Bitcoin Private

WHITEPAPER

Die vonRevolution von Privatsphäre

Verfüllung von Satoshi's Vision für 2018 und weiter

Februar 2018

Peer Reviewed

Autoren:

Bitcoin Private Community

Jacob Brutman, Ph.D. Jon Layton

Christopher Sulmone

Giuseppe Stuto

Geoff Hopkins

Rhett Creighton

Abstract

Das Internet hat den größten Wendepunkt in der Geschichte geschaffen. Während es unzählige Vorteile für den leicht zugänglichen Informationsspeicher gibt, sind die Menschen verpflichtet, ihre Privatsphäre im Austausch dafür aufzugeben. Zu oft und ohne Verschulden des Endbenutzers wird ein Dritter mit unzureichender Sicherheit verletzt und sensible Informationen werden kompromittiert oder gestohlen. Ein besseres System ist erforderlich, das vertrauenswürdige Zwischenhändler entfernt und zwei beliebige Personen befähigt, frei und sicher zu handeln. Eine neue Krypto-Währung, Bitcoin Private, wird hier als kostengünstiges, schnelles und privates Transaktionsnetzwerk präsentiert - eine wahre Erfüllung der Roadmap des Bitcoin-Schöpfers Satoshi Nakamoto. Bitcoin Private ist das Produkt einer Gabelung von Bitcoin mit Zclassic. Die resultierende Bitcoin Private Kette hat deutlich niedrigere Gebühren als Bitcoin, zusammen mit einer vier- bis sechsmal schnelleren Transaktionsgeschwindigkeit. Am wichtigsten ist, dass zk-SNARKs, eine Peer-Review-Technologie, die ursprünglich von der Zcash Foundation implementiert wurde, integriert ist. zk-SNARKs ermöglicht nachweislich anonyme und private Transaktionen - eine Leistung, die keine andere Datenschutztechnologie für sich beanspruchen kann. Die UTXO-Sets von Zclassic und Bitcoin werden die ersten Münzen in diesem neuen Ledger enthalten. Das bedeutet, dass ungefähr 20,4 Millionen von 21 Millionen Münzen zum Zeitpunkt der Gabelung vorhanden sein werden, wodurch sichergestellt wird, dass Bitcoin Private die niedrigste Inflationsrate hat, die es je im Krypto-Währungsuniversum gegeben hat. Abschließend werden in diesem Whitepaper Bitcoin Private, seine technologischen Vorteile, die kommerzielle Anwendbarkeit und das Potenzial der Kette für zukünftige Entwicklungen sowie seine gemeinschaftsorientierte Ausrichtung diskutiert.

Inhaltsverzeichnis

1. Einleitung

Meistens während der geschriebene Geschichte waren Transaktionen privat und ziemlich anonym. Die Information einer Transaktion wurde nur dem Absender und dem Empfänger mitgeteilt. In jüngster Zeit wurde die große Mehrheit der Finanztransaktionen durch Technologie erleichtert, wodurch es zunehmend schwieriger wird, die finanzielle Privatsphäre zu wahren. Die modernen Zahlungsmethoden (z. B. Kredit- / Debitkarte, ApplePay usw.) führen dazu, dass alle Informationen einer Transaktion digital gespeichert werden. Obwohl diese Transaktionsmethoden immense Vorteile mit sich bringen, sollten sie nicht das Recht auf finnanzielle Privatsphäre für den Durchschnittsverbraucher verletzen. Wenn man bedenkt, wie häufig Verstöße innerhalb großer Finanzinstitute auftreten, die zu erheblichen Datenlecks persönlicher und finanzieller Informationen führen, ist klar, dass finanzielle Datenschutzoptionen erforderlich sind.[1,2] Darüber hinaus wurden verschiedene Finanzinstitute beim Verkauf von Kundendaten,[3] sowie blocken von legalen Transaktionen erwischt.[4]

Im Oktober 2008 veröffentlichte Satoshi Nakamoto den akademischen Artikel "Bitcoin: Ein Peer-to-Peer-elektronisches Cash-System", in dem die Grundlage für die erste Kryptowährung dargelegt wurde.[5] Satoshis Vision war es, eine Währung zu schaffen, die es ermöglichte, die Kontrolle von Transaktionen durch Dritte, begrenzte Inflation und Währungsfreiheit durch Anonymität zu beseitigen. Seit dem Start von Bitcoin im Jahr 2009 wurden über 1000 verschiedene Kryptowährungen geschaffen und immense Fortschritte erzielt.[6] In der Tat sind andere Kryptowährungen im Bezu auf Gebühren und Transaktionsgeschwindigkeit besser als Bitcoin, allerdings ist es durch sein First Mover Vorteil am beliebtesten fürs Handeln.

Als die Bitcoin-Blockchain im Laufe der Jahre wuchs, traten bemerkenswerte Probleme auf, darunter eine feste, kleine Blockgröße (was zu höheren Gebühren führte), langsame Blockierungszeit (10 min Durchschnitt), lange Schwierigkeitsanpassungszeit (alle 2 Wochen) und die Entwicklung / Massenproduktion von speziellen ASIC-Mining-Geräten (zur schnellen Berechnung von SHA-256), zentraliesierte Bitcoin mehr. Damit Bitcoin diese Probleme lösen könnte, müsste die Migration von mehr als 50% seiner Miner der Änderung des Codes, ausführen und zustimmen. Bis heute ist kein solches Ereignis eingetreten. Dies hat die Entwicklung von Bitcoin Hard Forks (wie Bitcoin Cash und Bitcoin Gold) vorangetrieben, um einige dieser technologischen Verbesserungen

Zum Beispiel wurde Bitcoin Cash umgestaltet, um größere Blockgrößen zu ermöglichen (≥ MB vs. 1 MB), was die Gebühren senkt und den Transaktionsdurchsatz erhöht. Dies kam jedoch nicht ohne Kompromisse aus - sein Preispotenzial wurde durch das Fehlen einer festen Blockgröße und eines "Gebührenmarktes" geschädigt. Der Gebührenmarkt im Bitcoin mempool fordert große und kleine Transaktionen heraus, um mit den Opportunitätskosten der anderen zu konkurrieren; dies macht den Wert des Eigentums noch dringlicher und führt zu einer höheren Nachfrage. Bitcoin Gold ging einen anderen Weg, indem es die Blockzeit (2,5 min) reduzierte, den PoW-Algorithmus auf Equihash (ASIC-resistent) umstellte und einen erweiterten Schwierigkeitsanpassungsalgorithmus einführte, der bei jedem Block auftritt. Es erfüllte weitgehend sein Ziel als GPU-kompatible Bitcoin Fork, aber es fehlt die weit verbreitete Annahme von Bitcoin, und die Entwickler führten einen Premine Cash Grab durch, dieser wurde als weniger ethisch betrachten, da er hinter verschlossenen Türen stattfand.

Im Zentrum von Satoshis Vision steht die Fähigkeit der Technologie, eine deflationäre Einheit von finanziellem Wert zu manifestieren, die es uns auch ermöglicht, Anonymität zu genießen und zu nutzen. Das "Recht auf Privatsphäre" ist eine krönende Freiheit in der freien Welt,8 und ist wesentlich für die Prinzipien, die von Satoshi und der Kryptowährungsgemeinschaft aufgestellt wurden.[8] Finanzielle Privatsphäre ist ein kritischer Grundsatz in Satoshis Vision einer neuen digitalen Währungswelt, aber viele Menschen stecken immer noch an der Kreuzung mit pseudo-anonymen Transaktionen auf Blockchains fest. Darüber hinaus gibt es staatliche und privatwirtschaftliche Organisationen, die massive Datenmengen und maschinelles Lernen nutzen, um die Personen zu identifizieren, die mit einer solchen Transaktion in Verbindung stehen. Tatsächlich ist BitFury in der Lage, bis zu 15% der Bitcoin-Transaktionen ab Januar 2018 zu de-anonymisieren, eine Zahl, die täglich steigt und die Kryptowährungswelt in den kommenden Jahren deutlich verändern wird.[9] Dieser Mangel an Privatsphäre in Bezug auf Bitcoin ist ironisch angesichts der ursprünglichen Absicht seines Schöpfers, obwohl es eine Lösung gibt.

Verschiedene Kryptowährungen haben versucht, dieses Datenschutzproblem zu lösen. Leider sind viele von ihnen immer noch in der Lage, durch verschiedene Techniken kompromittiert zu werden, aufgrund ihrer On-Chain-Transaktionssysteme, die Anonymität durch Verschleierung oder TOR-Knoten versprechen. Im Jahr 2014 diskutierten bahnbrechende

Forschungsarbeiten von MIT-Forschern über "zero-knowledge interactive arguments of knowledge" oder zk-SNARKs.10 Bemerkenswert ist, dass Kryptowährungen, die zkSNARKs implementieren, abgeschirmte Transaktionen ermöglichen - Geldmittel sind völlig anonym, ohne Transaktions- oder Adressabgleich erscheint auf der Ledger. Im Jahr 2016 haben die Autoren dieser Studie Zcash entwickelt und auf den Markt gebracht, die erste Kryptowährung, die zk-SNARKs enthält. Eine "Gründersteuer" wurde in den Code von Zcash aufgenommen, die es dem Entwicklungsteam und frühen Investoren ermöglicht, 20% der von der Community geminten Münzen zu sammeln. Nachdem Rhett Creighton der Miner Community aufmerksam zugehört hatte, entschied er sich nur 8 Tage später, Zcash zu spalten, die Steuer des Gründers zu streichen und Zclassic zu schaffen - eine Zcash-Plattform, die auf Transparenz durch Gemeindeentwicklung aufbaut. Leider litt Zclassic unter den gleichen Ideen, die er auch in seiner Größe begründete: Das Fehlen einer Gründersteuer führte zu einem Mangel an aktiver Entwicklung. Es gibt jedoch verschiedene Governance-Methoden, die diese schwache Entwicklung verhindern können.

Bitcoin Private, eine vermeintliche "Forkl-Zusammenführung" von Bitcoin und Zclassic, soll der Bitcoin-Blockchain Privatsphäre und Spendability verleihen und gleichzeitig die Herausforderungen, Entscheidungen und Misserfolge früherer Forks erkennen. Um dies zu erreichen, wird Bitcoin Private eine größere Blockgröße (2 MB), eine kürzere Blockzeit (2,5 min) und einen ASIC-resistenten (GPU-freundlichen) Proof-of-Work (PoW)-Algorithmus fürs Mining verwenden - Equihash. Aufgrund des dualen Charakters dieses Zusammenschlusses wird sich zudem ein größerer Teil der Krypto-Community engagieren. Nach dem Snapshot erhalten ZCL (t & z) und BTC (segwit & normal) Adressen BTCP (1:1 für beide) an der gleichen Adresse. Dies ist eine einzigartige Fork und die Open Source Blockchain-Community beginnt endlich, die Formbarkeit von UTXO-Sets vollständig zu erforschen.

Table 1: *Vergleich von Bitcoin Private, Bitcoin, Bitcoin Cash, und Bitcoin Gold.*

	***Bitcoin** Private*	Bitcoin	Bitcoin Cash	Bitcoin Gold
Total Supply	21 Million	21 Million	21 Million	21 Million
Privatsphäre	zk-SNARKs	**x**	**x**	**x**
Block Zeit	2.5 min	10 min	10 min	2.5 min
Block Größe	2 MB	1 MB	8 MB	1 MB
PoW Algorithmus	Equihash	SHA256	SHA256	Equihash
Schwierigkeits Ausgleich	Jeden Block	2 Wochen	2 Wochen	Jeden Block
Geschlossener Premine	**x**	**x**	**x**	JA
Community-Driven	Ja	**x**	**x**	**x**
Kontrolle	Ja	**x**	**x**	**x**

2. Fork Methodik

Für Bitcoin Private wird ein "fork-merge" vorgeschlagen, bei dem die UTXOs zweier Kryptowährungen zu einer Blockchain zusammengefasst werden. Dies geschieht formell außerhalb der Zclassic-Blockchain, da zk-SNARKs und JoinSplit-Transaktionen grundsätzlich Teil dieser neuen Blockchain sind. Man kann das Lösen einer Blockchain mit einem Polymerisationsmechanismus vergleichen: Wenn der nächste Block gelöst ist, wächst die Blockchain, so wie ein Polymer durch die reaktive Zugabe von Monomer zum Ende der Polymerkette wächst. Während längere Polymerketten generell wünschenswert sind, da sie dem

resultierenden Kunststoff eine erhöhte Zähigkeit verleihen, führt eine Vergrößerung der Blockchain zu einem erhöhten Speicherverbrauch und deutlich längeren Knoten-Synchronisationszeiten. Glücklicherweise braucht dieser Snapshot nur den Adressstatus von Bitcoin und Zclassic zu einem einzigen Zeitpunkt abzurufen, der dann in die neue Chain übertragen wird. Dieser Ansatz ist effektiv und führt zu einer deutlichen Reduzierung des Speicherbedarfs der Blockchain, in diesem Fall von 157 GB auf nur noch 10 GB (beim Start). Zusätzlich werden die Bitcoin Private Nutzer Blockchain-Beschneidung und SPV-Techniken wie Electrum unterstützen, um die Belastung der Blockchain auf den Endgeräten zu reduzieren.

Ein bedeutendes Problem, das jeder Fork bewältigen muss, ist ein sogenannter "Replay-Angriff", bei dem eine Post-Fork-Transaktion auf der ursprünglichen Blockchain für die neue Blockchain gültig gemacht wird. Alle Coin Forks müssen einen Wiederholungsschutz haben, um Legitimität und Unabhängigkeit von der ursprünglichen Blockchain zu gewährleisten. Bitcoin Private bietet einen zweifachen Replay-Schutz, um gegen Replay-Attacken von Bitcoin und Zclassic geschützt zu sein. Dies ist ein untersuchtes Problem, und wir verwenden den Industriestandardansatz, der wie oben beschrieben in zwei Richtungen integriert wird. Dies ist bereits implementiert, und wir verwenden den Industriestandard-Ansatz (SIGHASH_FORKID), der gut untersucht ist und erfolgreich für Bitcoin Gold funktioniert hat.[11]

Der Snapshot von Bitcoin und Zclassic wird für die ersten Blöcke gesetzt, die nach 17 Uhr UTC am 28. Februar 2018 mit einem Zeitstempel versehen wurden, wobei der fork/main-net-Start ca. 2 Tage später erfolgt. Nach dem Start wird es rund 700.000 abbaubare Bitcoin Private geben. Es wurde eine Startblockprämie von 1,5625 Bitcoin Private sowie eine Halbierung alle 210.000 Blöcke (~1 Jahr) gewählt. Sollte sich dieses Experiment jedoch als erfolglos erweisen, kann ein Alternativplan umgesetzt werden, der in Abschnitt 7 skizziert ist.

3. Proof-of-Work: Equihash

Wie in der Einleitung erläutert, wird der Abbau von Bitcoin überwiegend von ASICs durchgeführt, spezialisierten Instrumenten, die in der Lage sind, GPUs deutlich zu überbieten. Im Gegensatz zu GPUs sind ASICs weitaus schwieriger zu erwerben und haben zu einer signifikanten Zentralisierung des Bitcoin-Mining geführt.

Tatsächlich hat Igor Homakov vorgeschlagen, dass über 60% der Bitcoin Netzwerk-Hash-Rate in China liegt.[12] In der Zwischenzeit sind ASIC-resistente Algorithmen weitaus eher dezentralisiert, da GPUs überall auf der Welt leichter verfügbar sind. Die Dezentralisierung des Netzwerk-Hash ermöglicht eine deutlich stärkere Demokratisierung der Blockchain, eine geringere Anfälligkeit für einen 51% Angriff und stellt sicher, dass die durch das Mining generierte Kryptowährung sowie die damit verbundenen Gebühren möglichst gleichmäßig in der gesamten Gemeinde verteilt werden. Dies verhindert außerdem, dass einige wenige Miner die Blockchaintwicklung beeinflussen und den Markt durch Mining von signifikant großen Mengen der Kryptowährung manipulieren können

Bitcoin Private wird den von Alex Biryukov und Dmitry Khovratovich an der Universität Luxemburg entwickelten, hoch angesehenen Equihash PoW-Algorithmus als asymmetrischen Proof-of-Work-Mechanismus (PoW) verwenden.[13] Im Gegensatz zu anderen ASIC-resistenten PoW-Algorithmen basiert Equihash auf dem "Birthday Problem" und dem erweiterten Wagner-Algorithmus, der zur Lösung dieses Problems verwendet wird. Darüber hinaus verfügt Equihash über eine "Gedächtnishärte", bei der eine steile Rechenstrafe mit einer Verringerung des Speicherverbrauchs und der Geschwindigkeit verbunden ist. Diese Eigenschaft erhöht den ASIC-Widerstand von Equihash aufgrund der Kosten für die Implementierung von mehr Speicher in ASICs, um sie mit GPUs oder sogar CPUs konkurrenzfähig zu machen. Die Autoren des Originalpapiers diskutieren, dass die Speicherhärte zwar nicht vor Botnet-basiertem CPU-Mining schützt, der hohe Speicherverbrauch jedoch extrem hoch wäre, so dass die Anwenderbasis infizierter PCs einen signifikanten Leistungsunterschied bemerken und die notwendigen Maßnahmen ergreifen würde, um die Infektion zu entfernen.

4. Transparent vs. Shielded Transactions

Bitcoin Private ist ein Zusammenschluss von zwei Transaktionssystemen - transparente und abgeschirmte Transaktionen. Transparente Transaktionen arbeiten nach den gleichen Prinzipien wie Bitcoin - Input, Output, Betrag und Signatur. Die Quellen aller Fonds, Destinationen und Beträge werden transparent auf der Blockkette gespeichert. Geschützte Transaktionen verschlüsseln umgekehrt diese Details in einem speziellen Abschnitt eines Blocks, der JoinSplit genannt wird. Diese Transaktionen sind nachprüfbar, aber für Dritte nicht

entzifferbar. Wenn Sie Schielded Notes ausgeben, wird die Integrität der Blockchain durch einen speziellen Zero-Knowledge-Proofs-Algorithmus namens zkSNARKs[6] erhalten. eser Algorithmus führt eine Reihe von Berechnungen durch, um die Summe der Eingangswerte zu den Ausgangswerten für jede geschirmte Übertragung anzuzeigen. Dann beweist der Absender, dass er die privaten Ausgabeschlüssel der Eingabescheine besitzt, und gibt ihm die Befugnis, diese auszugeben. Schließlich werden die privaten Ausgabeschlüssel der Eingabescheine kryptographisch mit einer Signatur über die gesamte Transaktion verknüpft, so dass die Transaktion von einer Partei, die diese privaten Schlüssel nicht kannte, nicht verändert werden kann.[14] Diese gesamte Methodik stützt sich auf das vertrauenswürdige Setup von Zcash: Bei der Einführung von Zcash wurden Schlüssel, die für Null-Wissen-Nachweise und private Transaktionen notwendig sind, generiert und anschließend vernichtet; dies wurde als "Zeremonie" bezeichnet.[6] Auf diese Weise kann das System eine "einmalige starke Fälschungssicherheit gegen ausgewählte Nachrichtenangriffe" sicherstellen. ”[10]

5. Freiwilliges Miner Beitragsprogram

Um eine Schatzkammer für den Unterhalt und die Entwicklung von Bitcoin Private zu schaffen, wurde ein freiwilliges Miner Contribution Program ins Leben gerufen. Im Rahmen dieses Programms werden 62.500 Bitcoin Private an Miner versteigert, bis zu insgesamt 50.000 Zclassic, die dem Bitcoin Private Treasury Fund über Hash Power gespendet wurden. Die Auszahlung für jeden beliebigen Miner im Programm kann durch folgende Gleichung bestimmt werden:

$$P = Z_m * 62{,}500/Z_p$$

Wo P die Auszahlung für den Bergmann ist, ist Zm die Zclassic, die vom Bergmann abgebaut wird, und Zp ist die gesamte Zclassic, die vom gesamten Pool abgebaut wird. Die 62.500 Bitcoin Private werden an der Fork erzeugt und an die entsprechenden Adressen der jeweiligen Miner verteilt. Die für dieses Programm eingerichtete ZCL-Multi-Sig-Wallet wird bis zu 50.000 Zclassic enthalten und anschließend in BTCP eingeteilt, um eine Schatzkammer für die Entwicklung, die Belohnung, das weitere Marketing und die Gesamtentwicklung von Bitcoin Private durch die Gemeinschaft einzurichten. Dies ist eine von mehreren Methoden, um das ursprüngliche Problem der veralteten Zclassic-Entwicklung anzugehen.

In mancher Hinsicht könnte man dieses Programm als eine "Premine" betrachten, ein Konzept, dem das Bitcoin Private Spendenteam vehement widerspricht. Premine wurden jedoch in der Regel von und direkt für die Kerngruppe durchgeführt, was hier nicht der Fall ist. In diesem Fall ist die Miner Community in der Lage, freiwillig Geld zu spenden, im Austausch für einen frühzeitigen Zugang zum Mining von Bitcoin Private. Darüber hinaus kann die Mining Community aufgrund des auktionsähnlichen Stils des Programms wählen, wie viel jeder gestiftete ZCL als Kollektiv wert ist (siehe Gleichung oben): Diese Art der marktwirtschaftlichen Methodik ist der Kern von Satoshis ursprünglicher Vision für Bitcoin. Diese Mittel werden für Börsennotierungen (50 %), Entwicklung (25 %), Marketing (15 %) und Allgemeines/Verwaltung (10 %) verwendet.

6. Treasury Fund Governance

Ein Treasury Fund Governance Council wurde aus drei Mitgliedern der Gemeinde und zwei Mitgliedern der Miner Community zusammengestellt, die als BTCP Developer Community, LLC, gegründet wurden. Zum Zeitpunkt der Veröffentlichung repräsentieren Jacob Brutman, Ph.D. (Operations Lead), Giuseppe Stuto (Marketing Lead) und Peter Hatzipetros (General Counsel) die Gemeinde, während Adib Alami und Evan Darby die Miner repräsentieren. Ein Satzungsdokument für den Rat wurde ebenfalls erstellt.[15]

7. Die Zukunft von Bitcoin Private

Die Verbesserung der Privatsphäre in allen Bereichen ist ein wichtiger Teil des Bitcoin Private Projekts. Derzeit ist zk-SNARKs sehr RAM- und CPU-intensiv während des Signierens der Transaktion, was bis zu einigen Minuten dauern kann. Eine der ersten Verbesserungen, die nach dem Fork umgesetzt werden, ist der neue Setzling, der als "Jubjub" bezeichnet wird und derzeit vom Zcash-Kernentwicklungsteam entwickelt wird.[16] Dieser neue Setzling wird eine signifikante Verbesserung der Geschwindigkeit und Benutzerfreundlichkeit von abgeschirmten Transaktionen für zk-SNARKs Privatsphären Coin ermöglichen. Eine weitere Methode zur Verbesserung der Privatsphäre von Bitcoin Private besteht darin, das derzeit in der Entwicklung befindliche Datenschutzprojekt "Dandelion" zu nutzen.[17] Diese Technik umfasst den "Stamm" (die Transaktionen) und den "Flaum" (Verschleierung). Während jedes Verschleierungsverfahren von Natur aus

weniger sicher ist als zk-SNARKs, könnte Dandelion Verschleierung sowohl zu transparenten als auch zu abgeschirmten Transaktionen von Bitcoin Private hinzugefügt werden, wodurch die Privatsphäre auf der ganzen Linie verbessert wird.

Die Möglichkeit, Bitcoin Private mit Blockkettenverbesserungen auszustatten, ist für das Projekt von großer Bedeutung. BIP9 wurde in die Blockchain integriert, um soft Fork und damit Verbesserungen zu ermöglichen.[18] Nachdem die richtige Codierung für Verbesserungen abgeschlossen ist, werden die Bergleute gebeten, die Bereitschaft zu signalisieren, die Änderung des Chaincodes zu akzeptieren. Wenn 95% der Miner den Wechsel akzeptieren, wird er "eingesperrt" und der Fork ist fertig. Wenn die Bergleute jedoch nicht innerhalb der vorgegebenen Zeitspanne die Bereitschaft signalisieren, versagt der soft Forkl und es finden keine Veränderungen statt. Die Unterstützung und Entwicklung des Bitcoin-Privatprojekts wird sich auf die kontinuierliche Sammlung von Treasury-Fonds in einer anderen Art und Weise als durch Spenden von Miningpools stützen. Das Bitcoin Private Beitragsteam lehnt jedoch jede Art von Besteuerung seiner Gemeinde ohne demokratische Zustimmung strikt ab. Daher wird eine der ersten vorgeschlagenen Änderungen über BIP9 die Parameter für die Sammlung von Treasury-Fonds betreffen. Auf diese Weise können die Miner selbst entscheiden, welchen Betrag sie bereit sind, als Kollektiv zu spenden, um den zukünftigen Erfolg des Programms zu sichern.

Wie in Abschnitt 2 erwähnt, könnte die geringe Menge an abbaubarem Bitcoin Private, die nach der Abspaltung verbleibt, einige Probleme verursachen, einschließlich der extrem niedrigen Netzwerk-Hash-Rate. Eine mögliche Lösung besteht darin, die Entfernung nicht abgeholter Coins aus dem Netz über BIP9 irgendwann anzubieten. Wenn diese Implementierung über BIP9 gewählt wird, würden im Laufe von zwei Jahren täglich ca. 0,14% aller nicht abgeholten Bitcoin Private Münzen aus dem Forkl entfernt. In diesem Szenario würden Bitcoin Private Coins gleichmäßig über alle Wallets hinweg entfernt: Jede Wallet mit nicht abgeholter Bitcoin Private aus dem Fork verliert ca. 0,14% ihr Coin pro Tag für 2 Jahre. Diese Methode würde einen beträchtlichen Teil der Coins für die Miner freigeben und gleichzeitig den Benutzern genügend Zeit geben, ihre gespaltenen Coins in Anspruch zu nehmen. Darüber hinaus sollte der geringe Prozentsatz der täglichen Entfernung verhindern, dass es zu einem Schock für die Marktkapitalisierung kommt.

As a Als Backup-Maßnahme wurde in Bitcoin Private eine "Schwierigkeits-Bombe" implementiert, um eine signifikante zukünftige Entwicklung zu ermöglichen, ähnlich wie bei Ethereum.[19] Wenn die Schwierigkeitsbombe verwendet wird, wird sie auf den alten Blockchain-Code angewendet und die Minener daran erinnert neue Code-Basis für kontinuierliche Verbesserungen. Diese Methode wird als letzter Ausweg betrachtet und nur unter extremen Umständen angewendet. Möglicherweise könnte die Bombe eingesetzt werden, um ein neues Governance-System einzuführen, wie zum Beispiel das System von Decred.[20] Dies wird eine weitere Demokratisierung und Dezentralisierung der Bitcoin Private-Blockchain ermöglichen. Momentan wird das Datum der Schwierigkeitsbombe auf den 2. März 2019 festgelegt, Hardforks können jedoch dazu verwendet werden, dieses Datum auf unbestimmte Zeit zu verlängern. Nicht zufällig wird die erste Halbierung um das Datum der Schwierigkeitsbombe herum stattfinden; Dadurch können Änderungen vorgenommen werden, falls sich das niedrige Inflationsexperiment als nicht erfolgreich erweisen sollte.

8. Commercial Applications

Die Zahlungsabwicklung ist nach wie vor einer der tiefgründigsten Anwendungsfälle von Bitcoin. Händler haben wahrscheinlich über $1 Milliarde Äquivalent von Bitcoin für das Jahr 2017 mit Bitcoin Zahlungsabwicklungsfirmen wie BitPay abgewickelt. Wallet-Nutzer dieser sehr gleichen Firma sichern über $1 Milliarde Wert der Anlagegüter pro Monat und schicken über $1.5 Milliarde Wallet zu wallet per Monat.[21]

Die Verbraucher erwarten eine gewisse Bequemlichkeit, wenn es um die Übertragung von Werten im Tausch gegen Waren und Dienstleistungen geht, und deshalb ist die Zahlungsabwicklung über das Internet alltäglich geworden. Zusammen mit dieser Erwartung der Bequemlichkeit, gibt es eine angenommene Ebene der Privatsphäre, die mit einer solchen Transaktion kommt. Unglücklicherweise gab es in den letzten zwei Jahrzehnten Entitäten, die davon profitieren, ein Online-Profil eines Verbrauchers zu erstellen, indem sie Online-Kreditkartentransaktionen verfolgen.[22] Dies ist unglaublich invasiv und dient als eine große unterstützende Prämisse dafür, warum ein Verbraucher Online-Transaktionen mit Krypto-Währung durchführen möchte. Trotz des technischen Designs der populärsten Krypto-Währung ist diese Privatsphäre auf der Blockkette

nicht mehr zu erwarten.[14] Bitcoin Private könnte jedoch über zk-SNARKs Transaktionen die Datenschutzbedürfnisse der Konsumenten erfüllen.

Bitcoin Private wird eine wichtige Rolle bei der Peer-to-Peer- und kommerziellen Übertragung von digitalen Assets spielen. Es bietet Anbietern eine getestete, sichere und weit verbreitete Krypto-Währungstechnologie mit dem zusätzlichen Vorteil nachweisbarer Anonymität und Privatsphäre. Möglicherweise kommen Hunderte bis Tausende von natürlichen Anwendungsfällen von Bitcoin Private im kommerziellen Einsatz. Während andere Z-Protokoll-Coins in der Lage sein könnten, diese Rolle zu erfüllen, hat sich in der Regel keiner dafür entschieden oder es ist ihnen gelungen. Dies ist wahrscheinlich auf den hohen CPU- und Speicherbedarf von geschirmten Transaktionen zurückzuführen; die Veröffentlichung von "Jubjub" sapling wird jedoch mobile geschirmte Transaktionen ermöglichen. Das Bitcoin Private Contribution Team hat den starken Wunsch, die Krypto-Währung in den Mainstream zu bringen und eine breite Anwendung zu ermöglichen. Daher wird kurz nach dem neuen Setzling ein vendorf-freundlicher Shielded-Transaction-Service freigeschaltet. Zusätzlich zu dem Standard-Anwendungsfall für Web-Anbieter könnten mobile Wallet Plattformen genutzt werden, um Bitcoin Private über transparente und abgeschirmte Transaktionen in Backstein- und Mörtelanwendungen zu speichern und zu übertragen. Darüber hinaus kann die gleiche Plattform von jedem Benutzer genutzt werden und ist nicht auf Geschäfte beschränkt. Bitcoin Private wurde bereits von verschiedenen Anbietern und Händlern als Zahlungsmethode für ihre Waren angesprochen. Ein Prozentsatz dieser kommerziellen Transaktionen könnte für die Bitcoin Private Treasury gesammelt werden, was die Notwendigkeit einer Treasury-Sammlung über den Bergbau zunichte machen könnte.

9. Community-driven Project

Viele Krypto-Währungsprojekte, ob Utility-Token oder Coins, behaupten, dass sie gemeinschaftsgesteuert und quelloffen sind. Obwohl dies in gewissem Umfang zutrifft, existiert in der Regel ein Kern-Entwicklungsteam, das die gesamte Zukunft des Projekts steuert. Es gibt nur wenige Ausnahmen (z.B. Decred), bei denen die Community die tatsächliche Kontrolle über die Zukunft hat, aber Entwicklungsteams sind immer noch oft verschlossene Türen. Während Community-Mitglieder Änderungen am entsprechenden Code vorschlagen können, können diese Anfragen unbemerkt bleiben. Das Bitcoin Private Projekt

stellt eine echte Gemeinschaftsarbeit dar, mit über 100 Spendern (6. Februar 2018) und wächst täglich.

Verschiedene Initiativen wurden implementiert, die Bitcoin Private von anderen Gemeinschaftsmünzen trennen. Zum Beispiel wurde ein weltweites, mehrsprachiges Botschafterprogramm ins Leben gerufen, mit dem Mitglieder der Community sich aktiv einbringen können, um Bitcoin Private zu fördern und die Community zu fördern. Darüber hinaus hat Bitcoin Private einen "Call for Developers" gestartet, in dem sich jeder bewerben kann, auch wenn er neu in der Blockchain-Technologie ist, und er kann auf sinnvolle Weise zum Projekt beitragen. Diejenigen ohne vorherige Erfahrung können von diesem Entwicklerprogramm lernen und beherrschen Blockchain-Technologie / Engineering. Diese beiden Programme haben in ein paar Tagen mehr als hundert neue Mitwirkende hinzugefügt und unser tägliches Beitragsteam auf weit über 300 Mitglieder erweitert. Die Größe des Bitcoin Private Contribution Teams zeigt die Hingabe des Projekts zu seiner von der Community inspirierten Inspiration und ist eine Leistung, die keine andere Kryptowährung nach bestem Wissen des Teams erreicht hat. Dies zeigt die wirklich dezentralisierte Art der Entwicklung von Bitcoin Private

10. Zusammenfassend/ Fazit

Bitcoin Private ist eine Krypto-Währung, die von einer vielfältigen Community entwickelt und gepflegt wird. Teammitglieder aus der ganzen Welt arbeiten täglich zusammen, um dieses Projekt zum Erfolg zu führen. Sie tun dies, weil sie glauben, dass das Projekt Satoshis ursprüngliche Vision von finanzieller Freiheit durch schnelle, kostengünstige, dezentrale und private Transaktionen erfüllt. Bitcoin Private's vorausschauende Einbeziehung des BIP9 Soft Fork-Vorschlags wird zukünftige Entwicklungen ermöglichen, und eine eingeschlossene Schwierigkeitsbombe wird alternative KOntroll Methoden voranbringen, sollte sich BIP9 als unwirksam erweisen. Die kommerziellen Anwendungen von Bitcoin Private sind vielfältig: von schnellen globalen Transaktionen bis hin zum Einkauf in lokalen Geschäften. Die Fusion Bitcoins Größe und Zclassics shielded Transactions Technologie, wird eine neue Ära der Blockchain Privatsphäre einleiten.

11. Dankung

Wir möchten die Mining Gemeinschaft für ihre großzügigen Spenden über das freiwilligen Miner Programm würdigen. Wir möchten auch dem Molekül Koffein dafür danken, dass es dem Team geholfen hat, viele lange Tage und Nächte durchzustehen; Ohne Kaffee wäre dieses Projekt nicht möglich gewesen. Vielen Dank auch an unser erstaunliches Entwicklungsteam - Sie sind die Grundlage, auf die wir uns verlassen. Abschließend möchten wir der gesamten Bitcoin Private Community danken - Sie sind das Rückgrat dieses Projekts und wir wären ohne Sie nicht hier.

12. Verweise/ Quellen

[1] *Dutch Banks Tax Agency Under DdoS Attacks a Week after Big Russian Hack Reveal*. https://www.bleepingcomputer.com/news/security/dutch-banks-tax-agency-under-ddosattacks-a-week-after-big-russian-hack-reveal/ (Accessed Feb. 5, 2018).

[2] The Biggest Data Breaches of the 21st Century. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the21st-century.html (Accessed Feb. 6, 2018).

[3] *What Chase and Other Banks won't Tell you about Selling your Data*. https://www.forbes.com/sites/adamtanner/2013/10/17/what-chase-and-other-banks-wont-tellyou-about-selling-your-data/#5eacaaf62c41 (Accessed Feb. 5, 2018).

[4] *Santander Totta has no Known Legal Basis to Block Bitcoin Related Transactions says Portuguese Consume Watchdog*. https://www.ccn.com/santander-totta-has-no-known-legalbasis-to-block-bitcoin-related-transactions-says-portuguese-consumer-watchdog/ (Accessed Feb. 5, 2018).

[5] Nakamoto S.; (2008) *Bitcoin: A peer-to-peer electronic cash system.*

[6] *List of Cryptocurrencies.* https://cryptocurrencyfacts.com/list-of-cryptocurrencies/ (Accessed Feb. 5, 2018).

[7] *Premine Endowment*. https://bitcoingold.org/premine-endowment/ (Accessed Feb. 2, 2018) [8] Brandeis, L.; Warren, S.; (1890) *The Right to Privacy*.

[9] "BitFury Group De-Anonymizes Over 15% of the Bitcoin ... - The Merkle." 11 Jan. 2018, https://themerkle.com/bitfury-group-de-anonymizes-over-15-of-the-bitcoin-network-with-newblockchain-analysis-tool/ (Accessed Jan. 30, 2018).

[10] Ben-Sasson, E; Chiesa, A; Garman, C.; Green, M,; Miers, I.; Tromer, E.; Virza, M. (2014) *Zerocash: Decentralized Anonymous Payments from Bitcoin*.

[11] *Interpreter.*cpp.

https://github.com/BTCPrivate/BitcoinPrivate/blob/6b6abb3d121ba5231e5d775e9e2287dbbf7687f6/src/script/interpreter.cpp#L1089 (Accessed Feb. 9, 2018) [12] Homakov, I. (2017) *Stop. Calling. Bitcoin. Decentralized*. https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27 (Accessed Feb. 4, 2018)

[13] Biryukov, A.; Khovratovich, D.; (2016) *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem.*

[14] *Zcash - How zk-SNARKs works in Zcash.* https://z.cash/technology/zksnarks.html (Accessed Feb. 3, 2018).

[15] *BTCP Developer Community, LLC Bylaws.* https://btcpfoundation.org/bylaws.pdf [16] *What is Jubjub?* https://z.cash/technology/jubjub.html (accessed Feb. 1, 2018).

[17] *Bitcoin Developers Reveal Roadmap for 'Dandelion' Privacy Project* https://www.coindesk.com/bitcoin-developers-reveal-roadmap-dandelion-privacy-project/ (accessed Feb. 5, 2018).

[18] *BIP9*. https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki (Accessed Feb. 7, 2018)

[19] *What is the Ethereum Difficult Bomb*. https://themerkle.com/what-is-the-ethereum-difficultybomb/ (accessed Feb. 5, 2018)

[20] *Decred Documentation.* https://docs.decred.org/ (Feb. 1, 2018).

[21] *Bitcoin Transactions aren't as Anonymous as Everyone Hoped*. https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-aseveryone-hoped/ (Accessed Feb. 5, 2018).

[22] *Google Now Tracks Your Credit Card Purchases and Connects them to its Online Profile of you.* https://www.technologyreview.com/s/607938/google-now-tracks-your-credit-card-purchasesand-connects-them-to-its-online-profile-of-you/ (Accessed Feb. 5, 2018).

13. Wichtige Angaben und Informationen

Alle Inhalte sind original und wurden von Bitcoin Private recherchiert und produziert, sofern nicht anders angegeben. Kein Teil dieses Inhalts darf ohne ausdrückliche Zustimmung von Bitcoin Private in irgendeiner Form reproduziert oder in einer anderen Veröffentlichung verwendet werden.

Dieses Dokument dient nur zu Informationszwecken und stellt weder ein Angebot zum Verkauf noch einen Versuch dar, ein Angebot zum Kauf oder Verkauf eines Wertpapiers in einer Rechtsordnung zu erbitten, in der ein solches Angebot oder ein solches Ausschreiben illegal wäre. Es gibt nicht genügend Informationen in diesem Papier, um eine finanzielle Entscheidung zu treffen, und die hierin enthaltenen Informationen sollten nicht als Grundlage für diesen Zweck verwendet werden. Dieses Papier stellt keine persönliche Empfehlung dar und berücksichtigt nicht die besonderen Anlageziele, finanziellen Situationen oder Bedürfnisse der Leser. Leser sollten prüfen, ob ein Hinweis oder eine Empfehlung in diesem Papier für ihre spezifischen Umstände geeignet ist und gegebenenfalls professionelle Beratung, einschließlich einer Steuerberatung, einholen. Der Preis und der Wert der Kryptowährung und das Einkomme können schwanken. Die Wertentwicklung in der Vergangenheit ist kein Hinweis auf die zukünftige Wertentwicklungen, zukünftige Renditen sind nicht garantiert und es kann zu einem Verlust des ursprünglichen Kapitals kommen. Wechselkursschwankungen können sich nachteilig auf den Wert oder den Preis bestimmter Anlagen auswirken. Informationen, die über Bitcoin Private bereitgestellt werden, sind nicht als Anlage-, Steuer- oder Rechtsberatung, als Empfehlung oder Verkaufsangebot oder als Aufforderung zur Abgabe eines Kaufangebots für Bitcoin Private Coins zu verstehen oder sollten als solche ausgelegt oder verwendet werden.

Bestimmte Aussagen, die hierin enthalten sind, können Aussagen über zukünftige Erwartungen und andere zukunftsgerichtete Aussagen sein, die auf den Ansichten und Annahmen von Bitcoin Private beruhen und bekannte und unbekannte Risiken und Unsicherheiten beinhalten, die dazu führen können, dass die tatsächlichen Ergebnisse, Leistungen oder Ereignisse wesentlich von denjenigen abweichen, die in diesen Aussagen ausdrücklich oder implizit zum Ausdruck gebracht werden. Zusätzlich zu den Aussagen, die aufgrund ihres Kontextes in die Zukunft gerichtet sind, kennzeichnen die Worte "kann, wird, sollte, könnte, kann, kann, erwartet, plant, beabsichtigt, antizipiert, glaubt, schätzt, prognostiziert, potenziell, projiziert oder fortbestehen" und ähnliche Ausdrücke zukunftsgerichtete Aussagen. Bitcoin Private übernimmt keine Verpflichtung, die hierin enthaltenen zukunftsgerichteten Informationen zu aktualisieren. Obwohl Bitcoin Private mit angemessener Sorgfalt darauf geachtet hat, dass die hierin enthaltenen Informationen zutreffend sind, übernimmt Bitcoin Private keine Zusicherung oder Gewährleistung (einschließlich Haftung gegenüber Dritten), weder ausdrücklich noch stillschweigend, hinsichtlich ihrer Genauigkeit, Zuverlässigkeit oder Vollständigkeit.