Konto immer noch Ether im Gegenwert von ca. 10 Mill. Dollar[9].

Dieser Hard Fork[10] war sehr kontrovers und führte schlussendlich zum Bruch in der Fangemeinde und dem Entstehen einer 2. Blockchain, die nun „Ethereum Classic“ heißt und diesen Hard Fork nicht mitgemacht haben. Die Währungen werden seitdem unter ETH für Ethereum und unter ETC für Ethereum Classic auf zahlreichen Börsen gehandelt.

Egal ob man nun der Meinung ist, dass Ethereum oder Ethereum Classic die bessere Philosophie vertritt, so hat dieser „Unfall“ sicher dazu beigetragen die Verwendung von komplizierten Smart Contracts mit wesentlich mehr Respekt entgegenzutreten. Eine gute Zusammenfassung der „Lessons Leaned“ wurde von Christoph Jentzsch, einem der Hauptentwickler der DAO, auf Medium.com[11] veröffentlicht.

Entwickler und Organisation

Ethereum wurde von Vitalik Buterin[12] (@VitalikButerin) Ende 2013 im zarten Alter von 19 Jahren zum ersten Mal in einem Whitepaper[13] beschrieben, nachdem er mehrere Jahre in verschiedenen Kryptoprojekten mitgearbeitet hatte. Die beschriebene Plattform: „Ethereum: Die nächste Generation elektronischer Verträge und die Plattform für dezentrale Anwendungen“, war auf Anhieb für viele der talentiertesten Entwickler und Mathematiker interessant. Die komplizierte Mathematik wurde in der Folge von Gavin Wood (@gavwood) in einem Yellowpaper[14] beschrieben, das im April 2014 veröffentlicht wurde.

[9] https://medium.com/curator-multisig-phf-official-channel/dao-token-holders-come-claim-your-money-b428f186572a#.razfy59f1
[10] https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/
[11] https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5#.u295ibqz6
[12] https://en.wikipedia.org/wiki/Vitalik_Buterin
[13] https://github.com/ethereum/wiki/wiki/%5BGerman%5D-White-Paper
[14] http://gavwood.com/Paper.pdf

Ab dann ging es sehr schnell und so wurde im Juni 2014 im schweizerischen Zug eine Stiftung eingerichtet und im Juli 2014 wurde der Crowdsale[15] von Ether Token gestartet, der für 42 Tage lief und am 2. September 2014 endete. Anfangs bekam man 2000 ETH pro Bitcoin (BTC) und es gab eine lineare Reduktion auf 1337 ETH pro BTC.

Schlussendlich wurde Bitcoins im Gegenwert von ca. 18 Mill. Dollar eingesammelt und damit gehört dieser Crowdsale zu den zehn erfolgreichsten Projekten[16] weltweit.

Die Ethereum Stiftung wird aktuell von Ming Chan, einer Absolventin des MIT (Massachusetts Institute of Technology, USA) gemanagt und diese unterstützt weiterhin Projekte mit besonderer Bedeutung. Die ursprünglichen Gründungsmitglieder sind vielfach in eigenen Ethereum Firmen aktiv und helfen heute das Ökosystem und die Basistechnologie weiterzuentwickeln.

Bild: DEVCON0 – erste Entwicklerkonferenz in Berlin, November 2014

[15] https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/
[16] https://en.wikipedia.org/wiki/List_of_highest_funded_crowdfunding_projects

Gavin Wood (rotes T-Shirt) arbeitet mit Ethcore hauptsächlich an Parity, einem der acht Ethereum Clients[17] der neben dem geth (go-ethereum) Client zu den am häufigsten verwendeten Clients zählt.

Joseph Lubin (rechts außen) hat die Ethereum Switzerland GmbH, die Vorgänger Gesellschaft zur Ethereum Stiftung mitgegründet, welche sich um die anfängliche Ethereum Entwicklung gekümmert hat und nun liquidiert[18] wurde. Anfang 2015 hat er ConsenSys in New York gegründet, wofür heute ca. 100 Mitarbeiter weltweit arbeiten und laufend mit zahlreichen Projekten[19] Aufmerksamkeit erreichen.

Christoph Jentzsch (Mitte, weißes Polo), Simon Jentzsch (hinten, 4. von rechts) und Stephan Tual (vorne, 4. von rechts) haben mit Slock.it ein nicht nur wegen „The DAO“ bekanntes Startup im IoT Bereich.

Zahlreiche andere Gründungsmitglieder arbeiten nach wie vor für die Ethereum Foundation, aber da die finanziellen Mittel Ende 2015 bereits massiv angegriffen waren und man die eingesammelten Bitcoins nicht rechtzeitig verkauft hatte, wurden von Ming Chan Anfang 2016 deutliche Kostenreduktionen[20] eingeführt. Aktuell scheint es keine wesentlichen finanziellen Probleme zu geben und ob sich die Ethereum Stiftung als dauerhafte Institution für die Weiterentwicklung des Protokolls positionieren kann, wird sich zeigen – wünschenswert wäre es auf jeden Fall.

Zwei weitere Gründungsmitglieder sollen hier auch noch erwähnt werden:

Vlad Zamfir (@VladZamfir, vorne, 2. von rechts) entwickelt für Ethereum die spieltheoretischen Voraussetzungen zur Umstellung von Proof-of-Work zu Proof-of-Stake. Diese Entwicklung läuft unter dem Namen „Casper“ und die Umsetzung ist für 2017 geplant.

[17] http://ethdocs.org/en/latest/ethereum-clients/choosing-a-client.html
[18] https://www.moneyhouse.ch/de/company/ethereum-switzerland-gmbh-20031937831
[19] https://en.wikipedia.org/wiki/ConsenSys
[20] http://allcoinsnews.com/2016/01/07/ethereum-foundations-cuts-costs-in-half-while-forming-long-term-strategies/

Viktor Tron (@zeligf, vorne, links) ist hauptsächlich mit der Entwicklung von Swarm – einer dezentralen Speicherlösung – beschäftigt. Es ist eine mit Ethereum eng verknüpfte Entwicklung und gehört als wichtiger Bestandteil zum dezentralen Gesamtkonzept.

Viele der Entwicklungen für Ethereum werden in Europa vorangetrieben, aber auch die Firma ConsenSys aus den USA ist wesentlich an den Fortschritten beteiligt.

Whitepaper, Yellowpaper und technische Informationen

Zu Ethereum gibt es jede Menge an Material zu lesen, wobei der Ersteinstieg natürlich auf der offiziellen Ethereum Webseite sein sollte – www.ethereum.org. Damit auch gleich zum ersten Satz auf der Webseite: „Ethereum is a decentralized platform that runs smart contracts“. Damit hat man auch den Hinweis auf die Haupteigenschaft von Ethereum – es geht nicht wie bei Bitcoin um digitales Geld für den Peer-2-Peer Austausch, sondern um die Ausführung von Programmen jeder Art auf einer Blockchain Plattform.

Wie schon in der Einleitung angedeutet wurden wesentliche Neuerungen mit Ethereum eingeführt, auf die ich nun etwas genauer eingehen möchte. Weitere Details finden sich im zugehörigen Whitepaper und Yellowpaper.

1. Accounts (Konten)

Ein wesentlicher Unterschied zu Bitcoin, welches ein rein transaktionsbasierendes System ist, ist die Verwendung von Konten bei Ethereum. Die Ethereum Blockchain verfolgt demnach den Status jedes Kontos, wovon es zwei Typen gibt – Externally Owned Accounts (EAO’s) und Contract Accounts. Die EAO’s enthalten die Werte und die Contract Accounts enthalten Werte und Speicher. Wenn nun zwischen EAO’s oder von einem EAO zu einem Contract Account ein Werttransfer stattfindet, dann wird dieser in der Blockchain dokumentiert und dauerhaft gesichert.

2. Ethereum Virtual Machine („EVM“)

Die EVM ist das Herzstück von Ethereum, wo der in einer höheren Programmiersprache (z.B. Solidity) geschriebene Code nach einer Kompilierung in Bytecode ausgeführt wird. Wenn der Bytecode in Ethereum gespeichert wird, wird ein Contract Account angelegt und bekommt

eine eindeutige Adresse, die dann von EAO's oder anderen Contract Accounts aufgerufen werden kann.

Die verwendeten Programmiersprachen sind „Turing complete", was so viel heißt wie, es kann jede Art von Logik abgebildet werden, um eine Turingmaschine[21] zu emulieren.

Ein offensichtliches Problem, das es zu lösen gab, ist das sogenannte Halteproblem[22], wo es darum geht, ob ein Programm zu einem Ende kommt. Würde ein Smart Contract nicht zu einem Ende kommen, dann würde die EVM dauerhaft beschäftigt sein – egal, ob das durch eine Attacke eines Angreifers auf das System oder einen Programmierfehler passiert ist. Damit wäre das System auch schnell einmal durch jeden Teilnehmer, und das kann jeder sein, lahmzulegen. Die Lösung dafür ist das sogenannte „Gas".

3. Gas

Neben Ether gibt es eine wertmäßig entkoppelte zweite Währung bei Ethereum – das „Gas". Gas kann man als den Treibstoff der Smart Contracts verstehen, um die Miner, die die EVM betreiben, zu bezahlen. Der Gaspreis richtet sich nach dem Preis der notwendigen Energie für einzelne Berechnungsschritte und wird regelmäßig angepasst.

Gas muss man aber nicht direkt kaufen, um Smart Contracts ausführen zu können, sondern das wird automatisch durch die EVM erledigt. Man spezifiziert lediglich beim Aufruf die maximalen Kosten (in Ether), die man gewillt ist für die Ausführung zu zahlen. Zahlt man zu wenig, wird der Smart Contract nicht ausgeführt oder verbraucht die Ausführung mehr als das maximal definierte Limit, dann stoppt die Ausführung.

Für die Programmierung ist es wichtig, sich mit den Gas-Preisen einzelner Rechenoperationen zu beschäftigen, da die EVM ein relativ teurer und langsamer Computer ist und man nur die Blockchain-relevanten Rechenoperationen dort ausführen sollte. Der Rest der Operationen sollte in der „DApp" erledigt werden.

[21] https://de.wikipedia.org/wiki/Turingmaschine
[22] https://de.wikipedia.org/wiki/Halteproblem

4. DApp

Eine DApp ist eine „Decentralized Application“, also ein Programm welches eine Schnittstelle zu einem Blockchain-System besitzt und mit dieser interagiert. Die DApp kann auf einem Mobilgerät oder jedem anderen Computer laufen, aber einzelne Funktionen werden dann auf der Blockchain ausgeführt – z.B. die Überweisung von Ether an jemand anderen. Eine Liste von vielen Ethereum DApp’s finden Sie hier.

5. Mining und Konsens

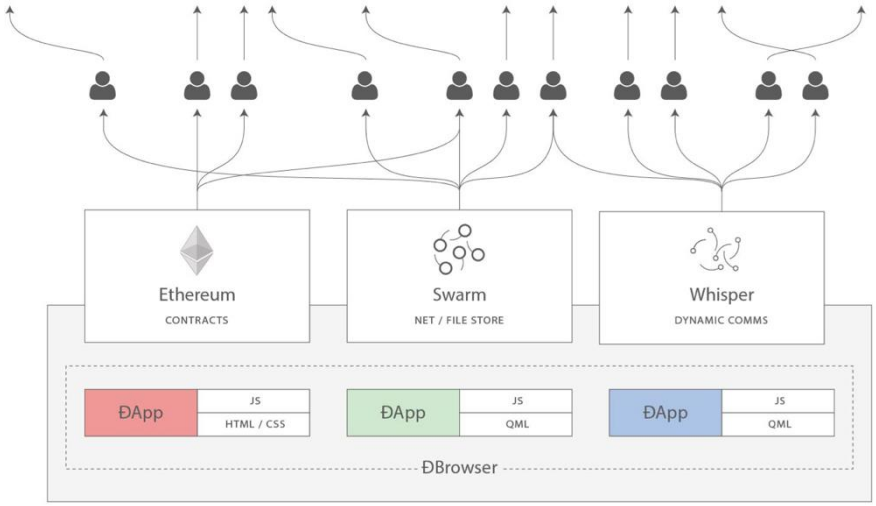
Die Sicherheit des Netzwerkes wird bei Ethereum wie auch bei Bitcoin über ein Belohnungssystem für die Miner erreicht. Es wird ca. alle 15 Sekunden ein neuer gültiger Block erzeugt, wobei der Miner Proof-of-Work (Algorithmus: Ethash) und eine vorgegebene Difficulty (Schwierigkeitslevel) nachweisen muss. Für diesen Miner gibt es dann 5 Ether als Belohnung und im Gegensatz zu Bitcoin werden diese Belohnungen über die Zeit nicht reduziert, man hat quasi eine konstante Inflation der Geldmenge. Weiters kommen die Transaktionsgebühren in Gas dazu und 1/32 von jedem hinzugefügten Uncle-Block (max. 2 dieser „Onkel-Blöcke“ sind erlaubt).

6. Uncle-Block (Onkel-Block)

Durch die geringe Blockzeit von 15 Sekunden kann es durch die Internet-Laufzeiten wesentlich leichter als bei Bitcoin vorkommen, dass sich Verzweigungen („Gabeln“) bilden, die vollkommen valide berechnet wurden. Zur Steigerung der Sicherheit verfolgt Ethereum deshalb das Konzept des schwersten Blocks mit der meisten benötigten Hash-Leistung – näheres dazu findet man im GOST Protokoll. Weiters werden auch die Miner von in die Blockchain aufgenommenen Uncle-Blocks belohnt – diese bekommen 4,375 Ether. Diese Lösung hilft auch gegen die ansonsten problematische Bevorzugung von großen Minern gegenüber den kleinen Minern im Netzwerk, wo es über die Zeit zu einer Konzentration der Miner kommen würde.

Ethereum, Swarm & Whisper

Obwohl Ethereum mit der Einführung von leicht programmierbaren Smart Contracts schon etwas sehr Besonderes darstellt, so ist das nur ein Teil des oftmals zitierten „Weltcomputers“.



Für die Speicherung von Daten ist eine Blockchain denkbar schlecht geeignet und für die dezentrale Kommunikation ist sie ebenso wenig gedacht. Dafür gibt es neben Ethereum auch noch Swarm für den Speicher und Whisper für die Kommunikation.

1. Swarm

Seit 15.12.2016 ist die erste Alpha-Version von Swarm verfügbar und kann von ambitionierten Entwicklern getestet werden. Die Unterschiede zu einer Cloud-Speicherlösung sind signifikant. Es handelt sich in der Endausbaustufe um einen Peer-2-Peer Speicher (wie auch Bittorrent), ohne Ausfallszeiten, Sicherheit gegen Distributed-Denial-of-Service (DDoS) Attacken, hohe Fehlertoleranz, komplett zensurresistent und durch ein eingebautes Belohnungssystem auch selbsterhaltend. Damit in Swarm gespeicherte Daten aktualisiert und verändert werden können, verwendet Swarm das Ethereum Name Service (ENS).

Durch die Adressierung über ENS kann es nicht zu einer DDoS Attacke kommen und da die „zerhackten“ Daten nur vom Eigentümer mit dem privaten Schlüssel zusammengebaut werden können, ist maximale Sicherheit bei maximaler globaler Verfügbarkeit mit eingebaut. Nähere Details findet man in zwei Orangepaper.

2. Whisper

Weil die Blockchain kein guter Ort zur Speicherung von Nachrichten ist, gibt es noch Whisper, dass wie das Internet Protokoll auch Datagramm[23] basierend ist. Damit lässt sich die Privatsphäre je nach Bedarf einstellen, je schneller die Informationsverteilung passieren soll umso mehr Routinginformationen müssen preisgegeben werden wobei Nachrichten immer verschlüsselt sind. Weitere Details findet man hier.

Die Dokumentation zu Whisper ist noch relativ dünn und es gibt nur wenige Anwendungen, die diese Funktionalität bisher nutzen. Slock.it demonstrierte die Öffnung eines über die Ethereum Blockchain bezahlten Schlosses und Status.im (Gewinner des Blockchain Startup Contests[24]) verwendet Whisper für ihren Instant Messaging Client „Status“.

Natürlich gibt es auch noch andere Weiterentwicklungen für Ethereum, die sich vor allem mit der Problematik der Skalierung, der Sicherheit, dem Konsens-Algorithmus und der Privatsphäre bei Transaktionen beschäftigen. Diese Aktivitäten sind unter anderem Inhalt des nächsten und vierten Teils dieses Weiterbildungsthemas „Aktuelle Weiterentwicklungen und potentielle Auswirkungen“.

[23] https://en.wikipedia.org/wiki/Datagram
[24] http://magazine.startus.cc/these-are-the-winners-of-the-2016-blockchain-startup-contest/

Rootstock

Rootstock (RSK) war die erste Plattform für Smart Contracts auf der Bitcoin-Plattform.

Die Idee dahinter war, die Möglichkeiten der Bitcoin-Blockchain um Smart Contracts auf Basis einer Turing Virtual Machine, raschere Zahlungen und einer höheren Skalierbarkeit zu erweitern und somit das Bitcoin-Ecosystem zu verbessern.

RSK arbeitet hier mit einer Sidechain der Bitcoin-Blockchain, Bitcoin können in die RSK-Chain transferiert werden und werden dort zu Rootcoins, diese können jederzeit wieder in Bitcoin gewechselt werden. Rootcoins werden zur Bezahlung der Miner verwendet, sind jedoch keine eigens gehandelte Kryptowährung, da sie direkt an Bitcoin gebunden sind, aus Bitcoin entstehen und wieder zu Bitcoin werden.

Entwickler und Organisation

Hinter Rootstock stecken in der Krypto-Entwicklerszene bekannte Namen, allen voran Sergio Demián Lerner (@SDLerner), der unter anderem auch 2015 ein Whitepaper zum Directed Acyclic Graph, dem DAG veröffentlicht hat, mit dem wir uns weiter unten bei IOTA und Byteball beschäftigen werden. Weitere Namen hinter Rootstock sind Diego Gutierrez Zaldivar (@dieguito), Rubén Ariel Altman (@raltman), Adrián Eidelman (@aeidelman), Gabriel Kurman (@gabrielkurman) und Adrián Garelik (@adriangarelik)[25]

Whitepaper und technische Informationen

Weitere Informationen zu Rootstock gibt es auf der Webseite http://www.rsk.co/. Dort findet sich auch das Whitepaper zu Rootstock wie auch zu Sidechains and Drivechains von Sergio Lerner.

Folgende Grundprinzipien stecken hinter Rootstock:

Bitcoin friendly: Rootstock unterstützt Bitcoin, indem es die Möglichkeit von Smart Contracts eröffnet. Das Fehlen von Smart Contracts wäre eine Gefahr für Bitcoin, hier wäre es möglicherweise von Ethereum an Wichtigkeit rasch überholt werden. Durch diese Zwei-Weg-Verbindung zwischen der Bitcoin- und der Rootstock-Blockchain und dem Fakt, dass Rootstock

[25] http://www.rsk.co/#team

nicht neu geschaffen wird, sondern immer aus Bitcoin entsteht, gibt es auch keine Konkurrenz zwischen den Währungen.

Sicherheit: Bei Rootcoin und Bitcoin gibt es ein merge-mining, d.h. Bitcoin-Miner minen auch Rootcoins mit. Dadurch erreicht RSK dieselbe Sicherheit hinsichtlich der Verhinderung von Double-Spending und Finalität der Transaktion.

Skalierbarkeit: RSK kann bis zu 100 Transaktionen pro Sekunde verarbeiten, das entspricht dem Niveau von Paypal – das ist deutlich mehr als Bitcoin, wo das Limit um die 7 Transaktionen pro Sekunde liegt.

Sofortzahlungen: Um neue Anwendungsfälle wie den lokalen Handel realisierbar zu machen, müssen die Bestätigungszeiten für die Transaktion sinken. RSK bietet mit neuen theoretischen Protokollen wie DECOR+GHOST[26] Blockintervallzeiten von durchschnittlich 10 Sekunden.

[26] https://bitslog.wordpress.com/2014/05/02/decor/

Counterparty

Wie Rootstock arbeitet auch Counterparty auf Basis der Bitcoin-Blockchain. Die eigene Währung XCP wird wie Rootcoins aus Bitcoin erzeugt, dient in der Counterparty-Blockchain als Zahlungsmittel und steht nicht in Konkurrenz zu Bitcoin.

Auch Counterparty möchte die Möglichkeiten von Bitcoin erweitern. Folgendes wird mit Counterparty auf der Bitcoin-Blockchain möglich:

Eigene Tokens kreieren

Jeder kann einen eigenen, digitalen Token kreieren – dieser kann die unterschiedlichsten Werte repräsentieren. Beispiele für Anwendungsfälle sind:

- Durchführung von Crowdfunding oder Wahlen
- Monetarisierung bei der Nutzung einzelner Anwendungen bei DApps (decentralized application)
- Repräsentierung eines Produktes oder einer Marke
- Eine Art „Blockchain domain name“ (https://coindaddy.io/)
- Zur Authentifizierung
- Um digitale Güter zu repräsentieren
- als Belohnung für Zeit und Ressourcen

Smart Contracts

Counterparty Smart Contracts basieren auf Ethereum und können in Solitidy geschrieben werden und erlauben auch die Interaktion mit Counterparty Tokens wie den Zugriff auf Bitcoin-Transaktionen über BTC-Relay, eine Verbindung zwischen der Bitcoin Blockchain und Ethereum Smart Contracts.

Asset Exchange ("DEX")

Counterparty agiert hier in der Rolle des Treuhänders, der Gelder für Handelsgeschäfte erst weiterleitet, wenn das Geschäft vollzogen ist. Hierdurch können Kosten und Zeit eingespart werden, da externe Treuhänder vermieden werden können.

Payment Channels

Hier möchte Counterparty in Zukunft auf Basis des Lightning Networks rasch und dezentralen Zahlungsverkehr ermöglichen, der letztlich in der Bitcoin-Blockchain dokumentiert wird.

Außerdem unterstützt Counterparty das Thema Wahl und Multisigniture, wo durch den Einsatz mehrerer Unterschriften für eine Transaktion neue Anwendungsmöglichkeiten eröffnet werden [27].

Entwickler und Organisation

Hinter den Gründern Robby Dermody, Adam Krellenstein und Evan Wagner steht ein größeres Team aus Entwicklern und Beratern[28]. Die not-for-profit Counterparty Foundation will das Wachstum und die Entwicklung der Counterparty-Plattform vorantreiben und hier auch die Community unterstützen[29].

Weitere Informationen

Auf der Counterparty-Webseite findet sich eine ausführliche Dokumentation, die sich auch an Entwickler richtet: http://counterparty.io/docs/

Interessant ist auch die Auflistung unterschiedlicher Projekte der Community. Darunter findet man zum Beispiel auch FoldingCoin, der von der Stanford University als Belohnung für das Zuverfügungstellen eigener Rechnerleistung für die medizinische Forschung ausgegeben wird, oder Spells of Genesis, ein Computerspiel – Mehr dazu hier:
http://counterparty.io/community-projects/

[27] https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do
[28] https://counterparty.io/platform/#team
[29] http://counterparty.io/foundation/

IOTA

IOTA sieht sich als Basisnetzwerk für das Internet of Things. Nicht nur Micro- und sogar Nanopayments (also Zahlungen im Cent-Bereich oder noch darunter) sollen hiermit in einem internationalen Umfeld ermöglicht werden, sondern auch der Datenaustausch zwischen den verschiedenen IoT-Geräten soll hier eine Plattform erhalten.

Das Besondere dabei ist, dass sämtliche Transaktionen ohne Gebühren erfolgen und dass das IOTA Netzwerk im Gegensatz zur klassischen Blockchain, wie wir sie von Bitcoin und anderen Altcoins kennen, skalierbar ist – beides sind bei der steigenden Zahl von IOT-Geräten Grundvoraussetzungen, um als Basisnetzwerk für IoT-Anwendungen dienen zu können. Die Basis für diese Eigenschaften ist eine neuartige Weiterentwicklung der Blockchain, die komplett ohne Blöcke auskommt, der sogenannte DAG (directed acyclic graph) oder auch Tangle genannt, was übersetzt so viel bedeutet wie Wirrwarr oder Durcheinander. Diese Entwicklung ermöglich die Skalierbarkeit, die kostenfreien Transaktionen wie auch die Datenintegrität und Datenübermittlung und garantiert auch Sicherheit, sollten einmal Quantencomputer zur Realität werden. Zwar ist diese Gefahr aktuell noch theoretisch, aber ein Quantencomputer könnte kryptografische Rätsel deutlich effizienter lösen als klassische Computer und somit eine Gefahr für Bitcoin aber auch für viele andere aktuelle Sicherheitskonzepte werden.

Entwickler und Organisation

IOTA wurde von dem Norweger David Sønstebø, einen Entwickler mit dem Pseudonym Come-from-Beyond bzw. Sergey und Serguie Popov gegründet, durchaus bekannte Namen im Kryptobereich, die schon in einigen anderen Projekten involviert waren,

Im März 2016 kündigten die drei die Gründung einer Foundation an, um die Entwickler- und Unterstützergemeinschaft für IOTA zu vergrößern. Die Motivation dahinter beschrieben sie folgendermaßen: “As we have seen with other projects: having the best technology is not enough. Open source technology can be ignored, cloned or come to a halt due to lack of sufficient or organized incentive for maintenance and growth. The crypto landscape is

littered with these projects that had a good idea but never gained momentum to make any use of it. IOTA is not going to end up like this."[30]

Die Gründung der Foundation, die an die Spende von 50 Mio. IOTAs gebunden war, gelang, wenngleich es auch Stimmen gab, dass hier zur Generierung der Spenden Druck auf die Inhaber von IOTAs ausgeübt wurde – nach dem Motto: „Entweder wird das Projekt unterstützt oder wir arbeiten nicht weiter an der IOTA-Blockchain." Die Gründer zeigen bislang wohl auch nicht besonderes Geschick beim Community-Management, Mitglieder der Gemeinschaft wurden wohl vom CEO David Sønstebø beleidigt, Informationen sind eher rar. Auch dass die Plattform für einen Umbau für einen Zeitraum von vier Wochen abgeschaltet wurde, stieß auf Kritik.[31]

Die fachliche Kompetenz des Gründerteams und anderer Entwickler und Unterstützer der Foundation wie auch die spannenden Möglichkeiten, die sich mit IOTA eröffnen, scheinen hier jedoch so manche soziale Schwierigkeit Wett zu machen. Das Fazit von Markus M. Bohl vom Altcoinspekulant-Blog dazu lautet: „Das Glas ist freilich trotz manch negativer Umstände mehr als halbvoll. Auch ich war relativ beeindruckt von dem Update am Samstag und den Weichenstellungen für die Zukunft. Das sieht sehr durchdacht aus und es konnte auch zusätzlich hochkarätiges Personal gewonnen werden. Dominik Schiener war ja bereits ein Glücksfall für das Projekt und nun zusätzlich die Verpflichtung von Gianluigi Davassi und Per Lind, können sich mehr als sehen lassen. Wenn das IOTA-Team nun weiter macht und IOTA auch tatsächlich bei einigen IoT-Firmen platzieren kann + evtl. noch ein positives Update zum Jinn-Prozessor*, dann könnte IOTA durchaus für ordentlich Furore machen. Ich halte mittlerweile eine Marktkapitalisierung ein dreistelliger Millionenhöhe für nicht ausgeschlossen. IOTA sammelte beim ICO übrigens rund eine halbe Million Dollar ein…"[32]

Also man kann gespannt darauf sein, ob bzw. wann es IOTA tatsächlich gelingt, in der Realwirtschaft eingesetzt zu werden. Interessant ist insbesondere auch die Hardware-Firma

[30] https://forum.iotatoken.com/t/iota-foundation-announcement/174?source_topic_id=1098
[31] https://altcoinspekulant.wordpress.com/2016/10/25/iotatoken-feiert-ersten-geburtstag-wichtige-updates/
[32] https://altcoinspekulant.wordpress.com/2016/10/25/iotatoken-feiert-ersten-geburtstag-wichtige-updates/

JINN des Gründungsteams, deren Zielsetzung es ist, einen auf einer Dreierlogik basierenden Prozessor zu entwickeln, einen ternären Computer, der aufgrund der damit erreichbaren Effizienzsteigerung für das Internet of Things wertvoll sein kann.

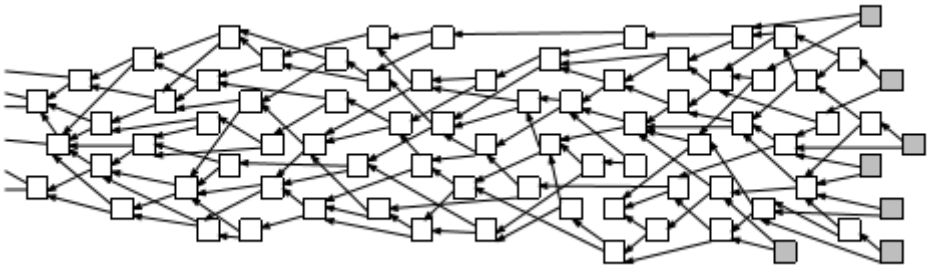
Whitepaper und technische Informationen

News zu IOTA und nützliche Informationen – auch für Entwickler, die die Möglichkeiten der aktuellen Beta-Version erkunden wollen – finden sich auf der Webseite https://www.iotatoken.com/.

Wer Lust darauf hat, kann hier auch das Whitepaper nachlesen.

Hier möchte ich Ihnen kurz eine Einführung zum Tangle geben. Denn im Gegensatz zur klassischen Blockchain von Bitcoin braucht der Tangle keine Miner und Knoten, um die Transaktionen in Blöcke einzubauen und zu bestätigen. Vielmehr muss ein jeder, der eine Transaktion einstellen möchte, zwei vorhergehende Transaktionen bestätigen. Erst das macht das System skalierbar, was für ein dichtes Netz aus IoT-Geräten unabdingbar ist, und ermöglicht den Verzicht auf Gebühren für die Transaktionen.

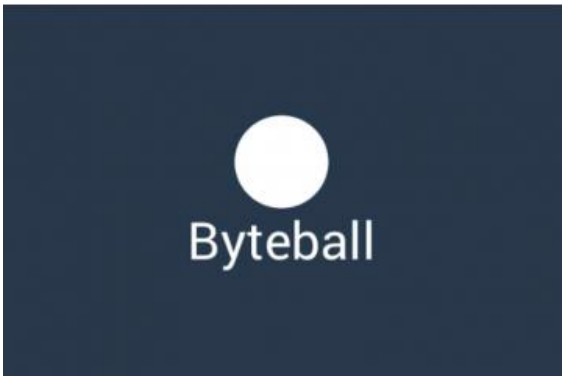
Hier eine Abbildung aus dem Whitepaper, wie man sich diesen Tangle vorstellen kann.



IOTA sieht sich als Plattform, die vor allem eines kann: effiziente, sichere, ressourcenschonende Transaktionen in Echtzeit ohne Gebühren zu ermöglichen. Sie wollen nicht die anderen Blockchains ersetzen, sondern sehen sich vielmehr als Ergänzung zu Ethereum, Rootstock und ähnlichem. Sie wollen das Basisnetzwerk für IoT-Geräte werden, für eine Zeit, in der Maschinen mit Maschinen interagieren, IoT-Geräte im Schatten den Strom direkt von der nächsten Solarzelle kaufen oder Rechenleistung je nach Angebot und Nachfrage automatisch geteilt wird.[33] Man darf gespannt sein, wie sich dieses Netzwerk weiterentwickeln wird.

[33] https://medium.com/@DavidSonstebo/iota-97592581f985#.7zygbqlmq

Byteball



Wie IOTA nutzt Byteball einen Directed Acyclic Graph (DAG), bei IOTA auch Tangle genannt. Byteball sieht sich jedoch nicht als Basisnetzwerk für das IoT, spezialisiert darauf Wert- und Datentransaktionen zwischen Maschine und Maschine abzuwickeln, vielmehr möchte Byteball eine Plattform für Transaktionen zwischen Menschen werden, also bestehende Kryptowährungen wie Bitcoin ablösen und hier anonyme Transaktionen ermöglichen wie auch die Möglichkeit für Smart Contracts bieten.

Wie IOTA ist Byteball aufgrund der innovativen Technologie des DAG skalierbar, eine Eigenschaft, woran bei Bitcoin noch gearbeitet werden muss. Im Gegensatz zu IOTA fallen bei Byteball jedoch Transaktionsgebühren an – wohl auch ein Grund, worum diese Plattform nicht als Basisnetzwerk für das Internet of Things dienen kann.

Die Gebühren betragen 1 BYTE für jedes transferierte Byte Daten. Und es wird kein kryptografisches Rätsel gelöst, um Transaktionen zu bestätigen. Vielmehr funktioniert der Bestätigungsmechanismus über eine Mainchain (MC), die es erlaubt, eine korrekte Reihenfolge der Transaktionen herzustellen. Diese Mainchain besteht aus Transaktionen von besonders vertrauenswürdigen Usern – sogenannten Witnesses- So gilt im Falle eines Double Spending die Transaktion, die in der Mainchain zuerst gereiht wurde. Das Besondere an dieser Plattform ist wohl der Blackbyte, wodurch anonyme Transaktionen ermöglicht werden.

Entwickler und Organisation

Im Gegensatz zu IOTA, wo eine Gruppe an Entwickler an der Technologie und der Markteinführung arbeitet, steckt hinter Byteball ein Name: Anton Churyumov, ein russischer Doktor der Physik und Mathematik, der seine Forschungskarriere aufgab und ab 2001 in unterschiedlichen Internet-Unternehmen mitentwickelte und diese aufbaute. Byteball ist sein erstes Kryptoprojekt.

Abgesehen von der Nutzung der DAG-Technologie sieht Churyumov keine Gemeinsamkeiten zu IOTA. Byteball sieht er durchaus als mögliche Datenbank, auf der Banken ihre Kundenkonten und Transaktionen speichern können, denn auch die Anforderungen der Regulationsbehörden können erfüllt werden.

Verteilung der Währung

Wer Bytes und Blackbytes haben wollte, konnte sich mit seiner Bitcoin-Adresse registrieren und erhielt entsprechend seines Bitcoin-Guthabens eine gewisse Menge an Bytes und Blackbytes. 98 Prozent aller verfügbaren Bytes werden so in mehreren Runden unter die Leute gebracht, je mehr Bitcoins jemand hat, umso mehr Bytes kann er halten. Churyumov sah in diesem Verteilungsschlüssel einerseits eine klare Regelung, andererseits eine Belohnung für die, die schon früh in Bitcoins eingestiegen sind und an dieses System geglaubt haben.[34] Bislang gab es eine Distributionsrunde am 25. Dezember 2016, bei der rund 10 Prozent der verfügbaren Bytes verteilt wurden. Für diese Runde waren rund 70.000 BTC registriert. Die zweite Verteilungsrunde ist für Mitte Februar 2017 geplant.

Whitepaper und technische Informationen

Mehr Infos zu Byteball gibt es auf https://byteball.org/ und wer sich in die technischen Details Details zu DAG und MC einlesen möchte, findet die Infos im Whitepaper hier.

Folgende Eigenschaften sind auf der Byteball-Webseite als besonders angeführt:

- Unveränderbarer Datenspeicher: Sobald Daten in der Byteball Datenbank gespeichert sind, lassen sie sich nicht mehr verändern oder entfernen.
- Finales Settlement: Sobald eine Transaktion eingebunden wurde, kann sie nicht mehr verändert werden, selbst von einem mächtigen Angreifer.
- Regulierte Assets nach KYC/AML Anforderungen können eingebracht werden
- Private Zahlungen, die nur Peer-to-Peer sichtbar sind, jedoch nicht in der öffentlichen Datenbank
- Bestätigung von Transaktionen über Multi-Signature ist möglich
- Treuhänderschaft möglich, wenn sich die Transaktionspartner nicht vertrauen
- Atomic exchange möglich: d.h. wenn verschiedene Kryptotoken zwischen zwei Personen ausgetauscht werden, muss nicht eine dritte Partei (Wechselbörse) als Treuhänder fungieren, um zu garantieren, dass beide ihren Teil erhalten. Hier werden entweder beide Transaktionen durchgeführt oder keine.
- Zahlungen möglich in einer Chat-Umgebung
- Besser als normale Blockchains wegen dem DAG

Man darf gespannt sein, wie sich dieses Projekt weiterentwickelt. Die Technologie und die Ansätze sind spannend und bieten ein weites Feld an Einsatzmöglichkeiten. Ob es Anton Churyumov gelingt, das System wachsen zu lassen, wird sich zeigen, die Plattform ist noch sehr jung.

[34] https://altcoinspekulant.wordpress.com/tag/anton-churyumov/

NEM

NEM steht für New Economy Movement und sieht sich als Bewegung, die Individuen ermächtigen möchte, indem sie eine neue Wirtschaft auf Basis von den Prinzipien Dezentralisierung, finanzielle Freiheit und Chancengleichheit erschaffen können. Sie behauptet von sich, einmalig im Blockchainbereich zu sein. Komplett neu programmiert, somit sicher, schnell und skalierbar wie auch einfach mit Hilfe einer API zu erweitern. Grundsätzlich ermöglicht die Plattform den Austausch vom Kryptotoken XEM, und dies weltweit ohne die Notwendigkeit eines Bankkontos. NEM sieht sich darüberhinausgehend als Peer-to-Peer-Plattform, Assests können kreiert werden, Namen vergeben und Nachrichten übermittelt.

Das Besondere an NEM ist auch der Bestätigungsmechanismus POI – also Proof of Importance[35]. Anstatt die Miner um die Wette rechnen zu lassen oder wie beim Proof of Stake (POS) (wie er bspw. bei NXT genutzt wird) die Anzahl der gehaltenen Kryptotoken die Wahrscheinlichkeit ergeben, einen neuen Block zu bestimmen, wird beim POI System neben den gehaltenen Token auch die Anzahl der Transaktionen und die Interaktionen in der Community ins Kalkül gezogen.

NEM möchte die Plattform für weitere spannende Projekte werden, aktuell kommen sie mit folgenden Anwendungsmöglichkeiten:

- Erste Multisig Blockchain Lösung
- Eine verschlüsselte Messaging Möglichkeit
- Geschütztes Wallet, das nicht immer online sein muss. Das Wallet ist passwortgeschützt, das Passwort wie der private Schlüssel verlassen nie den Computer, auf dem das Wallet läuft.
- Mosaics erlaubt Assets zu generieren, veränderliche oder fixe, gedeckelt oder nach oben offen, aufteilbar und unteilbar, inkludierbar in andere Tokens…
- Namespaces ist NEMs Namensservice – hier können Organisationen Brands bilden
- Wallets für Android, iOS und Desktops.
- Spam Schutz, der Attacken im Netzwerk verhindert, indem automatisch die Gebühren für den Angreifer steigen.

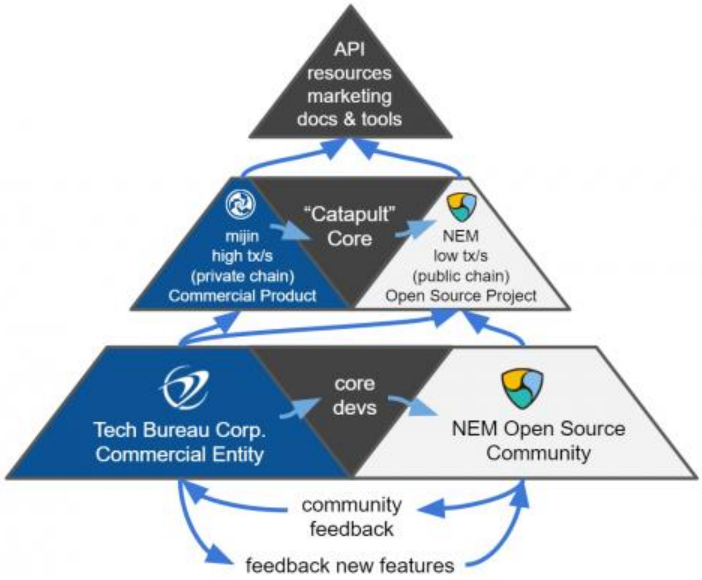
[35] https://cointelegraph.com/news/proof-of-importance-nem-is-going-to-add-reputations-to-the-blockchain

Technische Informationen findet man unter https://www.nem.io/NEM_techRef.pdf bzw. https://www.nem.io/.

Ein aktuelles Beispiel für die Entwicklung neuer Anwendungen auf Basis von NEM ist Landstead, eine Plattform, die erlaubt, ein Grundbuch auf der Blockchain zu führen. Eine kurze Einführung zu dem System finden Sie in diesem Video.

Weitere Projekte der Hauptentwickler

NEM ist ein Open Source Projekt, dessen Entwicklung im Jänner 2014 startete. Ab Herbst 2015 kooperierten die Hauptentwickler (BloodyRookie gimre Jaguar0625 Makoto) mit dem japanischen Tech Bureau, um die private, auf die Finanzindustrie zugeschnittene Blockchainlösung Mijin zu entwickeln, aktuell ist bereits der Nachfolger unter dem Namen Catapult in Entwicklung (Hier geht es zum Whitepaper). Hier wird der Versuch gemacht, die kommerzielle Software mit der Open Source Software NEM zu verbinden. Dadurch kann auf der einen Seite die private Blockchain für sensible Daten genutzt werden, auf der anderen Seite kann die eine Blockchain-Lösung von der anderen lernen, neue Applikationen bei Erfolg leicht von der einen Blockchain-Lösung auf die andere übertragen werden. (https://blog.nem.io/relationship-between-nem-mijin-catapult-u/)



Genau diese Offenheit für auf NEM aufbauende neue Anwendungen und die Zusammenarbeit mit Finanzinstituten über Mijin bzw. Catapult machen diese Plattform interessant. Man darf gespannt sein, was sich hier in den nächsten Monaten bzw. Jahren entwickelt.

Eine Auswahl weiterer Plattformen:

Das Blockchain-Ecosystem entwickelt sich zurzeit rasant, neue Projekte entstehen, andere verschwinden wieder in die Bedeutungslosigkeit. Wie sich einzelne Projekte weiterentwickeln, lässt sich schwer prognostizieren. Die wichtigsten Informationsquellen sind einschlägige Blogs und Online-Medien. Hier zum Abschluss will ich noch kurz auf ein paar weitere Plattformen hinweisen, ohne Wertung und Anspruch auf Vollständigkeit

Bigchain DB sieht sich als große Datenbank mit Blockchain-Eigenschaften und verbindet so die Eigenschaften einer verteilten Datenbank mit den Möglichkeiten der Blockchain.

Details dazu findet man auf https://www.bigchaindb.com/, das Whitepaper findet sich hier: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Ripple sieht sich als Blockchain-Plattform für den Banking Sektor und ist dort weit verbreitet. Die Transparenz der Blockchain führt aber zu Problemen bei den Kunden und könnte in der nächsten Entwicklungsstufe verschwunden sein. Mehr dazu gibt es auf https://ripple.com/.

Nxt wurde früher als innovative Plattform wegen des PoS (Proof of Stake) Mechanismus gelobt, ist mittlerweile aber eher bedeutungslos. Die ungerechte Erstzuteilung und die Tendenz zur Konzentration der NXT Coins stieß auf teilweise herbe Kritik. Mehr Infos unter https://nxt.org/.

Tezos sieht sich als sicheres Smart Contract Plattform. Mehr Infos unter https://tezos.com/

Synero sieht sich als die Zukunft für Content Creation, Publishing und Distribution und als dezentrales soziales Netzwerk. Mehr dazu unter http://www.synereo.com/. Vor kurzem hat sich die bisher geplante Technik der RChain abgespalten und geht nun eigene Wege.