Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

ÜBERBLICK MODERNE KRYPTOWÄHRUNGEN

Version 1.0 vom 23.05.2018
Alexander Marsalek – Alexander.Marsalek@a-sit.at
Bernd Prünster – Bernd.Pruenster@a-sit.at

Zusammenfassung: Dieses Dokument gibt einen Überblick über moderne auf Privatsphäre oder Skalierbarkeit optimierte Kryptowährungen. Konkret werden die auf Privatsphäre optimierten Kryptowährungen Dash, Monero, PIVX und Zcash, sowie die auf Skalierbarkeit optimierten Kryptowährungen IOTA und Nano vorgestellt und mit Bitcoin in Hinblick auf Skalierbarkeit und Privatsphäre verglichen. Diese Kryptowährungen wurden aus ca. 1000 Kryptowährungen aufgrund ihrer Features und ihrer Verankerung im Kryptomarkt ausgewählt um auch in diesem dynamischen Umfeld einen möglichst nachhaltigen Überblick zu geben. Die Studie zeigt, dass es bisher keiner Kryptowährung gelungen ist beide Probleme zu lösen.

Inhaltsverzeichnis

1. Einleitung

In diesem Dokument werden ausgewählte moderne Kryptowährungen vorgestellt. Als Vergleichsbasis dient die erste blockchainbasierte Kryptowährung *Bitcoin*, welche im folgenden Kapitel noch einmal kurz beschrieben wird. Als moderne Kryptowährungen qualifizieren sich neue Ansätze, die spezielle Aspekte oder Schwächen von Bitcoin verbessern bzw. beheben sollen. Konkret behandelt dieses Dokument die auf Privatsphäre und Anonymität optimierten Kryptowährungen *Dash*, *Monero*, *PIVX* und *Zcash*, sowie die auf Skalierbarkeit optimierten Währungen *IOTA* und *Nano*. Nicht alle im Zuge dieses Projektes analysierten Währungen werden in diesem Dokument behandelt. Beispielsweise wurde im Zuge dieses Projektes eine Schwachstelle in einer Kryptowährung gefunden, welche Double-Spending-Angriffe ermöglicht. Im Sinne von Responsible Disclosure wird diese Währung und deren Schwachstelle in diesem Dokument nicht behandelt. Des Weiteren werden *Ethereum* und *Ripple* hier nicht noch einmal betrachtet, da diese Währungen bereits zuvor im *Technologieüberblick Blockchain*-Bericht [1] behandelt wurden.
Im nächsten Abschnitt werden die Grundlagen zu Bitcoin vorgestellt. Anschließend werden der Reihe nach Dash, IOTA, Monero, Nano, PIVX und Zcash vorgestellt und mit Bitcoin verglichen.

2. Bitcoin

In diesem Abschnitt werden die wichtigsten Grundlagen zu Bitcoin und zur Blockchain wiederholt. Der folgende Text wurde weitgehend aus [1] übernommen und lediglich an den Kontext dieses Dokumentes angepasst.

Der Begriff *Bitcoin* wird oft als Synonym für unterschiedliche Komponenten und Aspekte des Systems Bitcoin verwendet. Tatsächlich umfasst dieses ein Bezahlsystem basierend auf einer Kryptowährung, die Kryptowährung selbst, ein *Peer-to-Peer-Netzwerk*[1], sowie eine Referenzimplementierung der Software. Diese wird benötigt um diesem Netzwerk beizutreten und Transaktionen abwickeln zu können. Weiters ist auch die *Blockchain* als zentrales Transaktionsregister und Eckpfeiler des Bezahlsystems ein zentraler Bestandteil von Bitcoin. Oft wird auch der Begriff *Kryptowährung* als Synonym für die Gesamtheit eines solchen Systems verwendet. Durch die enge Koppelung aller Komponenten ist es schwierig, diese isoliert zu betrachten, weshalb in diesem Abschnitt die Grundlagen des Systems Bitcoin in seinen wesentlichen Aspekten basierend auf [2] beschrieben werden.

Zur Veranschaulichung des grundlegenden Ablaufs und der Begriffe werden in Abbildung 1 jene Begriffe und Schritte einer Transaktion erläutert, die für das Verständnis von Bitcoin wesentlich sind. Die Begriffe werden anschließend in Abschnitt 2.1.1 genauer erläutert bzw. eine Transaktion in Abschnitt 2.1.3 beschrieben.

Eine Grundlage ist, dass bestimmte selbsterklärte Teilnehmer des Bitcoin-Netzwerks (sog. „Miner“) Werte generieren, indem sie kryptografisch schwere Rätsel lösen. Durch die Lösung des Rätsels erhält der Miner einen (Daten-)Block, der eine bestimmte Eigenschaft erfüllt. Dies dient als *Proof-of-Work.* Anschließend muss der Miner den erstellten Block an die ihm bekannten P2P-Teilnehmer schicken. Auf diese Weise baut sich bei jedem Teilnehmer dezentral ein öffentliches Transaktionsregister auf und jeder kann – über kryptografisch relativ einfache Funktionen – die Transaktionen überprüfen. Blöcke anderer Miner – die wiederum Daten anderer Transaktionen

[1] Ein *Peer-to-Peer-Netzwerk* (P2P-Netz) beschreibt eine dezentrale Netzwerkstruktur. Im Gegensatz zu hierarchischen Netzen (wie beispielsweise dem Telefonnetz) oder klassischen Client-Server Netzwerken sind P2P-Netze flach organisiert. Jeder Teilnehmer ist gleichzeitig Client und Server und trägt seinen Teil dazu bei, Informationen durch das Netzwerk zu leiten. Dadurch ergibt sich ein hohes Maß an Ausfallsicherheit, da es keinen Single Point-of-Failure gibt. Im Regelfall sind P2P-Netze logische Strukturen, welche auf bestehenden Netzwerken aufbauen; bestehende Infrastruktur wird verwendet, deren Organisation und Struktur jedoch verborgen. Den Teilnehmern eines P2P-Netzes erscheint ein solches Netzwerk so, als würde es sich tatsächlich um eine Gruppe von Teilnehmern handeln, welche alle auf einer einzigen Ebene miteinander verbunden sind.

verknüpfen – werden mit dem eben generierten verknüpft. Auf diese Weise sind alle Transaktionen miteinander verkettet.
Ein Benutzer, der Werte besitzt (sie in einer *Wallet* hält) gibt diese wiederum weiter, indem er eine Transaktion mit diesen eingehenden Werten generiert, signiert und weitergibt. Diese wird wiederum als Teil eines neuen verketteten Blocks im Transaktionsregister (d.h. der Blockchain) prüfbar protokolliert. (Rest-)Werte wie „Wechselgeld“ werden ebenfalls in die Transaktion aufgenommen.

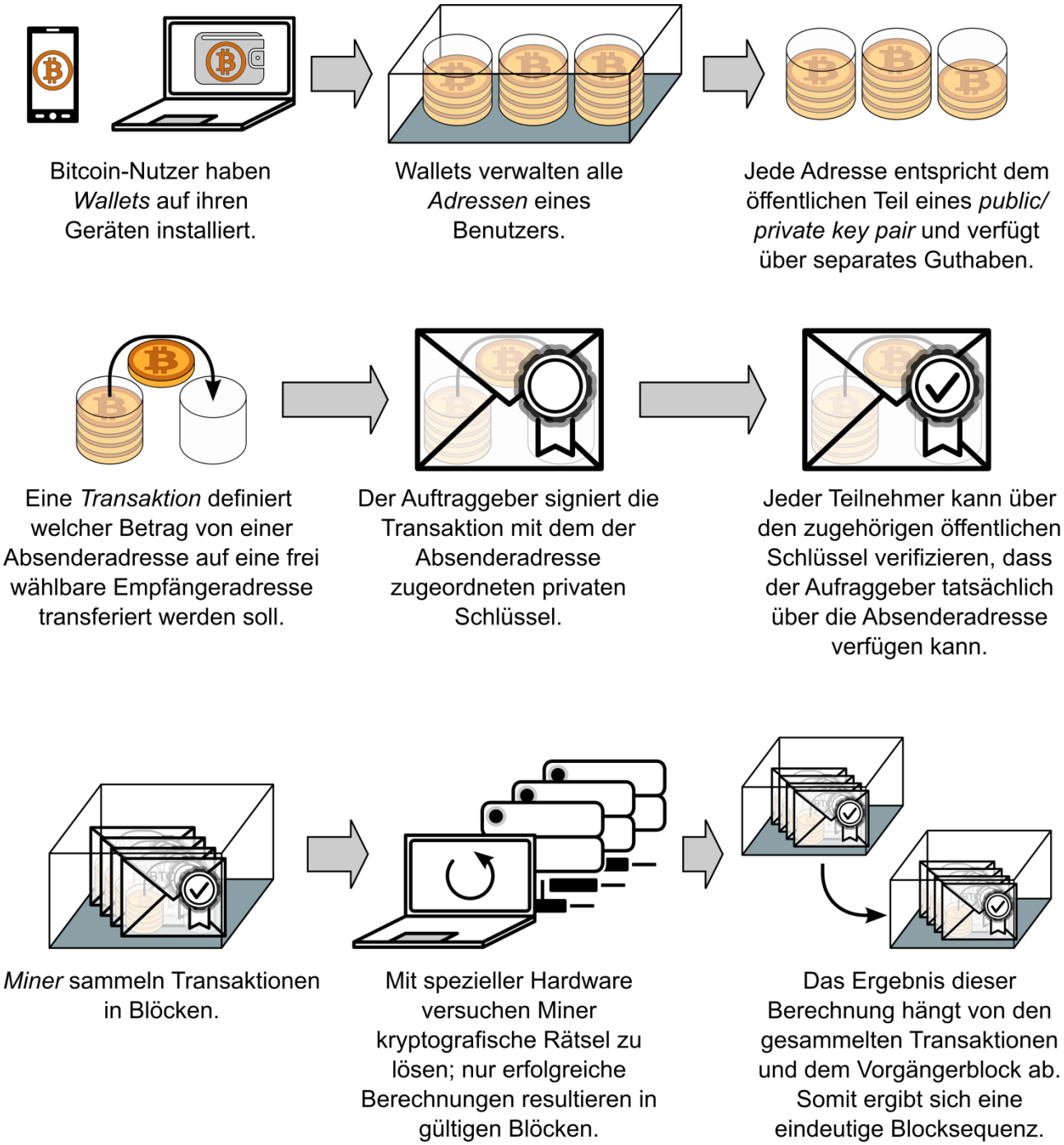

Abbildung 1: Illustration grundlegender Konzepte

2.1.1. Konzepte

Im Rahmen dieses Abschnitts werden grundlegende Konzepte von Kryptowährungen wie Bitcoin sowie die zugehörige Terminologie definiert. Nach Möglichkeit werden konkrete Beispiele angeführt.

Besonderes Augenmerk wird jedoch auf die Zusammenhänge der Begrifflichkeiten untereinander gelegt, um ein möglichst vollständiges Bild des Bitcoin-Systems darzulegen. Aus diesem Grund folgt die Definition auch nicht alphabetisch, sondern in der Reihenfolge, welche die Zusammenhänge am besten zum Ausdruck bringt.

2.1.2. Adresse

Die *Adresse* kann am ehesten als Äquivalent zur Kontonummer bzw. IBAN in traditionellen Zahlungssystemen angesehen werden, da Guthaben auch im Rahmen von Kryptowährungen an Adressen gebunden ist. Eine weitere Parallele ergibt sich, da auch Bitcoin-Transaktionen Guthaben zwischen Adressen transferieren. Allerdings gibt es gravierende Unterschiede gegenüber traditionellen Zahlungssystemen. Aus der dezentralen Struktur von Bitcoin ergibt sich der Umstand, dass jeder Teilnehmer seine Adressen selbst erstellt und diese auch keine Personenbindung besitzen, daher gibt es auch kein Verzeichnis gültiger Adressen. Der Adressraum ist mit 2^{160} so groß, dass doppelte Adressen de-facto ausgeschlossen sind. Dieser Fall wird im Protokoll schlichtweg nicht behandelt, da er irrelevant ist; durch den großen Adressraum wird die „unkontrollierte" Selbstverwaltung von Adressen ohne zusätzlichen Aufwand erst ermöglicht.[2] Das bloße Erstellen von Adressen führt auch nicht dazu, dass diese anderen Teilnehmern bekannt sind. Die Adresse des Begünstigten muss durch die Applikation des Bezahlenden jeweils erfragt werden. Dieser Adressaustausch ist nicht Teil der Bitcoin-Protokolle, sondern erfolgt auf Applikationsebene. Üblich sind anklickbare Links und QR-Codes, welche die Empfängeradresse enthalten. Erst wenn eine Adresse als Empfänger im Rahmen einer Transaktion referenziert wird, gibt es öffentliche Aufzeichnungen über deren Existenz (aber eben nicht über die Person des Begünstigen).

Der größte Unterschied zu Kontonummer und IBAN ist jedoch die Tatsache, dass es sich bei Adressen um Einwegtoken handelt. Bitcoin ist darauf ausgelegt, dass jede Adresse nur für eine einzige Transaktion verwendet wird. Somit besteht im Gegensatz zu einem Bankkonto keine Langzeitbindung zwischen Adresse und „Kontoinhaber". Auch deshalb sind Adressen ihren Besitzern nicht offensichtlich zuordenbar, wenn diese sie nicht freiwillig bekannt geben. Tatsächlich gibt es im Rahmen von Bitcoin kein Äquivalent zum klassischen Bankkonto.

Aus technischer Sicht handelt es sich bei einer Adresse um den öffentlichen Teil eines kryptografischen Schlüsselpaars (eines *public/private key pair*, siehe Anhang A: Relevante kryptografische Konzepte).

2.1.3. Transaktionen, UTXO

Bitcoin-Transaktionen unterscheiden sich grundlegend von Transaktionen im Rahmen traditioneller Zahlungssysteme. Transaktionen werden vollständig dezentral durchgeführt: Die einzigen in einer Zahlung direkt involvierten Parteien sind Auftraggeber und Empfänger. Statt auf vertrauenswürdige Dritte zu setzen, beruht die Sicherheit und Integrität des Systems auf kryptografischen Beweisen. Dritte sind nur dahingehend involviert, dass Transaktionen in der Blockchain protokolliert werden. Die Integrität einer Zahlung ist somit formal garantiert. Daher ist ein Wissen um die grundlegenden Konzepte asymmetrischer Kryptografie eine Voraussetzung, um die Funktionsweise von Bitcoin-Transaktionen nachvollziehen zu können. Entsprechende Informationen sind Anhang A: Relevante kryptografische Konzepte zu entnehmen.

Bei Inputs und Outputs handelt es sich um „unverbrauchte" bzw. noch nicht ausgegebene Währungseinheiten – Werte – welche entsprechend als *Unspent Transaction Outputs* (UTXO) (umgangssprachlich auch als „Bitcoins", bzw. schlichtweg Guthaben) bezeichnet werden. Kryptowährungseinheiten können genau wie traditionelle Zahlungsmittel nicht verbraucht werden, sondern lediglich den Besitzer wechseln. Besitzt jemand UTXO, bedeutet das schlicht, dass diese

[2] Adressen werden zufällig generiert. Kommt ein unzureichender Zufallsgenerator zum Einsatz, kann es zu Adresskollisionen kommen. Es gibt keine Möglichkeit zwischen „Original" und „Duplikat" einer Adresse zu unterscheiden, da es eine Adresse nur einmal geben kann. Wird eine bereits existierende Adresse erneut generiert, besitzen zwei Teilnehmer den zu dieser Adresse passenden privaten Schlüssel und können somit über das an diese Adresse gebundene Guthaben verfügen.

Partei über einen bestimmten Betrag frei verfügen kann. Unverbrauchtes Guthaben wird ausgegeben, indem es als Input in eine Transaktion aufgenommen wird und als Output an einen Empfänger „ausbezahlt“ wird. Auftraggeber und Empfänger werden nicht als Personen deklariert, lediglich deren Adressen. Transaktionen sind strukturell angelehnt an doppelte Buchführung (siehe Tabelle 1).

Input	**Adresse**	**Wert**		Output	Adresse	**Wert**
Input 1	A	0,15		Output 1	X	0,90
Input 2	B	0,20		Output 2	Y	0,25
Input 3	C	0,35				
Input 4	D	0,50				
Summe Inputs		1,20		Summe Outputs		1,15

	Inputs	1,20	
–	Outputs	1,15	
		0,05	(implizite Transaktionsgebühr)

Tabelle 1: Schematische Darstellung einer Transaktion

UTXO sind nicht aufteilbar, genauso wenig wie ein Teil einer Banknote einen Teil des Werts einer unversehrten Banknote repräsentiert. Stattdessen wird bei Bitcoin-Zahlungen genau wie im Rahmen traditioneller Zahlungssysteme „Wechselgeld gegeben“, indem ein entsprechender Wert in Form neuer UTXO als Output einer Transaktion angegeben wird, welche eine Adresse des Auftraggebers als Empfänger referenziert. Der Output einer Transaktion kann als Input in einer anderen Transaktion verwendet werden. Genau wie Banknoten durch Seriennummern gekennzeichnet sind, besitzen auch UTXO eine Art Seriennummer und sind somit eindeutig identifizierbar. Dadurch ist auch die gesamte Historie einer jeden Währungseinheit im zentralen Transaktionsregister protokolliert. Die Differenz aus der Summe der Outputs und der Summe der Inputs einer Transaktion ergibt die (implizite) Gebühr, welche für diese Transaktion anfällt. Deren Höhe wird vom Auftraggeber festgelegt. Abschnitt 2.1.6 behandelt Transaktionsgebühren im Detail.

Alle Transaktionen, sowie die Gesamtmenge aller Währungseinheiten (alle jemals existierenden UTXO) sind im System in der Blockchain als zentralem Transaktionsregister festgehalten. Daher sind auch alle Transaktionsdaten öffentlich bekannt. Gutgeschrieben werden kann der im Output einer Transaktion deklarierte UTXO jedoch nur der Adresse, welche in den definierten Freigabebedingungen der Transaktion referenziert ist.

Da es sich bei Bitcoin-Adressen um den öffentlichen Teil eines kryptografischen Schlüsselpaares handelt, lauten die Freigabebedingungen im Allgemeinen sinngemäß „der Besitz des privaten Schlüssels des Begünstigten“. In diesem Fall kann nur der Ersteller einer Adresse über die im Output einer Transaktion deklarierten UTXO verfügen und diese allenfalls in Form einer neuen Transaktion ausgeben. Hierfür wird eine neue Transaktion erstellt und mit dem der Adresse zugehörigen privaten Schlüssel signiert, wodurch bewiesen ist, dass man den dazugehörigen privaten Schlüssel besitzt.

2.1.4. Blockchain, Blöcke und Mining

Die Blockchain ist das zentrale Transaktionsregister von Kryptowährungen wie Bitcoin. Wie der Name vermuten lässt, besteht diese aus einzelnen Blöcken. Blöcke sind kryptografisch miteinander verkettet, woraus sich eine eindeutige Reihenfolge ergibt. Transaktionen werden in Blöcken zusammengefasst und dadurch validiert. Neue Blöcke können nur erstellt werden, indem ein kryptografisches Problem gelöst wird, dessen Lösung schwierig zu finden, aber einfach zu verifizieren ist. So ist es zum Beispiel auch schwierig ein Sudoku-Rätsel korrekt zu lösen, die Korrektheit einer Lösung ist jedoch von jedermann sehr einfach durch simple Additionen verifizierbar. Dasselbe Prinzip kommt auch beim Erstellen von Blöcken zum Einsatz. Durch die Schwierigkeit des zu lösenden Problems und der von jedem Teilnehmer unabhängig durchführbaren Verifikation der Lösung (und somit des Blocks) ist die Blockchain vor Manipulationen geschützt und deren Integrität garantiert. Auf Grund des Umstands, dass jeder Block (ebenso wie jede Transaktion) von allen Teilnehmern unabhängig voneinander überprüft wird, können sich ungültige oder gezielt

gefälschte Blöcke nicht im Netzwerk verbreiten, da diese verworfen werden. Offensichtlich handelt es sich hierbei um freiwilliges Verhalten aller Teilnehmer. Der Grund hierfür ist schlichtweg, dass man jederzeit selbst Opfer eines Betrugs werden kann, wenn man UTXO empfängt, welche nicht korrekt verarbeitet wurden. Genau wie bei Falschgeld, besteht die Gefahr, dass diese Outputs nicht angenommen werden. Die Chance hierfür ist jedoch um ein Vielfaches höher. Im Gegensatz zu Banknoten werden UTXO nicht auf optische und haptische Merkmale überprüft, sondern automatisiert nachprüfbare kryptografische und mathematische Beweise bestätigen bzw. widerlegen deren Authentizität.

Als Anreiz neue Blöcke zu erstellen dient das mit einem Erfolg einhergehende frische Kapital in Form neu erstellter UTXO. Dazu erstellt der Erzeuger des Blocks (im Kontext von Kryptowährungen als *Miner* bezeichnet) eine sogenannte *Coinbase* Transaktion. Die *Coinbase*-Transaktion ist immer die erste Transaktion die in einen neuen Block aufgenommen wird. Setzt sich der Block durch, bekommt der Ersteller die Belohnung ausgeschüttet. Ob und wann sich ein Block etabliert hängt von mehreren Faktoren ab. Im einfachsten Fall setzt sich der Block durch, welcher zuerst erzeugt wurde. Wenn es jedoch konkurrierende Blöcke gibt, welche auf demselben Vorgängerblock aufbauen, wird der Block mit dem höheren Proof-of-Work anerkannt (Für Details wird auf Kapitel 3 in [1] verwiesen). Im ersten Moment kann diese Tatsache den Eindruck vermitteln, dass jeder nach Belieben „Geld drucken“ kann. Tatsächlich ist dies aber streng reglementiert, da die Menge an ausgeschüttetem Kapital im System (d.h. in der Software aller Teilnehmer) definiert ist. Auch an dieser Stelle werden wieder kryptografische Verfahren – Hashfunktionen auf Basis von SHA-256 [3] – eingesetzt, mit deren Hilfe jeder Teilnehmer die Validität eines neuen Blocks überprüfen kann. Somit wird sichergestellt, dass der Ersteller eines Blocks auch tatsächlich das vorgegebene kryptografische Rätsel gelöst hat und somit nicht beliebig „Geld nachdrucken“ kann.

Zusätzlich zum frischen Kapital erhält ein Miner auch die Transaktionsgebühren aller in einen Block aufgenommenen Transaktionen. Über beides kann der Ersteller eines Blocks frei verfügen. Das Erstellen gültiger Blöcke wird (angelehnt an das Schürfen von Gold) als *Mining* bezeichnet. Die Schwierigkeit des zu lösenden kryptografischen Problems wird laufend an die Rechenleistung des Bitcoin-Netzwerkes angepasst. Bei zunehmender Popularität steigt somit die Gesamtrechenleistung und damit einhergehend auch der Energieverbrauch. Ziel ist es, dass alle 10 Minuten ein neuer Block erstellt wird. Da jeder Block vom vorherigen Block und den enthaltenen Transaktionen abhängt, ist eine Vorberechnung unmöglich. Im folgenden Abschnitt wird der Energieverbrauch betrachtet.

2.1.5. Energieverbrauch

Der Energieverbrauch des Bitcoin-Netzwerkes lässt sich nur sehr ungenau abschätzen, da die verwendete Hardware der Miner unbekannt ist. Dementsprechend gehen die Abschätzungen weit auseinander. So schätze Bergmann 2014 den Stromverbrauch auf 125-200 Megawatt [2], während Allied Controll auf 250-500 Megawatt kommt [3] und O’Dwyer und Malone auf 0,1-10 Gigawatt [4]. Die Schätzung von O’Dwyer und Malone würde in etwa dem Energieverbrauch von Irland (3GW) entsprechen. Im Jahr 2015 schätzte Malmo den Stromverbrauch auf 215 Megawatt [5]. Das Goverment Office of Science ging 2016 von einem Stromverbrauch von einem Gigawatt aus. Es gibt auch Prognosen für den zukünftigen Stromverbrauch, so schätzt beispielsweise Deetman, dass Bitcoin im Jahr 2020 zwischen 417 Megawatt und 14,6 Gigawatt an Energie benötigen wird [6]. Dies würde in etwa dem Energieverbrauch von Dänemark (14 GW[3]) entsprechen.
Die große Schwankungsbreite ergibt sich durch die unterschiedliche Effizienz der eingesetzten Hardware. Beispielsweise schafft eine herkömmliche CPU[4] weit unter einer Million Hashoperationen pro Joule, während eine Anwendungsspezifische integrierte Schaltung (ASIC)[5] über 1700 Millionen Hashoperationen pro Joule durchführen kann [4].
Da sich der Stromverbrauch des Bitcoin-Netzwerkes nur sehr ungenau abschätzen lässt, ist auch ein Vergleich mit bestehenden Zahlungssystemen sehr schwer. Je nachdem welche Annahmen man trifft, kann man sowohl zeigen, dass Bitcoin um 99,8% weniger Emissionen hat als das

[3] http://www.tsp-data-portal.org/Breakdown-of-Electricity-Capacity-by-Energy-Source#tspQvChart abgerufen am 20.10.2016
[4] Core i7 950 (0.126 Mhash/J)
[5] Monarch BPU 600 C (1714 Mhash/J)

Bankensystem [7], als auch das Bitcoin pro Transaktion etwa 5033 mal so viel Energie benötigt wie eine VISA-Transaktion [5]. Beide Aussagen sollten mit Vorsicht betrachtet werden.

2.1.6. Transaktionsgebühren

Da Transaktionen ohne den Einbezug Dritter erstellt werden, fallen zumindest theoretisch keine Transaktionsgebühren an. Im Rahmen des Miningprozesses können allerdings nicht beliebig viele Transaktionen in einen neuen Block aufgenommen werden, da die Blockgröße auf ein Megabyte begrenzt ist. Folglich werden jene Transaktionen priorisiert, welche die höchsten Transaktionsgebühren abwerfen. Deren Höhe ergibt sich schlicht aus der Differenz zwischen der Summe der Inputs und der Summe der Outputs einer Transaktion. Wenn eine Transaktion beispielsweise UTXO im Wert von 10 Währungseinheiten als Inputs und UTXO im Wert von 9 Währungseinheiten als Outputs enthält, ergibt sich *Collateral* (angelehnt an den finanziellen Terminus Sicherheit bzw. *Collateral*) im Wert einer Währungseinheit. Collateral wird an den Miner, der eine Transaktion in einen Block aufnimmt, ausbezahlt, bzw. an eine seiner Adressen gebunden. Miner werden daher Transaktion mit höheren Transaktionsgebühren bevorzugt in ihre Blöcke aufnehmen. Somit kann der Ersteller einer Transaktion über die Höhe der Transaktionsgebühren die Priorisierung von Transaktionen beeinflussen. Tatsächlich spielt dieser Aspekt jedoch eine verschwindend geringe Rolle und muss vom Durchschnittsnutzer nicht weiter beachtet werden, da die Wallet-Applikation sinnvolle Standardwerte verwendet.

2.1.7. Das Bitcoin-Netzwerk

Kryptowährungen wie Bitcoin sind dezentral organisiert. Der komplette Datenbestand an Transaktionen wird zwar in der Blockchain gesichert, welche als zentrales Transaktionsregister fungiert, jedoch wird die Blockchain selbst nicht an einem zentralen Ort gespeichert oder zentral verwaltet, sondern eben durch den Prozess des Minings stetig fortgeführt. Bitcoin spezifiziert ein Protokoll, welches alle Teilnehmer des Bitcoin-Netzwerks nutzen, um untereinander ständig Informationen auszutauschen und dadurch ein stets aktuelles Abbild der Blockchain zu verbreiten.
Wenn eine Transaktion durchgeführt wird, so wird diese vom Auftraggeber an jene Teilnehmer übermittelt, die ihm momentan bekannt sind. Diese leiten die eben erhaltenen Informationen wiederum an die ihnen bekannten Teilnehmer weiter. Somit propagieren alle, egal an welchem Punkt im Netzwerk erstellten (Transaktions-)Informationen durch das Netzwerk und erreichen nach wenigen Sekunden alle Teilnehmer. Dies entspricht dem Flooding-Ansatz, welcher auch von klassischen Routing-Protokollen verwendet wird. Da es sich dabei um kontrolliertes Flooding handelt, skaliert dieser Ansatz [8]. Die Integrität aller ausgetauschten Informationen, somit auch die Integrität neu erstellter Blöcke wird von jedem Teilnehmer des Netzwerks unabhängig verifiziert. Grundlage hierfür sind ebenfalls Verfahren aus dem Bereich der asymmetrischen Kryptografie. Wird eine Transaktion empfangen, welche bereits ausgegebene Währungseinheiten oder sonstige Unregelmäßigkeiten aufweist, wird diese nicht weitergereicht. Da Miner nur von gültigen Transaktionen in Form von Transaktionsgebühren profitieren, werden ungültige Transaktionen auch nie in neue Blöcke aufgenommen werden.

Im nachfolgenden Abschnitt wird der Ablauf einer Bezahlung von der Erzeugung einer Transaktion bis zu deren Einbettung in die Blockchain beschrieben. Die Grundkonzepte dieses Vorgangs sind auch auf andere Kryptowährungen anwendbar.

2.2. Bitcoin Eigenschaften

Aus der zuvor beschriebenen Funktionsweise von Bitcoin ergeben sich einige Eigenschaften, welche als verbesserungswürdig eingestuft werden können. Moderne Kryptowährungen versuchen ebendies zu erreichen. Dieser Bericht konzentriert sich auf Kryptowährungen die entweder die Performance (IOTA, Nano) oder die Privatsphäre (Dash, Monero, PIVX, Zcash) zu verbessern versuchen:

Bitcoin	
Release Datum	Jänner 2009
Symbol	BTC
Maximale Coin-Menge	Limitiert (21 Mio. BTC)
Marktkaptial	$165,432,367,600 USD[6]
Konsensus-Algorithmus	Proof of work (SHA-256)
Blockerstellungszeit	10 Minuten
Minebar	Ja (ASICs)
Sender Anonymität	Nein
Empfänger Anonymität	Nein
Betragsverschleierung	Nein
Verfolgbar	Ja
Skalierbarkeit	Beschränkt (1MB Blockgröße)

- **Performance**: Da die Blockgröße bei Bitcoin auf 1 Megabyte limitiert ist, kann nur eine bestimmte Anzahl von Transaktionen in einen Block aufgenommen werden. Dadurch kommt es immer wieder zu Verzögerungen. Durch den Proof-of-Work-Algorithmus, bei dem alle Miner Rechnenaufwand betreiben, aber jedes Mal nur einer als „Gewinner" hervorgeht, ergibt sich ein hoher Energieverbrauch pro Block bzw. pro Transaktion. IOTA und Nano versuchen dieses Problem zu lösen, indem die Blockchain durch einen verzweigten Graphen ersetzt wird. Andere Währungen hingegen propagieren eine dynamisch vorgegebene maximale Blockgröße als Lösungsansatz oder definieren eine größere maximale Blockgröße als festes Limit.
- **Privatsphäre**: Die öffentliche Blockchain von Bitcoin bietet eine hohe Transparenz und Nachverfolgbarkeit. Je nach Anwendungsfall kann dies aber ungewünscht sein. So kann die gesamte Weltöffentlichkeit nachverfolgen wer (welche Adresse) wem (an welche Adresse) wann wieviel überweist und auch die Guthaben aller Adressen abfragen. Zwar bieten Adressen eine gewisse Anonymität, allerdings nur bis sie benutzt wurden. Bitcoin bietet keine Möglichkeit den Sender, den Empfänger, den Betrag oder das Guthaben einer Adresse zu verstecken. Währungen wie Dash, Monero oder PIVX nehmen sich dieses Problems an.

3. Dash

Die Kryptowährung *Dash* [17] (ursprünglich XCoin, bzw. *Darkcoin* [18] genannt) verfolgt das Ziel, möglichst ohne den Einsatz zusätzlicher Systeme, Infrastrukturen, Dienstanbieter, oder Mittelsmänner im alltäglichen Zahlungsverkehr nutzbar zu sein.
Im offiziellen Whitepaper [19] werden Skalierbarkeit und (in Analogie an Bargeld) Anonymität als Voraussetzungen für Alltagstauglichkeit genannt. Dash wird dabei explizit als Weiterentwicklung von Bitcoin klassifiziert. Unter anderem wird ein breiter aufgestellter Proof-of-Work-Algorithmus auf Basis elf unterschiedlicher Hash-Funktionen eingesetzt. Dieser wurde in der Hoffnung entwickelt,

DASH	
Release Datum	18. Janner 2014
Symbol	DASH
Maximale Coin-Menge	18,900,000 DASH
Marktkaptial	$3,957,649,596 USD[7]
Konsensus-Algorithmus	Proof of Work (X11)
Blockerstellungszeit	2,5 Minuten
Minebar	Ja
Sender Anonymität	Ja (Optional)
Empfänger Anonymität	Nein
Betragsverschleierung	Nein
Verfolgbar	Nein
Skalierbarkeit	Beschränkt (2MB Blockgröße)

[6] Abgerufen von https://coinmarketcap.com/ am 04.05.2018
[7] Abgerufen von https://coinmarketcap.com/ am 04.05.2018

kommerzielles Mining mittels ASICs möglichst lange hinauszögern zu können. Inzwischen sind jedoch ASIC-Miner verfügbar. Strukturell unterscheidet sich Dash von Bitcoin dahingehend, dass das der Währung zu Grunde liegende Peer-to-Peer-Netzwerk aus zwei unterschiedlichen Klassen von Nodes besteht. Zum einen gibt es weiterhin reguläre Miner, bzw. Clients. Zusätzlich kommen jedoch auch so genannte *Master Nodes* zum Einsatz, welche zusätzliche Funktionalität zur Verfügung stellen und so zu einem Mehrwert und hoher Alltagstauglichkeit führen sollen.[8] Deren Funktionalität wird im nachfolgenden Abschnitt näher beschrieben.

3.1. Masternodes

Bei Master Nodes handelt es sich um Netzwerkteilnehmer, die nicht Teil des Mining-Prozesses sind, stattdessen jedoch für die Bereitstellung von anderen Diensten einen Anteil des Block-Rewards erhalten. Um Missbrauch, im Speziellen *Sybil-Attacken* [20] zu verhindern, müssen tausend Währungseinheiten[9] als *Collateral* hinterlegt werden. Fehlverhalten führt zum Verlust dieses Einsatzes. Durch den vergleichsweise hohen notwendigen Einsatz wird versucht zu verhindern, dass eine einzige Partei verhältnismäßig viele Master Nodes betreibt und so ungewollt hohen Einfluss auf die vom Netzwerk der Master Nodes bereitgestellten Zusatzfunktionen erlangt. Welcher Masternode, bzw. welche Menge an Master Nodes konkret für eine Aufgabe ausgewählt wird, hängt vom Hash des letztgültigen Blocks – und damit vom Zufall – ab. Ob sich ein Masternode korrekt verhält, bzw. ob dieser überhaupt einen Beitrag leistet, wird von anderen Masternodes überprüft.
Aktuell stellen Masternodes folgende für Endbenutzer relevante Dienste zur Verfügung: *PrivateSend* (anonymisierte Transaktionen) und *InstantSend* (die sofortige Bestätigung einer Transaktion, ohne, dass auf Blöcke gewartet werden muss). Nachfolgend werden diese Dienste im Detail erläutert.

3.2. Anonymisierte Transaktionen

Dash unterstützt anonymisierte Transaktionen im Rahmen des *PrivateSend*-Verfahrens, welches auf dem *CoinJoin*[10]-Konzept basiert. Währungseinheiten sind innerhalb Bitcoin- und Bitcoin-artiger Kryptowährungen über alle Transkationen hinweg nachverfolgbar (siehe Abschnitt 2.1.3). Der Währungsfluss lässt sich jedoch durch die Anwendung von *Mixen* [19] verschleiern. Im einfachsten (im Rahmen von CoinJoin) beschriebenen Fall werden Transaktionen mehrerer Teilnehmer, bzw. die Intention, Transaktionen durchführen zu wollen, von einer vertrauenswürdigen Instanz akkumuliert und in einer einzigen, umfangreicheren Transaktion zusammengefasst und schlussendlich abgewickelt. Damit ist von außen nicht nachvollziehbar, wer wem wie viel übermittelt hat. Was bleibt ist, die Information darüber, wer an der Transaktion beteiligt war, jedoch nicht der konkrete Währungsfluss. Dieser Privatsphäre-Zugewinn basiert auf dem Prinzip, dass einzelne beteiligte Akteure in der Masse aller beteiligten Instanzen sozusagen untertauchen, und die konkreten Aktionen einer einzelnen Partei nicht mehr nachvollziehbar sind. Anstatt wie bisher eindeutig nachverfolgen zu können wer an wen wie viel übermittelt, wenn zwei Parteien eine Transaktion ausführen, lässt sich lediglich folgendes beobachten: Mehrere Parteien zahlen Währungseinheiten in einen Topf ein. Anschließend erhält (typischerweise eine Übermenge) von Parteien (unterschiedliche) Anteile des Währungstopfs. Ausgehend von diesen Informationen kann keine Korrelation zwischen den Parteien hergestellt werden, abgesehen von der (nicht besonders aussagekräftigen) Beobachtung, dass diese an einer CoinJoin-Transaktion beteiligt waren. Dieser Prozess kann auch mehrfach verkettet ausgeführt werden, sodass eine ganze Reihe von Währungstöpfen nacheinander durchlaufen wird. Sind diese Töpfe auf mehrere Instanzen aufgeteilt, kann verhindert werden, dass Instanzen aussagekräftige Protokolle anfertigen können und den Zahlungsverkehr dadurch deanonymisieren.

Eine Schwachstelle dieses Konzepts stellt die Beteiligung einer notwendigerweise vertrauenswürdigen Instanz dar. Der zuvor genannte Topf ist ebenfalls eine gültige Kryptowährungs-Adresse, deren privater Schlüssel im Besitz der vertrauenswürdigen zentralen Instanz ist. Rein

[8] Masternodes können ebenfalls am Mining-Prozess teilnehmen, sind dazu jedoch nicht verpflichtet.
[9] Stand 09.04.2018 entsprechen 1000 Dash in etwa 260.000 Euro
[10] https://bitcointalk.org/index.php?topic=279249

technisch kann nicht verhindert werden, dass der Auszahlungsschritt nicht ausgeführt wird und sich die zentrale Instanz bereichert, indem die eingezahlten Beiträge schlicht einbehalten werden.
PrivateSend schafft hier insofern Abhilfe, als dass nicht eine zentrale Stelle für die Verschleierung eingesetzt wird, sondern immer mehrere unterschiedliche, zufällig ausgewählte Master Nodes. Um Master Nodes keinen Anreiz für Betrug zu bieten, ist die Größe des Topfs im Protokoll auf die Höhe des Einsatzes limitiert, der hinterlegt werden muss, um einen Master Node zu betreiben. Des Weiteren können nur Transaktionen über fixe Beträge (ähnlich wie Banknoten unterschiedlichen Werts) über dieses System verschleiert werden, um das Risiko der Nachvollziehbarkeit über die Höhe der Transaktionsbeträge zu minimieren.

Durch die Verschleierung von Geldflüssen wird eine Eigenschaft von Bargeld nachgebildet. Der Einsatz von PrivateSend ist jedoch optional. Für den Fall, dass sich ein Händler (beispielsweise aus rechtlichen Gründen) Nachvollziehbarkeit aller Zahlungseingänge wünscht, kann dieser schlicht darauf verzichten, derart anonymisierte Währungseinheiten zu akzeptieren. Eine weitere Eigenschaft, welche die allgemeine Akzeptanz von Dash im Alltag fördern soll, ist die – ebenfalls an Barzahlungen angelehnte – sofortige Zahlungsabwicklung. Erreicht wird dies mittels des nachfolgend beschriebenen *InstantSend*-Prozesses.

3.3. Sofortige Transaktionsabwicklung

Im Rahmen traditioneller Kryptowährungen, wie z.B. Bitcoin oder Ethereum werden Transaktionen (je nach Höhe) erst ab einer bestimmten Blocktiefe akzeptiert. Beispielsweise könnte ein Händler für eine Transaktion im Gegenwert von einigen tausend Euro eine Blocktiefe von sechs Blöcken voraussetzen, bevor die Ware ausgehändigt wird. Im Rahmen von Bitcoin würde daraus eine Wartezeit von einer Stunde resultieren. Tatsächlich werden Beträge in dieser Höhe jedoch oftmals für Güter (wie z.B. Schmuck, Designerkleidung, Unterhaltungselektronik, …) bezahlt, die man sofort erhalten möchte.
Das vom Dash-Masternode-Netzwerk bereitgestellte *InstantSend*-Verfahren schafft hier Abhilfe. Ein Quorum bestehend aus mehreren Master Nodes kann eine Transaktion auf Wunsch „einfrieren“. Dieser Vorgang kann innerhalb von vier Sekunden durchgeführt werden. Da das gesamte Dash-Netzwerk auf die von den Master Nodes zur Verfügung gestellten Informationen zugreifen kann, wissen alle Miner und alle Clients über diese eingefrorenen Transaktionen Bescheid. Die beteiligten Master Nodes bürgen mit ihrem Einsatz dafür, dass sie die Währungseinheiten des Transaktionseingangs und deren Zuordnung zu der vom Auftraggeber angegebenen Wallet-Adresse überprüft haben. Gleichzeitig wird damit auch dafür gebürgt, dass eine Transaktion in einen zukünftigen Block aufgenommen wird, und die in diese eingefrorene Transaktion eingehenden Währungseinheiten bis dahin nicht anderweitig ausgegeben werden können. Miner müssen vor der Aufnahme einer Transaktion in einen Block folglich prüfen, ob die betreffenden Inputs nicht in einer anderen Transaktion eingefroren sind.
Dadurch, dass dieses Verfahren vom dezentral organisierten Masternode-Netzwerk bereitgestellt wird, muss ähnlich wie im Rahmen anonymisierter Transaktionen keiner Instanz vertraut werden.

4. IOTA

IOTA	
Release Datum	21. June 2014
Symbol	IOTA
Maximale Coin-Menge	2,779,530,283 IOTA
Marktkaptial	$6,577,313,690 USD[11]
Konsensus-Algorithmus	Tip Selection Algorithm
Blockerstellungszeit	-
Minebar	Ja
Sender Anonymität	Nein
Empfänger Anonymität	Nein
Betragsverschleierung	Nein
Verfolgbar	Ja
Skalierbarkeit	Sehr gut

IOTA wurde als Kryptowährung für die Internet-of-Things (IoT) Industrie entwickelt. IOTA verwendet keine Blockchain, sondern einen sogenannten *Tangle*, einen verteilten, gerichteten, azyklischen Graph (DAG), als Transaktionsspeicher. Der Tangle wird als nächster Evolutionsschritt zur Blockchain beworben und soll Eigenschaften besitzen, welche Maschinen-zu-Maschinen-Mikrotransaktionen ermöglichen. Jeder Knoten in diesem Graph stellt eine Transaktion dar, und jede Kante A→B bedeutet, dass A die Transaktion von B direkt bestätigt. Ein gerichteter Pfad von A→B mit einer Mindestlänge von 2 bedeutet, dass A die Transaktion von B indirekt bestätigt. Dies hat zur Folge, dass der Genesis-Block (der erste Block) direkt oder indirekt von allen Transaktionen bestätigt wird. Um eine neue Transaktion hinzufügen zu können, muss im Gegensatz zu Bitcoin kein Block erschaffen werden und auch kein aufwendiges Rätsel gelöst werden, es reicht aus, zwei vorhergegangene Transaktionen zu bestätigen.

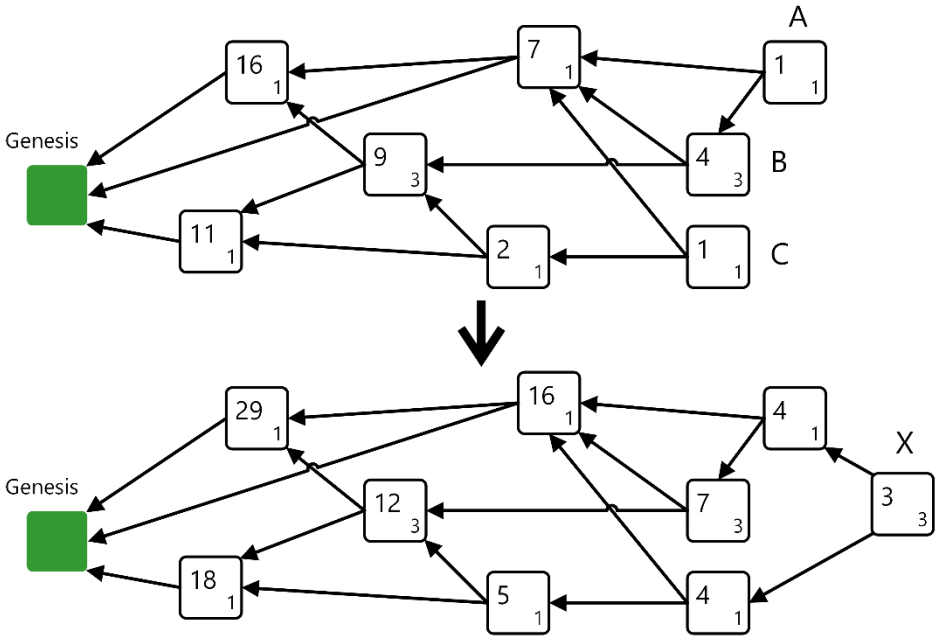

Abbildung 2: DAG mit zugewiesenen Gewichten bevor und nachdem eine neue Transaktion X eingefügt wurde. Die Boxen repräsentieren Transitionen, die Nummer rechts unten das Gewicht der Transaktion und die Nummer links oben repräsentiert das Gesamtgewicht der Transaktion.

Abbildung 2 visualisiert das Einfügen einer neuen Transaktion *X*, welche die beiden Tips A und C bestätigt. Als Tips werden noch nicht bestätigte Transaktionen bezeichnet. Jede Transaktion hat ein Gewicht der Form 3^n, wobei es sich bei n um eine positive Zahl aus einer definierten endlichen Menge handelt. Das Gesamtgewicht einer Transaktion ergibt sich aus der Summe aller gewichteten Transaktionen, die die Zieltransaktion direkt oder indirekt bestätigen. Das Eigengewicht wird durch eine Art Mini-Proof-of-Work generiert. Je höher der Proof-of-Work bzw. das Gewicht ist, desto wichtiger ist die Transaktion. Dieser Ansatz dient als Schutz vor Spam-Transaktionen, die sonst ohne Kosten möglich wären, da bei IOTA keine Transaktionsgebühren anfallen. Im Beispiel hat die Transaktion *X* ein Gewicht von 3. Da die Transaktion noch von keiner anderen Transaktion bestätigt

[11] Abgerufen von https://coinmarketcap.com/ am 04.05.2018

wurde hat sie auch ein Gesamtgewicht von 3. Durch das Einfügen von *X* erhöhen sich allerdings die Gesamtgewichte aller direkt oder indirekt bestätigten Transaktionen. Jede neue Transaktion bestätigt nur gültige Transaktionen. Jede zusätzliche Bestätigung einer Transaktion (direkt oder indirekt) erhöht das Maß an Sicherheit. Dieser Ansatz soll Double Spending verhindern: Es können niemals mehrere widersprüchliche Transaktionen gültig sein. Stehen zwei oder mehr Transaktionen im Konflikt miteinander, müssen sich die Nodes im Netzwerk für eine Transaktion entscheiden. Hierfür kommt ein *Tip-Selection-Algorithmus* zum Einsatz, welcher mehrmals ausgeführt wird, um den „besseren“[12] Tip zu finden. Ein weiter Unterschied von IOTA zu den meisten anderen Kryptowährungen ist, dass es kein Mining gibt und daher auch keine neuen Währungseinheiten erschaffen werden. Stattdessen hält der Genesis Block am Anfang alle Token und teilt diese an die Gründer auf, welche die Token ihrerseits weiterverteilen.
Derzeit bietet IOTA kaum Privatsphäre: Transaktionen sowie Beträge und Guthaben lassen sich nachverfolgen. Es wird allerdings an Technologien geforscht, um die Privatsphäre zu erhöhen, beispielsweise durch die Verwendung von Token-Mixer, *Masked Authenticated Meesaging* [17] oder der Integration des *TumbleBit*-Modells [18]. Nachdem IOTA für die Internet-of-Things (IoT) Industrie entwickelt wurde, liegt der primäre Fokus auf Skalierbarkeit und günstige Benutzung.

5. Monero

Monero	
Release Datum	18. April 2014
Symbol	XMR
Maximale Coin-Menge	Unlimitiert (18,4 Mio. XMR + 0,3 XMR/Min.)
Marktkaptial	$3,901,501,725 USD[13]
Konsensus-Algorithmus	Proof of work (Cryptonight)
Blockerstellungszeit	120 Sekunden
Minebar	Ja (CPUs, GPUs)
Sender Anonymität	Ja (Ring Signaturen)
Empfänger Anonymität	Ja (Stealth Addresses)
Betragsverschleierung	Ja (Ring confidential transations)
Verfolgbar	Nein (außer für Empfänger/Sender)
Skalierbarkeit	Gut (dynamische Blockgröße)

Monero ist eine dezentrale auf Privatsphäre, Anonymität und Dezentralisierung optimierte Blockchain-basierte Kryptowährung. Monero basiert auf dem *CryptoNote*[14]-Protokoll, welches im Gegensatz zu Bitcoin den Sender und die Empfänger einer Transaktion sowie den übermittelten Betrag durch kryptografische Verfahren schützt. Ein weiter Unterschied zu Bitcoin ergibt sich beim Konsensus-Algorithmus. Während Bitcoin auf einem auf SHA-256 basierten Verfahren beruht, verwendet Monero den *CryptoNight*[15]-Konsensus-Algorithmus. Dieser Algorithmus wurde entwickelt, um Zentralisierung zu verhindern und lässt sich auf handelsüblichen CPUs effizient berechnen. CryptoNights Proof-of-Work-Algorithmus benötigt 2MB möglichst schnellen Speicher, wodurch die Entwicklung von spezieller Mininghardware erschwert werden soll. CryptoNight lasst sich auf CPUs und GPUs in etwa gleich effizient berechnen. Im Vergleich spezialisierte Bitcoin Mininghardware ist deutlich schneller und effizienter als CPUs und GPUs (Faktor >>10000). Kürzlich wurde der Proof-of-Work-Algorithmus im Rahmen eines Hard-Forks modifiziert, da erste ASIC-Miner angekündigt wurden. Weitere Unterschiede zu Bitcoin gibt es bei der Blockgröße und beim nachjustieren des Schwierigkeitsgrades. Bei Bitcoin ist die maximale Blockgröße fix definiert, wodurch es immer wieder zu Verzögerungen bei der Aufnahme von Transaktionen in Blöcke kommt. Monero verwendet keine fixe Blockgröße. Definiert aber Strafen für überdurchschnittlich große Blöcke. Des Weiteren wird der Schwierigkeitsgrad nach jedem Block angepasst und nicht wie bei Bitcoin alle 2016 Blöcke. Der größte Unterschied liegt aber im Bereich der Privatsphäre. Monero bietet Sender- und Empfängeranonymität und verschleiert außerdem die verschickten Beträge sowie die Guthaben der einzelnen Adressen. Die Senderanonymität wird über Ringsignaturen sichergestellt [19]. Bei Nachrichten, die mittels einer Ringsignatur signiert wurden, kann nur festgestellt werden, dass der

[12] Für Details zum Tip Selection Algorithmus wird auf Abschnitt 4.1 in The Tangle [17] verwiesen.
[13] Abgerufen von https://coinmarketcap.com/ am 04.05.2018
[14] https://cryptonote.org/
[15] https://cryptonote.org/inside.php#equal-proof-of-work

Signator ein Mitglied einer Gruppe ist, jedoch verhindern Ringsignaturen, dass festgestellt werden kann, welches Gruppenmitglied eine Nachricht signiert hat. Die Empfängeranonymität wird über sogenannte *Stealth Addresses* gewährleistet [20]. Stealth Addresses verschleiern den Empfänger von Währungseinheiten. Es könnten beispielsweise 5 Personen an dieselbe Person Token überweisen, ohne dass eine der Personen erkennen könnte, dass eine der anderen Personen ebenfalls Token an denselben Empfänger bzw. an dieselbe Empfängerin geschickt hat. Der Sender bzw. die Senderin generiert hierfür im Auftrag des Empfängers bzw. der Empfängerin zufällige Einmaladressen. Der Empfänger bzw. die Empfängerin muss nur eine Adresse veröffentlichen, trotzdem bekommt er oder sie alle Bezahlungen auf unterschiedlichen Adressen, die nicht verknüpft werden können. Dadurch können nur der Sender bzw. die Senderin und der Empfänger bzw. die Empfängerin feststellen, ob eine Zahlung geschickt wurde. Damit dieser Vorgang funktioniert, unterschieden sich die Monero-Adressen von Bitcoin-Adressen. Bei Monero gibt es zwei private Schlüssel, einen *View Key* und einen *Spend Key*, und einen öffentlichen Schlüssel. Der Spend Key wird benötigt, um Zahlungen zu schicken. Mit dem View Key können eingehende Zahlungen eingesehen werden. Der öffentlichen Schlüssel dient wie bei Bitcoin als Empfangsadresse. Mittels View Key kann auch ein so genanntes *watch only wallet* erstellt werden. Mit diesem Wallet können Zahlungen nur beobachtet, aber nicht ausgelöst werden. Des Weiteren benutzt Monero *RingCT* (kurz für *Ring Confidential Transactions* [21]), um Beträge in Transaktionen zu verstecken. Dieses Feature wurde Anfang 2017 integriert. Zusammengefasst bietet Monero verschiedene Funktionen, die die Privatsphäre von Sendern und Empfängern erhöhen. Falls erwünscht, können Transaktionen aber durch Herausgabe des View Key und der Empfängeradresse transparent gemacht werden.

6. Nano

Nano, zuvor *RaiBlock* genannt, wurde 2014 vorgestellt und verwendet wie auch IOTA einen gerichteten azyklischen Graph anstelle der Blockchain. Jeder Account hat im Rahmen von Nano eine eigene Blockchain, die das Guthaben festhält. Jede Blockchain kann nur vom jeweiligen Eigentümer bzw. der jeweiligen Eigentümerin aktualisiert werden; dies dafür sofort und asynchron vom restlichen Netzwerk. Abbildung 3 visualisiert diese Blockchains bzw. Konten. Am Anfang enthält nur der Genesis-Account (das zum ersten Block gehörende Konto) ein Guthaben. Dieses Guthaben entspricht wie auch bei IOTA der maximalen Geldmenge im System.

NANO	
Release Datum	2014
Symbol	NANO
Maximale Coin-Menge	133,248,289 NANO
Marktkaptial	$1,252,403,335 USD[16]
Konsensus-Algorithmus	Voting
Blockerstellungszeit	-
Minebar	Nein
Sender Anonymität	Nein
Empfänger Anonymität	Nein
Betragsverschleierung	Nein
Verfolgbar	Ja
Skalierbarkeit	Sehr gut

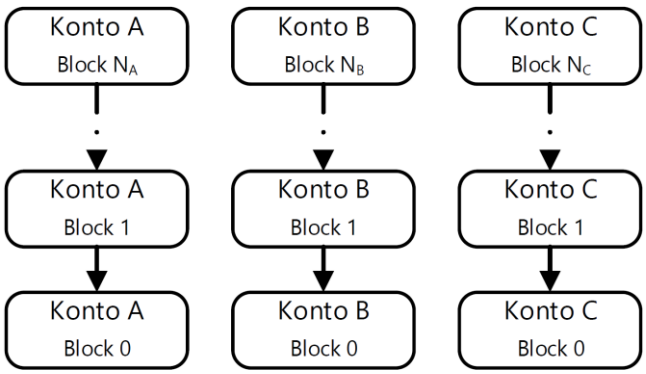

Abbildung 3: Jedes Konto verfügt über eine eigene Blockchain, die die Historie des Guthabens festhält.

[16] Abgerufen von https://coinmarketcap.com/ am 04.05.2018

Das Guthaben kann mittels *Send*-Transaktionen, welche auf der Genesis-Blockchain festgehalten werden, aufgeteilt werden. Um das Guthaben zu transferieren, muss der entsprechende Empfänger das Guthaben mittels einer *Receive*-Transaktion empfangen. Dabei wird das Guthaben sofort vom Sender abgezogen, dem Empfänger aber erst gutgeschrieben, wenn dieser die Receive-Transaktion erstellt.

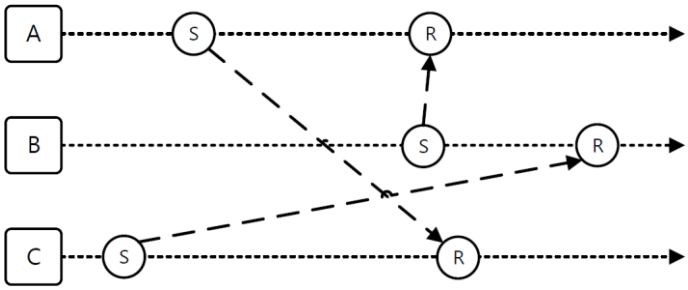

Abbildung 4: Um Guthaben zu verschieben wird eine Send Transaktion (S) sowie eine Receive Transaktion (R) benötigt. Jede dieser Transaktionen muss vom Besitzer der Kette signiert werden.

Forks – also wenn zwei oder mehr Blöcke auf einen Block aufbauen – können nur vom Besitzer der Blockchain ausgelöst werden, da nur dieser den benötigen Signaturschlüssel für diese Blockchain besitzt. Im Falle eines Forks kommt es zu einer Abstimmung. Die Stimmen werden nach vorhandenem Guthaben gewichtet. Jedes Konto kann zudem einen Stellvertreter definieren, der in dessen Namen abstimmen kann. Über sogenannte *change*-Transaktionen kann der Stellvertreter gewechselt werden. Jedes Konto kann als Stellvertreter handeln, die einzige Anforderung an den Stellvertreter-Knoten ist, dass dieser möglichst immer online ist. Als Spam-Schutz kommt ein Mini-Proof-of-Work zum Einsatz. Dieser Proof-of-Work kann vorberechnet werden, wodurch Nano sofortige Transaktionen unterstützt. Eine weitere Besonderheit von Nano ist der Wegfall von Transaktionsgebühren, sowie die sehr gute Skalierbarkeit.

7. PIVX

PIVX steht für *Private Instant Verified Transaction*. Bei PIVX handelt es sich um eine auf Privatsphäre optimierte Kryptowährung, welche das *Zerocoin*-Protokoll[18] implementiert. Zerocoin verspricht den Benutzern volle Privatsphäre. Des Weiteren verwendet PIVX das von Blackcoin[19] verbesserte *Proof-of-Stake* (PoS) 3.0 Protokoll anstelle eines Proof-of-Work Protokolls. Im Vergleich zu Bitcoin ergeben sich weitere Unterschiede, wie die Verwendung des *See-Saw*-Belohungsalgorithmus', der Verwendung von Masternodes und Stake-Nodes, der Unterstützung von *SwiftTX*-Transaktionen [22], der Verwendung des Zerocoin-Protokolls, sowie einer unlimitierten Coin-Menge[20]. Die Verwendung von Masternodes und die Unterstützung von SwiftTX-Transaktionen ähneln den Features von Dash. Im nächsten Abschnitt wird das Zerocoin-Protokoll vorgestellt.

PIVX	
Release Datum	01.02.2016
Symbol	PIVX
Maximale Coin-Menge	Unlimitiert
Marktkaptial	$323,030,053 USD[17]
Konsensus-Algorithmus	Zuerst POW, seit Sept. 2016 POS
Blockerstellungszeit	60 Sekunden
Minebar	Ja (POS)
Sender Anonymität	Ja (Optional)
Empfänger Anonymität	Nein
Betragsverschleierung	Ja (Optional)
Verfolgbar	Nein
Skalierbarkeit	Beschränkt (2MB Blockgröße)

7.1. Zerocoin-Protokoll

[17] Abgerufen von https://coinmarketcap.com/ am 04.05.2018
[18] http://zerocoin.org/
[19] https://blackcoin.co/
[20] Im Gegenzug werden Transaktionsgebühren vernichtet und nicht wie bei Bitcoin an die Miner ausbezahlt.

Das von PIVX verwendete Zerocoin-Protokoll beinhaltet ein Mixing-Service auf Protokollebene basierend auf Zero-Knowledge-Beweisen. Dieses Mixing-Service löst die Verbindung von Sender und Empfänger auf. Dieses Protokoll wird *zPIV* genannt, wobei PIV (eine Einheit von PIVX) von PIVX abgeleitet ist und der „z"-Prefix von Zerocoin. Jede Währungseinheit die über zPIV verschickt wird, ist vollkommen anonym und austauschbar, d.h. der Verlauf einer Währungseinheit, bzw. deren Geschichte, ist nicht bestimmbar. zPIV kann weiters die Transaktionsbeträge maskieren, um die Privatsphäre zu erhöhen. Um zPIV zu erhalten, müssen PIV eingetauscht werden. zPIV gibt es in verschiedenen Stückelungen[21]. Wenn zPIV ausgegeben werden, sendet das Wallet einen Zero-Knowledge-Beweis, welcher die Umwandlung in PIV erlaubt. Dies hat zu Folge, dass jedes Mal, wenn zPIV verschickt werden, neue Währungseinheiten erschaffen werden. Das „Wechselgeld" kann entweder in zPIV ausbezahlt werden, wobei dann die kleinste Einheit 1 zPIV ist und der Rest als Gebühr verloren geht, oder in PIV umgewandelt werden. Dabei ist zu beachten, dass jede zPIV-Stückelung eine eindeutige Seriennummer bekommt, welche in der lokalen Wallet-Anwendung gespeichert wird. Daher sollte nach jeder Umwandelung von PIV in zPIV ein Backup gemacht werden, da sonst bei Datenverlust zPIV verloren gehen können.

7.2. SwiftTX

Bei SwiftTX handelt es sich um Transaktionen, die innerhalb von Sekunden bestätigt werden und sofort ausgegeben werden können. Die PIVX-Masternodes garantieren die korrekte Abwicklung, wodurch nicht auf mehrere Bestätigungsblöcke zur Verifizierung gewartet werden muss.

7.3. See-Saw Reward-Mechanismus

Der See-Saw Reward-Mechanismus teilt den Blockreward auf Staker und Masternodes auf. Die Aufteilung geschieht auf Basis der Menge von Währungseinheiten die von Masternodes gehalten werden im Verhältnis zu der Menge von Währungseinheiten die von Staker gehalten werden. Durch den variablen Reward kann das Netzwerk für eine Ausgewogenheit zwischen Staker und Masternodes sorgen, indem je nach Bedarf Staker oder Masternodes einen höheren Anteil der Belohnung bekommen.

7.4. Masternodes

Um einen Masternode zu betreiben, wird ein Collateral von 10.000 PIV[22] benötigt. Masternodes stellen das Rückgrat für Services wie SwiftTX und Coin-Mixing da. Um diese Services anbieten zu können, sollten Masternodes möglichst durchgehend erreichbar sein. Als Gegenleistung erhalten Masternodes einen Anteil vom Block-Reward. Dieser Anteil ist bei Masternodes im Vergleich zu Staking-Wallets etwas höher (je nach Anzahl der Masternodes). Des Weiteren dürfen Masternode-Besitzer bei Abstimmungen über das Förderungsbudget und zu Entwicklungsvorschlägen teilnehmen.

[21] zPIV unterstützt die folgenden Stückelungen: 1, 5, 10, 50, 100, 500, 1000, 5000 zPIV
[22] Stand 9. April 2018 entsprechen 10000PIV in etwa 32000 Euro.

8. Zcash

Zcash	
Release Datum	Oktober 2016
Symbol	ZEC
Maximale Coin-Menge	21,000,000 ZEC
Marktkaptial	$1,167,918,463 USD[23]
Konsensus-Algorithmus	Proof-of-Wokrk (Equihash)
Blockerstellungszeit	2,5 Minuten
Minebar	Ja
Sender Anonymität	Ja (Optional)
Empfänger Anonymität	Ja (Optional)
Betragsverschleierung	Ja (Optional)
Verfolgbar	Nein (Optional)
Skalierbarkeit	Beschränkt (2MB Blockgröße)

Die Kryptowährung ZCash wird als eine Weiterentwicklung von Bitcoin mit einem Fokus auf Privatsphäre und nicht nachverfolgbare Transaktionsaktionen positioniert. Um diese Ziele zu erreichen, wird das eigens für diese Währung entwickelte *Zerocash*-Protokoll [28] eingesetzt. Zerocash selbst ist eine Weiterentwicklung von Zerocoin (siehe Abschnitt 7.1). Entsprechend verfolgen sowohl Zerocash und Zerocoin dieselben Ziele. Die Weiterentwicklungen (die sich auch direkt im Featureset von Zcash niederschlagen) betreffen die Effizienz der Transaktionsabwicklung, sowie die Anonymität von Transaktionen selbst.
Im Rahmen von Zcash sind weder Absender, Empfänger, noch der Wert einer Transaktion öffentlich nachvollziehbar. Erreicht wird dies ebenfalls wie im Rahmen von Zerocoin durch den Einsatz von Zero-Knowledge-Proofs. Der Einsatz dieser Mechanismen ist jedoch nicht zwingend erforderlich. Daher handelt es sich ebenso wie im Rahmen von Dash (siehe Abschnitt 3) um eine Opt-In-Möglichkeit für erhöhte Privatsphäre. Im Währungsnetzwerk von Zcash gibt es hierfür zwei separate Coin-Kontingente: so genannte *basecoins*, welche im Rahmen nachvollziehbarer Transaktionen benutzt werden, und *zerocoins*, welche es ermöglichen, Kapitalflüsse zu verschleiern. Eine Umwandlung einer basecoin in eine zerocoin ist ebenso möglich wie in die umgekehrte Richtung.
Die wichtigsten Eckdaten lassen sich aus den Projekt-FAQs[24], bzw. der Protollspezifikation[25] entnehmen.

9. Fazit

In diesem Dokument wurden die Kryptowährungen Dash, IOTA, Monero, Nano, PIVX und Zcash vorgestellt und in Bezug auf Anonymität, Privatsphäre und Skalierbarkeit mit Bitcoin verglichen. Tabelle 2 fasst die Ergebnisse zusammen. Im Rahmen der durchgeführten Recherchen hat sich herausgestellt, dass selbst moderne Kryptowährungen entweder Skalierbarkeit, oder Privatsphäre priorisieren. Da es bisher noch zu keiner Marktkonsolidierung gekommen ist und täglich neue Kryptowährungen auf den Markt drängen, handelt es sich bei den Ergebnissen in Teilen um eine Momentaufnahme. Gerade auf Grund dieser hohen, teilweise extremen Dynamik, wurden die analysierten Währungen im Hinblick auf ihren Innovationsgrad und ihre Verankerung im Markt ausgewählt, um trotz der Volatilität des Kryptowährungsmarktes einen möglichst nachhaltigen Überblick zu geben.
Derzeit gibt es keine Kryptowährung, die gleichzeitig die Ansprüche nach Privatsphäre und Skalierbarkeit zufriedenstellend bedient. Die aktuelle Marktsituation lässt den Schluss zu, dass eine hochskalierbare Kryptowährung, welche gleichzeitig ein hohes Maß an Privatsphäre gewährleistet technisch noch nicht umsetzbar ist. Auf Privatsphäre optimierte Kryptowährungen versuchen das Skalierungsproblem durch größere maximale Blockgrößen oder durch dynamisch vorgegebene Blockgrößen zumindest zu minimieren. An anderen Ansätzen wird derzeit noch geforscht. Tatsächlich hochskalierbare Kryptowährungen wie IOTA und Nano lassen derzeit noch gut integrierte Privatsphärefeatures vermissen. An einer Lösung für diese Unvereinbarkeit zwischen Skalierbarkeit und Schutz der Privatsphäre wird jedoch bereits im Rahmen von mehreren Kryptowährungen aktiv gearbeitet.

[23] Abgerufen von https://coinmarketcap.com/ am 04.05.2018
[24] https://z.cash/support/faq.html
[25] https://github.com/zcash/zips/blob/master/protocol/protocol.pdf

Tabelle 2: Überblick über Bitcoin und andere moderne Kryptowährungen

	Bitcoin	Dash	IOTA	Monero	Nano	PIVX	Zcash
Release Datum	Jänner 2009	18. Janner 2014	21. June 2014	18. April 2014	2014	01.02.2016	Oktober 2016
Symbol	BTC	DASH	IOTA	XMR	NANO	PIVX	ZEC
Maximale Coin-Menge	Limitiert (21 Mio. BTC)	18,900,000 DASH	2,779,530,283 IOTA	Unlimitiert (18,4 Mio. XMR + 0,3 XMR/Minute)	133,248,289 NANO	Unlimitiert	21,000,000 ZEC
Marktkaptial	$147.225.731.614 USD	$3,957,649,596 USD[26]	$6,577,313,690 USD	$3,901,501,725 USD	$1,252,403,335 USD[27]	$323,030,053 USD	$1,167,918,463 USD
Konsensus-Algorithmus	Proof of work (SHA-256)	Proof of Work (X11)	Tip Selection Algorithm	Proof of work (Cryptonight)	Voting	Zuerst POW, seit Sept. 2016 POS	Proof-of-Wokrk (Equihash)
Blockerstellungszeit	10 Minuten	2,5 Minuten	-	2 Minuten	-	60 Sekunden	2,5 Minuten
Minebar	Ja (ASICs)	Ja	Ja	Ja (CPUs, GPUs)	Nein	Ja (POS)	Ja
Sender Anonymität	Nein	Ja (Optional)	Nein	Ja (Ring Signaturen)	Nein	Ja (Optional)	Ja (Optional)
Empfänger Anonymität	Nein	Nein	Nein	Ja (Stealth Addresses)	Nein	Nein	Ja (Optional)
Betragsverschleierung	Nein	Nein	Nein	Ja (Ring confidential transations)	Nein	Ja (Optional)	Ja (Optional)
Verfolgbar	Ja	Nein	Ja	Nein (außer für Empfänger/Sender)	Ja	Nein	Nein (Optional)
Skalierbarkeit	Beschränkt (1MB Blockgröße)	Beschränkt (2MB Blockgröße)	Sehr gut	Gut (dynamische Blockgröße)	Sehr gut	Beschränkt (2MB Blockgröße)	Beschränkt (2MB Blockgröße)

[26] Abgerufen von https://coinmarketcap.com/ am 04.05.2018
[27] Abgerufen von https://coinmarketcap.com/ am 04.05.2018

Referenzen

[1] A. Marsalek und B. Prünster, „Technologieüberblick Blockchain," www.a-sit.at, Graz, 2016.

[2] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly, 2014.

[3] C. Bergmann, „Wie viel Strom verbrät das Bitcoin Netzwerk?," 15 Oktober 2014. [Online]. Available: https://bitcoinblog.de/2014/10/15/wie-viel-strom-verbrat-das-bitcoin-netzwerk/. [Zugriff am 20 10 2016].

[4] Allied Control, „Analysis of Large-Scale Bitcoin Mining Operations," 2014. [Online]. Available: http://www.allied-control.com/publications/Analysis_of_Large-Scale_Bitcoin_Mining_Operations.pdf. [Zugriff am 11 10 2016].

[5] K. J. O'Dwyer und D. Malone, „Bitcoin mining and its energy footprint," in *Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET*, Limerick, IET, 2014, pp. 280-285.

[6] C. Malmo, „Bitcoin hat ein großes Problem: Die Krypto-Währung ist einfach nicht nachhaltig," 10 August 2015. [Online]. Available: http://motherboard.vice.com/de/read/das-oeko-problem-von-bitcoin-darum-ist-die-krypto-waehrung-nicht-nachhaltig-3920. [Zugriff am 20 10 2016].

[7] S. Deetman, „Bitcoin Could Consume as Much Electricity as Denmark by 2020," 29 März 2016. [Online]. Available: http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. [Zugriff am 20 10 2016].

[8] H. McCook, „http://www.coindesk.com/microscope-true-costs-banking/," 12 July 2014. [Online]. Available: http://www.coindesk.com/microscope-true-costs-banking/. [Zugriff am 26 10 2016].

[9] Bitcoin Wiki, „Talk:Scalability," 20 12 2014. [Online]. Available: https://en.bitcoin.it/wiki/Talk:Scalability. [Zugriff am 15 09 2016].

[10] The Dash Network, „Dash Official Website | Dash Crypto Currency - Dash," 2018. [Online]. Available: https://www.dash.org/. [Zugriff am 09 04 2018].

[11] The Dash Network, „Darkcoin Is Now Dash," [Online]. Available: https://www.dash.org/general/2015/03/25/darkcoin-is-now-dash.html. [Zugriff am 09 04 2018].

[12] E. Duffield und D. Diaz, „Dash: A Privacy-Centric Crypto-Currency," 17 02 2018. [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper. [Zugriff am 05 04 2018].

[13] J. R. Douceur, „The Sybil Attack," in *Peer-to-Peer Systems*, Berlin, Springer, 2002, pp. 251-260.

[14] D. L. Chaum, „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," in *Communications of the ACM*, New Yor, NY, USA, ACM, 1984, pp. 84-88.

[15] P. Handy, „Introducing Masked Authenticated Messaging," 04 11 2017. [Online]. Available: https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e. [Zugriff am 02 03 2018].

[16] L. Tennant, „Research on Private Transactions in IOTA," 22 10 2017. [Online]. Available: https://blog.iota.org/research-on-private-transactions-in-iota-cd546751e2c4. [Zugriff am 02 03 2018].

[17] The Monero Project, „Ring Signature," [Online]. Available: https://getmonero.org/resources/moneropedia/ringsignatures.html. [Zugriff am 04 04 2018].

[18] The Monero Project, „Stealth Address," [Online]. Available: https://getmonero.org/resources/moneropedia/stealthaddress.html. [Zugriff am 04 04 2018].

[19] Shen Noether, Monero Research Labs, „Ring Confidential Transactions," [Online]. Available: https://eprint.iacr.org/2015/1098.pdf. [Zugriff am 05 04 2018].

[20] PIVX Community, „PIVX Features," [Online]. Available: https://pivx.org/de/what-is-pivx_de_was-ist-pivx/features_de_funktionen/. [Zugriff am 05 04 2018].

[21] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer und M. Virza, „Zerocash: Decentralized Anonymous Payments from Bitcoin," in *2014 IEEE Symposium on Security and Privacy*, IEEE, 2014, pp. 459-474.

[22] amaclin, „How does the ECDSA verification algorithm work during transaction?,“ 2014. [Online]. Available: http://bitcoin.stackexchange.com/questions/32305/how-does-the-ecdsa-verification-algorithm-work-during-transaction.

[23] Bitcoin Block Reward Halving Countdown, „Bitcoin Block Reward Halving Countdown,“ [Online]. Available: http://www.bitcoinblockhalf.com/. [Zugriff am 19 10 2016].

[24] G. F. Hurlburt und I. Bojanova, „Bitcoin: Benefit or Curse?,“ in *IT Professional*, IT Professional, 2014, pp. 10-15.

[25] Bitcoin Wiki, „Controlled Supply,“ 30 07 2016. [Online]. Available: https://en.bitcoin.it/wiki/Controlled_supply. [Zugriff am 20 09 2016].

[26] M. Tillier, „Is A Blockchain Without Bitcoin Possible Or Practical?,“ NASDAQ, 03 06 2015. [Online]. Available: http://www.nasdaq.com/article/is-a-blockchain-without-bitcoin-possible-or-practical-cm482964. [Zugriff am 11 04 2016].

[27] C. Bergmann, „Islands virtueller Zimbabwe-Dollar,“ 13 05 2014. [Online]. Available: http://bitcoinblog.de/2014/05/13/ein-digitaler-zimbabwe-dollar-fur-island/. [Zugriff am 14 03 2016].

[28] blockchain.info, „Blockchain-Größe,“ 2018. [Online]. Available: https://blockchain.info/de/charts/blocks-size.

[29] Blockchain Luxembourg S.A, „Bitcoin Block Explorer - Blockchain,“ 2018. [Online]. Available: https://blockchain.info/. [Zugriff am 12 02 2018].

[30] S. Popov, „The Tangle,“ 01 10 2017. [Online]. Available: https://iota.org/IOTA_Whitepaper.pdf. [Zugriff am 02 2018].

Anhang A: Relevante kryptografische Konzepte

Hashfunktionen

Eine *Hashfunktion* ist eine spezielle Form einer Einwegfunktion und bildet Werte beliebiger Größe auf Werte fixer Größe, den *Hash*, ab. Aus dieser Definition ergibt sich direkt eine gewisse Unumkehrbarkeit: Aus einem gegebenen Hash lässt sich der ursprüngliche Wert allein schon deshalb nicht ohne Weiteres berechnen, da nicht einmal die Größe des ursprünglichen Werts abgeleitet werden kann. Die Anforderungen an kryptografische Hashfunktionen umfassen diese, aber auch weitere Eigenschaften. Zusammengefasst sind dies:

- *Einwegcharakteristik (pre-image resistance)*: Es muss praktisch unmöglich sein, zu einem vorgegebenen Hash einen Eingangswert zu finden, welcher auf diesen abbildet.
- *Schwache Kollisionsresistenz (second pre-image resistance)*: Es muss praktisch unmöglich sein, zu einem gegebenen Eingangswert einen davon verschiedenen Eingangswert zu finden, welcher auf denselben Hash abbildet.
- *Starke Kollisionsresistenz (collision resistance)*: Es soll generell nicht möglich sein, zwei frei wählbare Eingangswerte zu finden, welche auf ein und denselben Hash abbilden.

Aus diesen drei Eigenschaften ergeben sich weitreichende Konsequenzen. Nachdem jegliche Form von Kollision praktisch nicht gezielt herbeigeführt werden kann, und ein gegebener Hash keinerlei Rückschlüsse auf den Eingangswert zulässt, bedeutet das im Umkehrschluss, dass bereits geringfügige Änderungen im Eingangswert zu gravierenden Änderungen im Hash führen. Wäre dies nicht der Fall, wären Korrelationen zwischen Hash und Eingangswert, und somit Rückschlüsse vom Hash auf den Eingangswert möglich. Diese Eigenschaft wird auch als Resistenz gegen *Beinahe-Kollisionen* (near-collision resistance) bezeichnet.
Auf Grund der Eigenschaften kryptografischer Hashfunktionen wird es beispielsweise unmöglich, ein Dokument, dessen Hash bekannt ist, unbemerkt zu manipulieren, da ein auch nur minimal verändertes Dokument auf einen völlig anderen Hash abbildet, wodurch eine Manipulation unmittelbar festgestellt werden kann. Wie schwierig derartige Manipulationen in der Praxis sind, hängt von der Qualität der verwendeten Hashfunktion ab. Die Berechnung eines Hash ist im Regelfall sehr effizient durchführbar.

Asymmetrische Kryptografie

Asymmetrische kryptografische Verfahren beruhen auf einer speziellen Klasse von Pseudo-Einwegfunktionen, so genannten *Trapdoor*-Funktionen. Genau wie Einwegfunktionen (ähnlich wie Hashfunktionen) sind diese auch in eine Richtung einfach berechenbar, jedoch praktisch nicht invertierbar. Die Besonderheit an Trapdoor-Funktionen ist, dass eine Invertierung sehr wohl einfach durchführbar ist, wenn man über eine spezielle Information verfügt. Mittels derartiger Funktionen lassen sich kryptografische Verfahren konstruieren, welche im Gegensatz zu symmetrischen Verfahren auf den Austausch von Schlüsselmaterial verzichten – Schlüssel werden nie zwischen mehreren Parteien geteilt.
Asymmetrische kryptografische Verfahren bedienen sich der Trapdoor-Charakteristik wie folgt: Schlüssel sind zweigeteilt in einen öffentlichen und einen privaten Teil, was als *public/private key pair* bezeichnet wird. Der öffentliche Teil kann (wie der Name vermuten lässt) veröffentlicht werden. Jeder im Besitz dieses öffentlichen Schlüssels kann Daten unter Zuhilfenahme dieses Schlüssels verschlüsseln. Eine Entschlüsselung ist jedoch ohne Kenntnis des privaten Schlüssels praktisch unmöglich und kann daher nur vom Besitzer des privaten Schlüssels durchgeführt werden. Eine direkte Konsequenz aus dieser Trapdoor-Eigenschaft ist die Tatsache, dass Schlüssel eindeutig einzelnen Parteien zugeordnet sind. Digitale Signaturen bauen auf ebendieser Tatsache auf.

Digitale Signaturen

Digitale Signaturen sind eine Anwendungsmöglichkeit asymmetrischer Kryptografie abseits von Datenverschlüsselung. Die oben beschriebene Trapdoor-Charakteristik wird sozusagen verkehrt herum eingesetzt: Um ein Dokument digital zu signieren wird zuerst dessen Hash berechnet und dieser anschließend mit dem privaten Schlüssel „verschlüsselt“. Eine solche Signatur kann von jedem, dem der zugehörige öffentliche Schlüssel bekannt ist, verifiziert werden und somit dem Besitzer des privaten Schlüssels zugeordnet werden. Durch den „vertauschten“ Einsatz von

öffentlichem und privatem Schlüssel und die eindeutige Zuordnung eines Schlüssels an eine Partei, ist es nicht möglich im Namen einer anderen Partei eine auf deren Namen lautende Signatur zu erstellen. Daher ist beispielsweise Identitätsdiebstal nur durch Entwenden des privaten Schlüssels möglich. Gleichzeitig sind digitale Signaturen auch nicht abstreitbar, da ein einmal gültig signiertes Dokument jederzeit mittels zugehörigem öffentlichen Schlüssel verifiziert werden kann. Auf Grund der oben beschriebenen Eigenschaften kryptografischer Hashfunktionen ist es auch nicht möglich ein einmal digital signiertes Dokument nachtäglich zu manipulieren ohne dass die zugehörige digitale Signatur ungültig wird.