Bitcoin Proof of Stake: Ein Elektronisches Peer-to-Peer- Cash-System

Bitcoin PoS Developers
support@bitcoinpos.net
www.bitcoinpos.net

1. Einleitung

Bitcoin Proof of Stake (Bitcoin PoS - BPS) ist die weltweit erste Integration der beiden wichtigsten technologischen Errungenschaften der Kryptowährung - Bitcoin - und der Nachweis des Stake-Konsenses.

Der Bitcoin-Kern verwendet auch heute noch Proof of Work, einen Konsensalgorithmus, der langsam, für 51% Angriffe offen, kostenintensiv, umweltschädlich und skalierbar ist. Es gibt jedoch viele Innovationen, die nur für Bitcoin gelten und erhalten bleiben müssen B. das 21-Millionen-Token-Versorgungsmodell und die bewährte Codebasis, die von vielen der weltweit führenden Software-Ingenieure und Kryptographen entwickelt wurden.

Durch die Kombination der stärksten Ressourcen von Bitcoin mit einem hocheffizienten, skalierbaren und flexiblen Proof-of-Stake-Konsensalgorithmus führt Bitcoin PoS ein neues Paradigma für das Kryptowährungsdienstprogramm ein. Bitcoin PoS bietet alles, was Bitcoin derzeit kann, und bringt gleichzeitig neue Fortschritte in der Blockchain-Technologie an Bord Bitcoin für die Zukunft.

2. Mission

Die Welt steht am Scheideweg. Das Vertrauen in Finanzinstitute ist so niedrig wie nie zuvor, doch die von Bitcoin eingeleitete Revolution der Kryptowährung ist für die Massen nicht eingetreten. Nach Jahren der Gelegenheit haben die meisten Kryptowährungsprojekte alltägliche Benutzer gescheitert, indem sie zu wenig Versprechen abgegeben und digitale Assets zu kompliziert gemacht haben.

Bitcoin PoS zielt darauf ab, die Vision von Satoshi Nakamoto von einem banklosen,

finanziell unabhängigen und Peer-to-Peer-E-Cash-System fortzusetzen. Bitcoin PoS ist einfach zu verwenden, skalierbar für die finanzielle Nutzung von Milliarden von Menschen weltweit, sicher - und vor allem einfach für bestehende Unternehmens-, Zahlungs- und Einzelhandelsanwendungen.

3. Was ist Proof of Stake?

Ein Konsens in Bitcoin wird erreicht, indem generierte Blöcke einen Beweis enthalten müssen, dass der Miner, der den Block generiert hat, eine rechenintensive Aufgabe gelöst hat. Leider tendiert das Konzept des auf Proof-of-Work (PoW) basierenden Systems dazu, sich letztendlich selbst zu zerstören.

Proof-of-Stake (PoS) soll die Art und Weise ersetzen, wie in einem verteilten System ein Konsens erzielt werden kann. Statt den Proof-of-Work zu lösen, muss der Staker, der einen Block generiert, den Nachweis erbringen, dass er Zugriff auf eine bestimmte Menge von hat Münzen, bevor sie vom Netzwerk akzeptiert werden. Das Erzeugen eines Blocks beinhaltet das Senden von Münzen an sich selbst, was den Besitz beweist. Die erforderliche Anzahl von Münzen (auch als Einsatz bezeichnet) wird vom Netzwerk durch einen Schwierigkeitsanpassungsprozess ähnlich dem PoW festgelegt, der eine ungefähre, konstante Blockierungszeit gewährleistet.

Wie in PoW wird der Blockgenerierungsprozess durch Transaktionsgebühren und ein im zugrunde liegenden Protokoll festgelegtes Versorgungsmodell belohnt. Dies kann nach allgemeiner Definition auch als Zinssatz angesehen werden. Die anfängliche Verteilung der Währung erfolgt normalerweise über einen Zeitraum des PoW-Bergbaus.[1]

4. Probleme der Bitcoin-Zentralisierung

Ein beliebtes Sprichwort lautet: Wenn es nicht kaputt ist, beheben Sie es nicht. Während viele Bitcoin-Befürworter sagen mögen, dass Bitcoin nicht kaputt ist, geht diese Perspektive schnell aus dem Fenster, wenn sie in Bezug auf die Zukunft gerahmt wird.

Aufgrund seines derzeitigen strombasierten bergbauabhängigen Designs fördert Bitcoin die Zentralisierung der Bergbauressourcen. Einfach ausgedrückt - Strom und die dazugehörige Bergbauhardware - sind kostspielige Ressourcen. Darüber hinaus erfordert der Abbau von Bitcoin, dass man über diese Ressourcen oder den ständigen Zugriff auf diese verfügt und über ein hohes Angebot verfügt.

4.1 Bitcoin PoW schafft Abhängigkeit von Elektrizität

Von allen Ressourcen, die von Bitcoin-Bergleuten am meisten geschätzt werden, steht Strom zu Recht ganz oben auf jeder Einkaufsliste für Bergleute. Der Zugang zu Elektrizität ist jedoch nicht in allen Ländern und Regionen einheitlich.

Das Ergebnis sind Stromengpässe, bei denen einige geografische Gebiete aufgrund geringerer oder höherer Preise pro kWh über andere steigen.[2] Auf diese Weise können Bergleute in Regionen mit billiger verfügbarem Strom die Bitcoin-Bergbauindustrie monopolisieren. Ein anderes Wort für Monopolisierung ist Zentralisierung, genau das Gespenst, das Satoshi Nakamoto im Original-Whitepaper von Bitcoin versprochen hat, zu besiegen.[3]

Um das Problem zu verschärfen, haben Regierungen in Ländern mit hohen Stromkosten die Bitcoin-Bergbauindustrie in keiner Weise anerkannt oder legitimiert, was bedeutet, dass Steuerabschreibungen und Subventionen nicht in Frage kommen. Angesichts der mangelnden Bereitschaft der Regierungen, die Stromkosten zu subventionieren, um die Dezentralisierung der

Bitcoin-Technologie zu fördern, gibt es keine Lösung für die Verbreitung und das Profitieren von Bergbaukartellen, von denen sich der größte Teil in China befindet.[4]

Anstatt die Zentralisierung aufgrund ihrer Abhängigkeit von Elektrizität abzuwenden, belohnt Bitcoin sie. Dank des Proof-of-Work-Algorithmus können diejenigen, die das größte Bergbauunternehmen mit Zugang zu billigem Strom schaffen, überdurchschnittliche globale Bergleute übertreffen, ausbauen und finanziell davon profitieren - dieselben Bergleute, die einst die Hoffnung hatten, ein alternatives Finanzsystem zu schaffen.

"*Jetzt sucht das Netzwerk nach kreativen Wegen, um Probleme der Zentralisierung des Bergbaus anzugehen. Mit dem Ziel, das Monopol für Bergbauhardware zu brechen und den dringend benötigten. Wettbewerb zu schaffen, startete der BitcoinCore-Mitarbeiter BtcDrak ein Bergbauprojekt und gründete eine ASIC-Chipherstellerfirma. Während einige entschieden dagegen sind, wird eine neue Initiative für die Blockchain Defensive PatentLicense vorgeschlagen, um dem AsicBoost-Patentmonopol, das den Wettbewerb blockiert, entgegenzuwirken, ohne das unberührte Protokoll zu gefährden. Möglichkeiten zur Nutzung erneuerbarer Energien ergeben sich als Mittel zur Dezentralisierung des Bergbaus. Die Idee ist, die überschüssige Kapazität aus der Solar- und Wasserkraftproduktion zu nutzen und sie für die Gewinnung von Bitcoin zu verwenden."* [5]

Obwohl versucht wird, dieses Paradigma zu ändern, wie aus dem obigen Zitat hervorgeht, sind sie immer noch von Elektrizität abhängig, wenn auch aus alternativen Quellen, und werden daher zu mehr davon führen.

4.2 Hardware-Zentralisierung für Bitcoin PoW Mining

Die Zentralisierung des Bitcoin-Bergbaus in chinesischen Regionen ist nur die Hälfte des Zentralisierungsproblems. Gleichzeitig ist die Tatsache, dass die größten Bitcoin-Mining-Hardwarelieferanten ausschließlich Chinesen sind, mit Titanen der Branche wie Bitmain und Canaan in diesen Reihen.

Wie groß sind diese Organisationen? Heute hat Bitmain einen Wert von mindestens 15 Milliarden US-Dollar und wird von weltbekannten Banken und Investoren wie Softbank und Tencent unterstützt.[6] Mit solchen Unterstützern können chinesische Mining-Hardwarelieferanten die Crypto-Mining-Industrie im Wesentlichen weiterhin praktisch ungehindert mit Hardware versorgen.

Infolgedessen konzentriert sich die Bitcoin-Hash-Rate stark auf Gebiete wie Sichuan, in denen teure und reichlich vorhandene Wasserkraft und Bergbau-Hardware von lokalen Lieferanten den perfekten Zusammenfluss für die Hashrat-Dominanz schaffen.

Bis Dezember 2019 stammten schätzungsweise 54% der gesamten Bitcoin-Hashrate aus der Provinz Sichuan [7], was ein ethisches Dilemma für Bitcoin-Unterstützer, -Entwickler und -Benutzer darstellt, das noch nicht beantwortet wurde Die Zeit schien bereit zu sein, China wegen der Vorherrschaft im Bergbau oder zumindest wegen der Umverteilung des Hashrats herauszufordern, aber diese Hoffnungen wurden durch die Zölle der US-Regierung auf chinesische Importe - einschließlich Bergbauhardware - zunichte gemacht. Daher gibt es heute keine Anstrengungen am Horizont, um den amtierenden Griff nach Haschrat in Frage zu stellen.

"Die Zentralisierung von Hashrate bedroht das ultimative Versprechen von Cryptocurrencynetworks: Keine Partei oder Gruppe kontrolliert das Hauptbuch oder den Transaktionsfluss", sagte der Miningexperte Kristy-Leigh Minehan gegenüber Crypto Briefing. "Eine beliebige Anzahl von Naturkatastrophen oder staatlichen Bedrohungen könnte zu

Netzwerkturbulenzen führen, sei es durch längere Blockzeiten, Transaktionskosten oder Transaktionszensur auf staatlicher Ebene."[8]

Da der Hash-Wert an einer Handvoll geografischer Standorte gespeichert ist, ist die Bedrohung für das Bitcoin-Netzwerk und der gesamte darin festgelegte Wert sehr real. Während es an der Spitze von Bitcoin möglicherweise keine Zentralbankorganisation gibt, haben die Umstände innerhalb der Regionen, die Bitcoinmining dominieren, einen realen - und besorgniserregenden - Einfluss auf die größte virtuelle Währung der Welt.

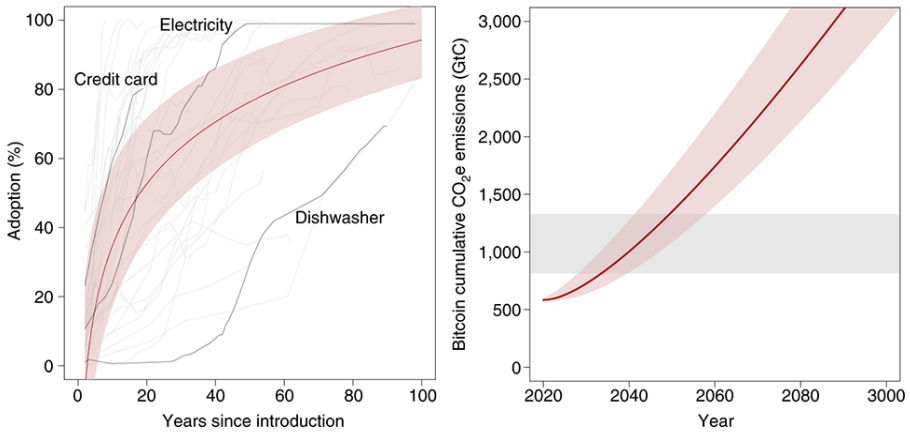
4.3 Bitcoin PoW belastet die Umwelt massiv

Die zentralisierten Bemühungen, Bitcoin abzubauen, stellen eine enorme Steuer auf die Umwelt dar und tragen maßgeblich zur globalen Erwärmung bei. In einem Bericht von Nature aus dem Jahr 2018 über den Beitrag von Bitcoin zum Klimawandel wurde geschätzt, dass BTC bei ausreichendem Wachstum eine wichtige Rolle bei der Überschreitung der Schwelle von 2 Grad Celsius spielen wird.[9]

Während sich die Welt auf Möglichkeiten zur Emissionsreduzierung konzentriert, gibt es derzeit keine Pläne anstelle eines umweltfreundlicheren Algorithmus oder einer Anpassung des PoW, um Umweltschäden zu vermeiden.

"Die geschätzten Emissionen, die Bitcoin allein im letzten Jahr verursacht hat, betragen 69 Millionen Tonnen CO2. Mora nennt die Zahlen umwerfend. „Das gibt uns Anlass zur Sorge. Wenn diese [Technologie] so unbedeutend ist und der Fußabdruck so groß ist, können Sie sich vorstellen, wenn dieses Ding abgehackt würde? "Mit zunehmender Beliebtheit von Bitcoin steigt der Energiebedarf dramatisch an. "Wir haben keine einzige Sache - keine Landwirtschaft, kein Transport -, von der wir uns vorstellen können, dass sie in zwei Jahrzehnten ausreichen würde, um den Planeten um zwei Grad zu erwärmen." Aber Bitcoin kann."[10]

Die Akzeptanz von Bitcoin ist im Vergleich zu den wichtigsten Fiat-Währungen immer noch sehr niedrig. Angesichts der Tatsache, dass die übergroßen Auswirkungen auf die Umwelt zu der Schlussfolgerung führen, dass die zunehmende Akzeptanz zunehmen sollte, wird die schädliche Abhängigkeit von fressendem Strom auch ungeheure Folgen haben.



Quelle: Nature.com

Derzeit verbraucht das Bitcoin-Netzwerk, das mit seinem Proof-of-Work-Algorithmus

betrieben wird, etwa 66,7 Terawattstunden - genug, um das gesamte Land der Tschechischen Republik mit Strom zu versorgen. Mit anderen, überragenden Maßnahmen übertrifft Bitcoin sogar die Schweiz und ist den mittelgroßen Ländern beim Energieverbrauch auf den Fersen.[11]

Während Bitcoin eine digitale Form der Währung ist, dh es ist kein Papier beteiligt und Bäume werden gerettet, ist die Ironie dass die Stromquelle für diese digitale Natur ohnehin einen sehr realen Einfluss auf die Umwelt hat.

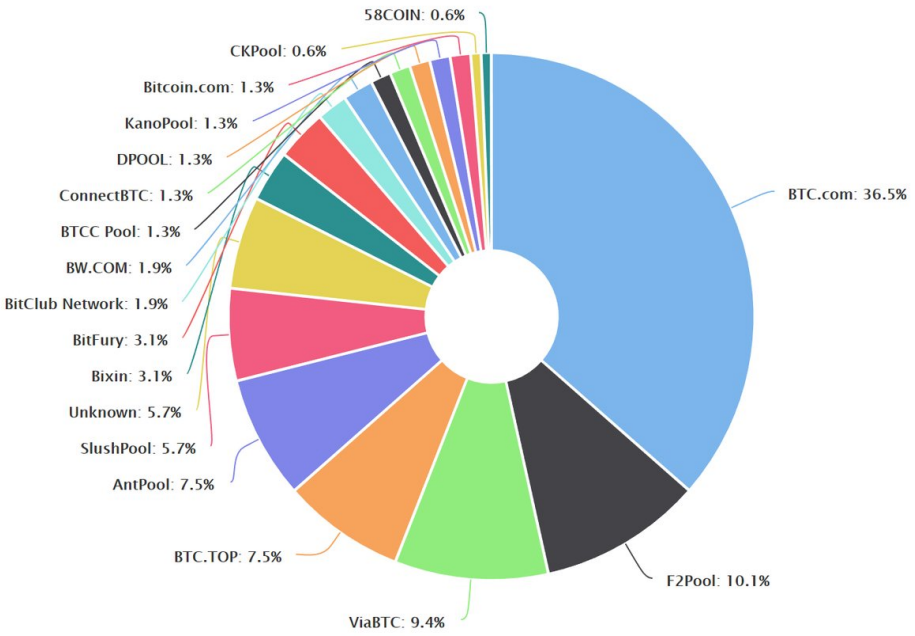
4.4 Die Bitcoin PoW-Zentralisierung ebnet den Weg für 51% Angriff

Als ob die Zentralisierung von Bitcoin aufgrund des Proof-of-Work-Algorithmus nicht bereits genügend Nachteile hätte, ist die Sicherheit ein weiteres wichtiges Anliegen. Wie bereits im vorherigen Abschnitt erwähnt, führt die Zentralisierung des Proof-of-Work-Mining-Prozesses zu einem unnötig konzentrierten Machtbereich für das Netzwerk.

Sollte ein Ereignis eintreten, sei es natürlich, kriminell oder auf andere Weise, wenn es energisch oder hoch genug ist, werden die gesammelten Ressourcen von Bitcoin habe keine Chance. Die Möglichkeit mit der höchsten Eintrittswahrscheinlichkeit ist natürlich der berühmte 51% -Angriff.

Im Wesentlichen bezieht sich ein Angriff von 51% auf die Möglichkeit, dass sich eine Gruppe auf einen Großteil der Hashrate des Bitcoin-Netzwerks konzentrieren und so das Netzwerk kontrollieren und die Macht haben kann, Transaktionen fälschlicherweise zu validieren. Während viele glauben, dass ein 51% iger Angriff des BTC-Netzwerks aufgrund der dafür erforderlichen finanziellen Ressourcen (Milliarden USD - diese Zahl schwankt mit den BTC-Werten) unwahrscheinlich ist, kann dies niemals ausgeschlossen werden.

Sollten sich die Leiter verschiedener Bergbauorganisationen dazu entschließen Es ist denkbar, dass ein 51% iger Angriff das Netzwerk lähmen und BTCuseless effektiv machen könnte.



Quelle: bitcoin.com

Die Aussage der Binance Academy zu 51% der Angriffe lautet, dass das folgende Szenario wahrscheinlich wäre, wenn eine gegen das Bitcoin-Netzwerk durchgeführt würde:

"Stellen wir uns noch ein Szenario vor, in dem eine böswillige Entität nicht durch Profit motiviert ist und beschließt, das Bitcoin-Netzwerk anzugreifen, um es zu zerstören, unabhängig von den Kosten. Selbst wenn es dem Angreifer gelingt, das Netzwerk zu stören, werden die Bitcoin-Software und das Bitcoin-Protokoll als Reaktion auf diesen Angriff schnell geändert und angepasst. Dies würde erfordern, dass die anderen Netzwerkknoten einen Konsens erzielen und sich auf diese Änderungen einigen, aber dies würde wahrscheinlich in einer Notsituation sehr schnell geschehen. Bitcoin ist sehr widerstandsfähig gegen Angriffe und gilt als die sicherste und zuverlässigste Kryptowährung, die es gibt."[12]

Diese Position ist irreführend. Was passiert, wenn auch Netzwerkknoten gefährdet sind? Es muss davon ausgegangen werden, dass jeder Angreifer oder jede Gruppe von Akteuren mit genügend Reichtum, Ressourcen und Einfluss, um einen 51% igen Angriff zusammenzuführen, auch andere Knoten dazu zwingen kann, bereit zu stehen, oder zumindest die Reaktion ausreichend stören kann, um sie zu verzögern und Bis November 2019 stammten 74% der Bitcoin-Hashrate aus China. Es gibt keinen Grund zu der Annahme, dass sich diese Zahl geändert hat - und angesichts der Schwere der im letzten Jahr auferlegten Zölle ist die Wahrscheinlichkeit eines Anstiegs dieser Hashratkonzentration hoch.[14]

5. Bitcoin PoS löst das Zentralisierungsproblem von Bitcoin

Die mit der Zentralisierung von Bitcoin verbundenen Probleme sind vielfältig und wurden in den vorangegangenen Abschnitten dokumentiert. Bitcoin PoS löst diese Probleme jedoch durch eine neuartige Lösung - nämlich durch Ersetzen des Bitcoin-Proof-of-Work-Algorithmus durch einen Bitcoin-Proof-of-Stake-Algorithmus.

Durch Ersetzen von Bitcoin PoW durch PoS werden die vier Probleme, die mit dem Proof-of-Work verbunden sind, kombiniert, um eine unnötige Lösung zu erstellen Zentralisierte Kryptowährung verschwindet. Bitcoin PoS ist weniger abhängig von Elektrizität, hat eine geringere Eintrittsbarriere in Bezug auf Hardware und ist daher leichter zugänglich und leicht zu dezentralisieren, umweltfreundlich aufgrund seines schonenden Stromverbrauchs und widerstandsfähiger gegen Angriffe von 51% aufgrund seines dezentralen Designs die Architektur.

5.1 Bitcoin PoS reduziert den Stromverbrauch um 99%

Seien wir ehrlich - die Welt befindet sich beim Energieverbrauch an einem großen Scheideweg. Wenn wir die Zukunft der Währung neu gestalten und eine bessere Finanzierungsmethode auf dem Spiel steht, muss dies den Anforderungen einer saubereren Wirtschaft entsprechen.

Daher ist ein Algorithmus für den Nachweis des Einsatzkonsens der einzige Weg zu gehen, und ist die Aktualisierung, die Bitcoin dringend benötigt. Bitcoin PoS reduziert den Energieverbrauch von Bitcoin um 99%, was vom Ethereum-Team bestätigt wurde.

Der gut dokumentierte Wechsel von Ethereum von PoW zu PoS wurde beschleunigt, teilweise aufgrund der Entdeckung des Teams, dass PoS eine drastische Reduzierung der Stromabhängigkeit darstellt. Unter dem Proof-of-Stake-Algorithmus planen die Entwickler von Ethereum, den Energieverbrauch in Blockchain um mindestens 99% zu senken [13], sodass

diejenigen, die noch PoW-Algorithmen verwenden, sich fragen, warum.

Durch die Reduzierung des Strombedarfs werden die Wettbewerbsbedingungen für die Netzwerkvalidierung wesentlich ausgeglichener. Ohne sich um eine billige Stromquelle sorgen zu müssen, können Netzwerkvalidatoren im Bitcoin PoS-Netzwerk die Energiequelle einfach von jedem Ort aus nutzen. Der Strom, den leichte Hardware für die PoS-Validierung benötigt, ist so beschaffen, dass nur minimaler Strom benötigt wird. Die Menge an Strom, die zum Betrieb eines Laptops benötigt wird, reicht aus. Darüber hinaus können Validatoren, die als Staker bezeichnet werden, in einem PoSnetwork die Aufgabe delegieren von einem Absteckbecken. Dies bedeutet, dass einzelne Staker das Netzwerk validieren können, ohne selbst Hardware ausführen zu müssen - während sich ihr Einsatz wie gewohnt noch in ihrem Portemonnaie befindet, wodurch auch die Zentralisierung von Mining-Pools umgangen wird.

5.2 Bitcoin PoS erleichtert das Abstecken

Der Nachweis von Arbeitsnetzwerken erfordert Bergleute mit Zugang zu billigem Strom und teuren Hardwaremining-Anlagen. Bitcoin PoS hingegen macht ein Mining-Rig überflüssig, da Proof-of-Stake-Netzwerke leichtgewichtig sind und keine übermäßigen Hardwareanforderungen an die Staker stellen.

Während Bergleute komplexe algorithmische Gleichungen lösen müssen und daher immer bessere Hardware-Bergleute benötigen, müssen Staker nur einen Konsens über jede Transaktion erzielen und werden für ihren Einsatz entsprechend ihrem Einsatz belohnt.

Dies senkt die Materialschwelle für potenzielle Teilnehmer und macht es möglich Möglicherweise tritt eine echte Dezentralisierung auf. Staker können normale Hardware wie einen Laptop oder einen Desktop-Computer verwenden oder ihren Anteil an einen Mining-Pool delegieren, während sie ihre abgesteckten BitcoinPoS-Münzen in ihrer Brieftasche behalten.

Die Reduzierung der Belastung der Netzwerkteilnehmer ist ein wichtiges Ziel des Bitcoin PoS-Designs. Je geringer die Belastung und Nachfrage der Staker ist, desto höher ist die Teilnahmequote und desto dezentraler und flexibler wird das Netzwerk. Wenn das Paradigma für die Teilnahme erfordert, dass ein Akteur über Ressourcen verfügt, werden wir nur eine Wiederholung des Hortens von Ressourcen sehen, die bereits in der Welt vorhanden sind.

Die Frage, die wir uns stellen müssen, lautet also: Sollte Blockchain für die 1% sein? Oder ist Blockchain ein Versuch, in die andere Richtung zu gehen und den Umfang der Teilnahme zu erweitern? Grundsätzlich glauben wir an Letzteres und haben Bitcoin PoS entwickelt, um die Massenbeteiligung zu fördern.

5.3 Bitcoin PoS ist umweltfreundlich

Die Zukunft liegt in unseren Händen. Jeder, der an der Zukunft beteiligt ist, ist es sich auch schuldig, nur an Netzwerken teilzunehmen, die die Auswirkungen umweltschädlicher Technologien wie PoW verstehen.

Daher ist das Bitcoin PoS-Team bestrebt, zunächst bessere Wege für die Blockchain zu finden Bitcoin grün machen. Jahrelang waren die Gewinne, die mit Bitcoin-Spekulationen erzielt wurden, nur grüne Dinge. Jetzt, da es ein Update für das Netzwerk gibt, das den Nachweis von Beteiligungen integriert, können sich Investoren, Spekulanten und Netzwerkteilnehmer gleichermaßen darüber freuen, dass dies eine Form der digitalen Währung ist, die die

Auswirkungen der Blockchain auf die Welt verringert.

Der Grund für den Nachweis von Marc Blinder von der Harvard Business Review beschreibt die umweltfreundliche Qualität des Pfahls in seiner Designqualität:

"Während Bitcoin, Bitcoin Cash und Ethereum für den Betrieb auf energieeffiziente, kryptografische Problemlösungen angewiesen sind, die als„ Proof of Work "bezeichnet werden, verwenden viele neuere Blockchains„ Proof of Stake "-Systeme (PoS), die auf Marktanreizen beruhen. Serverbesitzer auf PoS-Systemen werden als "Validatoren" bezeichnet - nicht als "Miner". Sie hinterlegen eine Einzahlung oder „setzen" eine große Menge an Kryptowährung ein, um das Recht zu erhalten, Blöcke zur Blockchain hinzuzufügen. In Proof of Worksystems konkurrieren Bergleute miteinander, um herauszufinden, wer das Problem am schnellsten lösen kann, und erhalten dafür eine Belohnung, die viel Energie verbraucht. In PoS-Systemen werden Validatoren jedoch durch einen Algorithmus ausgewählt, der ihren „Einsatz" berücksichtigt. Das Entfernen des Wettbewerbselements spart Energie und ermöglicht es jeder Maschine in einem PoS-System, jeweils an einem Problem zu arbeiten, im Gegensatz zu einem Proof of Work-System, bei dem eine Vielzahl von Maschinen das gleiche Problem lösen müssen. Zusätzlich, wenn ein Validator Wenn sie sich nicht ehrlich verhalten, werden sie möglicherweise aus dem Netzwerk entfernt, was dazu beiträgt, dass PoS-Systeme genau bleiben."[15]

Darüber hinaus ist der Nachweis des Einsatzes in seiner Architektur elegant einfach. Anstatt unergründlich komplexe Maschinen zur Lösung eines immer schwieriger werdenden Algorithmus zu benötigen, ist für die Staker nur Skin im Spiel erforderlich - ein Einsatz des Token des Netzwerks, der zur Validierung bereitgestellt wird. Aufgrund der Einfachheit des Nachweises des Einsatzes kann im Vergleich zu komplexeren Systemen weniger schief gehen, und es werden viel weniger Ressourcen benötigt, die die Umwelt belasten.

5.4 Bitcoin PoS ist sicherer gegen 51% Angriffe

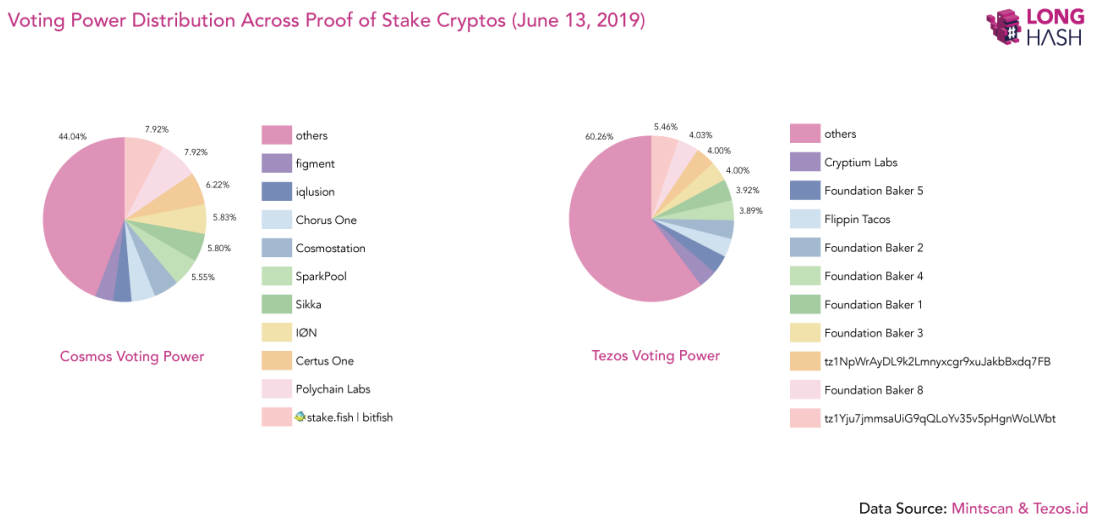
Sicherheit ist das Hauptanliegen von Befürwortern von Kryptowährungen, In-vestoren, Spekulanten und Netzwerken Teilnehmer. Wer möchte wegen eines Systemfehlers alles verlieren?

Bitcoin hat genau diesen Fehler - es wird Zentralisierung genannt. Bergbau schafft ein Paradigma von Zentralisierung, die das Gespenst eines 51% -Angriffs erhöht. Wenn ein sol-cher Angriff stattfinden sollte, das Ganze Das Netzwerk und sein Wert von mehreren Milliarden Dollar wären gefährdet. Es ist sicher zu sagen, dass in einem solchen Umstand wäre das Bitcoin-Netzwerk beendet.

Durch die Umstellung der gesamten aktualisierten Bitcoin-Codebasis auf den Nachweis des Einsatzes wird Bitcoin PoS vermieden die Möglichkeit eines 51% igen Angriffs mit seinem elegant einfachen De-sign. Während ein Angreifer muss Kontrollieren Sie 51% der Netzwerk-Hashrate für Bitcoin, wenn ein Angreifer einen Versuch mit Bitcoin PoS unternommen hat. Sie müssten mindestens 50% der Token-Versorgung des Netzwerks kontrollieren.

Dieser Unterschied ist sehr wichtig zu erkennen. Hashrate kann durch Erstellen konsolidiert werden gemeinsame Interessen der Leiter großer Bergbaukartelle. Token können jedoch nicht von konsolidiert werden die gleiche Anstrengung, da sie auf eine größere Anzahl von Akteuren mit unterschiedlichen Interessen verteilt sind, Ziele und Netzwerkwerte. Der Aufwand, der erforderlich ist, um Token-Inha-ber zum Verkauf oder zur Beitragszahlung zu bewegen Ihr Einsatz wäre unkalkulierbar schwierig, grenzt an Unmögliches und bleibt daher außerhalb des Umfang der Bedrohungen für Bitcoin PoS.

Abstecken von Pools, während dies für die Delegierung von Anteilen und die Verringerung des technischen Wissens von Vorteil ist von einzelnen Stakern gefordert, wurden als mögliche Quellen der Zentrali-sierung innerhalb der Nachweis des Pfahlökosystems. Da für das Abstecken von Pools jedoch keine physische Lagerhaltung erforderlich ist von Token, die eingesetzt werden und lediglich Delegierte des Einsatzes sind, besitzen Sie die Token nicht in einem verkaufsfähigen Format. Dies reduziert wiederum das Risiko von 51% Netzwerkangriffen nicht nur für Bitcoin PoS, sondern für alle Beweise dafür Stake-Netzwerke.



Quelle: Longhash.com

6. Bitcoin PoS-Architektur

Bitcoin PoS verwendet im Kern dieselbe aktualisierte Codebasis wie Bitcoin. Der signifikante Unterschied, ist jedoch der Konsensalgorithmus. Bitcoin PoS verwendet eher einen Einsatznachweis als einen Arbeitsnachweis. zur Konsensbildung.

Es ist wichtig zu beachten, dass Bitcoin PoS keine Bitcoin-Kettengabel ist. Stattdessen ist es ein ursprüngliche Implementierung der Bitcoin-Codebasis mit mehreren Leistungs- und Konsens-Upgrades Dies macht Bitcoin PoS zu einer überlegenen Wahl für Finanzanwendungen wie Zahlungen Verbessern Sie die Skalierbarkeit des Netzwerks erheblich.

Absteckungsvoraussetzungen

Beim Abstecken werden Gelder in einer Kryptowährungsbrieftasche gehalten, um den Betrieb von a zu unterstützen Blockchain-Netzwerk. Im Wesentlichen besteht es darin, Kryptowährungen zu sperren, um Belohnungen zu erhalten.

Die folgenden Voraussetzungen gelten für das Abstecken von BPS:

– Die zu steckenden Münzen müssen gereift sein; Dies bedeutet, dass die nicht ausgegebenen Ausgaben (UTXOs in kurz) muss eine Tiefe in der Hauptkette von mindestens 500 Blöcken haben (das ist die Münzbasis / Co-Aufnahme Reife)

– Die zu steckenden Münzen müssen in kompatiblen Adress- / Transaktionsty-pen vorliegen (bitte überprüfen) entsprechend; Zum Zeitpunkt des Schreibens dieses Dokuments werden nur P2PK und P2PKH unterstützt.

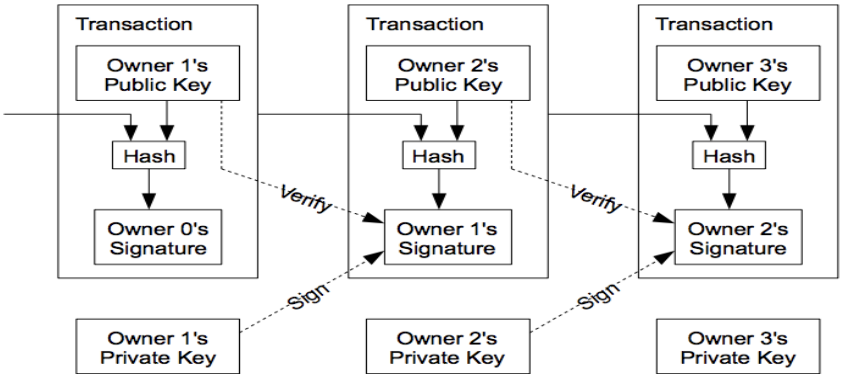
Blockstruktur

Bitcoin PoS verwendet PoS V3 als Konsensalgorithmus. Die Blöcke müssen diese Regeln einhalten:

- Muss genau 1 Abstecktransaktion haben
- Die Abstecktransaktion muss die zweite Transaktion im Block sein
- Die Coinbase-Transaktion muss einen Ausgabewert von 0 und einen einzelnen leeren Vout haben
- Für den Blockzeitstempel müssen die unteren 4 Bits auf 0 gesetzt sein (in der Quelle als "Maske" bezeichnet) Code. Dies bedeutet effektiv, dass die Blockzeit nur in Intervallen von 16 Sekunden dargestellt werden kann.Verringerung der Granularität
- Der Kernel-Hash des Blocks muss die gewichtete Schwierigkeit für PoS er-füllen
- Der Block-Hash muss im zweiten Vout der Abstecktransaktion mit dem öf-fentlichen Schlüssel signiert sein. Das Signaturdaten werden in den Block eingefügt (sind jedoch nicht im formalen Block-Hash enthalten)
- Die im Block gespeicherte Signatur muss "LowS" sein, dh nur aus einem Stück bestehen von Daten und muss so komprimiert wie möglich sein (keine zusätzlichen füh-renden Nullen in den Daten oder andere Opcodes)
- Die meisten anderen Regeln für Standard-PoW-Blöcke gelten (gültiger Merkle-Hash, gültige Transaktionen, Der Zeitstempel liegt innerhalb der zulässigen Zeitdrift usw)

Transaktionen

Bitcoin-PoS-Transaktionen funktionieren wie Bitcoin auf der Grundlage öf-fentlicher und privater Schlüsselsignaturen wobei ein öffentlicher Schlüssel verifiziert und ein privater Schlüssel vom Absender signiert wird.



Bei nicht nachgewiesenen Blockchain-Netzwerken werden doppelte Ausgaben durch das Fehlen von Blockchain-Netzwerken entmutigt Anreiz, jede Gabel abzustecken. Der Nachweis von Stake-Netzwerken wie Bit-coin PoS ist jedoch ein Anreiz jede Gabel stecken. Bedeutet dies, dass die Wahrscheinlichkeit von Transak-tionen mit doppelten Ausgaben in PoS höher ist? Systeme? Die Antwort ist nein.

Das obige Szenario wird allgemein als das Problem „Nichts auf dem Spiel“ bezeichnet - aber es macht fälschlicherweise mehrere drastische Annahmen, die in Wirklichkeit nahezu

unmöglich sind. Am meisten Ungeheuerlich von diesen Annahmen ist, dass jeder Staker jede Gabel stecken wird, wenn die Möglichkeit dazu besteht Das Sammeln von genügend Unterstützung pro Gabel, egal wie weit hergeholt, ist nahezu Null.

Weil ein Angreifer (oder eine Gruppe von Angreifern) massenhaft Anreize für Staker schaffen müsste Unterstützen Sie eine beschädigte Gabel, die Logistik und die Kosten dafür sind unerschwinglich.

Im Bitcoin-Paradigma des Proof-of-Work-Algorithmus ist dies nicht der Fall. Bergbaukartelle gibt es nicht Sie halten delegierte Münzen und vertreten auch nicht einfach die Interes-sen anderer. Sie besitzen ungerechtfertigt große Mengen an Hashrate, die einen Angriff mit doppelten Ausgaben ermöglichen sollte einer dieser interessierenden Köpfe zusammenarbeiten.

Daher sind Bitcoin PoS-Transaktionen währenddessen vor Angriffen mit dop-pelten Ausgaben geschützt Beibehaltung der grundlegenden Bitcoin-Transaktionsinfrastruktur, die Benutzer kennen und genießen.

MPoS-Konsens (Mutualized Proof of Stake)

Der Nachweis von Stake-Consensus-Algorithmen hat viele Formen. Es gibt de-legierte Nachweis des Einsatzes Systeme wie die von EOS verwendeten und BFT PoS-Systeme wie Cosmos. Im Falle der dPoS fügt einer bereits elegant einfachen Prämisse von PoS unangemessene Komplikationen hinzu Netzwerke. Zusätzlich bieten dPoS-Algorithmen die Möglichkeit eines erhöh-ten Netzwerks Zentralisierung und verursachen nicht genügend Kosten für einen Angreifer.

Um die Möglichkeit eines Angreifers, der die Bitcoin PoS-Blockchain stört, weiter zu verhindern, Die Mutualized Proof of Stake-Konsensfunktion wurde implementiert. Kurz ge-sagt, MPoS erstellt eine unglaublich hohe Kostenbarriere für böswillige Akteure - eine, die theoretisch unpassierbar ist

MPoS erklärt

Tore

1. Verhindern Sie, dass böswillige Miner das Netzwerk kostenlos angreifen, indem Sie teure, zu validierende Blöcke erstellen Erhalten Sie alle Gebühren durch den Abbauprozess an sich selbst zurück

2. Helfen Sie dabei, es einem Angreifer schwieriger und teurer zu machen, das Netzwerk zu erledigen

Verfahren

1. Wenn ein Staker einen Block abbaut, erhält er nur einen kleinen Teil der PoS-Belohnung und der Gebühren. Der Rest der Belohnung und Gebühren werden mit 9 anderen Personen geteilt.

2. Wenn ein Staker einen Block abbaut, wird sein Einsatzskript (sta-ketx.vout [0]) registriert, um einen dauerhaften Anteil der Belohnung zu erhalten 10 Blöcke, 500 Blöcke ab dem Zeitpunkt, als der Block abgebaut wurde

3. Somit gibt es in jedem Block 10 Belohnungsempfänger. Der Schöpfer des Blocks und 9 "gegenseitige Staker".

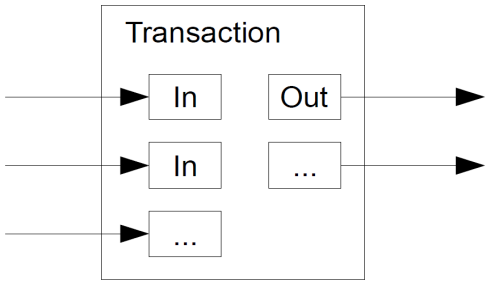
4. Nach 9 Blöcken gemeinsamer Belohnungen wird das Skript des Stakers ent-fernt und ein weiteres hinzugefügt, um es zu ersetzen

5. Wenn ein Einsatzskript in einem Zeitraum von 10 Blöcken mehr als 1 Block abgebaut hat, kann es einen Fall geben, in dem er 2x das erhält Aktie. Sobald jedoch die früheste Pfahlskriptinstanz 510 Blöcke von ihrem abgebauten Block überschreitet, wird sie gelöscht und die Belohnung fällt auf normal. Identische Stake-Skripte sollten nicht zu einem einzigen UTXO kombiniert werden, die Belohnungen sollten es sein dupliziert

Unter MPoS können Angreifer das Bitcoin PoS-Netzwerk nicht mit Gebühren spammen. Stattdessen Netzwerk Alle Teilnehmer teilen sich die Gebühren, anstatt die Gesamtheit der Gebüh-ren, die - wie sie sind - an einen einzelnen Blockersteller gehen normalerweise der Fall. Mit Gebührenbeteiligung und einer ständigen Rota-tion der Staker ist die Substanz hinter einem Spam-Angriff verschwindet. Außerdem, weil der MPoS-Algorithmus bereits war In unserem Testnetzwerk in großem Maßstab eingesetzt, war sein Erfolg bei weit verbreiteter Verwendung bereits bewiesen.

Stake Aggregation

Um Praktiken wie Transaktionsfluten zu eliminieren, durch die ein Staker einen Vorteil erzielen kann Bitcoin PoS setzt auf eine hohe Anzahl von Transaktionen (Fan-Out) und kom-biniert beim Erstellen mehrere Eingaben die Absteckтransaktion (Fan-In), bei der versucht wird, einen größeren Ein-satz für den Block zu schaffen. Um dem Unerwünschten entgegenzuwirken Auswirkungen dieses Eingangsreduzierungsmechanismus, die zu wirklich großen Transanktionsausgängen führen könnten, wenn Der Einsatz liegt über einem bestimmten Schwellenwert und wird ebenfalls in mehrere Outputs aufgeteilt.



Bitcoin PoS-Zahlungen

Von den vielen Anwendungsfällen, die für Kryptowährungen vorherrschen, ist der größte und gefragteste immer noch Zahlungen. Die Welt geht langsam aber sicher in eine papierlose Realität über, in der digital Zahlungen mit ähnlich digitalen Währungen sind König - nicht Bargeld.

Bitcoin hat den Weg für diese Realität frei gemacht, ist jedoch in mehreren Hauptkategorien gestolpert.

1. Bitcoin kann nicht auf die Bedürfnisse von Millionen oder Milliarden von Nutzern weltweit skaliert werden.

2. Bitcoin kann nicht einfach in vorhandene Zahlungsschienen und POS-Geräte integriert werden.

3. Bitcoin-Bestätigungen dauern viel zu lange und sind daher für Zahlungen in Echtzeit ineffizient.

Während einige Lösungen, wie das Lightning Network, vorgeschlagen und bear-beitet wurden, Sie fehlen noch im Raum und haben eigene Adoptionsprobleme.

Bitcoin PoS bietet im Zahlungsbereich mehrere Vorteile. Es ist ausdrücklich für

Integration in vorhandene Zahlungssysteme, Netzwerke und POS-Geräte für nahtloses Bargeld Krypto-Erfahrung. Dieser Übergang wird durch kluge Designfaktoren unter-stützt.

1. Die geringe Blockgröße von Bitcoin-Systemen ist eine Skalierungspflicht. Nachweis von Pfahlblockketten Bitcoin PoS reduziert die Blockzeiten, um mehr Transaktionen pro Sekunde zu verarbeiten, und macht sie so schnell genug, um die Geschwindigkeit des Echtzeitgeschäfts zu bewältigen.

2. Die Blockfinalität in Bitcoin PoS wurde gegenüber Bitcoin verbessert, was einen großen Vorteil schafft für Einzelhändler und Einzelhandelsnutzer, da Zahlungen fast sofort und endgültig abgewickelt werden.

3. Während Proof-of-Work-Skalierungslösungen die Netzwerkaktivität von der Hauptkette auf und ab bringen Seitenketten, Bitcoin PoS-Funktionen mit hohem Durchsatz bedeuten, dass die Skalierung in derselben Kette erfolgt ohne sich auf Lösungen von Drittanbietern verlassen zu müssen.

Bitcoin PoS Münzversorgung

Bitcoin PoS soll nicht mit Bitcoin konkurrieren. Stattdessen soll es Bit-coin aufgrund ersetzen Sein überlegener Konsensalgorithmus, leicht erleichterte Zahlungen und stark reduzierte Leistung Verbrauchsanforderungen.

Angesichts dieser Designziele ist es wichtig, die Bitcoin-Münzversorgung strikt einzuhalten Grundlagen, da Bitcoin PoS auf eine strikte Einhaltung der ursprünglichen Vision von Satoshi Nakamoto drängt einer bargeldlosen, banklosen und freien finanziellen Erfahrung von Drit-ten.

Maximaler Münzvorrat — 21 Millionen Bitcoin PoS (BPS)

Bitcoin PoS Block Zeit

Der Zeitabstand für den Bitcoin PoS-Block ist auf 3 Minuten festgelegt, so-dass er nicht nur mehr als dreimal beträgt schneller als Bitcoin, aber auch in der Lage, mehr als die dreifache Anzahl von Transaktionen abzuwickeln. Das Die Blockschwierigkeit wird unter Verwendung eines Algorithmus berechnet, der auf exponentiellen Anpassungen beruht Der Schwierigkeitsgrad wird bei jedem Block angepasst. Die Verwendung die-ses Algorithmus macht Blockzeiten vorhersehbarer und weniger anfällig für große Spitzen.

Bitcoin PoS Block Belohnungen

Die Bitcoin PoS-Emissionsrate ähnelt der von Bitcoin, mit dem Hauptunter-schied Token werden von Stakern geprägt und die Reduktionsrate beträgt 25% alle 700.000 Blöcke, beginnend mit dem Block 120k, der alle 4 Jahre auftritt.

Die Belohnungen für die Blöcke bis zu 120.000 werden folgendermaßen aufge-teilt:

- Blöcke 0 bis 40000 haben eine Belohnung von 50 BPS
- Blöcke 40000 bis 80000 haben eine Belohnung von 25 BPS
- Blöcke 80000 bis 120000 haben eine Belohnung von 12,5 BPS

Bei Block 120001 werden die BPS- und Bitcoin-Belohnung / der Bitcoin-Block bei 6,25 BPS ausgerichtet.

Die Blöcke von 0 bis 5000 sind ein Beweis für Arbeitsblöcke, die von den Entwicklern festgelegt wurden. Diese Es werden Mittel für die weitere Entwicklung und Wartung von Bitcoin PoS bereitgestellt.

Abgesehen von unter der Haube liegenden Unterschieden in Bezug auf Konsens-bildung und einem enormen Verbesserte Leistung, das Erscheinungsbild von Bitcoin PoS ist Bitcoin auf-fallend ähnlich und wird es auch Machen Sie den Übergang für Bitcoin-Benutzer einfach.

Der Nachweis des Einsatzes bietet den Einsatzkräften Belohnungen entspre-chend der Einsatzgröße. Genau wie beim Bitcoin-Proof von Work Mining, wo Belohnungen an den Bergmann gehen, der den Block löst (bekannt als Blockbelohnungen), Bitcoin PoS-Belohnungen gehen ebenfalls an den Staker, werden jedoch in 10 gleiche Belohnungen aufgeteilt (unter Verwendung des MPOS) Algorithmus; Die Chance, einen Block zu prägen, ist proportional zur Ein-satzgröße, dh je höher Je höher der Einsatz, desto höher ist die Chance, dass der Staker einen Block vor allen anderen prägt.

Bitcoin PoS erhebt Gebühren aus Transaktionen und verwendet die Gebührenbe-träge, um Staker zu belohnen die Aktivität der Sicherung / Validierung des Netzwerks.

Quelle: Ledger Academy

Der Nachweis des Work Mining erfordert unermüdliches Engagement, Energie-aufwand und einen hohen Start Kapital für die Investition von Hardware und technischem Wissen. Bitcoin PoS hingegen kann sein im Hintergrund anderer Aufgaben eingesetzt, so dass Sie die Möglichkeit ha-ben, passives Einkommen als Staker.

References

[1] https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[2] https://www.eia.gov/energyexplained/electricity/prices-and-factors-affecting-prices.php

[3] https://bitcoin.org/bitcoin.pdf

[4] https://www.forbes.com/sites/youngjoseph/2019/12/12/new-report-shows-china-dominates-bitcoin-mining-is-this-a-sign-of-worry/

[5] https://bitcoinmagazine.com/articles/op-ed-challenge-mining-centralization-unveils-bitcoins-elegant-design

[6] https://cointelegraph.com/news/bitmain-hits-15-billion-valuation-with-recent-backing-from-ubers-largest-shareholder

[7] https://cryptobriefing.com/bitcoin-mining-centralization-record-levels-majority-china/

[8] Ibid.

[9] https://www.nature.com/articles/s41558-018-0321-8

[10] https://www.forbes.com/sites/andreamorris/2018/10/29/bitcoin-predicted-to-be-the-nail-in-the-coffin-of-climate-change/#47a1917e745e

[11] https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison

[12] https://www.binance.vision/security/what-is-a-51-percent-attack

[13] https://cointelegraph.com/news/the-dangers-of-mining-pools-centralization-and-security-issues

[14] https://bitcoinist.com/ethereum-pos-blockchain-cut-energy/

[15] https://hbr.org/2018/11/making-cryptocurrency-more-environmentally-sustainable