Electronic Peer to Peer Cash Systems Herausforderungen und Chancen

Wanja Sajko
Student der Informatik plus Statistik
Ludwig-Maximilians-Universität München
W.Sajko@campus.lmu.de

Sebastian Prieler
Student der Informatik plus Mathematik
Ludwig-Maximilians-Universität München
S.Prieler@campus.lmu.de

***Zusammenfassung*—Als Satoshi Nakamoto sein Bitcoin-Paper veröffentlichte, revolutionierte er eine der größten Errungenschaften der Menschheit: Die Fähigkeit Werte bzw. Zeit, anfänglich mit Tauschwaren und später mit Münzen bzw. Geld, greifbar zu machen. Der rasante Wertanstieg der Kryptowährung Bitcoin zeigt, dass immer mehr Menschen ihre revolutionären Eigenschaften, wie Anonymität, Universalität und Dezentralität erkennen und schätzen.**

Die Herausforderungen, mit denen sich die Bitcoin-Gemeinschaft noch auseinandersetzen muss, verhindern bisher den großen Durchbruch. Bitcoin ist momentan ein Versprechen auf die Zukunft, also eine spekulative Wertanlange. Um mit Leitwährungen wie dem US-Dollar mithalten zu können, muss die Kryptowährung Zugänglichkeit, Effizienz, Stabilität, Sicherheit und Skalierbarkeit garantieren.

In dieser Arbeit untersuchen wir: Wo steht Bitcoin heute? Welche Herausforderungen muss sich Bitcoin stellen? Wie groß sind seine Chancen? Wir stellen dabei fest, dass es vielversprechende Lösungsansätze für die zu bewältigenden Schwierigkeiten gibt, die intensiv ausgearbeitet werden müssen. Außerdem werfen wir einen Blick auf Bitcoin im Vergleich zu anderen Electronic Cash Systems wie Bitcoin Cash und Ethereum. Wir kommen zu dem Schluß, dass, innovative, wissenschaftliche und praktische Lösungsansätze die komplexen Probleme lösen können und somit die Durchsetzungskraft von Bitcoin garantieren.

I. Einleitung

A. Historie

Bitcoin ist die erste und wohl bekannteste Kryptowährung. Mit ihr wurden theoretischen Konzepte, wie *bit gold* von Nick Szabo oder *b-money* von Wei Dai, endlich zur Realität. Bitcoin wurde am 31. Oktober 2008 ins Leben gerufen als der Erfinder unter dem Pseudonym Satoshi Nakamoto eine wissenschaftliche Arbeit mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“ veröffentlichte. Die Arbeit stellt ein *peer-to-peer* Netzwerk vor, das elektronische Transaktionen verwaltet. Der entscheidende Vorteil hierbei ist, dass auf eine zentrale Kontrollinstanz zwischen den Handelspartnern verzichtet wird. Am 3. Januar 2009 entstand das wirkliche Netzwerk und der Entwickler Satoshi Nakamoto schürfte den ersten Block, mit der Nummer 0 und erhielt eine Belohnung von 50 Bitcoins. Wenige Tage danach wurde der erste *open-source* Bitcoin Client veröffentlicht und damit die Handelsaktivitäten für die Kryptowährung möglich gemacht.

Im Moment sind ca. 18 Millionen Bitcoins in Umlauf. Sie können, anders als konventionelle Währungen, bis auf die achte Stelle nach dem Komma aufgeteilt werden. Im Dezember 2019 war der Wert einer Bitcoin durchschnittlich 7200 $. Damit ergibt sich eine Gesamtsumme von 129 Milliarden $. Durchschnittlich werden ca. 210 Transaktionen pro Minute getätigt. Im Vergleich dazu: Es sind 1750 Milliarden $ im Umlauf. 2016 wurden rund 130000 Transaktionen pro Minute durch Kredit- oder Bankkarten getätigt. Dies zeigt deutlich, dass Bitcoin noch ein relativ kleines Zahlungsmedium ist.

B. Grundlagen von Bitcoin

Bitcoin definiert eine elektronische Münze als Kette digitaler Signaturen. Die Blockchain ist die Menge aller Ketten im Netzwerk. Jede Transaktion besteht aus Zahlungen (*input*), die jeweils mit der entsprechenden Kennung des Besitzers versehen sind sowie Zahlungsempfängen (*output*). Es entsteht eine Kette aus Transaktionen, indem jeweils der *output* der letzten Transaktion als *input* der neuen Transaktion verwendet wird.

Jeder Benutzer besitzt Paare von privaten und öffentlichen Schlüsseln. Öffentliche Schlüssel werden zusammen mit dem *input* in die Transaktion geschrieben. Private Schlüssel werden dazu benutzt, den *output* der letzten Transaktion zu dekodieren und damit zu beweisen, dass die Bitcoin dem Benutzer gehören. Die Schlüsselpaare werden in sogenannten *wallets* gespeichert. Hauptsächlich werden *deterministic (seeded) wallets* benutzt [1]. Deswegen wird hier nur auf diese eingegangen. In *deterministic wallets* entstehen alle Schlüssel durch das Hashen des *seeds* - einer zufällig generierten Zahl. Alle Schlüssel basieren auf dem *seed*, deshalb ist es ausreichend, nur von diesem eine Sicherheitskopie zu erstellen.

Es gibt bei Bitcoin keine zentrale Verwaltungsstelle. Alle Transaktionen werden öffentlich angekündigt und zu dem Pool der noch nicht bestätigten Transaktionen hinzugefügt. Die Mehrheit der Knoten entscheidet dann, welche der Transaktionen aus dem Pool korrekt sind und ausgeführt werden. Das *double spending problem* tritt auf, falls ein Nutzer mehrere Transaktionen mit identischen *input* zeitnah dem Pool hinzufügt. Die richtige, also zeitlich frühere Transaktion wird bestätigt, falls das Protokoll von mehr als der Hälfte der Nutzer eingehalten wird. So wird ausgeschlossen, dass Münzen doppelt ausgegeben werden. Der Zahlungsempfänger kann außerdem überprüfen, ob er der erste Empfänger einer Münze

ist, indem er kontrolliert, ob zum Zeitpunkt der Transaktion die Mehrheit der Knoten zustimmte. (Abb. 1.).

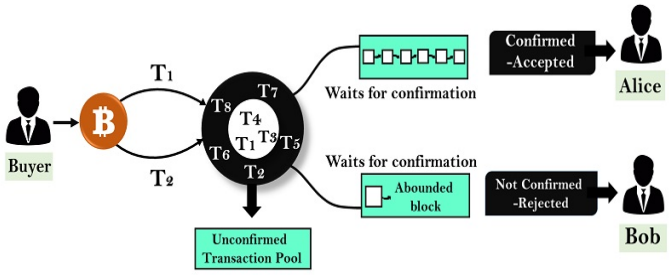

Abbildung 1. *double spending problem* [2]

Für diese Kontrollfunktion wird ein Zeitstempelnetzwerk eingerichtet, das den Hashwert jedes Blocks an Transaktionen veröffentlicht. Jeder Zeitstempel beinhaltet auch den vorherigen Zeitstempel und bildet damit eine Kette.

Als Zeitstempelnetzwerk setzt Nakamoto Satoshi [3] die Methode *Proof-of-Work*, im folgenden PoW abgekürzt, ein. Hierbei wird eine *nonce*, ein einmaliger Wert, für jeden Block inkrementiert und gehasht, bis eine Binärzahl gefunden wird, die mit einer Anzahl erforderlicher Null-Bits beginnt. Die dafür benötigte Arbeit ist exponentiell zu der Anzahl der erforderlichen Null-Bits. Sobald die Binärzahl gefunden wurde kann der Block nicht mehr verändert werden, ohne die Arbeit erneut ausführen zu müssen. Da alle späteren Blöcke miteinander verkettet sind, müsste man zum Ändern des Blocks auch die Werte aller nachfolgenden Blocks erneut bestimmen. Die Teilnehmer zeigen ihre Zustimmung, indem sie an dem nächsten Block in der Kette arbeiten. Stimmen sie nicht zu, arbeiten sie an einem anderen Zweig der Kette weiter. Solange mehr als die Hälfte der Teilnehmer sich an das Protokoll halten, wächst immer die richtige Kette am schnellsten. Außerdem ist die Kette mit den durchgeführten Transaktionen gleichzeitig die längste.

Um die Schürfer zu motivieren, erhalten sie jeweils nach dem Erstellen eines korrekten Blocks zwei Belohnungen. Als erste Belohnung erhält der Schürfer, also der Verifizierer der Zahlung, die Gebühr, die jeder Benutzer bei einer Transaktion entrichtet. Die zweite Belohnung ist die erste Transaktion eines Blocks, also die Erstellung einer neuen Münze, die dann dem Schürfer gehört. So wird sichergestellt, dass sich Knoten an dem System beteiligen, sowie neue Münzen erstellt und in Umlauf gebracht werden. Diese Belohnung wird laufend reduziert um zu vermeiden, dass die im Protokoll festgelegte Obergrenze von 21 Millionen Münzen vorschnell erreicht wird und keine weiteren mehr erstellt werden dürfen. Ab diesem Zeitpunkt ist Bitcoin vollständig inflationsfrei und der Anreiz besteht nur noch in Form der Transaktionsgebühren.

Die Funktionsweise von Bitcoin kann in 6 Schritte unterteilt werden [3]:

1) Neue Transaktionen werden an alle Knoten gesendet.
2) Jeder Knoten sammelt neue Transaktionen in einem Block.
3) Jeder Knoten arbeitet daran, einen schwierigen PoW für seinen Block zu finden.
4) Wenn ein Knoten einen PoW findet, sendet er den Block an alle Knoten.
5) Knoten akzeptieren den Block nur dann, wenn alle darin enthaltenen Transaktionen gültig sind und nicht bereits verwendet wurden.
6) Knoten drücken ihre Akzeptanz des Blocks aus, indem sie an der Erstellung des nächsten Blocks in der Kette arbeiten.

Da in Schritt 3 und 4 zwei Knoten an ein und demselben Block arbeiten können, werden eventuell verschiedene Versionen des nächsten Blocks gleichzeitig gesendet. Die Knoten, die beide Versionen zugeschickt bekommen haben, arbeiten an dem Block, den sie zuerst empfangen haben, speichern aber die andere Verzweigung für den Fall, dass diese länger wird.

Bitcoin funktioniert als *peer-to-peer* Netzwerk. Bei gängigen Client-Server-Netzwerken, zum Beispiel einem klassisches E-Mail Programm, kann der Benutzer mit seinem Endgerät auf die Dienste eines zentralen Servers zugreifen. Bei Bitcoin nutzen und speichern alle Geräte, die im Netzwerk integriert sind, gemeinsam Dateien. Dabei gibt es normalerweise keine zentrale Stelle, sondern nur gleichgestellte Teilnehmer (auch Knoten) mit jeweils einer Kopie der Dateien. Somit ist jeder Benutzer verantwortlich für seinen Knoten und muss ihn selbstständig verwalten, also zum Beispiel für Datensicherheit sorgen.

Obwohl die Knoten im Bitcoin Netzwerk gleichgestellt sind, können sie unterschiedliche Rollen annehmen [1]:

- *routing*
- *blockchain database*
- *mining*
- *wallet services*

Diese vier Funktionalitäten überschneiden sich oft. Alle Knoten sind immer *routing* Knoten, die Transaktionen verifizieren und verbreiten, sowie Verbindungen zu anderen Knoten entdecken und halten. Dazu gibt es *full nodes*, also volle Knoten, die immer eine komplette und aktuelle Kopie der Blockchain speichern. Diese können im Gegensatz zu *light nodes*, also leichten Knoten, Transaktionen autonom verifizieren. Leichte Knoten müssen immer die Hilfe eines vollen Knotens in Anspruch nehmen, da sie nur einen Teil der Blockchain speichern. *Mining nodes*, also Schürfknoten, versuchen Kryptopuzzles zu lösen, um neue Blocks erstellen zu können. Falls Schürfknoten keine vollen Knoten sind, müssen sie sich in *mining pools* mit einem Pool Server, der einen vollen Knoten betreibt, zusammenschließen. *Wallets* laufen meistens in *desktop clients* und sind daher hauptsächlich Teil von vollen Knoten. Sollte sich Bitcoin als Zahlungsmedium weiter verbreiten, werden immer mehr *wallets* auf mobilen Geräten laufen, die keinen vollen Knoten betreiben können.

C. Hypothese: Bitcoins Zukunftsaussichten

Immer mehr Menschen fangen an digital zu bezahlen. Auch Bitcoin gewinnt rasant an Zustimmung und entwickelt

sich kontinuierlich weiter. Daher ist es essentiell, die mit Bitcoin verbundenen Probleme zu lösen. Eines der größten Themen hierbei ist das *bottleneck* bei wachsender Anzahl an Transaktionen, also der Skalierbarkeit. Auch wir wollen Bitcoins Probleme, die einer großflächigen Verbreitung im Wege stehen, und deren Lösungsversuche betrachten. Kann Bitcoin diese Hürden überwinden und sich als weiträumig genutzte Währung etablieren oder wird eine bessere Kryptowährung dominieren?

Unsere Arbeit teilt sich im weiteren so auf:

- Teil II behandelt einige Aspekte der bisherigen Forschung.
- Teil III befasst sich mit Skalierbarkeit und stellt entsprechende Lösungsvorschläge vor.
- Teil IV evaluiert Bitcoin und vergleicht es mit Bitcoin Cash und Ethereum.
- Teil V geht abschließend auf soziale Aspekte und zukünftige Forschungsfragen ein.

II. Bisherige Forschung

Bitcoins Sicherheit basiert auf einem an alle Teilnehmer verteilten Protokoll. Dieses verspricht den Benutzern ausreichend Gewinn, sodass es sich nicht lohnt das System anzugreifen, sondern aktiv daran teilzunehmen. Nach bisherigen Annahmen muss sich eine Gruppe von über 50% aller Schürfer zusammenschließen, damit das Bitcoin-Netzwerk nicht mehr dezentral ist. Diese Gruppe könnte dann mehr als ihren vom Protokoll vorgesehenen Gewinn erzielen. Mit einer neuen Methode gibt es genau diese Möglichkeit auch für kleine Gruppen. Die Strategie heißt *selfish mining* und kann von Gruppen jeder Größe genutzt werden. Da Mitglieder einer solchen Gruppe mehr verdienen als andere, wird diese schnell auf mehr als 50% aller Teilnehmer wachsen und so das System zentralisieren. In ihrer Arbeit „Majority is Not Enough: Bitcoin Mining is Vulnerable“ [4] stellen die Autoren sowohl *selfish mining*, als auch eine Schutzmaßnahme gegen diese Attacke vor. Danach muss die angreifende Gruppe mehr als 25% aller Teilnehmer ausmachen, damit sich der Angriff lohnt.

In Zukunft müsste ein neues, skalierbares Protokoll implementiert werden, um die stetig wachsende Zahl an Transaktionen effizient zu verarbeiten. Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer und Robbert Van Renesse stellen in ihrer Ausarbeitung [5] ein neues Bitcoin Protokoll *Bitcoin-NG* vor, das genau diesen Zweck erfüllen soll. Bitcoin-NG reduziert die Konsensbildung soweit, dass sie nur durch die Netzwerkleistung limitiert ist. Außerdem wird die Verifikationsrate nur durch die Rechenleistung des Knotens beschränkt. Damit stellt Bitcoin-NG eine langfristige Lösung für das Problem der Skalierbarkeit dar. Es muss jedoch auf seine Sicherheit geprüft werden.

Es gibt viele Lösungsvorschläge, die versuchen, den Konsens über getätigte Transaktionen demokratischer, effizienter und skalierbarer zu machen. Doch bisher sind alle Ansätze auf Probleme gestoßen. In der Arbeit „Blockchain Trilemma Solver Algorand Has Dilemma over Undecidable Messages“ stellen die Autoren [6] den neuen Konsensalgorithmus *Algorand* vor und überprüfen seine Sicherheit. Dieser neue Algorithmus soll das lang bestehende Trilemma zwischen einem dezentralen Netzwerk, der Skalierbarkeit und der Sicherheit lösen. Nach Meinung der Autoren lassen sich die noch vorhandenen Schwächen des Algorithmus beseitigen.

Jeder (volle) Knoten müss über alle getätigten Transaktionen informiert sein. Dies führt dazu, dass Bitcoin in Zukunft mehr als 1TB Daten an Transaktionen pro Tag verschicken wird. Um das Netzwerk nicht zu überladen, erfordert es neue Wege, um alle anstehenden Transaktionen effizient durchführen zu können. Pedrosa Alejandro Ranchal, Potop-Butucaru Maria und Tucci-Piergiovanni Sara [7] stellen dazu *lightning factories*, eine Erweiterung von *lightning networks*, vor. Ein *lightning network* ist eine Schicht über Bitcoin, bestehend aus eins-zu-eins *lightning channels*. Sobald ein Kanal zwischen zwei Parteien geöffnet wurde, können diese beliebig Transaktionen abschließen, bis dieser wieder geschlossen wird. Diese Zahlungen werden nicht in der Blockchain veröffentlicht, es sei denn es gibt Uneinigkeiten über die korrekte Transaktion. Die Autoren stellen außerdem noch die Vorteile gegenüber den bereits existierenden *Duplex Micropayment Channel factories* vor. Die *lightning factories* lösen den trade-off zwischen der Lebensdauer der *Duplex Micropayment Channel factories* und dem Risiko, temporäre Gelder zu speichern.

Ghassan Karame weist in „ On the Security and Scalability of Bitcoin's Blockchain“ [8] mit zwei Studien darauf hin, dass es praktisch ausführbare Attacken auf das Netzwerk und die Validierungsschichten der Blockchain von Bitcoin gibt, welche die Möglichkeiten für Angriffe erhöhen. Außerdem zeigt er, dass, obwohl PoW für Dezentralität ausgelegt ist, bei großen Netzwerken die Validierung von immer weniger Parteien kontrolliert wird. Der Grund dafür ist, dass sich individuelle Nutzer größere Gewinne erhoffen, wenn sie ihre Ressourcen in *mining pools* kombinieren. Somit wird die Sicherheit des Bitcoin Netzwerks in Frage gestellt.

Der erhoffte Vorteil der kompletten Anonymität von Blockchain-Nutzern wird in „Toward De-Anonymizing Bitcoin by Mapping Users Location“ [9] näher untersucht. Die zwei Wissenschaftler haben an einem Algorithmus gearbeitet, der den physischen Ort von Bitcoin-Adressen bzw. deren Nutzer finden soll. Da man davon ausgehen kann, dass eine Transaktion mit mehreren Ausgangsadressen von einer Person getätigt wird, konnten die Autoren ihren Datensatz auf ca. 17 Millionen eigenständiger Nutzer zurückführen. Ihr Algorithmus war relativ erfolgreich und konnte mit einer Genauigkeitsrate von 72 Prozent die Zeitzone einer Ausgangsadresse bestimmen.

Um eine weltweite und vor allem nutzerfreundliche Funktionalität von Bitcoin zu garantieren, ist die Integration von Smartphones, also leichten Knoten, essentiell. In „Bringing Secure Bitcoin Transactions to Your Smartphone“ [10] arbeiten die Autoren an einer Lösung, um von einem Smartphone Transaktionen auszuführen zu können ohne deren Sicherheit zu kompromittieren oder auf volle Knoten angewiesen zu sein. Dies setzten sie durch *sharding*; also das Aufteilen des *unspent*

transaction output, um, damit ressourcenschwache Geräte diese nicht komplett laden müssen und ihre Transaktionen lokal verifizieren können.

Die Autoren von „Learning Blockchain Delays: A Queueing Theory Approach“ [11] haben die Ursachen der langwierigen und aufwändigen Transaktionen genauer untersucht. Ihre Arbeit stützt sich auf dem *queueing theory model*, das die Bestätigungszeiten von Transaktionen in verschiedene Kategorien einteilt und Verbindungen unter ihnen herstellt. Dieses Modell wird von dem *transaction classification framework* benutzt. Das Framework kann voraussagen, welche Transaktionen am wahrscheinlichsten akzeptiert werden. Die Autoren sind sich sicher, dass dieses Werkzeug für Bitcoin bzw. seine Skalierbarkeit essentiell ist.

III. Hauptteil

Die Skalierbarkeit von Bitcoin ist neben den Aspekten der Sicherheit und Dezentralität das Wichtigste, um den Erfolg von Bitcoin auch in Zukunft zu garantieren. Skalierbarkeit setzt unter anderem folgende Qualitäten voraus:

- Schnelle und sichere Ausführung und Verifikation von Transaktionen
- Nutzung ohne aktive Internetverbindung
- Minimierung der Abhängigkeit von Energiequellen

A. Schnelle und sichere Ausführung und Verifikation von Transaktionen

Die Autoren von „Challenges and Solutions on Architecting Blockchain Systems“ [12] stellten unter anderem fest, dass der PoW Ansatz zur Überprüfung der Korrektheit einer Bitcoin-Transaktion zeit- und rechenaufwendig ist. Er ist durch seine Eigenschaften eigentlich genau entgegengesetzt zu Skalierbarkeit konzipiert. Momentan können ca. 3-7 Übertragungen pro Sekunde verarbeitet werden. Somit ist Bitcoin um vieles langsamer als konventionelle Währungen. Es ist essentiell, diese Geschwindigkeit deutlich zu erhöhen und gleichzeitig die Sicherheit der Transaktionen zu gewährleisten.

Zwei Ansätze zur Umsetzung der Skalierbarkeit wären

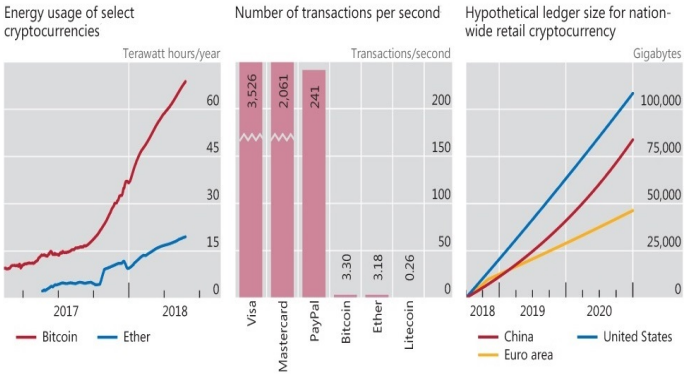

Abbildung 2. Bitcoins scalability problem [13]

die Verbesserung einzelner Knoten (vertikale Skalierung) oder die Verbesserung des gesamten Netzwerks (horizontale Skalierung), durch Hinzufügen vieler, starker Knoten. Um eine konstante Bearbeitungszeit bzw. Rechenanspruch zu garantieren, wird die Schwierigkeit eine Transaktion zu verifizieren stetig angehoben. Die Zeit um einen Block zu erarbeiten beträgt 10 Minuten. Dieses Zeitfenster wurde von Nakamoto selbst so festgelegt, da er sie als guten Kompromiss zwischen Schnelligkeit, Sicherheit und Stabilität für das Netzwerk ansah. Zusätzlich hängt das *peer-to-peer* Netzwerk von seinen schwächsten Knoten ab, da alle Teilnehmer im Netzwerk den aktuellen Stand der Blockchain kennen müssen. Somit fallen diese zwei Skalierungsmöglichkeiten für Bitcoin komplett aus.

Auch der Ansatz, die Blockgröße von 1MB zu erhöhen, klingt vielversprechend, ist aber nicht praktikabel. Eine niedrigere, minimale Bearbeitungszeit würde eine schnellere Transaktionsvalidierung ermöglichen, verlangt aber eine größere Bandbreite der Knoten und führt zu mehr Ungleichheiten zwischen ihnen, was mehr Instabilität im Netzwerk mit sich bringt. Um diese Bearbeitungszeit von 10 Minuten zu garantieren, darf die Blockgröße 4MB nicht überschreiten. Auch die erhoffte Lösung der Skalierbarkeit bleibt bei diesem Ansatz (der Erhöhung der Blockgröße) aus, da die Steigerung auf maximal 27 Transaktionen pro Sekunde nicht ausreichend wäre.

Deshalb wenden sich die meisten Forscher und Entwickler neuen Konsensalgorithmen zu, die für Bitcoin eine bessere Skalierbarkeit versprechen. Hierbei betrachten wir:

- *Proof-of-Stake*
- *Proof-of-Luck*

Proof-of-Stake, abgekürzt als PoS, basiert darauf, von Benutzern, die Transaktionen bestätigen wollen, einen Sicherheitseinsatz in Form von Bitcoin zu verlangen. Diese dürfen nur Transaktionen, die von geringerem Wert als ihr Einsatz sind, bearbeiten. So garantiert der Algorithmus, dass es sich für einen Nutzer nicht lohnt, die Transaktion zu manipulieren, da der Gewinn aus der Transaktion geringer ist als der Verlust seines Einsatzes. Ein Validierer wird zufällig vom Algorithmus in Abhängigkeit seines Einsatzes ausgewählt. Somit lässt sich nicht voraussagen, wer als nächstes einen Block bestätigt. Auch eine 51%-Attacke ist mit PoS sehr unwahrscheinlich, da man nicht die Mehrheit der Knoten, sondern die Mehrheit des Marktwertes von Bitcoin als Einsatz übergeben müsste. Dieser Konsensalgorithmus bietet somit eine adäquate, wenn nicht sogar eine bessere Sicherheit als PoW.

Da sich Schürfer unter PoW momentan in großen Gruppen zusammenschließen, wird ein Grundwert von Bitcoin, die Unabhängigkeit von einer zentralen Instanz, bedroht. Im Gegensatz dazu macht PoS das Netzwerk automatisch dezentraler. Der PoS-Algorithmus ermutigt auch leichte Knoten als Validierer zu handeln, da er nicht auf rechenaufwändiger Arbeit, sondern auf dem Sicherheitseinsatz in Bitcoin basiert. Die Notwendigkeit für zentrale Schürfgruppen entfällt, da Knoten keine große Rechenleistung mehr aufbringen müssen. Das Netzwerk ist also dezentraler und, da die einzelnen Knoten weniger Aufwand aufbringen müssen, werden Transaktionen schneller bestätigt und somit die Skalierbarkeit von Bitcoin garantiert.

Proof-of-Luck wählt einen Nutzer per Zufall zum Bestätigen des nächsten Blocks aus. Dafür benutzt der Algorithmus eine *trusted execution environment* Plattform, die einen *consensus leader* bestimmt. So ist der Prozess wieder dezentral, sehr energie- und ressourcensparend, auf eine bestimmte Zeit genormt und vor allem schnell ausführbar. Leichte Knoten können somit wieder am Konsensalgorithmus teilnehmen und *selfish mining* wird unterbunden. Bei *Proof-of-Luck* ist die Skalierbarkeit nur von der Anzahl der Teilnehmer im Netzwerk und ihrer Verbindungsgeschwindigkeit abhängig.

B. Nutzung ohne aktieve Internetverbindung

Obwohl die Welt immer besser vernetzt ist, braucht Bitcoin alternative Lösungen, damit Transaktionen nicht nur über das Internet getätigt werden können. Eine Netzwerkverbindung ist nicht immer garantiert. Durch Stromausfälle, schlechte Netzabdeckung oder restriktive Regierungen kann die Möglichkeit des Handelns mit Bitcoin unterbunden werden. Bei konventionellen Währungen kann jederzeit mit Bargeld bezahlt werden, falls Kreditkarten auf Grund von Netzschwierigkeiten nicht funktionieren. Außerdem ist Bargeld für ärmere Menschen und unterentwickelte Gebiete leichter zugänglich. Analog sollte auch Bitcoin Alternativen zu Transaktionen, die eine Netzverbindung benötigen, anbieten, um Menschen zu bedienen, die keinen Zugang zu guter Infrastruktur haben. Es gibt schon heute Lösungen wie Blockstream, die es ermöglichen, auf die Bitcoin Blockchain über ein Satellitensignal zuzugreifen. Ein anderer Lösungsweg ist die Transaktion via Radio. Einen guten Überblick des aktuellen Stands liefert der Artikel „No Internet, No Problem: How to Send Bitcoin by Amateur Radio“ [14]. Zum Beispiel haben zwei Wissenschaftler eine Bitcoin Transaktion über Radio ohne großen technischen Aufwand durchgeführt. Sie brauchten nur ein Funkgerät, eine Antenne und eine spezielle Anwendung für die Kommunikation. Somit konnten sie eine Transaktion zwischen Toronto und Michigan, also über eine Distanz von mehr als 500 km, tätigen.

Nick Szabo [15] hat bei einem Vortrag in Stanford ein ähnliches Konzept vorgestellt und die Vorteile der Übertragung von Bitcoin über elektromagnetische Wellen zusammengefasst. Er will Kurzwellenfunk, zwischen 1,6 und 30 MHz, nutzen, weil dieser die positive Eigenschaft hat, von der Ionensphäre reflektiert zu werden. Somit erhöht sich die Reichweite der Signale auf bis zu 2500 km. Durch die flächendeckende Übertragung über Radiosignale können volle Knoten immer miteinander, auch ohne Zwischenknoten, verbunden sein. So wird ein sicherer Konsens garantiert. Szabo erhofft sich durch diese Anwendung, Attacken auf die Netzwerktopologie sowie das Routing zu verhindern. Zusätzlich wird die Fläche für mögliche Attacken kleiner, da es sich bei Radiowellen um ein natürliches Phänomen handelt.

Durch solche Ansätze wäre Bitcoins Problem der Skalierbarkeit bereits auf der Ebene der Infrastruktur angesprochen.

C. Minimierung der Abhängigkeit von Energiequellen

Wie bereits festgestellt birgt der PoW Ansatz von Bitcoin einige Probleme. Neben der schwer zu realisierenden Skalierbarkeit, wegen der geringe Anzahl an Transaktionen, behindert auch die enorm hohe Rechenleistung und der damit einhergehende Energieaufwand das Netzwerk in seiner Entwicklung. Das gesamte Bitcoin Netzwerk verbraucht jetzt schon 71,04 TWh pro Jahr und liegt damit in seinem Energieverbrauch, verglichen mit allen Ländern der Erde, auf Platz 40. Doch auch bei dieser Berechnung kann man nicht sagen, ob der tatsächliche Energieverbrauch nicht viel höher liegt. Der Wert von 71,04 TWh pro Jahr lässt alle Energiekosten, die durch die Kühlung der Rechner entstehen außer acht. Für einzelne Maschinen ist das zwar kein Problem, aber da der Großteil der Hashrate durch Rechenzentren abgedeckt wird, sollte auch dieser Faktor berücksichtigt werden. Rechenzentren veröffentlichen keine Angaben zu ihren Kosten und Arbeitsweisen, sodass keine wirkliche Aussage über deren Effizienz gemacht werden kann.

Neben dem enorm hohen Energieverbrauch und dem schlechten Einfluss durch Bitcoin auf das Klima wollen wir noch ein anderes Problem untersuchen. Die Transaktionsgebühren werden, auf Grund der geringer werdenden Belohnungen, immer wichtiger, um die Schürfer für ihre Arbeit zu entlohnen. Betrachtet man zusätzlich die Energiekosten, die durch eine einzige Transaktion entstehen, wird klar, dass kostendeckende Gebühren nicht wettbewerbsfähig sind. Eine Transaktion verbraucht 659 KWh: Bei einem durchschnittlichen Preis von 10¢ pro KWh kostet eine Transaktion damit knapp 66 $. Das ist für kleine Transaktionen nicht tragbar und würde das Ende für Bitcoin als weiträumig genuztes Zahlungsmedium bedeuten.

Eine Alternative zum bisherigen PoW Ansatz muss gefunden werden, ebenso muss neue Hardware entwickelt werden, die energieeffizienter arbeitet. Einen Ansatz für bessere Schürf-Technologie stellte Intel mit ihrem Patent von 2018 vor.Der neu entwickelte Schürf-Prozessor mit speziellen Hardware Beschleunigern soll den Energieverbrauch aktueller *application-specific integrated circuit machines* (ASIC), die heutzutage fast ausschließlich für das Schürfen verwendet werden, verringern. Alleine das Verankern von Parametern in der Hardware, die zur Berechnung der Bitcoin Kryptopuzzles nötig sind, soll die Energiekosten bereits um 15% senken. [16] Andere Maßnahmen, wie die Optimierung von Dateipfaden für mehrstufige SHA-256 Hashes, werden zwar angesprochen, allerdings ohne spezifische Angaben zur Energieeinsparung. Ob Methoden zur schnelleren und energieeffizienteren Berechnung von Kryptopuzzles in Zukunft reichen werden, ist zum jetzigen Zeitpunkt nicht absehbar.

Wir wollen deswegen *Proof-of-Capacity* [17], im folgenden PoC, als weitere Alternative zu PoW untersuchen. PoW benötigt teure und nur für Kryptopuzzles nutzbare Hardware. Um funktionsfähig zu bleiben müssen Schürfer die Hardware regelmäßig warten und verbessern. PoC benutzt im Gegensatz zu PoW nicht die Rechenleistung der Knoten als Ressource

sondern deren Speicherplatz Kryptopuzzles werden nicht mehr gelöst, indem immer neue Zahlen gehasht werden, sondern nur noch potenzielle Lösungen auf der Festplatte gespeichert werden, bevor es überhaupt zum Schürfprozess kommt. Je größer die Festplatte ist, desto mehr mögliche Lösungen können gespeichert werden und umso höher sind die Chancen, das Kryptopuzzle zu lösen. Der große Vorteil besteht darin, dass die Arbeit zur Findung der möglichen Lösungen, nur einmal ausgeführt werden muss und danach für jeden kommenden Block verwendet werden kann. Im PoW Ansatz müssen dagegen für jeden Block extrem viele Hashes berechnet werden.

Wie eine solche Implementierung aussehen könnte, sieht man anhand der Kryptowährung Burst. In PoC Algorithmen gibt es zwei Phasen [17]:

1) *plotting*
2) *mining*

Plotting ist das Erstellen von Dateien, die aus einer sehr großen Menge bereits gehashter Zahlen bestehen. Die erstellten Hashes werden einmal in große Gruppen, so genannte *nonces*, und einmal in Zweierpaare, die *scoops*, unterteilt. Jede *nonce* kann durch eine Indexnummer referenziert werden. Der*plotting* Prozess benötigt immer die Burstadresse, eine einmalige Adresse, des Benutzers. Im Schürfprozess wird wie im PoW Ansatz versucht, ein gegebenes Kryptopuzzle zu lösen. Dazu benötigt der Benutzer die *generation signature* des letzten Blocks, die Blockgröße und das *base target*. Das *base target* repräsentiert den Schwierigkeitsgrad des Kryptopuzzles und wird anhand der letzten 24 Blöcke erstellt. Mit diesen drei Informationen berechnet der Schürfer einen neuen Hashwert, den *generation hash*. Dieser gibt an, welchen *scoop* er pro *nonce* benutzten soll, um eine *deadline* zu berechnen. Diese wird berechnet indem der Inhalt des *scoops* durch das *base target* geteilt wird. Die so berechneten *deadlines* werden verglichen und die niedrigste ausgewählt. Die *deadline* gibt die Zeit an, die der Schürfer warten muss, bevor er den Block erstellen kann. Hat ein anderer Schürfer also *deadline* berechnet die kleiner ist alle anderen, darf er den Block erstellen, da er am kürzesten warten muss. [18]

Bitcoin erstellt im Schnitt einen Block in 10 Minuten. Es dauert also lange bis der Block mit der eigenen Transaktion tief genug in der Blockchain verankert ist, um sicher zu sein. Die Bestätigungszeit von Burst hingegen ist um einiges schneller, da hier im Durchschnitt 1 Block pro 4 Minuten erstellt werden kann. Auch was den Energieaufwand betrifft sind Transaktionen in einem PoC Ansatz vorzuziehen. Eine Burst Transaktion benötigt im Durchschnitt 3 Wh. Das sind nur 0,000046% der Energiekosten einer Bitcoin Transaktion. Der Schwierigkeitsgrad im jetzigen Bitcoin Netzwerk ist höher als bei Burst. Trotzdem wird auch bei steigendem Schwierigkeitsgrad der Burst Kryptopuzzles, der Energieaufwand allgemein geringer bleiben, da die Energiekosten für Speichermedien wesentlich kleiner sind. PoC könnte damit auch für das Bitcoin Netzwerk eine gute Alternative bilden, vor allem da PoW und PoCsich sehr ähneln und damit die grundlegende Funktionsweise erhalten bleibt.

IV. Evaluation

Nachdem wir uns mit den unterschiedlich Aspekten von Skalierbarkeit im Hinblick auf Bitcoin auseinandergesetzt haben, wollen wir nun andere Electronic Cash Systems betrachten. Dazu haben wir haben uns mit Bitcoin Cash und Ethereum beschäfftigt und diese mit Bitcoin verglichen.

Bitcoin konnte den größten Anstieg im Marktwert und in Transaktionen im Jahr 2017 verzeichnen. Aufgrund der limitierten Blockgröße von 1MB stauten sich die Transaktionen. Um eine Zahlung schnell validieren zu lassen mussten hohe Transaktionsgebühren bezahlt werden. Diese stiegen Anfang 2018 bis auf den Rekordwert von 12.50 $. Folglich verlor Bitcoin seine Stellung als alternatives Zahlungsmittel.

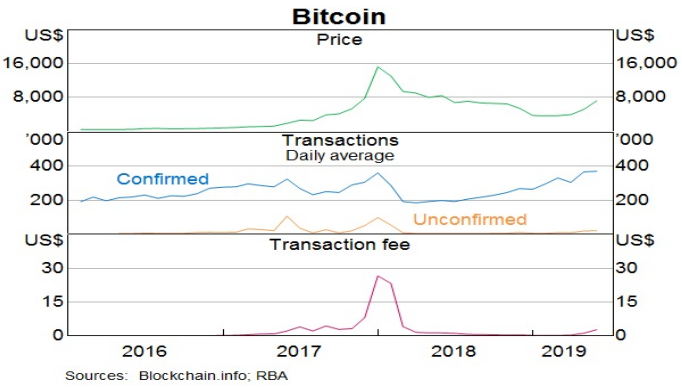

Abbildung 3. Bitcoin Überblick [19]

Als Reaktion auf diese Vorkommnisse wurde Bitcoin Cash (BCH) von Schürfern und Entwicklern, die keine Zukunft mehr in Bitcoin sahen, entworfen. Sie wollten eine neue Kryptowährung, die effizient skaliert. Dazu erhöhten sie die limitierte Blockgröße auf 8MB und führten ein flexibles Schwierigkeitsniveau ein, das auch bei einer kleinen Anzahl an Schürfern eine hohe Verifikationsrate garantieren soll. Die Blockgröße sollte zudem alle vier Jahre erneut erhöht werden.

Die erhöhte Blockgröße führt dazu, dass Transaktionen schneller ausgeführt werden, weil mehr Transaktionen auf einmal validiert werden können. Durch die schnelle Ausführung der Transaktionen sinken auch ihre Gebühren, da es nun keine Konkurrenz mehr um Blockplätze gibt.

Vertreter des klassischen Bitcoin Netzwerks argumentieren, dass es bei steigender Blockgröße für kleinere Knoten zunehmend schwieriger ist, Transaktionen zu validieren. Alle (vollen) Knoten müssen bei einer erhöhte Blockgröße mehr Daten herunterladen, hochladen und speichern. Knoten mit geringerer Kapazität sind dadurch nicht mehr konkurrenzfähig und das System würde langsam von wenigen großen Knoten abhängig sein.

Bitcoins Grundgedanke ist ein dezentrales Netzwerk. In den letzten Jahren hat es stark mit einer fortschreitenden Zentralisierung des Netzwerks zu kämpfen. Wo früher noch

Privatpersonen mit ihren Graphikkarten Kryptopuzzles gelöst haben, stehen heute riesige Serverfarmen und *mining pools*. Der einfache Benutzer ist ausgeschaltet. Inzwischen liegt mehr als die Hälfte der Hashrate in den Händen von vier bis fünf Gruppen.

Allgemein steigt der Wert eines Netzwerks mit der Transaktionsgeschwindigkeit und mit abnehmenden Transaktionsgebühren. Doch sowohl die schnelle Transaktionsgeschwindigkeit als auch die niedrigen Transaktionsgebühren von Bitcoin Cash sind eher der niedrigen Nutzerzahl, als der erhöhten Blockgröße zuzuschreiben. Die durchschnittliche Blockgröße in Bitcoin Cash liegt zur Zeit zwischen 0KB und 250KB. Die tatsächliche Blockgröße wird also nur zu knapp 3% ausgenutzt. Bitcoin steht immer noch vor demselben Problem. Die Blockgröße von 1 MB ist fast immer ausgelastet. Die Anzahl der validierten Transaktionen stagniert während die Menge der Transaktionen, die noch auf ihre Bestätigung warten, kontinuierlich hoch ist.Zwar wurden durch *SegWit*, ein Verfahren zur besseren Ausnutzung der Blöckgröße, Fortschritte gemacht, doch die durchschnittliche Wartezeit einer Transaktion beträgt momentan immer noch zwischen 15 und 30 Minuten. Das macht Bitcoin extrem anfällig für *floodattacks*. Diese sind Attacken auf das Netzwerk, bei denen extrem viele Transaktionen gleichzeitig getätigt werden. Das führt bei einem Netzwerk, dass schon vollständig ausgelastet ist zum kompletten Erliegen.

„The Ethereum blockchain is almost full“ gab Vitalik Buterin in einem Gespräch mit *The Star* zu [20]. Demnach ist auch für die sehr beliebte Kryptowährung Ethereum Skalierbarkeit eine wesentliche Hürde, die es noch zu überwinden gilt. Die Ethereum-Gemeinschaft beschäftigt sich intensiv mit dem Blockchain-Trilemma von Sicherheit, Dezentralisierung und Skalierbarkeit, in der Hoffnung, dass die Kryptowährung alle drei Kriterien schneller und besser erfüllt als die Konkurrenz.

Ein neues Konzept um dieses Ziel zu erreichen ist ZK Sync. Dieses verspricht die Transaktionen pro Sekunde (TPS) von Ethereum auf den gleichen Stand wie bei der Kreditkarte VISA zu bringen. Wenn das gelingt, wäre eine enorme Verbesserung: Von durchschnittlich 15 TPS auf ca. 2000 TPS. Zum erreichen dieser Steigerung wird auf der Schicht 2, also eine Ebene über der Ethereum Blockchain, skaliert. ZK steht hier für *zero knowledge proof*, einem Protokoll, bei dem die Nutzerdaten geheim bleiben. Ziel ist es, nur die wichtigsten Informationen für die Verarbeitung von Transaktionen aufzunehmen, um effizienter zu arbeiten. Außerdem werden die Berechnungen nicht auf der Blockchain ausgeführt, sondern ausgelagert. Damit soll die Skalierbarkeit weiter verbessert werden.

Die Blockgröße von Ethereum ist ein weiterer Faktor, mit dem bessere Skalierbarkeit erreicht werden kann. Während Bitcoins Blockgröße auf 1MB beschränkt ist, kann diese bei Ethereum durch seine Nutzer angepasst werden. Die Größe ist im Bitcoin-Protokoll festgelegt und ist deswegen sehr schwer anzupassen. Bei Ethereum hingegen wird die Blockgröße durch das sogenannte *gas limit*, einem von den Nutzern veränderbaren Faktor aus der Blockchain, bestimmt. So wird durch die Mehrheit der Knoten alle 13 Sekunden entschieden, ob die Blöcke größer oder kleiner werden. Auf diese Weise wird optimale Leistung, die auf die Nutzer ausgerichtet ist, garantiert. Die Skalierbarkeit bzw. das Erreichen einer höheren Anzahl TPS kann so im Moment schnellstens gelöst werden.

Vitalik Buterin sieht in der Kombination aus PoW und PoS einen Lösungsansatz für das Trilemma. PoW kann nur Sicherheit sowie Dezentralität garantieren, da es sonst durch knappe Ressourcen eingeschränkt ist. Deswegen sollen die besonderen Eigenschaften von PoS das fehlende Kriterium Skalierbarkeit erfüllen. Dieses neue Protokoll, die Kombination aus PoW und PoS, heißt Casper. [21]

Casper verlangt, wie PoS, einen Einsatz von den Nutzern. Diese werden nicht zufällig ausgewählt, sondern können sofort anfangen, Blocks der Kette hinzuzufügen. Wenn sie einen Block entdecken, den sie als korrekt einschätzen, müssen sie einen Wetteinsatz für ihre Einschätzung abgeben. Falls der Block an die Kette angehängt wird, bekommen die Nutzer eine Belohnung. Falls sie jedoch gegen das Protokoll verstoßen, verlieren sie ihren kompletten Einsatz. Casper ist nur eine Zwischenlösung um den Umstieg von PoW zu PoS für Ethereum und die Nutzer leichter zu machen.

Dem erhofften Ziel der Skalierbarkeit kommt Ethereum mit Casper und dem kommenden Umstieg auf PoS deutlich näher, da PoS das *sharding* im Gegensatz zu PoW ermöglicht. So wird die Verarbeitung von Blocks viel schneller möglich sein. Somit wird sich die momentane Transaktionsgeschwindigkeit nochmals verbessern und Ethereum kann eine größere Nutzeranzahl bedienen.

V. Schluss

A. Gesellschaftliche Aspekte

Wie viele große technologische Fortschritte der Menschheit hat auch Bitcoin das Potenzial, menschliche Interaktionen zu revolutionieren. Durch seine speziellen Eigenschaften hat Bitcoin den status quo des Geldwesens, also das staatliche Monopol darüber, in Frage gestellt. Menschen, die Zugang zu minimaler Technik haben, können dank Bitcoin international Handel betreiben. Grenzen oder andere staatliche Einschränkungen gelten für die Kryptowährung (noch) nicht. In Ländern mit instabilen oder fast wertlosen Währungen, wie zum Beispiel momentan in Venezuela, haben Bürger die Chance, auf Bitcoin auszuweichen, um sich und ihrer Familie Sicherheit zu bieten. Oftmals ist es in solchen Ländern verboten andere staatliche Währungen wie den US-Dollar oder den Euro zu besitzen und damit einzukaufen. In solchen Fällen bietet Bitcoin einfachen Menschen die Möglichkeit, die staatliche Kontrolle zu umgehen.

Einige sehen in Bitcoin eine Verbesserung der Stabilität und des Vertrauens im Vergleich zu konventionellen Währungen. Bei letzteren ist man auf Institutionen wie Banken angewiesen oder muss sein Geld privat aufbewahren. Somit kann man den Zugang zum eigenen Geld in Krisen ohne vorzeitige Warnung verlieren. Bitcoin kann den Menschen unter Umständen mehr Kontrolle über ihr Geld bieten. In der Geschichte kam es schon häufiger vor, dass Menschen, die ihre freie Meinung

äußerten oder nicht in eine Gesellschaft passten, der Zugang zu ihrem Geld verwehrt wurde. Da Bitcoin seinen Nutzern einen relativ hohen Grad an Anonymität bietet, kann man auch hier politischen oder gesellschaftlichen Übergriffen ausweichen.

Es muss erwähnt werden, dass Bitcoin den Kauf von illegalen Waren ermöglicht. Es lassen sich kriminelle Aktivitäten wie Menschenhandel oder Kinderpornographie finanzieren. In manchen Ländern sind einige Arzneimittel oder natürliche Substanzen illegal, obwohl diese für viele Menschen lebenswichtig sind. Weil sie mit ihrer staatlichen Währung diese nicht kaufen können ohne das Risiko einer Strafverfolgung einzugehen, ist Bitcoin eine gute Alternative.

B. Zukünftige Forschungsfragen

Da Bitcoin so weitreichenden Einflüss hat, sind auch die aktuellen Forschungsfragen sehr vielseitig. Natürlich muss man die wirtschaftliche Zukunft von und mit Bitcoin untersuchen. Wie wird sich Bitcoin preislich entwickeln, falls die 20 Million Grenze erreicht wird? Wie werden sich Wirtschaftsstrukturen verändern, falls wirklich eine kritische Masse an Personen Bitcoin verwendet?

In den Sozialwissenschaften wird man untersuchen, wie Bitcoin Gesellschaftsstrukturen verändert. Wie werden die Politik und die Zentralbanken auf Bitcoin und den möglichen Verlust der Monopolstellung reagieren?

In der Informatik wird man sich hauptsächlich auf die Verbesserung der grundlegenden Blockchain Technologie sowie Bitcoin konzentrieren. Wie kann man Blockchain auch mit minimalen Ressourcen verwenden? Wie garantiert man die Sicherheit von Blockchain und Bitcoin auch im Hinblick auf immer bessere Computer wie z.B. Quantencomputer? Welche neuen Algorithmen zur Bestätigung von Transaktionen bieten sich an, damit die Skalierbarkeit von Bitcoin gewährleistet ist?

C. Zusammenfassung

In unserer Arbeit betrachteten wir verschiedene Probleme und aktuelle Forschungsfragen, die Bitcoins Erfolg und weitere Verbreitung momentan noch einschränken. Wir stellten für diese Lösungsansätze aus der Krypto-Gemeinschaft vor. Da Bitcoin in Konkurrenz mit vielen anderen Währungen steht, haben wir zwei von ihnen unter verschiedenen Aspekten betrachtet und mit Bitcoin verglichen.

D. Ausblick

Wir sind überzeugt, dass Bitcoin auch in der näheren Zukunft die dominante Kryptowährung bleiben wird. Trotz der Problematiken, die wir hier angesprochen haben, wird sich Bitcoin behaupten. Das Interesse und Engagement der Bitcoin-Gemeinschaft ist unermesslich und die Entwicklung von immer raffinierteren Lösungen wird Bitcoin für viele Menschen nicht nur zugänglich, sondern auch wirklich nutzbar machen. Natürlich muss Bitcoin die notwendigen Verbesserungen schnellstmöglich umsetzen, um mit anderen, sehr innovativen Kryptowährungen konkurrieren zu können und für die Zukunft gerüstet zu sein. Die Vorteile, die Bitcoin mit sich bringt, haben uns überzeugt und wir werden die weitere Entwicklung dieser faszinierenden Idee sehr gespannt verfolgen. Wir hoffen, dass Bitcoin den Sprung von einem spekulativen Versprechen auf die Zukunft zu einer seriösen Währungen, die die Konkurrenz mit den Weltwährungen nicht scheuen muss, schafft.

LITERATUR

[1] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc., 1st ed., 2014.

[2] "Blockchain double spending." https://www.javatpoint.com/blockchain-double-spending.html. Accessed: 2020-01-17.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009.

[4] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, pp. 95–102, June 2018.

[5] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, (Santa Clara, CA), pp. 45–59, USENIX Association, Mar. 2016.

[6] M. Conti, A. Gangwal, and M. Todero, "Blockchain trilemma solver algorand has dilemma over undecidable messages," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, ARES '19, (New York, NY, USA), pp. 16:1–16:8, ACM, 2019.

[7] A. R. Pedrosa, M. Potop-Butucaru, and S. Tucci-Piergiovanni, "Scalable lightning factories for bitcoin," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, SAC '19, (New York, NY, USA), pp. 302–309, ACM, 2019.

[8] G. Karame, "On the security and scalability of bitcoin's blockchain," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, (New York, NY, USA), pp. 1861–1862, ACM, 2016.

[9] J. DuPont and A. C. Squicciarini, "Toward de-anonymizing bitcoin by mapping users location," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, CODASPY '15, (New York, NY, USA), pp. 139–141, ACM, 2015.

[10] D. Frey, M. X. Makkes, P.-L. Roman, F. Taïani, and S. Voulgaris, "Bringing secure bitcoin transactions to your smartphone," in *Proceedings of the 15th International Workshop on Adaptive and Reflective Middleware*, ARM 2016, (New York, NY, USA), pp. 3:1–3:6, ACM, 2016.

[11] S. Ricci, E. Ferreira, D. S. Menasche, A. Ziviani, J. E. Souza, and A. B. Vieira, "Learning blockchain delays: A queueing theory approach," *SIGMETRICS Perform. Eval. Rev.*, vol. 46, pp. 122–125, Jan. 2019.

[12] G. Fournier and F. Petrillo, "Challenges and solutions on architecting blockchain systems," in *Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering*, CASCON '18, (Riverton, NJ, USA), pp. 293–300, IBM Corp., 2018.

[13] "Cryptocurrencies: looking beyond the hype." https://www.bis.org/publ/arpdf/ar2018e5.htm.html. Accessed: 2020-01-17.

[14] N. Bester, "No internet, no problem: How to send bitcoin by amateur radio." https://news.bitcoin.com/no-internet-no-problem-how-to-send-bitcoin-by-amateur-radio/. Accessed: 2019-12-06.

[15] N. Szabo, "Weak-signal radio communications for bitcoin network resilience." https://stanford2017.scalingbitcoin.org/files/Day2/Weak-Signal-Radio-Communications-for-Bitcoin-Network-Resilience.pdf. Accessed: 2019-12-06.

[16] V. B. Suresh, S. K. Satpathy, and S. K. Mathew, "Optimized sha-256 datapath for energy-efficient high-performance bitcoin mining," Nov. 27 2018. US Patent 10,142,098.

[17] S. Gauld, F. von Ancoina, and R. Stadler, "The burst dymaxion," 2017.

[18] A. Scott, "Bitcoinburst." https://hackernoon.com/burst-part-3-proof-of-capacity-the-green-alternative-8e2651211671.html. Accessed: 2020-01-12.

[19] "Cryptocurrency: Ten years on." https://www.rba.gov.au/publications/bulletin/2019/jun/cryptocurrency-ten-years-on.html. Accessed: 2020-01-17.

[20] M. Lewis, "Vitalik buterin speaks to the star about the future of ethereum." https://www.thestar.com/business/2019/08/19/ethereums-vitalik-buterin-on-reducing-cryptocurrencys-risks.html. Accessed: 2020-01-17.

[21] V. Buterin and V. Griffith, "Casper the friendly finality gadget." https://github.com/ethereum/research/blob/master/papers/casper-basics/casper_basics.pdf. Accessed: 2020-01-12.