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

ABSTIMMUNGEN IN DER ÖFFENTLICHEN BLOCKCHAIN

Version 1.0 vom 15.12.2018
Alexander Marsalek – Alexander.Marsalek@a-sit.at

Zusammenfassung: Dieses Dokument beschreibt verschiedene Abstimmungsverfahren für öffentliche Blockchain-basierte Systeme. Die Verfahren werden nach den Stimmgewichtungsverfahren gruppiert vorgestellt. Konkret werden Stimmgewichtungsverfahren nach Kapital, Rechenleistung und „Coin Days Destroyed“ behandelt. Im Anschluss werden die Verfahren verglichen und ein Fazit gezogen.

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument beschreibt verschiedene Abstimmungs- und Signalisierungsverfahren für öffentliche Blockchain-basierte Systemen. Dabei handelt es sich nicht um Wahlen im rechtlichen Sinn. Insbesondere gelten andere Grundsätze, da nicht jede Wählerin bzw. jeder Wähler zwangsweise nur über eine Stimme verfügt und auch nicht jede Stimme den gleichen Einfluss auf das Wahlergebnis haben muss bzw. soll. Zusätzlich handelt es sich zumeist nicht um geheime Wahlen. Stattdessen werden Stimmen je nach Verfahren mit der Kapitaleinlage gewichtet, oder basierend auf der vorhandenen Rechenleistung ausgegeben. Ein Vergleich mit rechtlichen Wählen macht daher wenig Sinn. Stattdessen geht es bei den vorgestellten Verfahren um Möglichkeiten über die Zukunft des jeweiligen Systems abzustimmen. Im nächsten Abschnitt wird das notwendige Hintergrundwissen vermittelt. Abschnitt 3 vergleicht die verschiedenen Verfahren und Abschnitt 4 liefert ein Fazit.

2. Hintergrund-Wissen

Bei einer Blockchain handelt es sich um eine kryptografisch verkettete Liste von Datensätzen mit eindeutiger Reihenfolge. Diese Datensätze werden in Blöcken gespeichert. Neben den Nutzdaten enthält jeder Block auch eine Referenz zum vorherigen Block sowie andere nützliche Informationen wie einen Zeitstempel oder Daten, die die Gültigkeit des Blocks bestätigen. Die Blockchain wurde 2008 von Satoshi Nakamoto als verteilte Datenbank im White Paper zur Kryptowährung Bitcoin beschrieben [1]. Bei Bitcoin wird die Blockchain zur Speicherung aller Transaktionen verwendet. Dadurch kann beispielsweise verhindert werden, dass die selben Währungseinheiten mehrfach ausgegeben werden (*Double Spending*). Bei Bitcoin muss ein Rätsel gelöst werden, um einen neuen Block erstellen zu können. Der Schwierigkeitsgrad des Rätsels wird alle 2016 Blöcke (ca. alle zwei Wochen) angepasst, mit dem Ziel eines mittleren Blockerstellungsintervalls von 10 Minuten. Die Lösung des Rätsels dient als Proof-of-Work. Der Proof-of-Work dient einerseits als Schutz gegen Veränderungen und Manipulationen der Blockchain und wird andererseits benötigt, damit mehrere verschiedene Parteien, die sich nicht kennen oder vertrauen müssen, ein gemeinsames Ziel erreichen können. Des Weiteren kann mittels des Konsensus-Algorithmus und dem Proof-of-Work die derzeit gültige Kette ermitteln werden. Bei Proof-of-Work stellt jeder Teilnehmer, auch Miner genannt, seine Rechenleistung zur Verfügung. Als Belohnung bekommt der Miner, dessen Block vom Netzwerk akzeptiert wird, neue Währungseinheiten ausgeschüttet. Es gibt jedoch inzwischen auch andere Konsensus-Algorithmen die das gleiche Ziel verfolgen, aber deutlich weniger Rechenleistung benötigen. Ein Beispiel hierfür ist Proof-of-Stake, wo jeder Teilnehmer einen Teil des eigenen Kapitals als „Pfand“ hinterlegt. Abbildung 1 zeigt eine simple Blockchain.

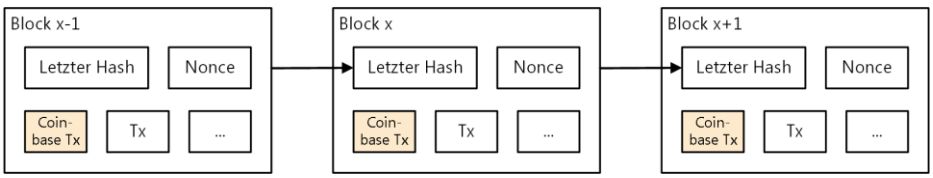

Abbildung 1: Blockchain: Eine Kette bestehend aus mehreren Blöcken (von links nach rechts gezeichnet).

Durch die Verkettung erhält man neben einer eindeutigen Reihenfolge der Blöcke auch noch weitere Eigenschaften wie einen gewissen Schutz vor Manipulationen. Um eine Transaktion oder einen Block zu entfernen, müsste ein Angreifer bzw. eine Angreiferin auch alle danach folgenden Blöcke neuberechnen, da die ehrlichen Teilnehmer im Netzwerk immer diejenige Kette, die den größten akkumulierten Proof-of-Work enthält, als gültig werten und diese Kette erweitern versuchen. Im nächsten Abschnitt wird der Sinn und die Funktionsweise von Bitcoin Improvement Proposals vorgestellt.

2.1. Bitcoin Improvement Proposal

Bei einem *Bitcoin Improvement Proposal*, kurz BIP handelt es sich um ein Dokument für die Bitcoin Community, welches Informationen zu neuen Features enthält. Diese Features können Bitcoin

direkt, dessen Prozesse oder auch die Umgebung betreffen. Ein BIP sollte eine möglichst präzise technische Spezifikation enthalten. Technisch gesehen handelt es sich bei einem BIP um eine Textdatei, die versioniert gespeichert wird. Dadurch werden alle Änderungen nachvollziehbar dokumentiert.
Der Prozess von BIPs wurde im BIP 1 [2] spezifiziert und im BIP 2 [3] noch einmal verbessert. BIP 2 definiert, dass jedes BIP mit einer neuen Idee beginnen soll und das pro BIP ein Hauptverantwortlicher definiert werden sollte. Dieser Hauptverantwortliche erstellt das Dokument entsprechend der Regeln und kümmert sich um Diskussionen und probiert eine Einigung innerhalb der Community zu erreichen.

BIP 2 spezifiziert die folgenden drei Arten [3] [4]:

- **Standard Track:** Diese Art von BIP betrifft die meisten oder alle Implementierungen von Bitcoin. Beispiele sind Änderungen am Netzwerkprotokoll, in den Validierungsregeln von Blöcken oder Transaktionen, sowie alle anderen Änderungen, welche die Interoperabilität betreffen. Diese Art von BIP benötigt eine Referenz-Implementierung. BIP 91 [5] ist ein Beispiel für ein Standard Track BIP.
- **Informational**: Diese Art von BIP beschreibt Design Probleme oder generelle Anleitungen oder Informationen für die Bitcoin Community, aber beschreibt kein neues Feature. Diese Art von BIP benötigt keine Mehrheit und kann von Benutzern und Benutzerinnen sowie von Entwicklerinnen und Entwicklern ignoriert werden. BIP 32 [6] ist ein Beispiel für dies Art von BIP.
- **Process**: Diese Art von BIP beschreibt einen Bitcoin-Prozess oder schlägt eine Änderung eines Bitcoin-Prozesses vor. Diese Art von BIPs ähnelt den *Standard Track* BIPs, betrifft aber nicht das Bitcoin Protokoll direkt. Beispiele sind Änderungen an den Werkzeugen oder Umgebungen die in der Bitcoin-Entwicklung benutzt werden. BIP 2 [3] ist ein Beispiel für ein Process-BIP.

Bevor ein BIP einreicht wird, sollte abgeklärt werden, ob es schon ältere ähnliche oder gleiche BIPs gibt. Falls es sich um eine neue Idee handelt, wird im nächsten Schritt die Bitcoin Community (per Mailinglisten bzw. in Foren) befragt, ob die Idee eine Chance hat, akzeptiert zu werden. Dadurch wird verhindert, dass unnötig Zeit in eine Idee investiert wird, welche keine Chance auf Akzeptanz hat. Dazu gehören beispielsweise Ideen, die die Grundannahmen von Bitcoin, wie Dezentralisierung oder 21 Millionen Währungseinheiten, verändern wollen. Des Weiteren werden in diesem Schritt auch Ideen aussortiert, die nur für den Autor oder eine sehr kleine Menge von Benutzerinnen und Benutzern relevant ist. Hat die Idee eine Chance, wird sie entsprechend des definierten *BIP Formats* niedergeschrieben und der Hauptverantwortliche stellt eine „git push“-Anfrage an den *BIP Editor*. Bei „git“ handelt es sich um eine Software zur Versionsverwaltung von Dateien, wodurch alle Änderungen nachvollziehbar dokumentiert werden.
Der *BIP Editor* kontrolliert, ob die vorherigen Schritte eingehalten wurden und vergibt anschließend eine BIP Nummer und ordnet das BIP einem Track zu. Derzeit ist Luke Dashir der BIP Editor.
Das BIP Format definiert Regeln und Strukturen, an die sich ein BIP halten muss. Beispielsweise muss ein BIP im MediaWiki-Format [7] geschrieben sein und folgende Struktur aufweisen:

- **BIP Kopf**: Der Kopf enthält Metainformationen über das BIP.
- **Abstract**: Eine kurze, ca. 200 Wörter lange, Beschreibung über das technische Problem.
- **Copyright**: Jedes BIP muss ein Lizenzmodel definieren. Empfohlen werden die folgenden Modelle: BSD-2, BSD-3, CC0-1.0 oder GNU-All-Permissive. Eine Liste der akzeptierten und nicht akzeptablen Lizenzen Modellen gibt es in BIP 2 [3].
- **Spezifikation**: Dieser Abschnitt soll die technischen Details enthalten. Diese müssen genau genug sein, um eine interoperable Implementierung zu ermöglichen.
- **Motivation**: Dieser Abschnitt motiviert, warum die vorgeschlagene Änderung notwendig ist.
- **Begründung**: In diesem Abschnitt werden Design-Entscheidungen und alternative Designs erklärt. Des Weiteren sollen hier wichtige Diskussionspunkte mit der Community angeführt werden und bewiesen werden, dass die Community einen Konsens gefunden hat.
- **Rückwärts-Komptabilität**: Alle BIPs, die Änderungen vorschlagen, welche nicht abwärtskompatibel sind, müssen in diesem Abschnitt die Inkompatibilitäten angeben, deren Auswirkungen bewerten, sowie angeben, wie mit diesen Problemen umgegangen wird.

- **Referenz-Implementierung**: Bevor ein BIP den Status „Final“ erreichen kann, muss es eine Referenz-Implementierung geben. Zudem muss es eine Dokumentation und Testfälle für die finale Implementierung geben.

Danach können Miner Ihre Unterstützung für BIPs signalisieren bzw. für dessen Umsetzung abstimmen. Es gibt verschiedene Definitionen, wann eine Wahl gewonnen wurde, beispielsweise wird oft 55% als Mehrheit gesehen [8] [9]. Je nach BIP und BIP Art sind auch oft höhere Zustimmungswerte notwendig um eine Aufteilung des Netzwerkes zu verhindern. Es wird beispielsweise zwischen „Soft Forks“ und „Hard Forks“ unterschieden. Bei „Soft Forks“ werden die Regeln für gültige Transaktionen oder Blöcke strenger. Ein Beispiel wäre die Verkleinerung der maximalen Blockgröße. „Soft Forks“ sind abwärtskompatibel, d.h. auch ältere Softwareversionen erkennen Blöcke bzw. Transaktionen die nach den neuen „Soft Fork“-Regeln erstellt wurden als gültig an. „Hard Forks“ hingegen weichen die bisherigen Regeln auf. Ein Beispiel wäre die Vergrößerung der maximal erlaubten Blockgröße. „Hard Forks“ sind nicht abwärtskompatibel, d.h. es müssen alle oder zumindest ein hoher Anteil der Teilnehmer die neue Softwareversion verwenden, um eine Aufteilung der Blockchain in zwei Ketten zu verhindern. Im nächsten Abschnitt werden verschiedene Abstimmungsmöglichkeiten vorgestellt.

3. Abstimmungen in der öffentlichen Blockchain

Abstimmungsverfahren in Blockchains können verschieden gruppiert werden, beispielsweise basierend auf dem Stimmgewichtungsverfahren oder ob die Stimmen direkt in der Blockchain abgegeben werden und dadurch auch eine Durchsetzung mittels Konsensus-Algorithmus möglich ist oder ob die Stimmen mittels einer externen Lösung gesammelt und ausgewertet werden. In diesem Dokument werden die Ansätze basierend auf dem Stimmgewichtungsverfahren gruppiert und erklärt.

3.1. Gewichtung nach Kryptowährungskapital

Bei diesem Ansatz dürfen alle Teilnehmerinnen bzw. Teilnehmer abstimmen, welche Währungseinheiten in der jeweiligen Kryptowährung kontrollieren bzw. besitzen. Abgegebene Stimmen werden bei diesem Verfahren mit dem hinterlegten Kapital gewichtet. Beispiele für diesen Ansatz sind Bitcoinocracy [10] und DECENT Voting. Diese beiden Ansätze werden in den nächsten Abschnitten vorgestellt.

3.1.1. Bitcoinocracy

Bei Bitcoinocracy kann jede Teilnehmerin bzw. jeder Teilnehmer die oder der Bitcoin Cash hält, abstimmen. Bitcoinocracy will eine transparente Abstimmungslösung bieten, welche dabei helfen soll, dezentrale Entscheidungen im Hinblick auf Veränderungen im Bitcoin Eco-System zu bilden. Da abgegebene Stimmen mit dem dahinterstehenden Kapital gewichtet werden, ergeben sich Entscheidungen, die mittels Geld „gesichert“ sind. Technisch gesehen unterschreiben Wählerinnen und Wähler definierte Aussagen mit ihrem privaten Wallet-Schlüssel. Im Falle der Zustimmung wird der Präfix „I believe that“, zu Deutsch „Ich glaube, dass“ vor die Aussage gestellt. Um gegen eine Aussage zu stimmen, muss der Präfix „I doubt that“, zu Deutsch, „Ich bezweifle, dass“ vor die Aussage gestellt werden. Anschließend muss die unterschriebene Aussage noch an Bitcoinocracy übermittelt werden. Dies kann direkt auf der Bitcoinocracy-Homepage mittels kopieren und einfügen erledigt werden. Es ist nicht direkt möglich nur mit einem Teil des Kapitals abzustimmen. Dies kann jedoch indirekt erreicht werden, indem das Kapital auf verschiedene Adressen aufgeteilt wird. Abbildung 2 zeigt einen Auszug, der derzeit populären Abstimmungen.

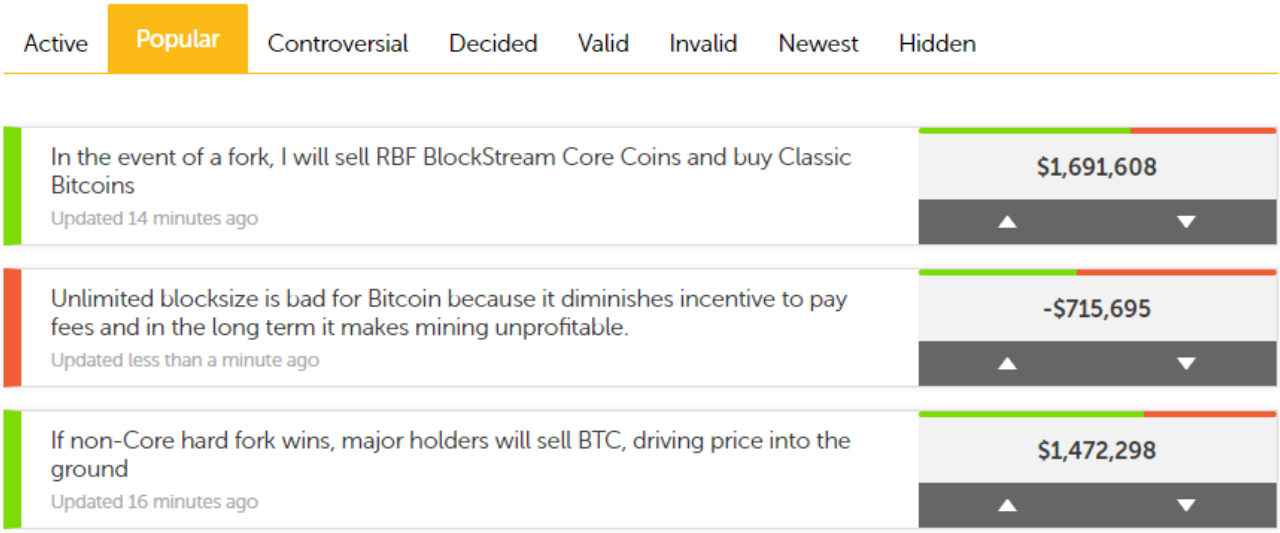

Abbildung 2: Populäre Abstimmungen auf Bitcoinocracy.

Abbildung 3 zeigt das Formular zur Stimmabgabe. Durch einen Klick auf „Agree“ oder „Doubt“ wird die zu unterschreibende Aussage vorbereitet und muss anschließend nur noch signiert und abgeschickt werden.

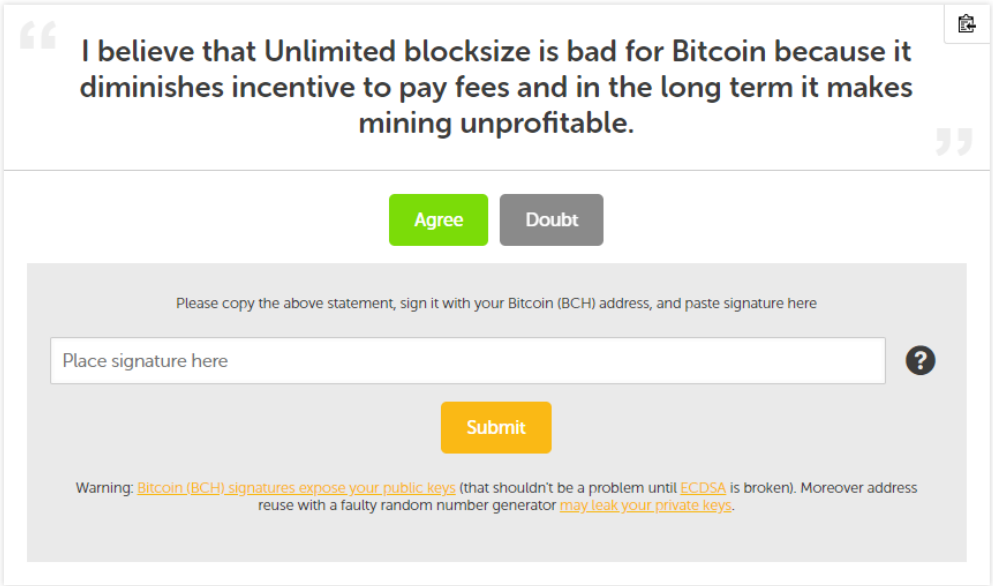

Abbildung 3: Stimmabgabeformular bei Bitcoinocracy.

Abbildung 4 zeigt einen Auszug der abgegebenen (pseudoanonymen) Stimmen. Durch einen Klick auf das Info-Symbol kann die dazugehörige Signatur angezeigt werden. Alternativ bietet Bitcoinocracy die Liste auch im JSON-Format an, wodurch die automatische Auswertung erheblich erleichtert wird.

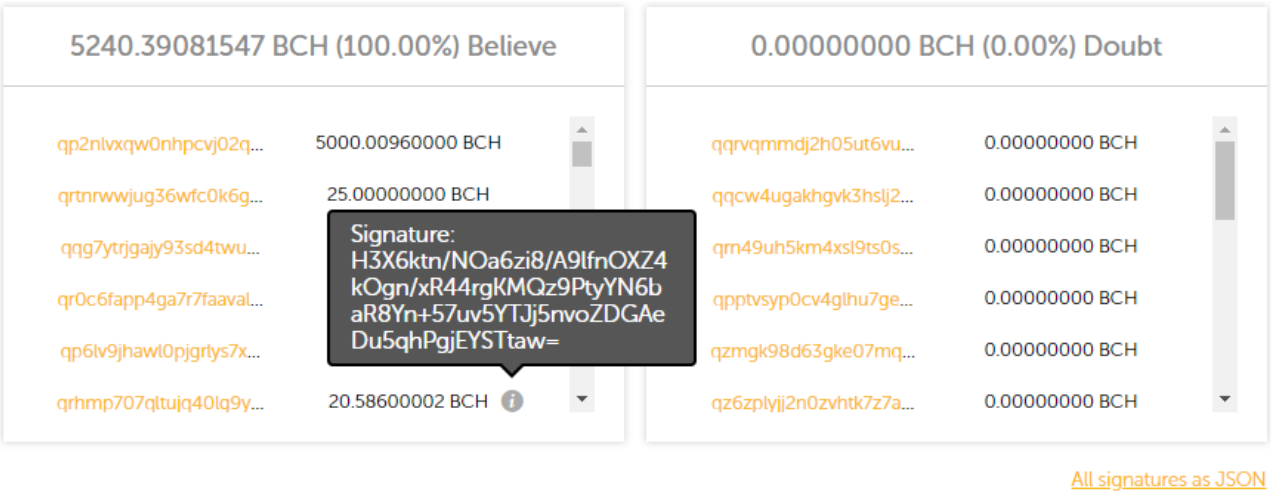

Abbildung 4: Abgegebene Stimmen.

Bei dieser Implementierung handelt es sich um eine informative Wahl, d.h. das Ergebnis hat keine direkte Auswirkung auf die Blockchain und wird auch nicht vom Konsensus-Algorithmus durchgesetzt.

3.1.2. DECENT Voting

Bei DECENT handelt es sich, nach eigenen Angaben, um ein fortgeschrittenes Blockchain Ecosystem. DECENT [11] verwendet einen Delegated Proof-of-Stake (DPOS) [12] Konsensus Algorithmus. Generell hat bei DPOS basierten Systemen jede Halterin bzw. jeder Halter von Währungseinheiten ein Stimmrecht. Im Falle von DECENT werden hierfür sogenannte DCT-Token benötigt. Die Miner heißen bei DECENT Zeugen. Die Zeugen können, ähnlich wie bei herkömmlichen Wahlen, ein Dokument erstellen, in dem sie Ihre bisherigen Leistungen, Ziele und Versprechen darlegen. Basierend auf diesem Dokument und den bisherigen Aktionen der Zeugen können alle Token-Besitzerinnen und Besitzer sich ihren Favoriten oder ihre Favoriten auswählen und für ihn oder für sie stimmen. Die Stimme wird mit dem hinterlegten Kapital gewichtet. Es ist nicht möglich, die Stimme aufzusplittern, stattdessen erhält jeder Favorit das gesamte Stimmgewicht. Alle 24 Stunden werden die Stimmen ausgewertet und die 33 Zeugen mit den meisten Stimmen dürfen dann eingehende Transaktionen validieren und in Blöcke aufnehmen. Unter https://voting.decent.ch/ sieht man die Zeugen sowie die Anzahl der für sie abgegebenen Stimmen. Abbildung 5 zeigt die fünf Zeugen mit den meisten Stimmen. Bei einem aktuellen Kurs von ca. 0,13 USD pro DCT hat der derzeit führende Miner ungefähr Stimmen im „Wert“ von 495000 USD bekommen, was ungefähr 7% der Marktkapitalisierung entspricht.

Miner	Link to proposal	Votes (Represented in DCT)
roelandp ●	Proposal	3,685,203 DCT
bigone ●		3,525,635 DCT
jvper ●	Proposal	3,515,294 DCT
decent ●		3,515,210 DCT
bitcoiner ●		3,481,917 DCT

Abbildung 5: Auszug der fünf Miner mit den meisten Stimmen. (Stand 19.11.2018)

Im nächsten Abschnitt wird das sogenannte „Coin Days Destroyed“-Gewichtungsverfahren beschrieben.

3.2. Gewichtung nach „Coin Days Destroyed“

Bei „Coin Days Destroyed“ werden abgegebene Stimmen nicht mit dem hinterlegten Kapital gewichtet, sondern mit dem Produkt aus dem überwiesenen Kapital und der Anzahl der Tage, die das Kapital nicht bewegt wurde. Dadurch kann beispielsweise verhindert werden, dass sich Teilnehmer kurz vor einer Wahl größere Mengen an Währungseinheiten kaufen, um eine Wahl zu beeinflussen und anschließend die Währungseinheiten gleich wieder abstoßen. Dieses Vorgehen ist zwar nach wie vor möglich, allerdings hat die abgegebene Stimme ein geringeres Gewicht.
Die Idee hinter dem Verfahren ist, wie auch bei Gewichtung nach Kapital, dass Teilnehmer, die mehr ins System investiert haben, mehr Stimmrechte haben als andere. Zusätzlich wird hier noch das „Alter“ der Tokens berücksichtigt. Ursprünglich wurde „Coin Days Destroyed“, bzw. im Fall von Bitcoin „Bitcoin Days Destroyed“ als alternative Maßeinheit fürs Transaktionsvolumen entworfen. Diese Maßeinheit verhindert, dass einzelne Teilnehmer das Transaktionsvolumen künstlich vergrößern können, indem sie Währungseinheiten zwischen ihren eigenen Adressen verschieben.
„Coin Days Destroyed“ wurde vom Bitcoin Core Entwickler Peter Todd [13] als Gewichtungsfaktor für Stimmen vorgeschlagen. Bisher scheint dieser Ansatz aber noch nicht umgesetzt worden zu sein.
Abbildung 6 zeigt die „Coin Days Destroyed“ für Bitcoin und Bitcoin Cash über einen Zeitraum von 30 Tagen.

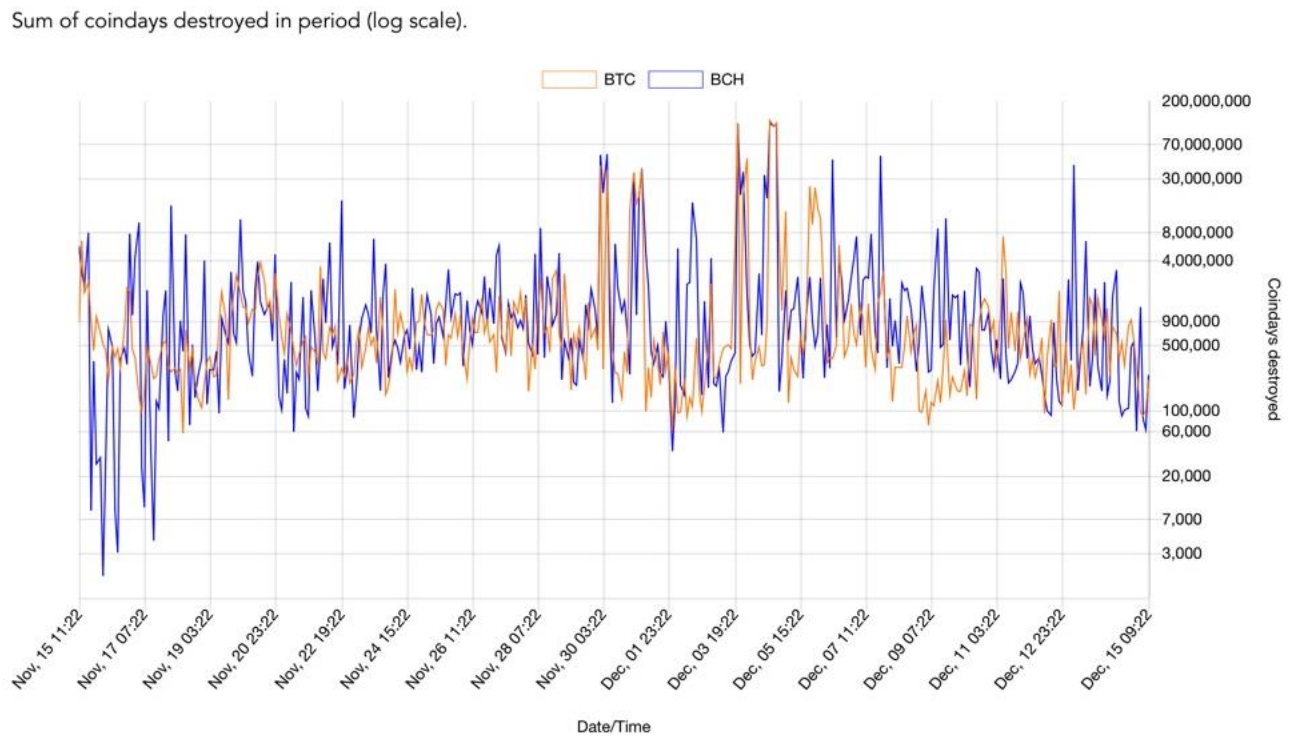

Abbildung 6: Coin Days Destroyed Chart für Bitcoin und Bitcoin Cash.

3.3. Rechenleistung basierte Stimmrechte

Bei diesem Verfahren kann jeder Miner pro erstelltem Block in einer Proof-of-Work-basierten Kryptowährung eine Stimme zu einem Thema abgeben. Da die Wahrscheinlichkeit das Blockrätsel zu lösen mit der vorhandenen Rechenleistung steigt, erhält statistisch gesehen jeder Miner Stimmrechte proportional zu dessen Rechenleistung im Netzwerk. Im Folgenden wird diese Abstimmungsart anhand von Bitcoin erklärt.

3.3.1. Bitcoin Miner Voting

In Bitcoin werden sogenannte Bitcoin Improvement Proposals (BIPs) erstellt und anschließend können Miner ihre Zustimmung signalisieren. BIP 9 legte den Grundstein für Abstimmungen auf der Blockchain.

BIP 9 [14] schlägt vor, das Versions-Feld als Bit-Vektor zu interpretieren, wodurch zeitgleich über mehrere Soft-Fork-Änderungsvorschläge abgestimmt werden kann. Durch Einschränkungen von BIP 34, BIP 65 und BIP 66 sowie einer Fixierung der ersten drei Bits auf „001“ ergibt sich eine Limitierung auf maximal 29 gleichzeitige Abstimmungen. Blöcke, deren Versions-Feld, als Bit-String interpretiert, nicht mit „001“ beginnen, werden für Wahlen nach BIP 9 ignoriert. Des Weiteren definiert BIP 9, dass jeder Soft-Fork von folgenden Parametern definiert wird:

- **Name**: Der Name soll einzigartig sein, damit Soft-Forks eindeutig identifizierbar sind und es zu keinen Verwechslungen kommt. Es wird vorgeschlagen, „bipN“ als Name zu verwenden, wobei „N“ für die BIP Nummer steht.
- **Bit**: Das Bit gibt an, welches der 29 möglichen Bits dieser Abstimmung zugeordnet ist. Im Wahlzeitraum muss dieses Bit eindeutig einem Soft-Fork zuordenbar sein.
- **Startzeitpunkt**: Dieser Zeitpunkt definiert die minimale Median-Blockzeit, ab der das zuvor definierte Bit diesem Abstimmungsvorgang zugeordnet ist. Der Startzeitpunkt sollte ungefähr ein Monat, nachdem die Software mit der Soft-Fork Unterstützung veröffentlicht wurde, angesetzt werden und selbstverständlich in der Zukunft liegen.
- **Timeout**: Dieser Zeitpunkt gibt an, ab welchem Zeitpunkt ein Soft-Fork als fehlgeschlagen gilt, falls davor nicht der Status „LOCKED_IN“ erreicht wurde. Der Status LOCKED_IN“ wird erreicht, falls mehr als 1916 Blöcke (95% von 2016 Blöcken in einer Periode) Unterstützung signalisieren. Das Timeout sollte ein Jahr nach dem Startzeitpunkt liegen.

Abbildung 7 zeigt die Anzahl der abgegebenen Stimmen zum Thema Blockgröße, im Zeitraum Anfang 2015 bis Ende 2017. Es ist zu erkennen, dass die überwiegende Mehrheit der Blöcke keine Stimme enthalten. Des Weiteren verändert sich das Stimmabgabeverhalten mit der Zeit.

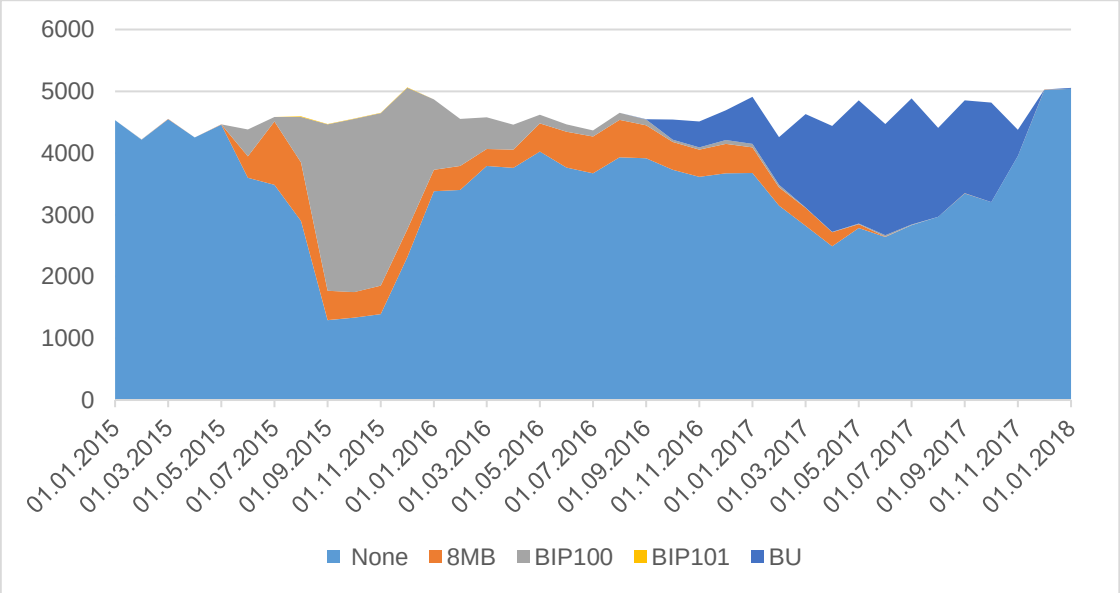

Abbildung 7: Anzahl der abgegebenen Stimmen zur Blockgröße. Quelle: [15]

Abbildung 8 zeigt die Anteile der Blöcke, die im Zeitraum Dezember 2016 bis Dezember 2017, Segregated Witness, kurz SegWit, Unterstützung signalisiert haben.

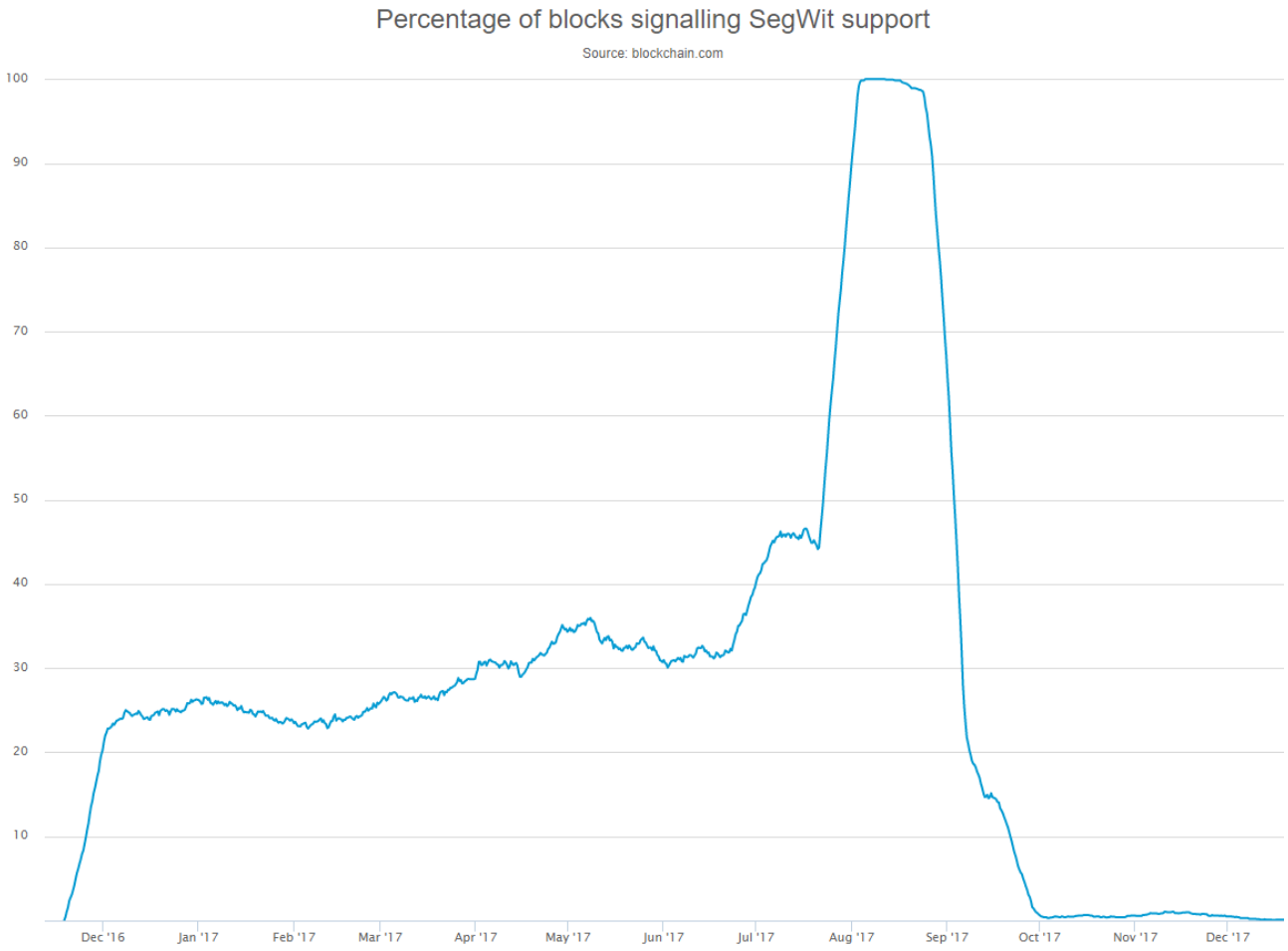

Abbildung 8: Prozent der Blocke die SegWit Unterstützung signalisieren. Quelle: [16]

Ein Nachteil beim Miner Voting ist, dass nicht alle Teilnehmer ein direktes Stimmrecht haben. Stattdessen können nur Miner wählen bzw. einen Pool unterstützen der ihre Meinung vertritt. Es ist umstritten, ob BIP 9 als Voting-Mechanismus gedacht ist bzw. war [17]. Im nächsten Abschnitt wird ein Fazit gezogen.

4. Fazit

Dieser Bericht gibt einen Überblick über verschiedenen Abstimmungsverfahren für Blockchain-basierte Systeme. Bei diesen Systemen kommen andere Stimmgewichtungsverfahren zum Einsatz, als in demokratischen Wahlen. Beispielsweise können Stimmen nach dem Kapital oder nach der vorhandenen Rechenleistung der Teilnehmerin bzw. des Teilnehmers gewichtet werden. Bei keinem dieser Verfahren kommt der Ansatz „eine Person – eine Stimme“ zum Einsatz. Des Weiteren unterstützen die vorgestellten Blockchain-basierten Abstimmungsverfahren keine geheimen Wahlen. Stattdessen werden Stimmen entweder pseudoanonym oder gleich öffentlich abgegeben. Aus diesen und anderen Gründen eignen sich diese Verfahren nicht für öffentliche Wahlen. Auch gibt es im Umfeld von Blockchain-basierten Systemen Kritik, da je nach Stimmgewichtungsverfahren verschiedenen Teilnehmer diskriminiert werden. So haben beispielsweise bei Gewichtung nach Rechenleistung normale Benutzerinnen und Benutzer, Händlerinnen und Händler sowie Tauschstellen kein aktives Stimmrecht. Bei Gewichtung nach Kapital oder nach Coin Days Destroyed haben hingegen alle Teilnehmerinnen und Teilnehmer ein Stimmrecht. Jedoch zählen nicht alle Stimmen gleich. Stimmen von kapitalstarken Teilnehmerinnen und Teilnehmern werden zum Nachteil kapitalschwächerer Teilnehmer stärker berücksichtigt. Es ist jedoch davon auszugehen, dass weiterhin aktiv in diese Richtung geforscht wird und bessere bzw. fairere Abstimmungssysteme entwickelt werden.

Referenzen

[1] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Zugriff am 02 03 2018].

[2] A. Taaki, „BIP 1 - BIP Purpose and Guidelines," [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki. [Zugriff am 13 11 2018].

[3] L. Dashjr, „BIP 2 - BIP process, revised," [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki. [Zugriff am 13 11 2018].

[4] S. Khatwani, „What is a BIP (Bitcoin Improvement Proposal)? Why do you need to know about it?," [Online]. Available: https://coinsutra.com/bip-bitcoin-improvement-proposa/. [Zugriff am 13 11 2018].

[5] J. Hilliard, „BIP 91 - Reduced threshold Segwit MASF," [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0091.mediawiki. [Zugriff am 13 11 2018].

[6] P. Wuille, „BIP 32 - Hierarchical Deterministic Wallets," [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki. [Zugriff am 13 11 2018].

[7] MediaWiki, „Hilfe:Formatierung - MediaWiki," [Online]. Available: https://www.mediawiki.org/wiki/Help:Formatting/de. [Zugriff am 13 11 2018].

[8] A. Madeira, „What is a BIPS – Bitcoin Improvement Proposal?," 2015. [Online]. Available: https://www.cryptocompare.com/coins/guides/what-is-a-bips-bitcoin-improvement-proposal/. [Zugriff am 13 11 2018].

[9] L. Dashjr, „BIP 18 - hashScriptCheck," [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0018.mediawiki. [Zugriff am 13 11 2018].

[10] Saint Bitts LLC., „Vote with your Bitcoin (BCH) signature - Bitcoinocracy," [Online]. Available: https://vote.bitcoin.com/. [Zugriff am 12 11 2018].

[11] DECENT, „New Voting Tool Launched!," 06 2018. [Online]. Available: https://decent.ch/blog/new-voting-tool-launched/. [Zugriff am 19 11 2018].

[12] U. Negin, „Delegated Proof of Stake (DPOS) erklärt," 07 2018. [Online]. Available: https://blockchainwelt.de/delegated-proof-of-stake-dpos/. [Zugriff am 19 11 2018].

[13] P. Todd, „Consensus Critical Voting Considerations," 09 04 2016. [Online]. Available: https://petertodd.org/2016/consensus-critical-voting-considerations. [Zugriff am 19 11 2018].

[14] P. Wuille, P. Todd, G. Maxwell und R. Russell, „BIP 9 - Version bits with timeout and delay," [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki. [Zugriff am 10 11 2018].

[15] Bitcoinity.org, „Block size votes - Bitcoinity.org," 2018. [Online]. Available: https://data.bitcoinity.org/bitcoin/block_size_votes/all?c=block_size_votes&t=b. [Zugriff am 14 11 2018].

[16] Blockchain Luxembourg S.A., „Percentage of blocks signalling SegWit support," 2018. [Online]. Available: https://www.blockchain.com/charts/bip-9-segwit?timespan=all. [Zugriff am 13 11 2018].

[17] E. Lombrozo, „Forks, Signaling, and Activation," 2017. [Online]. Available: https://medium.com/@elombrozo/forks-signaling-and-activation-d60b6abda49a. [Zugriff am 15 12 2018].

[18] A. Sward, Vecna und F. Stonedahl, „Data Insertion in Bitcoins's Blockchain," 2017. [Online]. Available: https://digitalcommons.augustana.edu/cscfaculty/1/. [Zugriff am 04 06 2018].

[19] G. Ateniese, B. Magri, D. Venturi und E. Andrade, „Redactable Blockchain – or – Rewriting History in Bitcoin and Friends," 11 05 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7961975/. [Zugriff am 06 06 2018].

[20] I. Puddu, A. Dmitrienko und S. Capkun, „μchain: How to Forget without Hard Forks," 2017. [Online]. Available: https://eprint.iacr.org/2017/106.

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

[22] Bitcoin Wiki, „Technical background of version 1 Bitcoin addresses,“ [Online]. Available: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses. [Zugriff am 17 09 2018].

[23] Bitcoin Wiki, „Script,“ [Online]. Available: https://en.bitcoin.it/wiki/Script. [Zugriff am 17 09 2018].

[24] Bitcoin Wiki, „OP_RETURN,“ [Online]. Available: https://en.bitcoin.it/wiki/OP_RETURN. [Zugriff am 17 09 2018].

[25] A. Marsalek und B. Prünster, „Überblick E-Voting,“ 2018. [Online]. Available: https://technology.a-sit.at/ueberblick-e-voting/. [Zugriff am 08 11 2018].

[26] „Grundsätze des Wahlrechts,“ Republik Österreich, Parlamentsdirektion, [Online]. Available: https://www.parlament.gv.at/PERK/PARL/DEM/GRUNDS/index.shtml. [Zugriff am 15 02 2018].

[27] DECENT, „DECENT: Blockchain Content Distribution,“ [Online]. Available: https://decent.ch/. [Zugriff am 19 11 2018].