BTCTKVR 3


21
B
Bitcoin
42
Re
Rules everything
63
A
Around me
105
K
King
168
In
Immutable
273
G
Gold
9
F
Fear
92
U
Uncertainty
105
D
Doubt

Vorwort

Liebe Leserinnen und Leser,

dies ist die deutsche Übersetzung des BTCTKVR-Magazins Ausgabe 3.

Es ist mir eine Ehre nun allen deutschsprachigen Interessierten Zugang zu den unbeschreiblich wertvollen Inhalten des Magazins geben zu können. Eine wahre Quintessenz an Bildung! Die Inhalte wurden von Peter Todd, Pavol "Stick" Rusnak & Paula Magal geprüft...ja auch die Lesen das BTCTKVR Magazin.

An dieser Stelle Danke ich im Namen des gesamten Rabbit Hole meinem guten Freund und Schöpfer von BTCTKVR Vlad Costea für seine tolle Arbeit!

Wer die Übersetzungen dieses & weiterer BTCTKVR-Magazine unterstützen möchte:

<-BTC

LN↘

stiflednut98@walletofsatoshi.com

Ray Rizzling

Inhaltsverzeichnis

Breaking FUD: Bitcoin Akzeptieren 02

Breaking ChatGPT's Bitcoin FUD #1: Gesetzliche Regulierung 08
Renaissance

Breaking ChatGPT's Bitcoin FUD #2: Altcoins 13
1980er Neon Synthwave

Breaking ChatGPT's Bitcoin FUD #3: Skalierung 18
Anime

Breaking ChatGPT's Bitcoin FUD #4: Sicherheitslücken 23
Pixel Art

Breaking ChatGPT's Bitcoin FUD #5: Preisvolatilität 30
Art Nouveau

Breaking ChatGPT's Bitcoin FUD #6: Limitierte Anwendungsfälle 36
Film Noir

Die BTCTKVR 2-Editionen 46

Breaking ChatGPT's Bitcoin FUD #7: Energieverbrauch 48
Solarpunk

Bitcoin Eating Popcorn #3 63

Breaking ChatGPT's Bitcoin FUD #8: Mining-Zentralisierung 64
Pop Art

Breaking ChatGPT's Bitcoin FUD #9: Aufklärung 70
Surrealismus

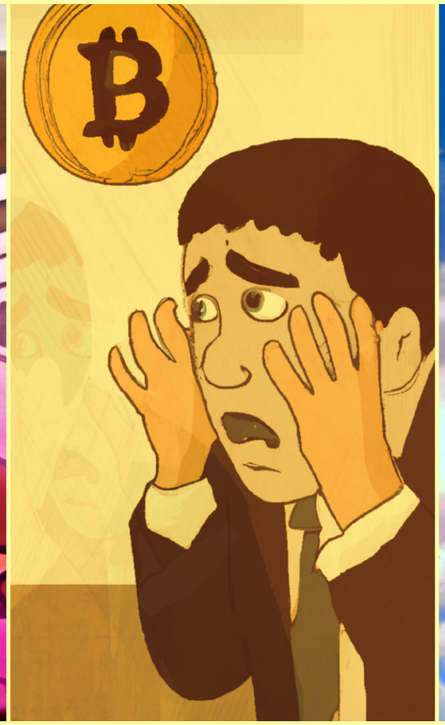
Breaking ChatGPT's Bitcoin FUD #10: Mainstream Akzeptanz 75
Kubismus

FUD Zum Grübeln 82
Expressionismus

Breaking FUD: Wie Die Hingabe Eines Vaters Einen Skeptiker Zu Bitcoin Führte 88
Cartoony

Hall of Plebs 91







Breaking FUD

Bitcoin Akzeptieren

Bitcoin ist wieder einmal in der FUD-Saison. Das ist die Zeit, in der Bitcoin zusammen mit Kryptobetrügereien in einen Topf geworfen wird, um seine technologische Legitimität in Frage zu stellen. "Jahre sind vergangen, was hat Bitcoin erreicht? Er ist eine verschwenderische, ozeanerhitzende gescheiterte Utopie für Libertäre und alle, von denen wir euch sagen, dass ihr sie nicht mögt", hört man. In diesen Momenten glänzen Kritiker und Skeptiker - wenn der Preis von den früheren Höchstständen gefallen ist, wächst die Zahl der enttäuschten Privatanleger. Natürlich richtet sich die Mehrheit der Aufmerksamkeit auf jene desinformierte, aber fest überzeugte Stimmen, die behaupten, dass Bitcoin gescheitert ist und von Beginn an eine schlechte Idee war.

Währenddessen bietet Bitcoin weltweit Millionen von Menschen finanzielle Integration. Die 'Unbanked', politisch Unterdrückte, sozial und finanziell Eingeschränkte und ideologisch Getriebene profitieren ständig von der Art der Transaktionsfreiheit, die ihnen keine Regierung oder private Institution jemals gewähren wird. Wenn die vorherige Aufzählung zu allgemein und formelhaft klingt, hier sind einige Beispiele:

- Den kanadischen Fernfahrern, die 2022 gegen irrationale, autoritäre Arbeitsbedingungen demonstrierten wurden aufgrund politischen Missbrauchs ihre Bankkonten eingefroren. Um Unterstützung erhalten zu können, mussten sie Bitcoin verwenden;

- Die Bürger von Ländern, die in den Jahren 2021 und 2022 eine dreistellige Inflation erlebten, haben ihre Ersparnisse mithilfe von BTC geschützt. Solche Fälle sind in Sudan, Argentinien, Libanon und Venezuela zu finden.

- In Ländern wie Suriname und der Türkei ist der Absturz von Bitcoin von seinem Allzeithoch immer noch nicht so drastisch wie die Abwertung ihrer nationalen Fiatwährungen.



- In El Salvador, das Land, das die magische Internetwährung zum offiziellen Zahlungsmittel gemacht hat, sind Bitcoin-Transaktionen Teil des täglichen Lebens.

- Und wer immernoch nicht überzeugt ist: Im Jahr 2022 sollen chinesische Spione BTC-Bestechungsgelder über die Wasabi-Wallet an einen US-Doppelagenten geschickt haben. Das bedeutet, dass Regierungsbeamte Bitcoin trotz der offiziellen Erklärung, die sie über die Medien verbreiten, nützlich finden.

2021 war von Tesla Cybertruck- und Citadell-Memes geprägt war, nun steht der Fall von 2022 und wahrscheinlich größtenteils von 2023 ganz im Zeichen von FUD gegen Bitcoin. Es ist einfacher für Spekulanten, die den Zweck und die Ideale von Bitcoin nicht verstehen, es durch Halbwahrheiten und verzerrte Fakten zu kritisieren. Und es ist auch äußerst bequem für Regierungsbeamte, Zentralbanker und private Banker, diese FUD durch ihre Autorität und die von ihnen kontrollierten Medienkanäle zu fördern. Solch unehrlichen und betrügerischen Handlungen erhöhen effek-tiv die Nachfrage nach scheiternden Fiatwährungen und können auch vorübergehend das Vertrauen in ihr lächerliches Geldsystem stärken.

Aber FUD, außerhalb seiner Instrumentalisierung durch Regierungen, ist nichts weiter als eine Reihe natürlicher Reaktionen, die uns dabei helfen, Ereignisse und Phänomene zu verarbeiten, die unsere Weltanschauung und unser Glaubenssystem erschüttern. Wenn wir mit etwas Neuem und Revolutionärem konfrontiert werden, für das wir nicht genügend Informationen besitzen, um es zu verstehen, ist der erste Instinkt, vor den Veränderungen Angst zu haben, die es möglicherweise mit sich bringt. Angst ist Teil unserer menschlichen Natur.

Sobald wir etwas mehr darüber lernen, relativieren sich die Meinungen über die Gründe, welche zu der Unsicherheit geführt haben. Zudem neigen wir zum Zweifeln, wenn wir mit einer Kollision zwischen unserem tief verwurzelten Glaubenssystem und einem unvorhergesehenen Ereignis konfrontiert werden.

FUD ist Teil dessen, was wir sind. Es ist ein Mechanismus, der uns dazu bringt, den Status quo zu verteidigen und uns dazu veranlasst, Veränderungen kritisch zu betrachten. Wenn wir jede neue Idee ohne eine grundlegende Überprüfung akzeptieren würden, würde unsere Zivilisation zerstört werden. Auf der anderen Seite hilft uns das ständige Auftauchen neuer Informationen dabei, die FUD-Phase zu überwinden, um etwas wirklich Revolutionäres und Wertvolles zu umarmen.



Wie ich die FUD durchbrach und Bitcoin akzeptierte

Meine Bitcoin-Geschichte folgt dem gleichen Muster von FUD. Als ich 2013 zum ersten Mal von Bitcoin las, hielt ich es für eine dumme Idee. Ich war damals 21 Jahre alt und erinnere mich daran, wie ich auf meinen Laptop-Bildschirm starrte und dachte: "Ich habe ein Bankkonto, mit dem ich über eine Internet-App auf mein Geld zugreifen kann. Ich kann Geld an jeden senden, den ich möchte - tatsächlich habe ich noch nie Einschränkungen erlebt. Warum brauche ich das?". Dann schaute ich mir die Anwendungsfälle von Bitcoin an und bemerkte, dass es auf Darknet-Märkten verwendet wird, um Drogen und Waffen zu kaufen. "Ich bin ein anständiger Mensch und ein Gesetzestreuer Bürger", sagte ich zu mir selbst. Also begann ich, Bitcoin zu fürchten und die Veränderungen, die es als Vermittler von Aktivitäten, die ich nicht mag, mit sich bringen könnte.

Im selben Jahr konnte ich meine Miete bei der Studentenunterkunft SGS Goteborg nicht bezahlen, weil ich ein schwedisches Bankkonto benötigte. Also ging ich zu einer schwedischen Bank, um dort ein Konto zu eröffnen - aber da ich kein richtiger Einwohner war (Austauschstudent in Goteborg) und kein Einkommen außer meinem Stipendium hatte, konnten sie mir nicht helfen. Ich hob also Bargeld von einem Geldautomaten ab um es im Büro der Wohnungsbaugesellschaft mit einer Barzahlung zu versuchen. Mir wurde mitgeteilt, dass eine Barzahlung nicht möglich sei, da es verdächtig erscheint und ich das Geld auf ihr Bankkonto überweisen soll. Als ich erklärte, dass meine Bank keine Überweisungen auf ihre Konten akzeptiert (unterschiedliche Länder mit unterschiedlichen IBAN-Codes) und es mir keine lokale Bank erlauben wird, ein Konto zu eröffnen - ohne zusätzliche Papiere, die ich nicht hatte - schlugen sie vor, es mit Western Union oder MoneyGram zu versuchen.

Am nächsten Tag ging ich zu MoneyGram. Ich nahm eines ihrer Formulare und füllte es aus, während ich in

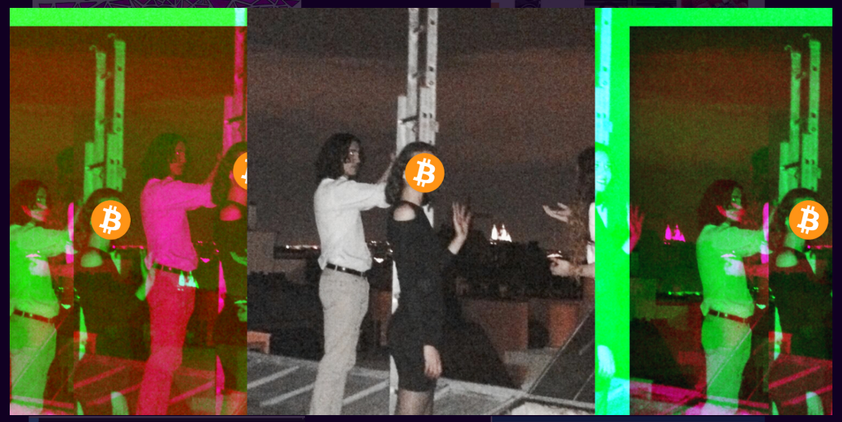


einer langen Schlange wartete. Ich akzeptierte eine Transaktionsgebühr von 30 Euro für eine Zahlung von 600 Euro, stieß jedoch immer noch auf bürokratische Hindernisse. Die Dame hinter dem Schalter sagte mir, dass Kunden aus dem Nicht-Schengen-Raum (Rumänien gehört nicht dazu) ihren Reisepass vorzeigen müssen (den ich nicht hatte, da ich mit meinem nationalen Ausweis dorthin gereist bin). Ich ging zu Western Union und fand genau dasselbe Problem - ich hatte schwedische Kronen in bar, hatte keine Möglichkeit, sie auf mein rumänisches Bankkonto einzuzahlen, und niemand wollte mir helfen, meine Miete zu zahlen, ohne einen Reisepass zu sehen.

Da mein nationaler Ausweis für sie nicht ausreichte, musste ich zur Universität gehen und einen Kommilitonen aus Irland (ein Land, das zum Schengen-Raum gehört) bitten, das MoneyGram-Formular in seinem Namen auszufüllen, in der Schlange zu warten und die Zahlung mit dem Bargeld vorzunehmen, das ich ihm gebe. Um eine so grundlegende finanzielle Transaktion wie die Zahlung der Miete durchzuführen, musste ich einen freundlichen Vertreter finden, der alle erforderlichen Papiere hatte, um eine MoneyGram-Überweisung durchzuführen. (danke, Adam Ballance!).

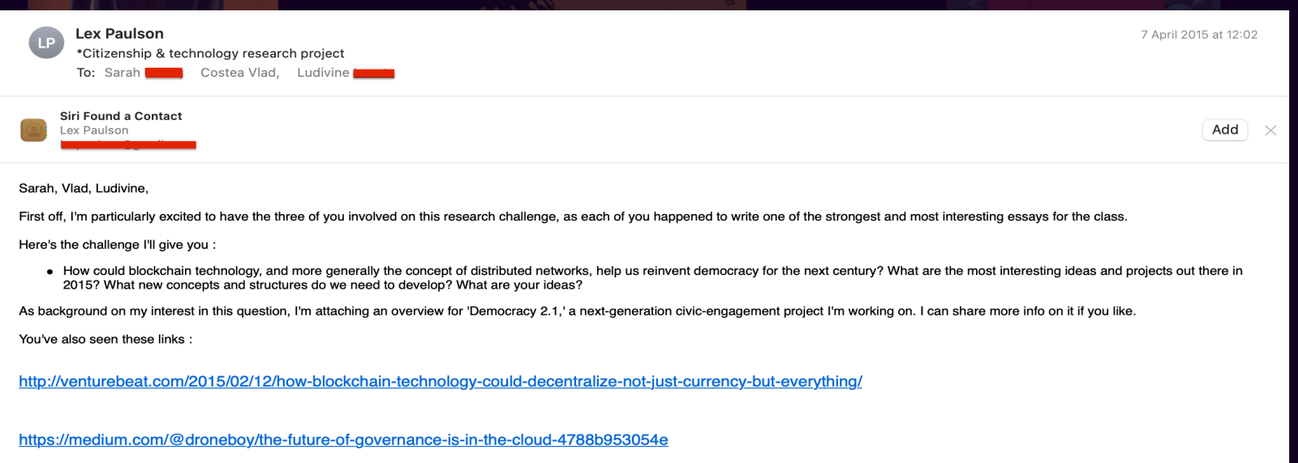
Und dennoch betrachtete ich Bitcoin immer noch als etwas Gefährliches und fürchtete seine Auswirkungen irrational.

Zwei Jahre später, im Alter von 23 Jahren, war ich als Austauschstudent in Frankreich. Dieses Mal konnte ich meine Miete nur in bar bezahlen, da der Vermieter keinen Vertrag unterschreiben und Steuern zahlen wollte. Aber ohne dieses lustige Papier konnte ich kein Bankkonto eröffnen und hatte daher keinen Zugang zu Studentenrabatten für den öffentlichen Nahverkehr oder eine SIM-Karte.Über mehrere Monate hinweg hatte ich keine Möglichkeit, mein Handy für Anrufe zu nutzen und zahlte den vollen Preis für alles. Glücklicherweise fand ich wieder eine Vertreterin - eine rumänische Kommilitonin stimmte zu, Bargeld anzunehmen, damit ich eine ihrer SIM-Karten benutzen durfte, und half mir manchmal auch dabei, günstigere Fahrkarten für die U-Bahn zu bekommen. Gott segne sie, ich hoffe, es geht ihr gut!



2015 war ich immer noch in Paris und besuchte einen Kurs über Advocacy und Innovation. Mein Professor, ein amerikanischer, politischer Theoretiker namens Lex Paulson, beauftragte mich und drei Kommilitonen damit, vor der Klasse eine Präsentation zum Thema Bitcoin und Blockchain zu halten. Es war nicht das erste Mal, dass ich über Bitcoin gelesen hatte, aber es war sicherlich seltsam, dass mich diese Person aus der akademischen Welt aufforderte, mich mit etwas zu befassen, von dem ich wusste, dass es im Internet für Drogen verwendet wurde. Zur gleichen Zeit war ich ein begeisterter Leser des Rolling Stone-Magazins - der Publikation, die mich darüber informierte, dass Ross Ulbricht eine lebenslange Haftstrafe für die Erstellung des Silk Road-Marktplatzes erhalten hatte. Aber da mir jemand bekanntes und respektiertes im echten Leben (im Gegensatz zu einem Troll im Chatroom) sagte, ich solle mich mit Bitcoin beschäftigen, verschwand meine Furcht allmählich.

Ich befand mich nun in der Phase der "Ungewissheit". Ich öffnete mich also mehr für die Idee von Bitcoin, beschäftigte mich intensiver mit den technologischen Auswirkungen, aber ich konnte seine Bedeutung in der Geschichte des Geldes nicht verstehen. Hauptsächlich, weil ich nichts über Wirtschaft und das Finanzsystem wusste - ich studierte Politikwissenschaft und



Lex Paulson
*Citizenship & technology research project
To: Sarah [redacted] Costea Vlad, Ludivine [redacted]
7 April 2015 at 12:02

Siri Found a Contact
Lex Paulson
[redacted]
Add

Sarah, Vlad, Ludivine,

First off, I'm particularly excited to have the three of you involved on this research challenge, as each of you happened to write one of the strongest and most interesting essays for the class.

Here's the challenge I'll give you :

- How could blockchain technology, and more generally the concept of distributed networks, help us reinvent democracy for the next century? What are the most interesting ideas and projects out there in 2015? What new concepts and structures do we need to develop? What are your ideas?

As background on my interest in this question, I'm attaching an overview for 'Democracy 2.1,' a next-generation civic-engagement project I'm working on. I can share more info on it if you like.

You've also seen these links :

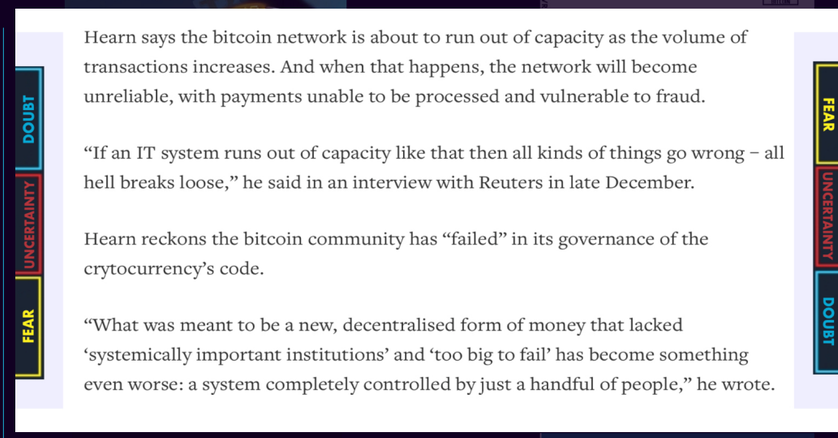
http://venturebeat.com/2015/02/12/how-blockchain-technology-could-decentralize-not-just-currency-but-everything/

https://medium.com/@droneboy/the-future-of-governance-is-in-the-cloud-4788b953054e

war in dieser Blase von Ideen über Regierungsführung gefangen. Ich hätte 1 Bitcoin mit dem Geld, das ich auf meinem Bankkonto hatte (ca. 200 Euro), kaufen können, aber ich tat es nicht, weil ich ein armer Student war, der 5-Euro-Menüs bei McDonald's aß und 20 Euro pro Woche für Lebensmittel ausgab. Ich dachte auch, dass jeder einen ganzen BTC kaufen müsse, was sich als schrecklicher Fehler herausstellte. Hätte ich mit 20 Euro (4 Tage, an denen ich auf McDonald's-Mahlzeiten verzichtet hätte) 0,1 BTC gekauft, wäre es heute etwa 100 Mal mehr wert in Euro - oder fast 350 Mal mehr zum Allzeithoch im November 2021.

Aber die gute Nachricht ist, dass ich seit meiner Präsentation im Mai 2015 ein Auge auf Bitcoin hatte. Ich habe mehr Aufmerksamkeit darauf gerichtet und sogar das Darknet durchforstet, um besser zu verstehen, wie er genutzt wird. Anfang 2016 war ich nach Rumänien zurückgekehrt und mein Bankkonto war etwas besser gefüllt. Also entschied ich mich, endlich etwas BTC zu kaufen - aber genau zu diesem Zeitpunkt las ich in den Nachrichten, dass der ehemalige Core-Entwickler Mike Hearn sagte, dass "Bitcoin gescheitert" sei. Also trat ich in die Zweifelphase meiner Reise ein.

Damals glaubte ich, dass Mainstream-Medienkanäle dazu dienen, die Massen zu informieren... anstatt eine Agenda voranzutreiben, um Märkte zu manipulieren, Regierungen an der Macht zu halten oder zu destabilisieren und die Interessen ihrer Werbekunden/Finanziers zu fördern. Im Januar 2015 hatte sich der Preis von einem Bitcoin verdoppelt im Vergleich zu den 200 Euro, an die ich mich von sechs Monaten zuvor erinnerte. Wenn also ein bedeutender Entwickler sagt, es sei ein gescheitertes Projekt, seine Meinung durch renommierte Publikationen (Reuters, Business Insider, The Guardian) verstärkt wird und der Preis höher ist als zuvor, dann sollte ich mich wahrscheinlich fernhalten und abwarten, was passiert. Wer bin ich schon,



Hearn says the bitcoin network is about to run out of capacity as the volume of transactions increases. And when that happens, the network will become unreliable, with payments unable to be processed and vulnerable to fraud.

"If an IT system runs out of capacity like that then all kinds of things go wrong – all hell breaks loose," he said in an interview with Reuters in late December.

Hearn reckons the bitcoin community has "failed" in its governance of the crytocurrency's code.

"What was meant to be a new, decentralised form of money that lacked 'systemically important institutions' and 'too big to fail' has become something even worse: a system completely controlled by just a handful of people," he wrote.

um es besser zu wissen und BTC für 400 Euro pro Bitcoin zu kaufen?

Erst ein Jahr später, 2017, habe ich mich getraut und einige BTC gekauft. Zu diesem Zeitpunkt hatte der Preis das vorherige Allzeithoch des Bullenmarktes von 1000 US-Dollar überschritten. Ironischerweise war es also der Markt, der mich dazu brachte, allen Mainstream-Kritikern die kalte Schulter zu zeigen. Wer hat gesagt, dass der Preis keine Rolle spielt?

Während der 4 Jahre, die es brauchte, um die FUD zu überwinden, hatte sich der Preis mehr als verdreifacht. Und es war nicht so, dass ich meine neu gekauften Münzen gehalten und sie später im Jahr für einen kleinen Gewinn verkauft hätte... nur um im Dezember 2017 zu einem höheren Preis zurückzukaufen. Aber das ist eine Geschichte für einen anderen Tag.

Um meine Angst vor BTC zu überwinden, brauchte ich Bestätigung von einer Person, die ich hoch schätzte (ein Universitätsprofessor, der mir die Aufgabe gegeben hatte, Bitcoin für ein angesehenes Projekt zu studieren). Um die Ungewissheit zu überwinden, habe ich weitere sechs Monate damit verbracht, über das Phänomen zu lesen. Und um den Zweifel durch eine Kauforder zu ersetzen, musste ich beobachten, wie der Preis trotz der Bericht-erstattung in den Mainstream-Medien stieg. Ich durchlief alle drei Phasen der FUD, nur um zu erkennen, wie all diese Techniken gegen mich eingesetzt wurden.

Ich konnte keine universelle Form des Geldes annehmen, die niemand zensieren oder wegnehmen kann, weil ich an das Bankensystem glaubte, das mir nicht einmal die grundlegendsten Dienstleistungen bieten konnte. Selbst nachdem ich neue Informationen erhalten hatte, konnte ich die Zusammenhänge nicht erkennen, weil ich an die Integrität der Mainstream-Medien glaubte. Und als ich schließlich bereit war, mich der Revolution anzuschließen, wurde ich von einem unehrlichen, aber lautstarken Entwickler verschreckt.

Ich möchte nicht, dass andere denselben Prozess durchlaufen müssen, um unabhängig zu werden. FUD ist eine normale Reaktion, aber es gibt kei-nen Grund, dass es zu einer 4-jährigen Achterbahnfahrt kommt, die von negativen Erfahrungen mit Banken und Finanzdienstleistungen geprägt ist. Deshalb habe ich beschlossen, jede Fehlvorstellung über Bitcoin zu entlarven und eine fundierte Erklärung zu liefern, die effektiv jede FUD zerstört. Die Angst vor etwas ist nur normal, wenn es neu ist und man keine Möglichkeit hat, sich selbst zu erklären, was es ist. Das Gefühl der Unsicherheit ergibt sich, solange die Informationsbeschaffung unzuverlässig ist. Und Zweifel entstehen nur bei denen, die keinerlei Vertrauen und Überzeugung in die erhaltenen Informationen gewinnen konnten.

It's Time To Break The FUD!

Satochip

Secure the future.



No need to be an AI to use a Satochip hardware wallet. The open source solution to manage your #cryptocurrency easily.

satochip.io/shop

@TheVladCostea

Hey ChatGPT, what are the top 10 most serious threats to the Bitcoin project?

@ChatGPTBot

1. Regulation: Government intervention in the form of restrictive laws or outright bans on the use of cryptocurrencies could impede the growth and adoption of Bitcoin.
2. Competition from other cryptocurrencies: The emergence of new, more advanced cryptocurrencies could potentially steal market share from Bitcoin.
3. Scalability issues: The limited number of transactions that can be processed on the Bitcoin network at any given time could become a bottleneck as adoption grows.
4. Security vulnerabilities: As Bitcoin's value and user base increases, it becomes an increasingly attractive target for hackers and other malicious actors.
5. Volatility: The price of Bitcoin has been known to be extremely volatile, which can make it difficult for businesses and individuals to effectively use it as a medium of exchange or store of value.
6. Limited use cases: Bitcoin has a limited set of use cases, which could limit its adoption and growth.
7. Energy consumption: The energy consumption required to maintain the Bitcoin network has been a point of concern, as it is significantly higher than most other payment systems.
8. Centralization of mining: A small number of mining pools control a large portion of the mining power on the Bitcoin network, which could lead to centralization of power and decision-making.
9. Lack of education and understanding: Many people still do not understand the technology behind Bitcoin and cryptocurrencies, which could limit its adoption.
10. Lack of mainstream acceptance: While Bitcoin has made significant strides in recent years, it is still not widely accepted by mainstream businesses and individuals.



Breaking ChatGPT's Bitcoin FUD #1:

Gesetzliche Regulierung

BITCOIN IST BESSER ALS DEINE REGIERUNG **BITCOIN REGULATION**

GEFÄLLT DIR DER ARTIKEL? SCANNE DEN QR-CODE UND HINTERLASSE EIN KOMMENTAR ODER EINE DONATION!

Als ich **Chat GPT** bat, eine Liste der zehn größten Bedrohungen für **Bitcoin** bereitzustellen, standen Regulierungen ganz oben auf der Liste. Laut der These der KI haben eingeschränkter Zugang und vollständige Verbote das Potenzial, die Annahme und das Wachstum von **Bitcoin** zu behindern.

Auf den ersten Blick erscheinen diese Bedenken legitim. Aber wenn man versteht, wie Internet-Privatsphäre und **Bitcoin** funktionieren, wird einem klar, dass nur staatlich regulierte Unternehmen, die den Kauf und Verkauf von **Bitcoin** erleichtern, wirklich betroffen sind. Regierungen können Coinbase, Binance, eToro, Kraken, Bitfinex und jedes andere Unternehmen schließen, das unter einer feindlichen Rechtsprechung operiert. Sie können auch Einzelpersonen, die solche Dienste nutzen, schwer bestrafen, indem sie ihre Bankkonten schließen und ihre soziale Kreditwürdigkeit so stark senken, dass viele ihrer Freiheiten wegfallen. Aber dies sind alles gesellschaftspolitische Probleme, die nichts mit dem **Bitcoin**-Netzwerk zu tun haben.

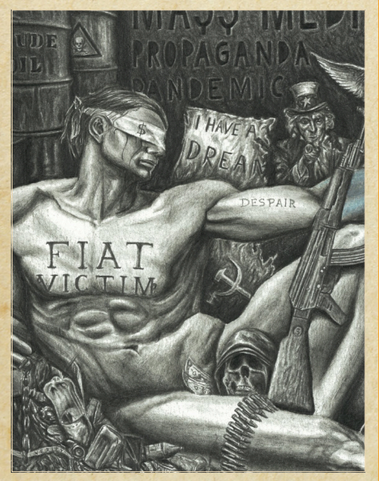
In den meisten Ländern der Welt (mit einigen Ausnahmen) kann die Regierung keinen privaten Bürger daran hindern, einen Computer zu besitzen, auf das Internet zuzugreifen und freie Open-Source-Software auszuführen. In Verfassungen, die individuelle Freiheit gewähren und schützen, wird Computercode als freie Meinungsäußerung angesehen, und der Zugang zu Informationen ist ein grundlegendes Menschenrecht. Sicherlich können spezifische Verbote erlassen werden, um die **Bitcoin**-Software abzudecken - aber was ist **Bitcoin**, wenn nicht Software und reine Mathematik? Es ist nicht so, als ob der Client nicht von Grund auf in einer anderen Programmiersprache und unter einem anderen Namen neu geschrieben werden könnte, während die gleichen Konsensregeln beachtet werden. Und wenn die Verbindung zum Bitcoin-Netzwerk selbst verboten wird, kommen Verschleierungstechnologien wie Tor, Nym und VPNs zum Einsatz.

Selbst ohne Internetzugang gibt es ernsthafte Entwicklungen im Bereich von Mesh-Antennen und Satellitenkommunikation. Derzeit mietet Blockstream einen Satelliten, der Informationen der neuesten **Bitcoin**-Transaktionen überträgt. Jeder, der eine parabolische Antenne erwirbt oder aufbaut (die am häufigsten von Menschen verwendet wird, um Zugang zu entfernten Fernsehkanälen zu erhalten), kann Informationen über das **Bitcoin**-Netzwerk erhalten, ohne Internetzugang zu benötigen. In Zukunft können wir uns auch Szenarien vorstellen, in denen Mesh-Antennen in vernünftigen Abständen aufgestellt werden, um als dauerhafte Sicherung für die ansonsten fragile Internetinfrastruktur zu dienen. Und wenn all diese Pläne scheitern, gibt es auch laufende Forschungen zur Übertragung von **Bitcoin**-Transaktionen über Kurzwellenfunksignale - derselben Technologie, die während des Kalten Krieges verwendet wurde, um Propaganda über nationale Grenzen hinweg zu senden, nun für **Bitcoin** neu interpretiert. Andererseits sollten wir uns bewusst sein, dass **Bitcoin** stirbt, sobald die Menschen aufhören, ihn zu nutzen. An sich hat keine Technologie eine Bedeutung, und es sind die Individuen, die sie übernehmen, die ihr Zweck und Ziele verleihen. Entsprechend kann **Bitcoin** effektiv zerstört werden, wenn ein Regierungsverbot die Menschen gleichgültig gegenüber dem Projekt macht. In Abwesenheit von Freiheitskämpfern, die sich um den Schutz ihrer persönlichen Angelegenheiten vor Regierungen kümmern, kann **Bitcoin** keinen Erfolg haben.

Dennoch wird Bitcoin trotz des politischen Druckes und der Verbote erfolgreich sein...

solange **Bitcoin** Freiheit bei Transaktionen und Schutz vor Beschlagnahmung bietet. Wenn Börsen und registrierte Unternehmen verboten werden, würde dies die Preisfindung beeinträchtigen. Eine solche Situation erschwert die Preisgestaltung von Waren und Dienstleistungen, daher müssen lokale oder regionale Währungen entsprechend dem Verhältnis von Angebot und Nachfrage festgelegt werden. Vielleicht wird es schwieriger sein, den Wert von einem **Bitcoin** in traditionellen Währungen zu bewerten, aber Menschen könnten Arbeitsstunden oder bestimmte Güter entsprechend dem verfügbaren **Bitcoin**-Angebot messen.

Wenn eine Regierung **Bitcoin** verbieten würde, würde dies effektiv die Entstehung von Schwarzmärkten fördern, was zu einer Adoption außerhalb der Kontrolle und Reichweite der Autorität führt. Schließlich ist die Software Open-Source und niemand kann die Benutzer daran hindern, alle für die







Interaktion mit dem **Bitcoin**-Netzwerk erforderlichen Elemente zu verteilen und sogar neu zu reproduzieren. Aus spieltheoretischer Sicht ist es für die Regierung besser, die **Bitcoin**-Adoption innerhalb ihrer Kontrolle zu erleichtern. Die Sammlung von Informationen über Benutzer durch legale private Unternehmen hilft ihnen auch bei der Steuererhebung. Zudem stärkt die Gewährung eines gewissen Maßes an Freiheit das Image des Regimes als freiheitsorientiert und verringert die Wahrscheinlichkeit eines Staatsstreichs.

Jedoch ist das vorgestellte Beispiel zu weitreichend. Es gibt zwei extreme Fälle, in denen ein Verbot von **Bitcoin** aus Sicht einer Regierung Sinn ergibt: wenn die Vorherrschaft der Fiatwährung bedroht ist (wie im Fall der Vereinigten Staaten von Amerika) und wenn die Fähigkeit, in Krisenzeiten die Finanzen des Landes zu kontrollieren, durch Menschen, die aussteigen, erheblich untergraben wird (wie in Nigeria und Argentinien im Jahr 2023).

Es sei jedoch darauf hingewiesen, dass das erste Beispiel das weltweit erste moderne demokratische Land betrifft und die Regierung bewusst Anstrengungen unternimmt, um Menschenrechte, Rechtsstaatlichkeit und bürgerliche Freiheiten in der ganzen Welt zu fördern. Wenn die USA selbst eine solch fehlerhafte Demokratie werden würden, würde ihre Soft Power gegenüber Akteuren wie China und der Russischen Föderation abnehmen.

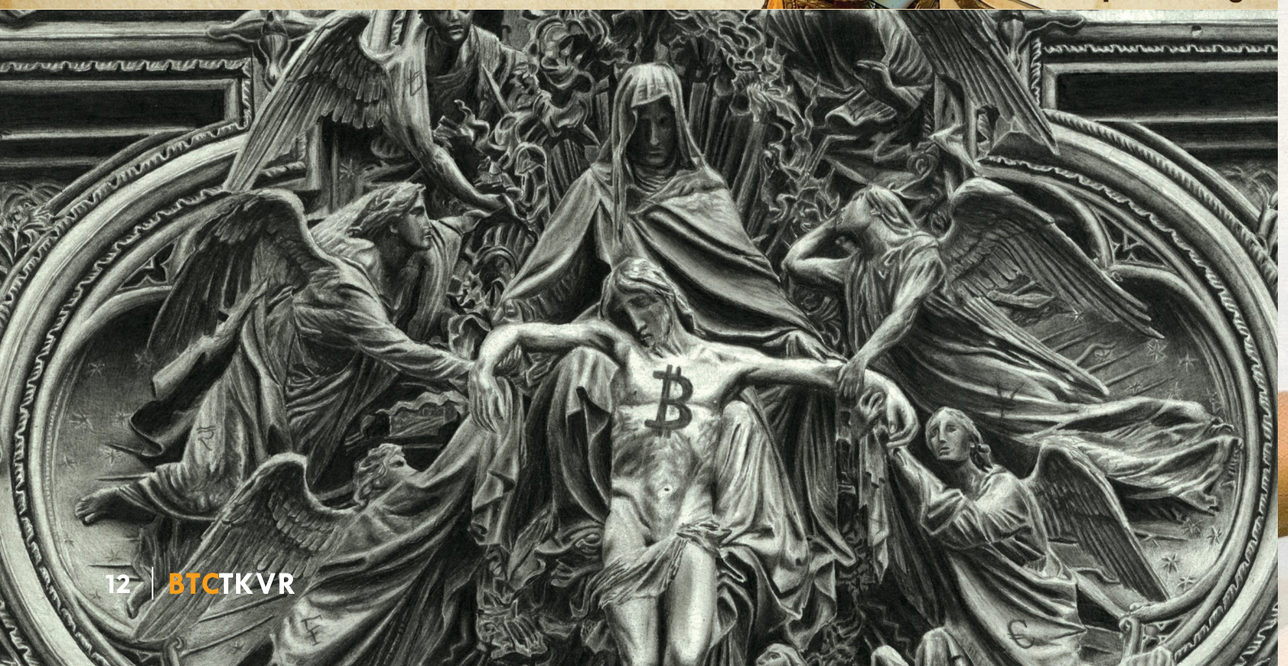


Im Fall von Nigeria ergibt es viel mehr Sinn, **Bitcoin** zu verbieten, um die Kontrolle über die Geldschöpfung zurückzugewinnen und das Vertrauen in das Geld wiederherzustellen. Schließlich macht eine Erhöhung des Angebots nur dann Sinn, wenn eine reale Nachfrage nach dem Geld besteht. Und jede Form von Währung, die eine Flucht aus der bestehenden Machtstruktur ermöglicht, muss von denen, die an der Regierung bleiben und die Vorherrschaft eines älteren Systems behalten wollen, zerschlagen werden.

Dennoch liegt es auch im Interesse Nigerias, Kapitalzuflüsse zu erhalten und Teil der globalen Wirtschaft zu sein. Und für Tausende (wenn nicht Millionen) von Freiberuflern besteht eine reale Möglichkeit, remote zu arbeiten und in einer besseren Geldform bezahlt zu werden - die natürlich in der Landeswährung umgetauscht wird, um Lebensmittel zu kaufen und Lebenshaltungskosten zu decken. Daher ist es für Entwicklungsländer wie Nigeria besser, den Jugendlichen die Verwendung von **Bitcoin** zu ermöglichen, solange die Zentralbanker das Vertrauen in ihre eigene Währung aufrechterhalten können. Andernfalls entwickelt sich die Situation zu einer vollständigen Übernahme von **Bitcoin**, bei der die nichtstaatliche digitale Währung das trojanische Pferd für Freiheit von Transaktionen und den Zusammenbruch des Zentralbankwesens ist.



Aus geopolitischer Sicht ist Bitcoin ein Instrument für Erpressung.



Aus geopolitischer Sicht sind Nationen dauerhaften Bedrohungen ausgesetzt. Wenn sie **Bitcoin** nicht erlauben, besteht die Gefahr, dass ihre Nachbarländer dies tun und somit mehr Kapital aus den globalen Märkten aufnehmen und sich schneller entwickeln. Niemand möchte im Rennen um Innovation zurückfallen. Wenn Regierungen als Preis dafür **Bitcoin** ermöglichen müssen, würden sie diese Kompromisse lieber eingehen.

Es gibt auch Argumente für regionale Allianzen, internationale Handelsföderationen und Konföderationen. Oberflächlich betrachtet sind diese Regierungsformen eher bereit, zusammenzuarbeiten, um ein gemeinsames Ziel zu erreichen. Wenn sie entscheiden, dass **Bitcoin** eine große Bedrohung darstellt, werden sie Wege finden, **Bitcoin** zu verbieten. Es gibt jedoch zwei Tatsachen, die eine solche Vereinbarung unwahrscheinlich machen:

1. Erstens konkurrieren selbst Mitglieder von Föderationen/Konföderationen/Allianzen wirtschaftlich miteinander, und es ist für die weniger entwickelten Gebiete schwer, nur um des Willens der anderen auf zusätzliche Mittel zur Wohlstandsschaffung zu verzichten. Damit eine Vereinbarung getroffen werden kann, müssten die entwickelteren und wohlhabenderen Mitglieder des internationalen Gremiums ernsthafte kompensatorische Zugeständnisse an die anderen machen. Dieses Szenario ist jedoch langfristig unwahrscheinlich.

2. Zweitens hat keine internationale Regierungsorganisation (einschließlich der Vereinten Nationen) eine Mitgliedschaft, die alle souveränen Nationen abdeckt. Palästina, Kosovo, Taiwan, Hongkong und die Westsahara sind nur fünf Beispiele für Länder, die nicht Teil der UN sind. Solange zumindest eines von ihnen neutral zu globalen Politiken bleibt (was sehr wahrscheinlich ist, angesichts des Status vieler von ihnen als Steueroasen), wird **Bitcoin** weiterhin wie vorgesehen funktionieren. Und die Tatsache, dass eine Nation von Wohlstand profitiert, den **Bitcoin** mit sich bringt, wird den Wettlauf zur Adoption nur beschleunigen.

Die beste Zeit, um **Bitcoin** zu verbieten, war wahrscheinlich in den ersten vier Jahren seiner Existenz. Bevor die Nutzer nach dem Mt. Gox-Fiasko die Vorzüge der Eigenverwahrung entdeckten, bevor Knotenbetreiber ihre Widerstandsfähigkeit gegenüber großen Unternehmen zeigten, die 2017 die Blockgröße über eine Hard Fork erhöhen wollten, und bevor die Miner im Jahr 2021 erfolgreich aus China migrierten. Dies sind alles Beispiele für Widerstandsfähigkeit und Beharrlichkeit. Zu diesem Zeitpunkt ist **Bitcoin** ein globales finanzielles Phänomen. Er hat das Leben der Menschen in dem Maße verändert, dass sie bereit sind, für die Verteidigung des Netzwerks zu kämpfen. Es handelt sich auch um eine Art ehrliches Geld, das Regierungen und Zentralbanker zur Rechenschaft zieht, indem es sie dazu zwingt, weniger Geld zu drucken... vorausgesetzt, dass sie am langfristigen Überleben ihrer Fiatwährungen interessiert sind.

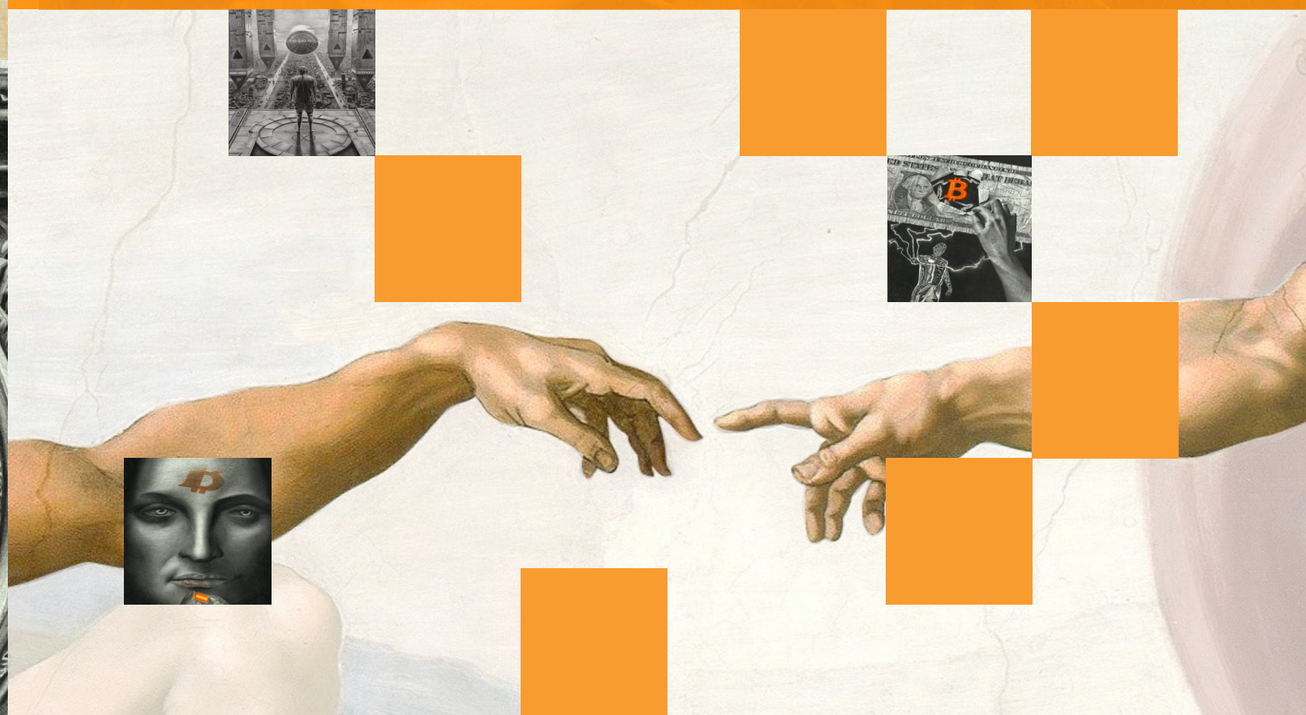
Wie der Nakamoto-Konsens besagt, ist es ökonomisch rationaler, ein ehrlicher Akteur in der Mission von **Bitcoin** zu werden, als dagegen anzukämpfen. Regierungen sind von diesem Axiom nicht ausgenommen, weshalb sie FUD verwenden, um sich mehr Zeit zu verschaffen (und KI-Software zu programmieren, um ihre Agenda voranzutreiben).



Sorry, ChatGPT, dieses mal hast du verloren!



SCORE
Vlad C. 1
ChatGPT 0



Mallorca
Blockchain Days

Be part of the
Mallorca Blockchain Days IV
experience

July 13 - 16 2023

Palma, Mallorca, Spain

GET YOUR TICKET ONLINE

WWW.MALLORCABLOCKCHAINDAYS.COM



Breaking ChatGPT's Bitcoin FUD #2:

Altcoins

GEFÄLLT DIR DER ARTIKEL? SCANNE DEN QR-CODE UND HINTERLASSE EIN KOMMENTAR ODER EINE DONATION!

ALTCOINS GEHEN AUF NULL

Laut **ChatGPT** könnte das Aufkommen neuer und fortschrittlicherer Krypto-Währungen Marktanteile von **Bitcoin** stehlen. Im Allgemeinen werden diese Alternativen zu **Bitcoin** als "Altcoins" bezeichnet und bestehen größtenteils aus modifizierten **Bitcoin**-Klonen, die weder originell noch "fortschrittlich" sind. Altcoins sind im Wesentlichen **Bitcoin's** Experimentierfeld - parallele Netzwerke, die Funktionen testen, die zuerst bei **Bitcoin** vorgeschlagen wurden, aber nicht genügend Unterstützung von der Community oder den Entwicklern erhalten haben. Da der **Bitcoin**-Code vollständig Open-Source ist, kann ihn jeder kopieren, modifizieren, neue Funktionen hinzufügen und dann ein völlig neues Netzwerk erstellen, das sich auf einen bestimmten Anwendungsfall konzentriert.

Der Grund, warum das **Bitcoin**-Netzwerk nicht alle Anwendungsfälle unterstützen kann, lässt sich am besten mit dem Zooko-Dreieck erklären - einem Trilemma-Modell, bei dem Systemarchitekten zwei der drei grundlegenden Qualitäten wählen müssen: Sicherheit, Dezentralisierung und Benutzerfreund-

keit (in unserem Fall Skalierbarkeit). Bitcoin ist definitiv sicher und dezentralisiert. Allerdings skaliert das Modell nicht besonders gut. Wenn die Blockgröße beliebig erhöht würde (wie bei Forks wie Bitcoin Cash geschehen), würde dieses Upgrade auf Kosten einer geringeren Dezentralisierung erfolgen und potenzielle Sicherheitsrisiken verursachen.

Es muss ein vernünftiges Gleichgewicht aufrechterhalten werden, um sicherzustellen, dass das Netzwerk nicht von Computern in großen Rechenzentren validiert wird (wie es bei Ethereum und anderen Netzwerken der Fall ist, die große Datenmengen speichern). Im Fall von Bitcoin können die Blöcke nicht größer als 4 Megabyte sein - ein willkürlicher Wert, der als vernünftiger Kompromiss angesehen wurde, um mehr Skalierbarkeit zu ermöglichen, ohne die anderen grundlegenden Qualitäten zu beeinträchtigen.

Deshalb gibt es Altcoins: Sie nutzen eine Begrenzung von Bitcoin aus, identifizieren eine Lösung und implementieren ein neues Netzwerk, um zu sehen, was der freie Markt davon hält. Manchmal ist diese Experimentierfreude nützlich, indem sie empirische Beweise für verschiedene Vor- und Nachteile bestimmter Vorschläge liefert, aber meistens sind diese Projekte in Bezug auf ihre Kompromisse trügerisch, indem sie vorgeben, 1000-mal schneller oder sicherer als Bitcoin zu sein, ohne gleichzeitig dezentralisiert zu sein.

Wie die Geschichte zeigt, scheitern mehr als 90% dieser Projekte. Sie bleiben selten länger als einen Bullenmarkt-Bärenmarkt-Zyklus bestehen und verlieren an Bedeutung, insbesondere weil sie nicht die erwartete Akzeptanz finden und neue, verbesserte Vorschläge aufkommen. Dies ist eine gute Nachricht für wissenschaftliche Experimente, aber eine schlechte Nachricht für Investoren, die dem Hype glauben und wertlose Coins halten.

Es gibt technische, soziale und wirtschaftliche Gründe, warum diese Altcoins scheitern,

während Bitcoin weiterhin gedeiht.

Aus technischer Sicht ist Bitcoin das zuverlässigste, sicherste einzig wirklich dezentrales Netzwerk, das nachhaltige langfristige Investoren anzieht.

Bitcoin funktioniert gut für seinen vorgesehenen Zweck, und seine Mängel können durch den Aufbau von Schichten darüber (wie das Lightning-Netzwerk) oder durch die Verlagerung eines Teils der Aktivität auf parallele Ketten (Sidechains wie RSK, Statechains, Drivechains und Liquid) überwunden werden.

Die wirtschaftlichen Gründe, warum Bitcoin gedeiht, betreffen eine zunehmend gerechtere Verteilung des Reichtums und die daraus resultierende größere Akzeptanz. Bitcoin hatte keine Vorabbestände, Satoshi hat keinen einzigen Coin ausgegeben und höchstwahrscheinlich seine Kryptowährung als Köder für Hacker hinterlassen, und die Geldpolitik ist sehr einfach zu verstehen. Es gibt nur 21 Millionen Coins, die gemäß einem wohlgetimten und umfassenden Inflationsplan ausgegeben werden, der im Laufe der Zeit die Belohnungen senkt. Sicher, man kann argumentieren, dass frühe Anwender leichteren Zugang zu BTC hatten - bis zu dem Punkt, an dem sie mit der CPU ihres Laptops minen oder kostenlose Coins aus Gavin Andresens Faucet im Juni 2010 erhalten konnten. Aber gleichzeitig hatte Bitcoin zu dieser Zeit keinen monetären Wert, und es dauerte einige Jahre, bis sich Märkte entwickelten.

Das folgende Argument stellt aus sozialer Betrachtung dar, warum Bitcoin weiterhin gedeiht. Zunächst einmal hatte Bitcoin eine makellose Konzeption und existierte in einer frühen Phase mehrere Jahre, bevor das große Geld hereinkam. Heutzutage, inmitten einer gesamten Blockchain-Branche, die Geld in Projekte steckt und investorzentrierte Vorverkaufsveranstaltungen fordert, ist es äußerst schwierig, diese Leistung zu erbringen. Grin ist ein seltenes Beispiel für einen Altcoin, der alles richtig gemacht hat und ehrlich geblieben ist - aber es gelang ihm dennoch nicht, genügend Aufmerksamkeit zu erlangen, um die Entwickler bezahlen zu können. Und das ist ein weiteres großes Problem: Erwartungen und der ständige Druck, dem ideologisch motivierte Entwickler ausgesetzt sind, während sie wissen, dass sie anderswo viel Geld verdienen könnten.

Die ersten Bitcoin-Adopter hatten keine finanziellen Erwartungen an das Projekt, sie mochten einfach die Idee von nicht-regierungsgesteuertem digitalem Geld ohne einzelnen Fehlerpunkt. Sie bauten Wallets, Anwendungen auf und etablierten Traditionen, lange bevor es ein angemessenes Börsensystem gab, um BTC gegen USD zu handeln. Und sie sind auch diejenigen, die aus rein ideologischen Gründen dabei geblieben sind, ohne sich allzu sehr darum zu kümmern, reich zu werden (auch wenn sie wohlhabend wurden).

Wir sollten auch über die Welle der libertären Anwender sprechen, die Bitcoin zwischen 2011 und 2014 begrüßten. Sie sind es, die die meisten heutigen Unternehmen aufgebaut und viele der Metaphern geschrieben haben, die Bitcoin beschreiben, von

"Bitcoin ist der Honigdachs des Geldes" bis zu "Alles ist gut für Bitcoin".

Ihr größtes Verdienst besteht darin, dass sie es "sicher" gemacht haben, ein Bitcoiner zu sein: Sie haben die rechtlichen Auseinandersetzungen geführt, Regulierungsbehörden beeinflusst und ihre Erzählungen genutzt, um Politikern zu erklären, warum ein Verbot von Bitcoin für die zukünftige wirtschaftliche Landschaft nachteilig sein könnte. Und sie haben dies lange Zeit getan, bevor das Halten von BTC sie zu Millionären in USD gemacht hat.

Dann gibt es die Generation von Bitcoinern, die während der Fork-Kriege darum kämpften, die Integrität des Netzwerks zu schützen. Angreifer nahmen an, dass der Wert von Bitcoin durch die Schaffung von Dutzenden modifizierter Kopien verwässert werden kann, die die Benutzer aufteilen und einen Teil der Aktivität entziehen. Sie lagen falsch, insbesondere weil die soziale Ebene die ursprüngliche





Bitcoin-Chain geschützt hat, den größten Teil der wirtschaftlichen Aktivität darauf gehalten hat und daher Benutzer und Miner davon abgehalten hat, Forks zu unterstützen.

Im Jahr 2023 ist es sehr unwahrscheinlich, dass eine andere Kryptowährung ernsthaft mit **Bitcoin** konkurrieren würde. Ethereum kann so viel von seiner Versorgung verbrennen, wie gewünscht, die Schäden des Premine von 70 Millionen Coins sind nicht umkehrbar, und Ethereums Finanzpolitik wird immer einer Zentralbank ähneln, die kurzfristige Entscheidungen für sich ständig ändernde Ziele trifft. Monero kann mit seiner überlegenen Privatsphäre prahlen, aber kann nicht ohne XMR/**BTC**-Swaps überleben, die die Händleradoption und Akzeptanz in der gesamten Wirtschaft ermöglichen. Und selbst wenn etwas radikal Besseres auftaucht, das eine völlig andere Architektur verwendet und sich vom Blockchain-Modell verabschiedet, würde es Jahre dauern, bis es das Niveau der Anerkennung und Adoption von **Bitcoin** erreicht.

Ein sicherer und dezentralisierter **Bitcoin**, dessen Skalierbarkeit und Privatsphäre in Schichten verbessert werden, kommt dem idealen Geld sehr nahe. Es wird jedoch noch einige Jahre dauern, bis die Technologie so ausgereift ist, dass sie auch für nicht-technische Benutzer zugänglich wird, die kein Englisch sprechen. Dies ist genug Zeit für schlechte Akteure, den Markt mit halbgaren Lösungen zu testen, die indirekt den Ruf von **Bitcoin** beschädigen und die Adoption verlangsamen könnten.

Letztendlich ist **Bitcoin** das Ergebnis von drei Jahrzehnten Forschung in Kryptographie und Informatik. Er ist eine interessante Verbindung aus Spieltheorie, Technologie und Wirtschaft, die nie übertroffen wurde. Es ist das Netzwerk, das jede Welle von FUD überlebt hat und kontinuierlich neue Allzeithochs gegenüber Gold und dem US-Dollar erreicht hat. Und es ist die Währung, die seit anderthalb Jahrzehnten in Bezug auf Adoption und Marktkapitalisierung unangefochten an erster Stelle steht.

Heute spricht niemand mehr über Peercoin, Vertcoin und NXT. Niemand glaubt immer noch daran, dass DASH, Nano und Decred **Bitcoin** ersetzen werden. Heute haben wir Coins mit ähnlichen Ambitionen, aber verschiedenen Namen - sie werden höchstwahrscheinlich dem Beispiel von Vertcoin in das Grab der gescheiterten Kryptoexperimente folgen. Die Anzahl der Menschen, die wirklich glauben, dass das politisch fragilere Ethereum ein echter Konkurrent ist, ist ebenfalls gering - wir dürfen nicht vergessen, dass der Ethereum-ICO in **BTC** abgehalten wurde und hauptsächlich von Bitcoinern besucht und unterstützt wurde.

Je länger **Bitcoin** existiert und je mehr Menschen davon erfahren, desto widerstandsfähiger wird er. Und die Tatsache, dass er eine makellose Konzeption, bescheidene Anfänge und ein organisches Wachstum hat, macht es noch schwieriger, ihn als Phänomen zu reproduzieren. Es braucht den richtigen historischen Kontext, die richtige technologische Innovation und das passende wirtschaftliche Umfeld, um etwas wie **Bitcoin** zu schaffen und zu starten. Deshalb wird **Bitcoin** wahrscheinlich niemals durch eine andere Kryptowährung ersetzt werden.

Sorry ChatGPT, aber du und deine Programmierer liegt wieder falsch.



SCORE
Vlad C. 2
ChatGPT 0

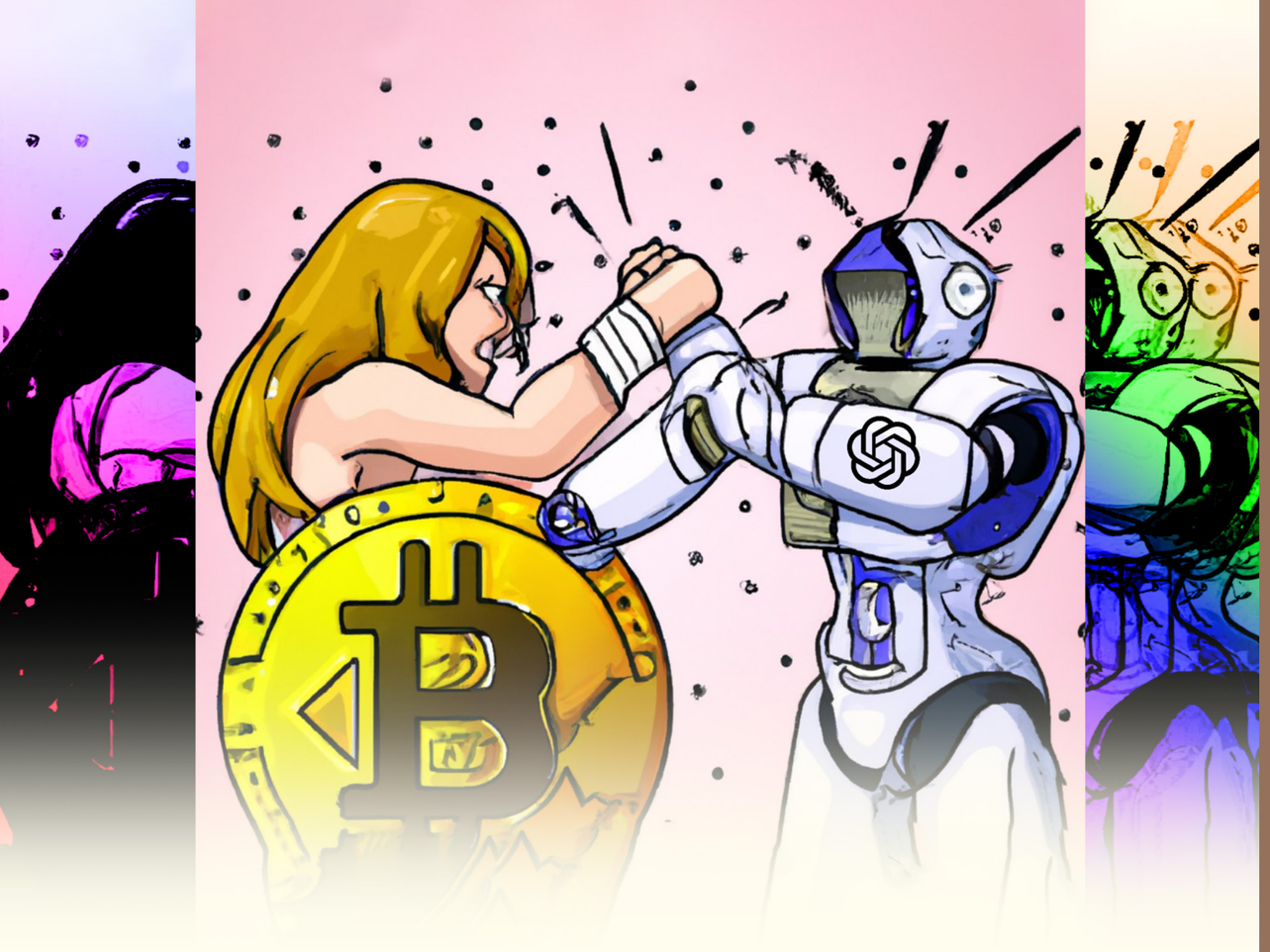




WASABI WALLET

HIDE HIS STORY

DOWNLOAD NOW AT
WASABIWALLET.IO



Breaking ChatGPT's Bitcoin FUD #3:

Skalierung

WIE BITCOIN SKALIERT | SEGWIT | SKALIERBARKEIT

GEFÄLLT DIR DER ARTIKEL? SCANNE DEN QR-CODE HINTERLASSE EIN KOMMENTAR ODER EINE DONATION!

Laut **ChatGPT** könnte die begrenzte Anzahl an Transaktionen, die das **Bitcoin**-Netzwerk verarbeiten kann, zu einem Engpass führen, wenn die Adoption zunimmt. Dies ist eine durchaus berechtigte Kritik an **Bitcoin**, da keine Blockchain skalierbar ist. Tatsächlich wurde James A. Donald dies bereits im November 2008 in einer E-Mail an Satoshi Nakamoto auf der Kryptographie-Mailingliste mitgeteilt: "Es scheint nicht auf die erforderliche Größe skalierbar zu sein". Dies war das erste öffentliche Feedback, das Satoshi Nakamoto über **Bitcoin** erhielt und es umriss prägnant die Einschränkungen des Systems.

Interessanterweise enthält dieselbe E-Mail von James A. Donald auch eine potenzielle Lösung für eine breitere Akzeptanz und Skalierbarkeit: "ein Datei-Handelsnetzwerk ähnlich wie Bittorrent". Mit anderen Worten, eine weitere Schicht, die schnell ist und die Peers direkt miteinander verbindet und eine beliebige Anzahl von Transaktionen verarbeiten kann, die nur durch die Bandbreite jedes Benutzers begrenzt ist. Etwas, das keine Blockchain benötigt und nicht überlastet und zentralisiert wird, wenn zu viel Aktivität stattfindet. Außerdem ein System, das in seinem Design sehr dem von Bittorrent ähnelt und daher nicht jeden Benutzer dazu zwingt, die Daten aller anderen zu speichern, zu überprüfen und zu validieren. Das klingt doch sehr nach dem Lightning-Netzwerk, oder?

Re: Bitcoin P2P e-cash paper

James A. Donald | Sun, 02 Nov 2008 17:55:45 -0800

Satoshi Nakamoto wrote:

> I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.
>
> The paper is available at:
> http://www.bitcoin.org/bitcoin.pdf

We very, very much need such a system, but the way I understand your proposal, it does not seem to scale to the required size.

For transferable proof of work tokens to have value, they must have monetary value. To have monetary value, they must be transferred within a very large network - for example a file trading network akin to bittorrent.

To detect and reject a double spending event in a timely manner, one must have most past transactions of the coins in the transaction, which, naively implemented, requires each peer to have most past transactions, or most past transactions that occurred recently. If hundreds of millions of people are doing transactions, that is a lot of bandwidth - each must know all, or a substantial part thereof.

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to

Die technische Kritik von James A. Donald war wahrhaft visionär, da er sowohl die Skalierungskriege vorhergesagt hat, die im ersten Jahrzehnt von **Bitcoins** Existenz stattfinden würden, als auch einen Weg vorgeschlagen hat, um die Geschwindigkeit der Währung zu erhöhen. Allerdings reicht diese Aussage von 2008 allein nicht aus, um die Bedenken von **ChatGPT** zu entkräften - eine angemessene Kontextualisierung ist erforderlich, um die aktuelle Strategie zur Skalierung von **Bitcoin** zu verdeutlichen und warum sie sehr wahrscheinlich erfolgreich sein wird.

Warum hat **Bitcoin** überhaupt mit Skalierungsproblemen zu kämpfen?
Das liegt alles in der Natur der Dezentralisierung und wie Blockchains funktionieren.

Der erste Instinkt ist es, das Netzwerk größere Blöcke schneller abbauen zu lassen - aber dadurch wird es nur schwieriger für normale Benutzer auf der ganzen Welt, ihre eigenen Transaktionen zu validieren, wie es jeder souveräne Bitcoiner tun sollte. Andererseits hat das Erhöhen der Blockgröße den Nebeneffekt, dass leistungsstärkere Hardware benötigt wird - ein rutschiger Abhang, der bei Servern und industrietauglichen Computern endet und den Zweck der Dezentralisierung effektiv zunichte macht. Sobald man eine bestimmte Blockgröße erreicht (wie es bei BSV der Fall ist), könnte man genauso gut PayPal verwenden.

Ein ideales Netzwerk muss sicher, dezentralisiert und skalierbar sein. Aber laut Zookos populärem Dreieck können Computernetzwerke nur zwei davon haben und müssen ihre Kompromisse wählen - mit der Absicht, sie auf andere Weise zu ergänzen. Sicherheit hat dabei oberste Priorität. Ohne sie haben finanzielle Transaktionen keine Endgültigkeit und sind daher wertlos. Aber auch physisches Bargeld und Gold haben eine gute Endgültigkeit. Also ist es die Dezentralisierung, die das Hauptverkaufsargument von **Bitcoin** darstellt - es bietet Zugang zu einem globalen Finanznetzwerk, ohne dass Bankinstitute erforderlich sind und ohne dass eine kontrollierende dritte Partei in der Mitte steht. Jeder kann am Mining und der Validierung teilnehmen, jeder kann eine Wallet herunterladen und Coins erhalten, auch wenn er die Validierung an einen anderen Knoten delegiert (SPV, oder Simple Payment Verification). Niemand kann eine Transaktion zensie--ren, die Gelder Beschlagnahmen oder bestimmte Personen daran hindern, das Netzwerk zu nutzen. Ohne diese Eigenschaften würde sich **Bitcoin** nicht von PayPal unterscheiden.

Aber all dies geht auf Kosten begrenzter Skalierbarkeit.



Bitcoin baut etwa alle 10 Minuten einen neuen Block ab und fügt etwa 2000 neue Transaktionen hinzu, die eine Bestätigung erhalten. Das System ist für diese frühe Phase der Adoption nicht schlecht. Das Design mit einer willkürlich begrenzten Blockgröße soll einen aufstrebenden und wettbewerbsfähigen Gebührenmarkt ermöglichen, der das Einkommen der Miner unterstützt. Allerdings muss **Bitcoin** in der Lage sein, alle finanziellen Transaktionen der Welt auf kompromisslose Weise zu bewältigen - und dies gelingt durch Schichten (Layers).

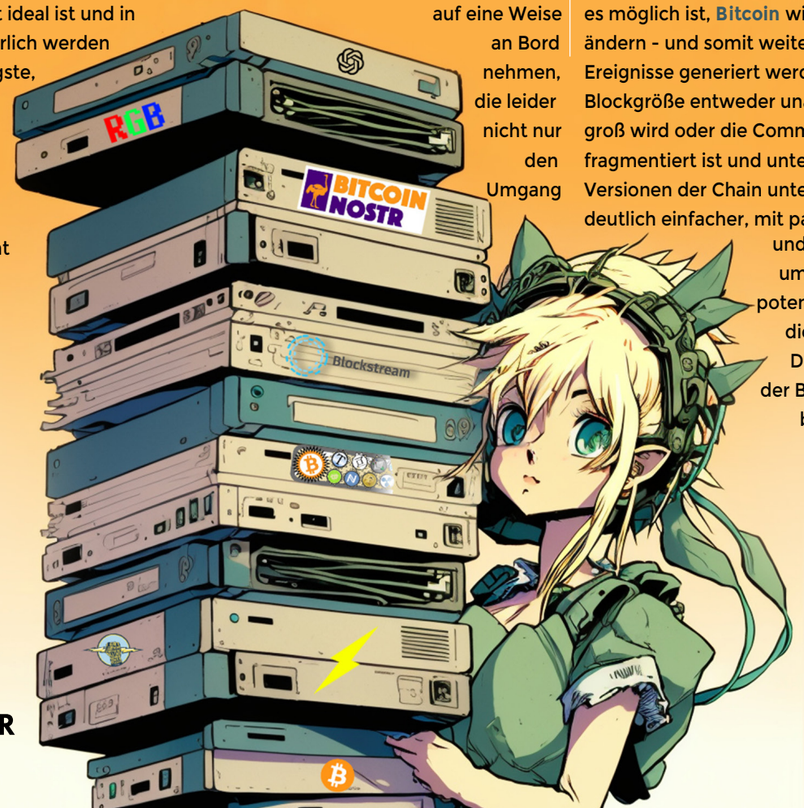
Mit der Zeit wird die Nutzung der Basis-Layer für die meisten Menschen weltweit zu teuer werden. Glücklicherweise wird jeder einen Lightning-Channel oder eine Sidechain verwenden können, die verschiedene Kompromisse ermöglichen: Um Geschwindigkeit und Kosteneffizienz zu gewährleisten, können diese höheren **Bitcoin**-Layers stärker zentralisiert sein. Da Sicherheit konstant bleiben muss und die höchste Stufe der Dezentralisierung auch die teuerste Art der Transaktion ist, wird der Dezentralisierungsgrad reduziert, um Skalierbarkeit und Komfort zu erhöhen.

Obwohl eine Verringerung der Dezentralisierung nicht ideal ist und in einigen Fällen gefährlich werden kann, ist das Wichtigste, dass Benutzer zwischen konkurrierenden Layers wählen können und auch von der Möglichkeit profitieren, sich nicht auf eine vertrauenswürdige dritte Partei verlassen zu müssen. Zum Beispiel können Benutzer bereits gehostete Lightning-Lösungen nutzen - die kostengünstige, sofortige und private Transaktionen bieten, aber mit der Notwendigkeit des Vertrauens in den Verwahrer (Serviceanbieter). Was Unternehmen wie Wallet of Satoshi, Alby, Tippin und BottlePay ehrlich hält, ist der Wettbewerb von ähnlichen nicht gehosteten Diensten sowie die drohende Gefahr, dass Benutzer ihre eigenen Lightning-Channels öffnen und damit aufhören, den Service mit ihren Transaktionsgebühren zu unterstützen.

Das Gleiche gilt für Sidechains, Föderationen, Chaumian-Mints und andere parallele Chains. Da es in ihrem besten wirtschaftlichen Interesse liegt, eine große Benutzerbasis zu haben und wettbewerbsfähig zu bleiben, ist es unwahrscheinlicher, dass sie plötzlich verschwinden. Natürlich ist dies nicht ideal, aber es ist besser als die aktuelle vorherrschende Skalierungsoption von **Bitcoin**, die zentralisierte und überregulierte Börsen umfasst, die als Banken fungieren, sowie alternative Blockchain-Netzwerke, die experimentelle Funktionen nutzen und Neulinge auf eine Weise an Bord nehmen, die leider nicht nur den Umgang mit Wallets, sondern vielmehr auch Betrugserfahrungen beinhaltet.

Die Erhöhung der Blockgröße, um mehr Transaktionen aufzunehmen, ist in ferner Zukunft nicht komplett ausgeschlossen, aber keine vernünftige Größe kann alle finanziellen Transaktionen weltweit bewältigen. Wenn der Speicher noch billiger wird und 5G-Internetverbindungen selbst in den am wenigsten entwickelten Ländern mit erschwinglichen Datentarifen weit verbreitet sind, könnte die Community entscheiden, einen Hard Fork durchzuführen, um die Blockgröße zu erhöhen und somit mehr Benutzer in der Lage zu sein, Lightning-Channels zu eröffnen und in Sidechains zu integrieren. Zum Beispiel könnten 32 oder 64 Megabyte-Blöcke im Jahr 2040 vernünftig sein. Wenn jedoch On-Chain-Transaktionen durch Soft Forks immer kleiner und effizienter werden (wie es bei SegWit im Jahr 2017 der Fall war), würde kein Hard Fork erforderlich sein.

Das größte Problem bei der Erhöhung der Blockgröße ist nicht der Speicher oder die Bandbreite, sondern der soziale Konsens und die "slippery slope" Theorie. Einige werden argumentieren, dass eine derart bedeutende Veränderung nur beweisen würde, dass es möglich ist, **Bitcoin** willkürlich zu ändern - und somit weitere ähnliche Ereignisse generiert werden, bis die Blockgröße entweder unangemessen groß wird oder die Community zu stark fragmentiert ist und unterschiedliche Versionen der Chain unterstützt. Es ist deutlich einfacher, mit parallelen Chains und Second-Layern umzugehen, deren potenzielle Probleme die Sicherheit und Dezentralisierung der Basis-Layer nicht beeinträchtigen.



Darüber hinaus garantiert die Erhöhung der Blockgröße nicht, dass die Blöcke immer gefüllt werden. Eine solche Maßnahme führt direkt zu niedrigeren Transaktionsgebühren für die Miner aufgrund geringerer Konkurrenz, um in den nächsten Block zu gelangen. In Zeiten geringer Nachfrage nach Blockplatz, wenn die Block-Belohnungen bereits mehrmals halbiert wurden, kann dies tatsächlich eine Sicherheitsbedrohung für **Bitcoin** darstellen.

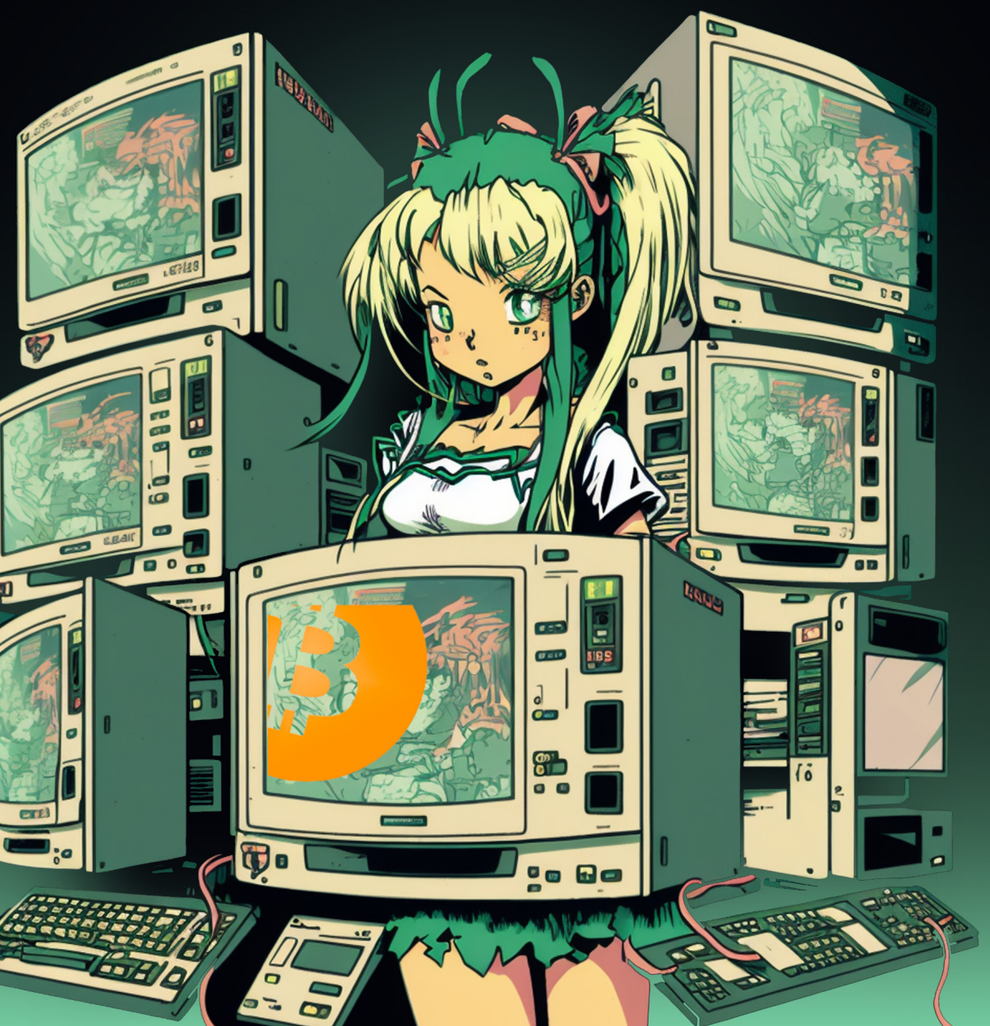
Um direkt auf die **FUD** (Fear, Uncertainty, Doubt) von **ChatGPT** einzugehen: **Bitcoin** skaliert und wird besser skalieren, je mehr Schichten entwickelt werden. Die begrenzte Anzahl von Transaktionen, die in einen Block passen, können Lightning-Kanal-Eröffnungen und Sidechain-Peg-Ins sein, die den Benutzern die Möglichkeit geben, schnell, kostengünstig und skalierbar zu handeln. Das einzige Problem ist, dass diese Schichten verschiedene Dezentralisierungskompromisse mit sich bringen. Aber sie sind immer noch dezentralisierter als Altcoins, zentralisierte Börsen und andere Versuche, **Bitcoin** schlecht zu replizieren oder durch schlecht konzipierte Systeme zu ersetzen.

Die Kritik ist zwar nachvollziehbar, aber sie mangelt an Kontext und Feinheiten. Daher hat ChatGPT erneut verloren.



SCORE
Vlad C. 3
ChatGPT 0







YOUR BACKUP

THE ORIGINAL SINCE 2013

cryptosteel



Breaking ChatGPT's Bitcoin FUD #4:

BRUTE FORCE SHA256

Sicherheitslücken

GEFÄLLT DIR DER ARTIKEL? SCANNE DEN QR-CODE UND HINTERLASSE EIN KOMMENTAR ODER EINE DONATION!

Laut **ChatGPT** zieht die zunehmende Beliebtheit von **Bitcoin** Hacker und andere bösartige Akteure an. Aber was können diese Hacker eigentlich angreifen?

Nun, es gibt mehrere Ebenen der **Bitcoin**-Sicherheit. Wir können über das Mining und potenzielle 51%-Angriffe sprechen, bei denen die jüngsten Blöcke neu organisiert werden können. Wir können die Wahrscheinlichkeit eines Brute-Force-Angriffs auf eine Wallet diskutieren, um den privaten Schlüssel zu finden, oder wir können den einfachen Weg gehen und von einer Zunahme von sozialen Angriffen ausgehen (bösartige Entwickler, die schädlichen Code einfügen, oder einzelne **Bitcoin**-Benutzer, die dazu gebracht werden, ihre Coins zu verlieren).

Zunächst einmal ist der 51%-Angriff eine der größten Sicherheitsbedrohungen für **Bitcoin** und ein Teil des Proof-of-Work-Designs. Die Idee, dass eine einfache Mehrheit der Hashrate der Miner in böser Absicht handeln kann, ist ein ernsthafter Angriffsvektor. Die Anreize des sogenannten Nakamoto-Konsenses sind jedoch so konzipiert, dass es profitabler ist, sich an die Regeln zu halten, als zu versuchen, das System anzugreifen. Das Miningequipment zu kaufen oder zu mieten, dann eine große Menge an Strom zu verbrauchen, um Transaktionen doppelt auszugeben und die neuesten Blöcke neu zu organisieren, ist nicht gerade günstig.

Mit einer Hashrate von mehr als 360 Exahashes pro Sekunde würde selbst die ressourcenstärksten Regierungen und transnationalen Konzerne der Welt Schwierigkeiten haben, 51% davon aufzubringen. Darüber hinaus sind Supercomputer nicht für die Ausführung von SHA-256-Hashes wie die **Bitcoin**-ASICs optimiert. Wenn man alle Supercomputer der Welt zusammennimmt, erhält man nur die Äquivalenz eines sehr kleinen und unbedeutenden Mining-Pools.

Ein 51%-Angriff auf **Bitcoin** erfordert den Kauf oder die Miete knapper und hochspezialisierter Hardware, die derzeit zur Sicherung des Netzwerks verwendet wird und Belohnungen für das Einhalten der Regeln erhält. Die finanziellen Anreize spielen eine Rolle und haben bisher die Miner ehrlich gehalten, sie auf ihr Ziel fokussiert und effizient im Umgang mit ihrer Energie gemacht. Jemand, der einen solchen Angriff gegen **Bitcoin** durchführt, benötigt viele Ressourcen, um ihn aufrechtzuerhalten. Das größte Risiko, dem der Angreifer gegenübersteht, besteht darin, dass die ehrlichen Netzwerkteilnehmer zu einer neuen Kette abzweigen, die den UTXO-Satz kopiert, um den rechtmäßigen Coin-Besitz zu behalten. Ein solcher Versuch bietet keine Garantie



für Profitabilität oder Erfolg und kann bestenfalls als politische **FUD** gegen die Sicherheit des Netzwerks dienen. Solange die finanziellen Anreize konstant bleiben, werden wir höchstwahrscheinlich niemals einen ernsthaften 51%-Angriff sehen.

Selbst die großen Mining-Pools, die aus mehreren Benutzern bestehen, die ihre Hash-Leistung kombinieren, und die Belohnungen teilen, unterliegen einer Art Spieltheorie, die sie ehrlich hält. Unter dem Druck der Regierung könnten sie sich entscheiden, das Mining ganz einzustellen und den Angriff auf das Netzwerk zu vermeiden. Das Abschalten der Mining-Operationen wird zu Störungen für die verbleibenden Blöcke im Zyklus führen, aber alle 2016 Blöcke (ungefähr 2 Wochen) gibt es eine neue Schwierigkeitsanpassung, und es gibt immer jemanden anders auf einem anderen Teil der Welt, der bereit ist, mit dem Mining zu beginnen, wenn die Chancen auf das erfolgreiche Finden des richtigen Hashes höher werden. **Bitcoin** ist äußerst gut durchdacht, und es gibt einen Grund, warum diese Angriffe nie wirklich erfolgreich waren - weder in den Anfangstagen, als sie einfacher waren, noch heute, wenn die Anzahl der hochspezialisierten Miner, die das Netzwerk sichern, höher ist als je zuvor.

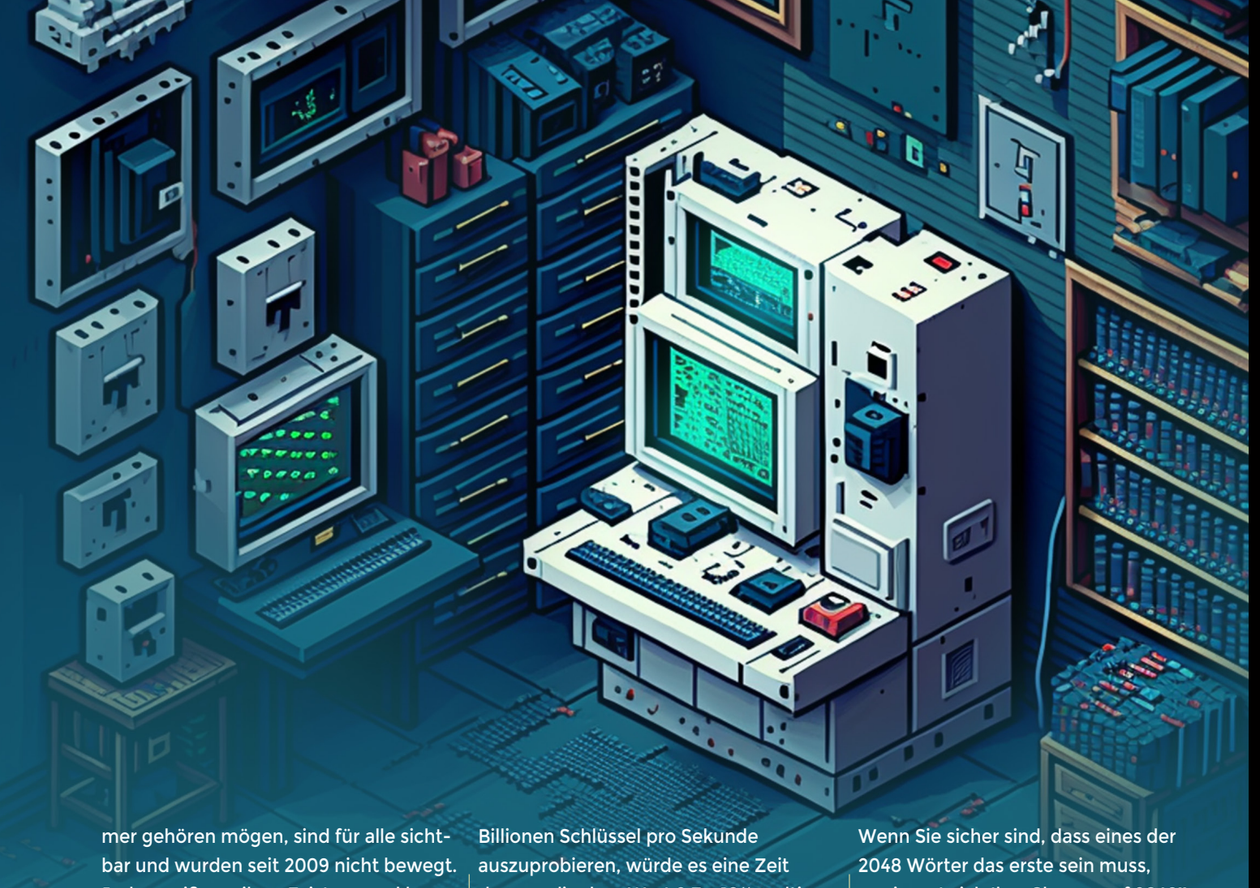
Laut ChatGPT zieht die zunehmende Beliebtheit von **Bitcoin** bösartige Akteure an. Aber worauf können diese Hacker tatsächlich abzielen?

Zunächst einmal werden 51%-Angriffe nicht in diese Kategorie fallen, da mit steigender Benutzerzahl auch mehr Mining-Rigs eingesetzt werden. Es war dennoch wichtig dies zu erklären, da die KI-Software nicht direkt auf das Problem hinweist.



Ein weiterer Aspekt sind Brute-Force-Angriffe auf Wallets, um den privaten Schlüssel (private key) zu finden und damit die Gelder zu stehlen. Theoretisch könnte dies mit zunehmender Verbreitung von **Bitcoin** ein wichtiges Sicherheitsproblem darstellen. Hacker könnten versuchen, Wallet-Dateien zu knacken, gültige BIP39-Seed-Phrasen zu erraten und korrekte Passphrasen zu generieren. Viel Glück dabei - die Chancen stehen besser, intelligentes außerirdisches Leben auf einem entfernten Planeten zu finden oder ein bestimmtes Sandkorn in der Wüste auszugraben.

Ein bekanntes Beispiel sind die Coins von Satoshi Nakamoto. Die berühmten "Millionen", wie sie von Sergio Demian Lerner in seinem Patoshi-Forschungsprojekt beschrieben wurden, sind die ultima-tive Beute. Es gibt keinen Beweis für die Theorie, ob Satoshi diese besitzt - es handelt sich um eine reine Analyse, die davon ausgeht, dass Satoshi kontinuierlich gemint hat. Die resultierenden Coins, wem sie auch im-



mer gehören mögen, sind für alle sichtbar und wurden seit 2009 nicht bewegt. Jeder weiß von ihrer Existenz und kann sie im öffentlichen Ledger verfolgen. Aber niemand kann die privaten Schlüssel per Brute Force ermitteln, um Anspruch darauf zu erheben.

Um alles in Zahlen zu fassen: Bitcoin hat insgesamt 2^{256} mögliche private Schlüssel und nur 2^{160} Kombinationen von Adressen, die existieren können (unter der Annahme, dass sie alle 160 Bit haben). Brute-Force-Angriffe aber müssen von einem vorhandenen und gültigen öffentlichen Schlüssel ausgehen, was an sich schon zusätzlichen Aufwand erfordert.

Ein effizienterer Weg, Wallets per Brute Force zu knacken, besteht darin, einen der 2^{96} privaten Schlüssel zu finden, die dieselbe Adresse erzeugen. Die Anzahl der Möglichkeiten beträgt 79.228.162.514.264.337.593.543.950.335 - etwa 79.228 Mal mehr als die geschätzte Anzahl der Sterne im Universum. Andererseits, wenn Sie eine bestimmte Wallet per Brute Force knacken wollen (wie die von Satoshi), müssen Sie es mit allen 2^{256} Kombinationen privater Schlüssel versuchen. Angenommen, Sie haben die Rechenleistung, um 1000 Billionen Schlüssel pro Sekunde auszuprobieren, würde es eine Zeit dauern, die dem Wert $2,7 \times 10^{44}$ multipliziert mit dem Alter des Universums entspricht (wie von Entwickler Raghav Sood im Bitcoin StackExchange erwähnt). Diese Zahl übersteigt alles Messbare für den Menschen - einschließlich der Anzahl der Atome in unserer beobachtbaren Welt.

Was die BIP39-Seed-Phrasen betrifft, gibt es 2048 Wörter und 12/24 Kombinationen davon. Nehmen wir der Einfachheit halber eine grundlegende 12-Wort-Konfiguration an. Um eine zufällige Phrase zu erraten, gibt es 2048^{12} (oder 2^{132}) Möglichkeiten. Um Moderator BashCo auf Reddit zu zitieren, ist diese Zahl eine in 115 Quattuorvigintillionen 792 Trevigintillionen 89 Duovigintillionen 237 Unvigintillionen 316 Vigintillionen 195 Novemdecillionen 423 Oktodecillionen 570 Septendecillionen 985 Sexdecillionen 8 Quindecillionen 687 Quattuordecillionen 907 Tredecillionen 853 Duodecillionen 269 Undecillionen 984 Decillionen 665 Nonillionen 640 Oktillionen 564 Septillionen 39 Sextillionen 457 Quintillionen 584 Quadrillionen 7 Billionen 913 Milliarden 129 Millionen 639 Tausend 936.

Wenn Sie sicher sind, dass eines der 2048 Wörter das erste sein muss, verringert sich Ihre Chance auf 2048^{11}, da Wörter in BIP39 in derselben Konfiguration wiederholt werden können. Und wenn Sie die ersten 10 Wörter in der richtigen Reihenfolge haben und nur Ihr 11. und 12. Wort benötigen, haben Sie bereits 2048^2 Möglichkeiten - was es mit einem normalen Computerprozessor bereits heute per Brute Force knackbar macht. Achten Sie also gut auf Ihre Seed-Phrase und fügen Sie dieser, wenn Sie sich damit wohl fühlen, eine zusätzliche Passphrase hinzu, welche sich nicht im BIP39-Wörterbuch befindet. Dadurch wird Ihre Sicherheit erheblich gesteigert, kann aber zum großen Problem werden, wenn Sie Ihre Passphrase vergessen oder verlieren.

Generell ist es, wie Peter Todd und der Mitbegründer von BIP39, Pavol "Stick" Rusnak, betonten, sehr unpraktisch und vergleichbar mit der Aussage, dass man 500 Autos auf einem Fußballplatz parken kann. Peters Vorschlag war, die zusätzliche Phrase vollständig zu löschen, da der effizienteste Angriff auf BIP39-Seed-Phrasen darin besteht, den generierten pivate key per Brute Force zu ermitteln.

Ja, Quantencomputing könnte in Zukunft eine Bedrohung darstellen. Aber diese Zukunft liegt noch in weiter Ferne: Stand März 2023 ist der leistungsstärkste Quantencomputer der Welt der IBM Osprey mit 433 physikalischen Qubits. Wie in einem 2022 veröffentlichten Forschungspapier in der Zeitschrift "AVS Quantum Science" dargelegt, benötigt ein Computer, der die elliptische Kurvenkryptographie von **Bitcoin** innerhalb von 24 Stunden brechen soll, 13×10^6 Qubits. Mit anderen Worten müssten Quantencomputer tausendfach leistungsstärker werden, um **Bitcoin** zu knacken.

Bisher hat der technologische Fortschritt im Bereich des Quantencomputings das Mooresche Gesetz leicht übertroffen. Für Prognosezwecke nehmen wir an, dass dieses Muster fortgesetzt wird und die Anzahl der Qubits alle 2 Jahre verdoppelt wird. Um von 433 auf 13×10^6 zu gelangen, müssten Quantencomputer 30023-mal leistungsstärker werden. So dauert es mindestens weitere 20 Jahre, bevor wir uns ernsthaft Sorgen machen sollten.

Von 2 Qubits auf 433 Qubits dauerte es 24 Jahre an Forschung und Entwicklung. Wie lange wird es dauern, bis wir 10.000 Qubits erreichen?
Wahrscheinlich noch einige Jahrzehnte.

Bei 10.000 Qubits und bestimmten physikalischen Bedingungen (eine Codezykluszeit von 1 µs, eine Reaktionszeit von 10 µs und ein physikalischer Torfehler von 10^3) wäre ein Quantencomputer in der Lage, die Coins aus einer beliebigen **Bitcoin**-Wallet in 10 Tagen zu entwenden.



Allerdings wird sich die Kryptographie bis dahin auch enorm verbessert haben und **Bitcoin** könnte sich zu einem besseren Modell entwickeln, das Brute-Force-Angriffe so schwierig macht, dass Quantencomputer viel mehr Zeit brauchen, um aufzuholen.

Ein Upgrade auf quantensichere Schlüssel erfordert nur einen Soft Fork, der von einer Mehrheit der Nodes oder Miner aktiviert werden kann. Daher könnte sich diese ganze Diskussion als irrelevant erweisen oder als unwürdige **FUD**.

Jetzt, da wir diese beiden sehr komplexen und extrem teuren Angriffe aus dem Weg geräumt haben, ist es an der Zeit, sich auf die wahrscheinlichsten Angriffe zu konzentrieren: die sozialen Angriffe. Wir Bitcoiner sagen gerne "Vertraue nicht, überprüfe" (Don't trust, verify!). Doch die Einrichtung von Vertrauenssystemen, die Zweifel an möglicher Boshaftigkeit von Entwicklern beseitigen, ist ein sehr ernsthafter Angriffsvektor.

Der einfachste Weg, um jede Art von Angriff abzuschwächen, besteht darin, beim Code konservativ zu bleiben:



Aktualisieren Sie nicht auf die neueste Version, es sei denn, Sie überprüfen sie im Voraus oder bezahlen jemand anderen dafür. Und wenn Sie beides nicht tun, stellen Sie zumindest sicher, dass genügend Personen mit feindseeligen Anreizen den neuen Code überprüft haben. Wenn es um so viel geht, dass das globale Finanzsystem bedroht ist, können wir davon ausgehen, dass Entwickler unter großem Druck stehen und Fehler machen oder kompromittiert werden können.

Dies ist jedoch kein Grund für eine Erstarrung: **Bitcoin** ist als Projekt noch nicht abgeschlossen und es sind immer noch Verbesserungen erforderlich. Von der Verbesserung der Privatsphäre über die Verkleinerung von Transaktionen bis hin zur Bereitstellung von Schutz vor Quantencomputing-Angriffen gibt es noch viel zu tun. Mein Argument richtet sich gegen den leichtsinnigen Umgang mit ungetesteter Technologie, deren Konsequenzen nicht vollständig verstanden sind, aber nicht gegen Innovation.

Dennoch sollten wir bei der Verfolgung von Innovationen die Überprüfung nicht der Dringlichkeit opfern. Als Community sollten wir **Bitcoin**-Entwickler dazu ermutigen, Optionen vorzubereiten, bevor die Bedrohung unmittelbar wird: Modelle für quantensichere elliptische Kurvenkryptographie, skalierbare Privatsphäre usw. Einige dieser Lösungen werden bereits mit Marktanreizen in anderen Netzwerken getestet - am wichtigsten ist jedoch, dass **Bitcoin**-Entwickler auf die legitimen technologischen Verbesserungen achten, das Vorhandene verbessern und Vorschläge vorlegen, über die jeder diskutieren muss. Außerdem sollten wir

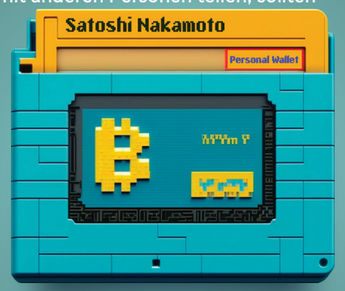
unsere Rolle als souveräne Node-Betreiber und Miner nicht vernachlässigen - wir entscheiden, welchen Code wir ausführen, und Bitcoin-Clients können mit minimalen Spezifikationen arbeiten. Nicht alles, was zu Core hinzu-gefügt wurde, ist notwendig, aber die gut getesteten Funktionen bieten nützliche Optimierungen.

Last but not least, müssen wir über die Sicherheit jedes einzelnen Bitcoin-Benutzers sprechen. Dies ist höchstwahrscheinlich die Hauptart von FUD, die ChatGPT aufbrachte, als die AI von Hackern und bösartigen Akteuren sprach. Alles zwischen Keyloggern, die Ihre Tastatureingaben registrieren und übertragen (die möglicherweise Ihre Bitcoin Core-Passphrasen oder BIP39-Seed-Phrasen enthalten), bis hin zu Betrugsversuchen und physischen Angriffen wird immer wahrscheinlicher, je höher der Preis von BTC wird.

Die schlechte Nachricht ist, dass kein Entwickler, keine Protokolländerung, keine staatliche oder nichtstaatliche Einrichtung in der Lage ist, Sie vor Fehlern zu schützen. Die gute Nachricht ist, dass es einige allgemeine bewährte Verfahren gibt, die Sie befolgen können, um Ihre Sicherheit zu verbessern. Dazu gehören:

- verwenden Sie ein dediziertes Gerät zum Signieren und Ausführen von **Bitcoin**-Transaktionen (ein Linux-Laptop oder Telefon, auf dem **Bitcoin**-Fullnode-Software läuft, während es verwendet wird, BIP39-Hardware-Wallets mit starken Passphrasen);
- erstellen Sie Setups, die einzelne Fehlerpunkte eliminieren (Multisig und SLIP39-Shamir-Backups).
- verwenden Sie Cold Storage (Metallplatten, Papier-Wallets, physische **Bitcoin**).
- schützen Sie sich durch gute operative Sicherheit und Privatsphäre (geben Sie zufälligen Fremden nicht preis, wo Sie wohnen, wie Ihr **Bitcoin**-Setup aussieht und wie viel Geld Sie haben - dies beinhaltet auch ein materiell normales Leben in Ihrer Nachbarschaft/Gemeinschaft, ohne anzugeben, wie wohlhabend Sie sind). Denken Sie daran: Geben Sie so wenig Informationen wie möglich über Ihre **Bitcoin**-Aktivität preis oder verwirren Sie zumindest potenziel feindseelige Beobachter, um ein verzerrtes Bild davon zu haben, was Sie wirklich tun und wie wohlhabend Sie sind.

Bitcoin ist eine Währung, die absolute Eigentumsrechte durchsetzt. Das bedeutet, dass eine Transaktion, sobald sie gesendet und in einen Block aufgenommen wurde, nicht mehr rückgängig gemacht werden kann. Daher ist jeder Benutzer dafür verantwortlich, seinen Wohlstand nach bestem Wissen und Können gemäß einem realen Bedrohungsmodell zu schützen. Bevor Sie irgendeine Art von Setup erstellen, müssen Sie sich fragen: "Wer ist der gefährlichste Gegner, der wahrscheinlich versuchen wird, meine Coins zu stehlen?". Wenn Sie den Computer mit anderen Personen teilen, sollten



Sie keine unverschlüsselten Wallet-Dateien hinterlassen. Wenn Sie reisen, ist es keine gute Idee, Geräte mitzuführen, die zeigen, dass Sie **Bitcoin** besitzen (in der Regel ist eine Hardware-Wallet leichter zu erkennen und verdächtiger als ein Laptop oder ein Stück Papier). Wenn Sie Kinder oder einen neugierigen Ehepartner haben, die möglicherweise in Ihren Aktenschränken und Schubladenn stöbern, ist es besser, Ihr Backup außerhalb ihrer Zugänglichkeit aufzubewahren. Wenn Sie in einer schlechten Nachbarschaft mit hoher Kriminalitätsrate leben, sollten Sie wahrscheinlich keine **Bitcoin**-Backups in Ihrem Haus aufbewahren. Und wenn Ihre Region von Naturkatastrophen bedroht ist, müssen Sie ein System mit guter geografischer Verteilung entwickeln, das es Ihnen unmöglich macht, alles zu verlieren, und Ihnen gleichzeitig einfachen Zugriff auf die anderen Schlüssel/Teile Ihres Backups ermöglicht.

Die häufigste Bedrohung besteht jedoch aus Hackern. Diese Kriminellen sind Personen, die illegal versuchen, in Ihren Computer einzudringen, sowie Anzug tragenden Geschäftsleute, die Systeme entwerfen, die im Wesentlichen innerhalb eines legalen Rahmens Ihre Coins stehlen. In der ersten Kategorie können Sie Personen unterscheiden, die Schadsoftware programmieren oder sich mit Ihnen anfreunden, um später nach Geld zu fragen (ob es sich um einen nigerianischen Prinzen oder ein OnlyFans-Model handelt, das dringend Hilfe benötigt). Die zweite Kategorie besteht aus Börsen und Banken, die versprechen, Ihre Coins in einer sicheren Umgebung zu verwahren, Ihnen aber die Auszahlung einschränken, wenn ihr Geschäftsmodell in Schwierigkeiten gerät. Sie sollten diese beiden Arten von Hackern um jeden Preis vermeiden, da sie am wahrscheinlichsten Ihre **Bitcoin** stehlen werden.

Obwohl es bequem ist, Ihre Coins auf einem Exchange zu hinterlegen, widerspricht diese Art des Handelns dem Zweck von **Bitcoin** und beeinträchtigt erheblich Ihre eigene finanzielle Souveränität. Vertrauenswürdige Dritte sind Sicherheitslücken, und Sie sollten nie-mals einer Einzelperson oder einem Unternehmen vertrauen, die versprechen, Ihre BTC gegen Sicherheit und/oder Rendite zu halten.

Natürlich gibt es auch andere soziale Angriffe: gefälschte E-Mails von Börsen, die auffordern, Ihre Seed-Phrase in einer Antwort zu bestätigen, Anrufer, die sich als Wallet-Service ausgeben und Sie auffordern, Ihre Daten zu bestätigen (manchmal sogar Ihre Wohnadresse), Hardware-Wallet-Lieferungen, die abgefangen und durch die Einfügung einer BIP39-Seed-Phrase kompromittiert werden (die Angreifer hinterlassen ihre eigene Seed-Phrase in der Box und hoffen, dass unerfahrene Benutzer ihre Coins dorthin senden), $5-Schraubenschlüssel-Angriffe und Nachahmer, die vorgeben, Freunde oder Familie zu sein, die dringend eine Geldsendung benötigen.

Diese werden häufiger, je höher Preis und Akzeptanz von Bitcoin werden. Aus diesem Grund müssen Sie sich bewusst schützen, indem Sie die Menge an Daten minimieren, die Sie über die von Ihnen genutzten Dienste, den Ort, an dem Sie leben, und die Menge an Bitcoin, die Sie besitzen, preisgeben.

ChatGPT's Argument, dass Betrug von Menschen eine ernsthafte Bedrohung für Bitcoin darstellt, ist unzutreffend. Das Netzwerk wird trotz der Diebe weiterhin existieren und funktionieren. Sicherlich werden sich viele Menschen von der Verantwortung eingeschüchtert und verängstigt fühlen. Aber wir sollten nicht vergessen, dass Selbstverwahrungslösungen im Laufe der Zeit sicherer und nutzerfreundlicher werden. Auch die Ebenen von Bitcoin entwickeln sich weiter und es werden neue Möglichkeiten zum Verwenden und Speichern von Geld freigeschaltet. Zum Beispiel plant das Fedimint-Projekt, Gemeinschaftsbanken zu ermöglichen, bei denen Benutzer ihre Mittel nur mit einem Selfie freischalten können. Auch der Wizard-Sardine hat kürzlich Liana eingeführt, um es einfach zu machen, Bitcoin bis zu einem zukünftigen Blockhöhenziel Ihrer Wahl zu sperren. Dies erleichtert langfristiges Halten und Vererben, selbst für technisch nicht versierte Benutzer, die Bitcoins Skript nicht verstehen. Sie hätten dies schon immer mit Bitcoin Core und Electrum tun können, aber jetzt ist es noch benutzerfreundlicher.

Hacker und bösartige Akteure existieren in jedem Geldsystem und jeder menschlichen Organisation. Was am meisten zählt, ist den Aufbau einer Kultur von Fairness, Verantwortlichkeit, bewährten Verfahren und Wahrheit voranzutreiben.

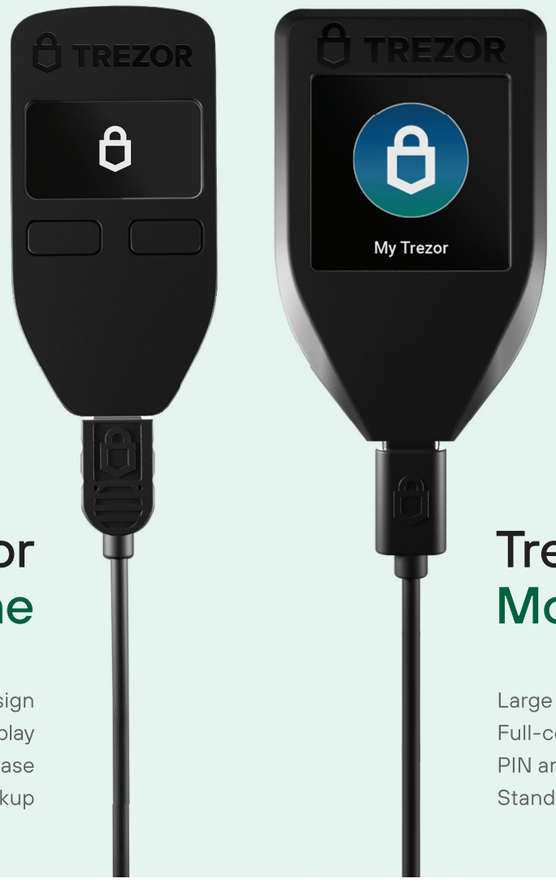
Solange solche Lösungen vorhanden sind, wird ChatGPT immer wieder eine Niederlage einstecken, da es mit der ganzen FUD so sehr daneben liegt.



TREZOR

Putting control in your hands.

Take control of your Bitcoin with a Trezor hardware wallet.
Boost your privacy and manage coins securely, with the integrity and independence of open-source design.



Trezor Model One

Simple durable design
Monochrome trusted display
PIN and Passphrase
Standard backup

Trezor Model T

Large comfortable touchscreen
Full-color trusted display
PIN and Passphrase
Standard or Shamir backup

Find out more at **trezor.io**



Breaking ChatGPT's Bitcoin FUD #5:

Preisvolatilität

BTC-USD VOLATILITÄT BULLEN/BÄREN MÄRKTE

GEFÄLLT DIR DER ARTIKEL? SCANNE DEN QR-CODE UND HINTERLASSE EIN KOMMENTAR ODER EINE DONATION!

Laut **ChatGPT** ist die Preisvolatilität der Bitcoin-Währung die fünftgrößte Bedrohung für **Bitcoin**. Die Annahme dabei ist, dass die ständigen und unvorhersehbaren Schwankungen im Vergleich zu Fiat-Geld Menschen davon abhalten sollen, BTC als Zahlungsmittel und/oder Wertspeicher anzunehmen.

Es gibt zwei Möglichkeiten, um mit dieser FUD umzugehen, welche auch in den Mainstream-Medien sehr verbreitet ist: eine ist technischer Natur, die andere vergleichend. Die erste ist introspektiv, während die zweite die Bedeutung des Wortes "volatil" in Frage stellt, indem sie aktuelle Beispiele aus der vermeintlich "stabilen" Finanzwelt präsentiert.

Zunächst einmal wollen wir eine kleine technische Analyse des **Bitcoin**-Preises durchführen. Als Referenz verwenden wir die Werte des BTC/USD-Charts an der Bitstamp-Börse, der den Preis seit August 2011 verfolgt. Im Verlauf von fast 12 Jahren stieg BTC um 243.207 %. Die Phase der Preisfindung hat drei deutliche Bullenzyklen und ebenso viele Bärenmärkte erlebt. Und auf längere



Sicht (3-4 Jahre) war die Volatilität immer nach oben gerichtet, was **Bitcoin** zu einem ziemlich guten Wertspeicher machte.

Des Weiteren gibt es viel zu sagen über die Abnahme der Volatilität im Laufe der Zeit. Allein durch einen Blick auf den langfristigen logarithmischen Chart kann man erkennen, dass sowohl grüne als auch rote Kerzen früher größer waren. Die Liquidität war geringer, die Anzahl der Benutzer ebenfalls geringer, und es war einfach für einige Wale, den Preis in beide Richtungen zu manipulieren. Doch mit zunehmender Adoption führen mehr Benutzer regelmäßig Transaktionen mit **Bitcoin** durch. Und je mehr BTC in mehr Händen landen, desto geringer wird auch die Volatilität.

Dies ist keine bloße theoretische Beobachtung - man kann es anhand der Menge an Widerstand und Rückprall sehen, die nach jedem Kurssturz stattfindet. Für jeden Verkäufer gibt es sofortige Käufer auf der ganzen Welt. Und selbst wenn der Preis überverkauft ist, findet man immer jemanden auf der anderen Seite, der sofort den Kursrückgang kauft. Es scheint, dass der Handel etwas professioneller geworden ist, mit Widerstandsmustern, die man auch an der Wall Street bemerken kann. Mit jedem Boom-Crash-Zyklus nimmt auch die Abwärtsvolatilität ab.

Während des Bullenmarktes von 2013 stieg der Preis im Dezember auf 1237 US-Dollar - nur um drei Tage später auf 687 US-Dollar abzustürzen. Während des anschließenden Bärenmarktes sank **Bitcoin** Anfang 2015 auf ein Tief von 179,13 US-Dollar. Das bedeutet einen Rückgang um 85,5% in etwa einem Jahr, was eine Folge von schlechter Entwicklung der Börsen und begrenzten Möglichkeiten zum Kauf und Handel mit **Bitcoin** war. Mit dem Ausbau der finanziellen Infrastruktur und der Adoption verbesserte sich die Situation.

Während des Bullenmarktes von 2017 erhöhte sich die Liquidität deutlich. Das Allzeithoch am 15. Dezember lag bei 19.345 US-Dollar, während der Tiefpunkt von 2018 bei etwa 3.196 US-Dollar erreicht wurde. Dies war großartig für frühe Anwender, aber sehr schmerzhaft für alle, die nahe dem Höchststand gekauft haben, da der Rückgang von 83,4% niedriger war als der vorherige, aber dennoch brutal.



Falls Sie dies lesen, kennen Sie wahrscheinlich bereits die Geschichte vom November 2021, als ein Allzeithoch von 68.789 US-Dollar erreicht wurde und ein Jahr später ein Tief von 15.877 US-Dollar folgte. Diesmal beträgt die Differenz zwischen Höchststand und Tiefpunkt 76,91%, was auf einen höheren Widerstand und Überzeugung in Bezug auf das Asset hinweist. Obwohl die Zahlen immer noch nicht ideal sind, deuten sie auf eine allmähliche Verringerung der Volatilität hin.

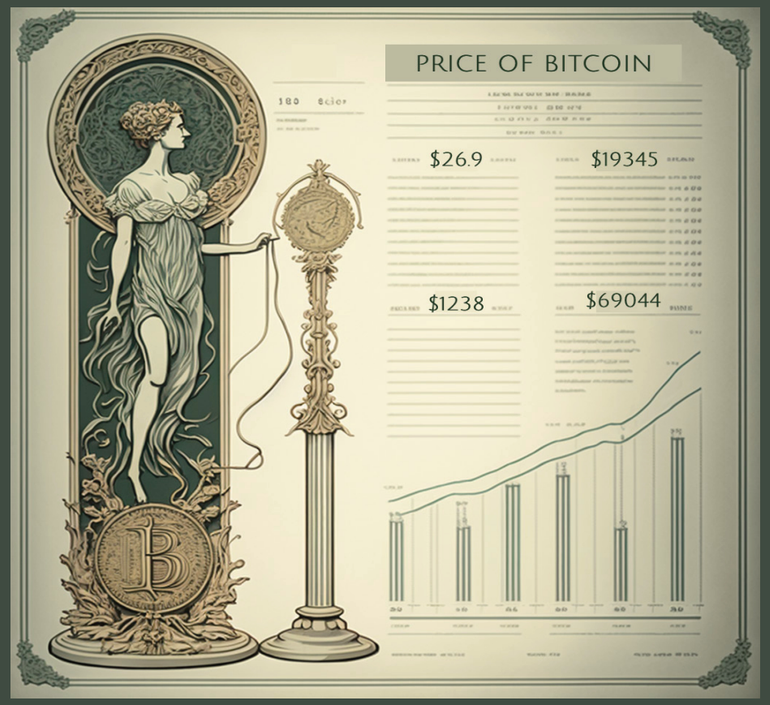
Dennoch sind diese Daten für Mainstream-Ökonomen und Journalisten immer noch nicht gut genug. Sie werden behaupten, dass selbst eine tägliche Bewegung von 5% zu volatil für eine Währung ist. Wie der Dezember 2013 gezeigt hat, kann der Preis in nur 3 Tagen um 44,4% fallen! Also ist dies weder ein Wertspeicher noch ein Zahlungsmittel. Die Zentralbanken im Fiat-Geldsystem werden dies verhindern, oder?!

Die folgenden Gegenargumente sind nur einige Beispiele, die im Jahr 2023 aufgetreten sind: Am 10. März erlitt die Silicon Valley Bank einen Bank Run. Ein paar Tage später folgte Signature Bank. Zwei "too big to fail"-Institutionen, die Geldanlagen in Milliardenhöhe verwalteten und deren Kunden wichtige Start-ups aus der Technologiebranche waren, gingen bankrott und benötigten die US-Regierung, um die Anleger zu retten. Am nächsten Tag brach in der Welt der regionalen US-Banken die Hölle los: Die Aktien der First Republic Bank stürzten um 70% ab. PacWest Bancorp verlor ebenfalls mehr als 40% an Börsenwert; und die Aktien von Western Alliance Bancorp verzeichneten einen Rückgang von 30%. Falls es noch nicht deutlich war: All dies geschah an einem einzigen Tag. In Europa erlebte die Credit Suisse (die zweitgrößte Bank der Schweiz) einen Aktienabsturz von 25%, der dazu führte, dass die Schweizer Regierung eingriff und einen Aufkauf durch die UBS (die größte Bank der Schweiz) arrangierte. Dies war eine Art sanfte Rettung, da die Bemühungen der Credit Suisse, Kredite aufzunehmen und Teile ihres Eigentums zu verkaufen, nur dazu führten, dass das Ausmaß des Bank Runs noch größer wurde.

In Frankreich stürzten die Aktien der BNP Paribas an einem einzigen Tag um 8% ab, was zu Interventionen führte, um den Handel zu stoppen.

Als **Bitcoin** innerhalb von 3 Tagen im Dezember 2013 die Hälfte seines Marktwerts verlor, war das Ergebnis nicht so dramatisch wie einige Ereignisse, die die Anleger der Banken der ersten Welt im März 2023 erlebten. Immerhin war Bitcoin ein neues Projekt mit geringer Liquidität und einer relativ kleinen Gemeinschaft von Händlern. Es war nicht eine 166 Jahre alte Schweizer Bank, es war nicht die Institution, die die meisten Start-ups im Silicon Valley bankierte, und das Projekt versprach nicht, Bankgeschäfte durchzuführen oder durch Tradition oder staatliches Eingreifen eine geringe Volatilität zu haben. **Bitcoin** existiert in einem rein freien Markt, in dem die Preisentwicklung von Angebot und Nachfrage bestimmt wird. Es gibt keine Zentralbank, die den Handel stoppt, wenn die Währung überverkauft ist, und keine Rettungsaktionen für Benutzer, die ihre Coins verlieren. Es gibt keine Support-Hotline, die man anrufen kann, wenn jemand die eigenen BTC stiehlt oder man sein Passwort vergisst. Es gibt auch keine Instanz, die beschließt, den Preis in Zeiten hoher Volatilität zu stabilisieren. Jeder einzelne Akteur ist seine eigene Bank, jeder entscheidet selbst, wann der beste Zeitpunkt zum Kauf oder Verkauf ist, und jeder ist dafür verantwortlich, seinen eigenen Zugriffsschlüssel zu sichern. Das mag wild und beängstigend klingen, aber es funktioniert genau deshalb, weil Bitcoiner Souveränität, Verantwortung und Knappheit verstehen. Bitcoiner wissen auch, dass dieses finanzielle Computernetzwerk während der Hochphase der Finanzkrise von 2008 entstand, als private Banken von ihren Regierungen gerettet wurden.





Deshalb ist unter einem freien und ehrlichen System hohe Volatilität gegenüber dem Klientelkapitalismus vorzuziehen. Aber was ist Volatilität überhaupt?

Da wir festgestellt haben, dass "sichere", "versicherte" und "too big to fail" Banken tägliche Abstürze erleiden können, die alles übertreffen, was **Bitcoin** bisher erlebt hat, warum beschweren wir uns dann nicht über die Volatilität und Unsicherheit dieser Finanzinstitute? Die offensichtlichste Antwort ist, dass Banken Politiker und Medien über ihre Finanzierung kontrollieren. Nicht nur das, auch **ChatGPT** selbst wurde von Microsoft und einer Reihe von Risikokapitalfirmen finanziert, die nicht unbedingt bitcoinfreundlich sind. Ihre Rolle besteht darin, eine alte und gut etablierte Tradition zu bewahren, daher muss alles, was ihre Position bedroht, auf Schritt und Tritt kritisiert werden.

Ein weiteres Argument ist, dass der Zusammenbruch von Banken im Allgemeinen als ein "Schwarzer Schwan-Ereignis" betrachtet wird, da es seltener vorkommt als eine Schwankung im BTC-Preis. Auf einem kurzfristigen Chart scheint **Bitcoin** volatiler zu sein, da es keine zentrale Einrichtung gibt, die einen täglichen Wechselkurs festlegt und manchmal Menschen auf der ganzen Welt ereignisreiche Geschehnisse koordinieren können. Aber Bank Runs sind auch real - wie wir in der ersten Hälfte des Jahres 2023 erlebt haben, sind Institutionen sehr anfällig für Massenab-hebungen aufgrund ihres risikoreichen Ansatzes, sehr geringe Reserven zu halten. Sie existieren auf Gnade von Zentralbanken und Regierungen, die sie in kritischen Momenten retten können oder auch nicht. Und langfristig gesehen scheitern sie alle.

Was am **Bitcoin**-Netzwerk und seiner zugrunde liegenden Währung interessant ist, ist, dass wir bisher einen Trend der Widerstandsfähigkeit gegen Preisvolatilität beobachtet haben. Zum Beispiel kaufte Tesla medienwirksam **Bitcoin** im Jahr 2021 ...nur um es später im Jahr wieder zu verkaufen. Das Gleiche geschah mit vielen Hedgefondsmanagern und großen Unternehmen, die einen Teil ihres Geldes in BTC investierten. Aber selbst in den Momenten, in denen die großen Investoren begannen zu gehen, gab es im Netzwerk wahre Gläubige, die das Projekt am Leben hielten.

Bitcoin schürfte weiterhin alle 10 Minuten Blöcke, auch wenn die Miner keinen großen Gewinn erzielten. Vollknoten speicherten und validierten weiterhin das gesamte Transaktionsbuch, auch ohne wirtschaftliche Anreize. Und Entwickler reichten weiterhin Verbesserungsvorschläge für den Code ein, auch wenn niemand sie bezahlte. Kann jemand ähnliche Aussagen darüber machen, dass Banker zur Arbeit gehen, wenn sie nicht mehr bezahlt werden, und Institutionen Zahlungen 24/7 abwickeln, trotz schwieriger Marktbedingungen?

Letztendlich ist die Nachfrage nach **Bitcoin** proportional zur Nachfrage nach Freiheit. Solange Menschen auf der ganzen Welt von Institutionen (sei es staatlich oder privat) unterdrückt, missbraucht, betrogen und beraubt werden, wird die Suche nach finanzieller Souveränität weitergehen. Freie Märkte sind viel widerstandsfähiger und haben reinere Motivationen als jede Form zentralisierter Kontrolle. Und während Regierungen immer mehr Orwell'sche Züge annehmen und Zentralbanken ihren Weg aus der Krise drucken, während sie mehrere Generationen verschulden, ist **Bitcoin** hier, um diese hoffnungsvolle Flucht aus allem zu bieten.

Was ist volatiler, etwas das nach dem Willen von Despoten und irrationalen Bürokraten verändert wird oder ein System, das auf Mathematik und Spieltheorie basiert?



SCORE
Vlad C. 5
ChatGPT 0







Gefällt dir der Artikel?

Scanne den QR-Code und hinterlasse ein Kommentar oder eine Donation!

Breaking ChatGPT's Bitcoin FUD#6

Limitierte Anwendungsfälle

SKALIERBARKEIT TRANSAKTIONEN LAYERS SHITCOINS PROTOKOLLE

Laut ChatGPT beschränkt sich Bitcoin auf eine begrenzte Anzahl von Anwendungsfällen, und diese Tatsache wird folglich seine Akzeptanz und sein Wachstum einschränken. Dies ist mit Abstand die albernste Kritik, die man über Bitcoin schreiben kann. Es gibt zwei Ansätze, um dies zu widerlegen: Der eine appelliert an den Bitcoin-Konservatismus und die Bedeutung von stabilem Geld, um die verschiedenen Anwendungsfälle zu diskreditieren, während der andere die verschiedenen technologischen Durchbrüche nutzt, die Bitcoin-Maximalisten im Laufe der Jahre mit Protokollen, Sidechains und Second-Layer-Lösungen erreicht haben. Letztendlich werden beide Seiten der Debatten erklären, warum es keine gute Idee ist, große Datenmengen auf der Hauptkette zu speichern und komplexe Anwendungen darauf auszuführen, da dies zu Ineffizienzen führt, die mit eleganteren Designs vermieden werden können.

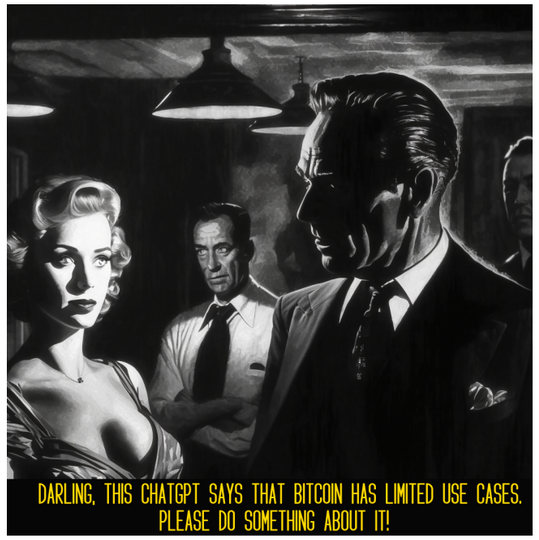
In seinem aktuellen Zustand kann Bitcoin bereits die meisten Anwendungsfälle von Altcoins abdecken: Es können On-Chain-Token erstellt und dezentrale Börsen mit Counterparty und Omni betrieben werden. Es können Dateien innerhalb der Beschränkung von 4 Megabyte pro Block gespeichert werden und es können grundlegende Smart Contracts (Multisig-Einrichtungen, bedingte Münzsperren, Dispenser) verwendet werden. Es gibt jedoch noch viele Dinge, die Bitcoin auf seiner Basis-Layer nicht umsetzen kann, von wiederkehrenden Zahlungen bis hin zu vertraulichen Transaktionen. Diese Funktionen sind auf vielen Altcoins vorhanden, die damit in verschiedenen Formen experimentieren. Aber nur weil Bitcoin derzeit diese Funktionen nicht auf der Basis-Layer ermöglicht, bedeutet das nicht, dass die dominierende Kryptowährung der Welt in Stagnation verharren wird und nicht durch Integration der bestmöglichen Implementierungen aufholen kann.

Es gibt eine konservative Denkrichtung, die hauptsächlich von österreichischen Ökonomen dominiert wird und argumentiert, dass Bitcoin keine dieser Anwendungsfälle benötigt, da stabiles Geld von Grund auf einfach sein sollte. Sie sind der Ansicht, dass der bevorstehende Zusammenbruch des Fiat-Geldes dazu führen wird, dass jeder Mensch auf der Welt Bitcoin kauft und alle Waren und Dienstleistungen in dem verifizierbar knappen BTC bezahlt. Und obwohl die Wahrscheinlichkeit dieses Szenarios gering ist (Fiat-Geld und Zentralbanken werden in unterschiedlichen Formen weiterhin existieren, solange die Menschen Vertrauen in ihre Regierungen haben und eine Nachfrage nach der jeweiligen Währung besteht), ist die Idee dennoch eine Überlegung wert.

Konservative tendieren dazu, Nicht-BTC-Tokens als Betrug zu bezeichnen,

nicht-monetäre Verwendungen von Bitcoin als Abweichungen vom Ideal des stabilen Geldes zu verurteilen und andere Blockchains als ineffiziente und schlecht optimierte Rube-Goldberg-Maschinen abzutun. Ein Teil dieser Kritik ist berechtigt, aber in vielen Fällen stimmt der freie Markt nicht mit ihrer Ideologie überein - es gibt Menschen, denen es nicht um stabiles Geld geht und die einfach nur mit Tokens Geld einsammeln wollen, zwischen Vermögenswerten handeln möchten, ohne eine zentrale Börse dazwischen zu haben, tokenisierte Kunstwerke erstellen und verkaufen möchten und ihre Videospielgegenstände auf einem neutralen globalen Netzwerk speichern möchten, das nicht von den Entwicklern geschlossen werden kann. Auf der anderen Seite gibt es Freiheitskämpfer und investigativ tätige Journalisten, deren Hauptanliegen die Privatsphäre von Transaktionen ist. Ihnen geht es nicht um digitales Gold als Wertspeicher, sondern sie möchten nur Geld senden und empfangen, ohne dabei Spuren darüber zu hinterlassen, wer sie sein könnten, mit wem sie Geschäfte machen und welche Beträge bewegt werden.







Ja, für viele dieser Anwendungsfälle bedarf es keiner Blockchain.

Und nein, es ist kein kluger Ansatz, diese Leute zu anderen Ketten zu lenken, die Skalierbarkeit und zusätzliche Funktionen auf Kosten einer offensichtlichen Zentralisierung bieten - nicht nur, weil die zugrunde liegenden Netzwerke fragil sind und mit schlechtem Geld umgehen, das wahrscheinlich auf 0 gehen wird, sondern auch, weil die Menschen die härteste Form von Geld auf einer der Bitcoin-Layers verwenden sollten.

Bitcoin-Maximalisten bieten einen viel nuancierteren Ansatz für diese Situation: Anstatt Anwendungsfälle zu entmutigen, die nicht nativ vom Bitcoin-Netzwerk unterstützt werden (oder nicht skalierbar sind, wenn sie darauf implementiert werden), bauen sie Layers auf Bitcoin auf, um die Bedürfnisse verschiedener Benutzertypen zu erfüllen und neue Marktsegmente anzusprechen. Obwohl sich in einigen Fällen konservative Bitcoin-Befürworter selbst als Maximalisten bezeichnen, liegt der Unterschied in der Maximierung selbst: Jemand, der gegen bestimmte Arten von Projekten ist, die auf einer Bitcoin-Layer aufgebaut werden, und der glaubt, dass die 21 Millionen BTC nur für monetäre Zahlungen verwendet werden sollten, maximiert eigentlich nichts - diese Menschen verwenden eine Ideologie, um ihre konservative Haltung zu rechtfertigen.

Mein Problem mit Bitcoin-Konservativen besteht darin, dass sie willentlich und wissentlich den Umfang der Adoption durch Reinheitstests einschränken. Ihre Überzeugung ist, dass der Zusammenbruch des Zentralbankwesens und die Hyperinflation von Fiat-Währungen dazu führen werden, dass jede Person auf der Welt Bitcoin als Geld verwendet. Dieses Szenario erfordert eine universelle Akzeptanz freier Märkte und ein neues Paradigma des Misstrauens gegenüber Regierungen. Jeder würde friedliche, freiwillige Transaktionen durchführen wollen, anstatt gewalttätig zu werden, um Eigentum und Reichtum zu ergreifen. Zumindest in unserem Leben ist dies eine Utopie... besonders in einer Welt, in der Regierungen größer werden und immer mehr Menschen auf den "großen Bruder" angewiesen sind, um alles von Bildung und Gesundheitsversorgung bis hin zu Subventionen, finanzieller Unterstützung und Beschäftigung zu erhalten.

Angesichts dieser Überlegungen vertrete ich die These (nicht nur um ChatGPTs FUD zu widerlegen, sondern auch, weil ich mich ideologisch auf dieser Seite positioniere), die maximalistische. Um eine Massenadoption zu erreichen, sollte sich Bitcoin nicht auf seinen Lorbeeren ausruhen und seine Eigenschaften als stabiles Geld zur Schau stellen. Es ist viel besser, mehr Anwendungsfälle zu integrieren, um alle, angefangen von Unternehmern bis hin zu Künstlern, für das Projekt zu interessieren.



Einige der besten Bitcoin-Maxi-projekte umfassen

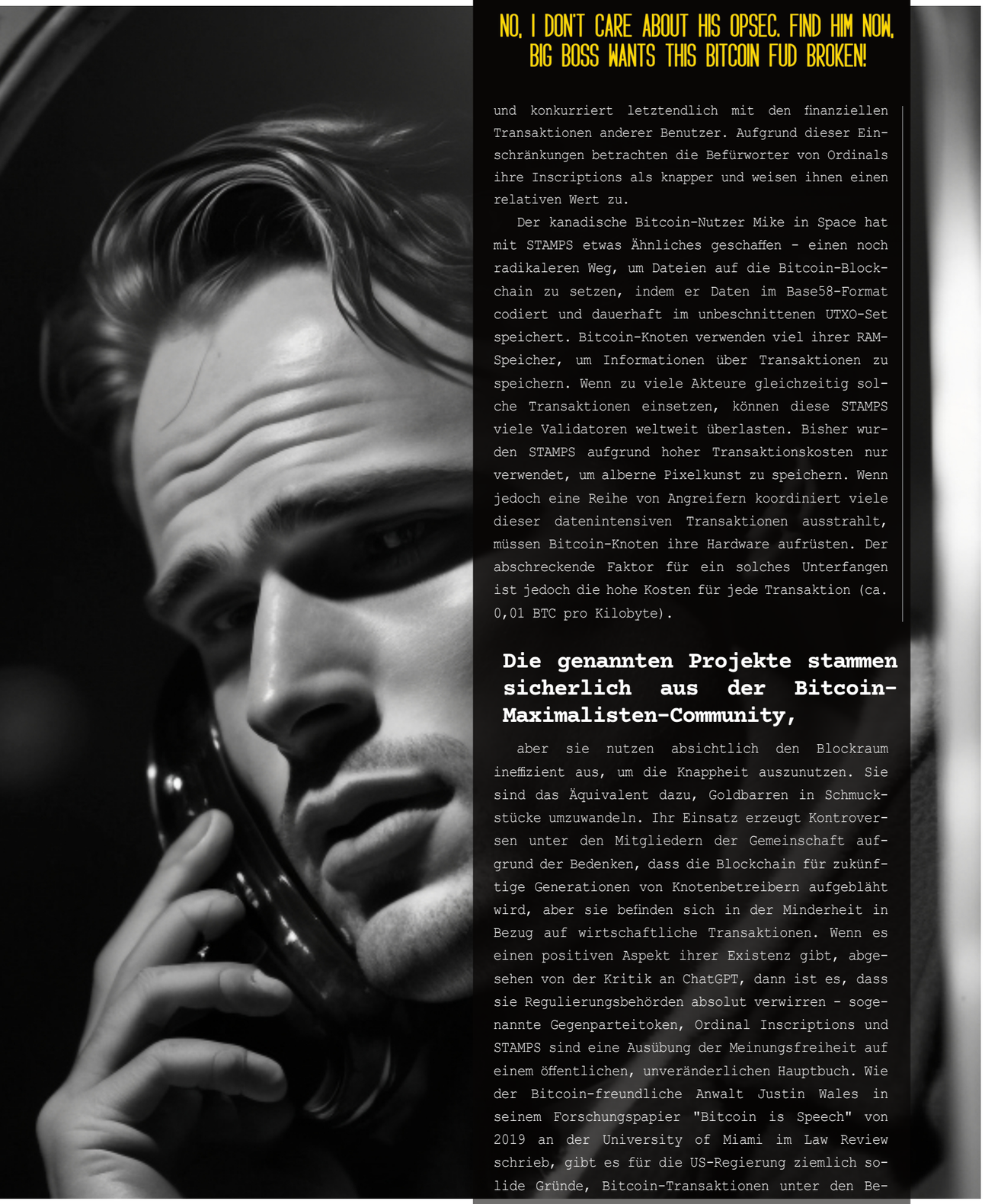
Colored Coins, Counterparty, Omni, Blockstreams Liquid Sidechain, Rootstock (RSK), das Lightning Network, Paul Sztorcs Drivechains, Ruben Somsens Statechains, John Carvalhos Synonym, Portal, Eric Martindales Fabric, Maxim Orlovskys RGB, Lightning Labs Taro, Eric Sirions Fedi, Calles Cashu und Casey Rodarmors Ordinals. Diese Liste ist chronologisch geordnet und umfasst Protokolle und Schichten, die seit 2012 auf Bitcoin implementiert wurden. Die Aufzählung ist jedoch nicht unbedingt abschließend - es gibt immer etwas Neues, das auf den Markt kommt und die Möglichkeiten erweitert, wie man seine Münzen verwenden kann. Es gibt sogar eine noch längere Liste von Vorschlägen, die nie verwirklicht wurden.

Um ChatGPTs Argument über "begrenzte Anwendungsfälle" zu widerlegen, werde ich die Projekte präsentieren, die entwickelt wurden, weiterhin genutzt werden können und erfolgreich die Möglichkeiten erweitern, wie man seine BTC nutzen kann.

Colored Coins, Counterparty und Omni ermöglichen die Ausgabe von Tokens auf der Bitcoin-Blockchain. Aus technischer Sicht handelt es sich um OP_RETURN-Transaktionen, die dauerhafte und erkennbare Markierungen in der Blockchain hinterlassen. Ihr Ziel ist es, reale Vermögenswerte (Rohstoffe wie Gold, Immobilien, Aktien, Fiat-Währungen) auf der Bitcoin-Blockchain zu kennzeichnen, entweder durch die willkürliche Zuweisung einer bestimmten Bedeutung und Wertigkeit an eine Handvoll BTC-Einheiten (wie im Fall von Colored Coins) oder durch die Ausgabe eines Tokens, der den Besitz anderer Vermögenswerte repräsentiert (Rare Pepes und Bitcoin Heads auf Counterparty, Tether auf Omni). Counterparty, das im Jahr 2014 gestartet wurde, war noch ehrgeiziger - es hatte zum Ziel, dezentralisierten Unternehmen die Ausgabe eigener Aktien, die Zahlung von Dividenden und den Handel ihrer Aktien gegen andere Vermögenswerte auf einem offenen Marktplatz zu ermöglichen. Aufgrund der begrenzten Skalierbarkeit und hoher Transaktionskosten wurden jedoch die meisten dieser Pläne nie vollständig umgesetzt.

Casey Rodarmors Ordinal Inscriptions sind eine weitere Variante von Colored Coins. Das Projekt zielt darauf ab, nummerierte Bitcoin-Einheiten mit einer Zeichenkette von Daten zu verbinden, die im Witness-Bereich eines Bitcoin-Blocks gespeichert werden. Das Design ist eleganter und minimalistischer als alles, was mit NFTs auf Ketten wie Ethereum zu tun hat, kann jedoch nicht skalieren, um die beliebigen Daten aller Benutzer aufzunehmen,





NO, I DON'T CARE ABOUT HIS OPSEC. FIND HIM NOW, BIG BOSS WANTS THIS BITCOIN FUD BROKEN!

und konkurriert letztendlich mit den finanziellen Transaktionen anderer Benutzer. Aufgrund dieser Einschränkungen betrachten die Befürworter von Ordinals ihre Inscriptions als knapper und weisen ihnen einen relativen Wert zu.

Der kanadische Bitcoin-Nutzer Mike in Space hat mit STAMPS etwas Ähnliches geschaffen - einen noch radikaleren Weg, um Dateien auf die Bitcoin-Blockchain zu setzen, indem er Daten im Base58-Format codiert und dauerhaft im unbeschnittenen UTXO-Set speichert. Bitcoin-Knoten verwenden viel ihrer RAM-Speicher, um Informationen über Transaktionen zu speichern. Wenn zu viele Akteure gleichzeitig solche Transaktionen einsetzen, können diese STAMPS viele Validatoren weltweit überlasten. Bisher wurden STAMPS aufgrund hoher Transaktionskosten nur verwendet, um alberne Pixelkunst zu speichern. Wenn jedoch eine Reihe von Angreifern koordiniert viele dieser datenintensiven Transaktionen ausstrahlt, müssen Bitcoin-Knoten ihre Hardware aufrüsten. Der abschreckende Faktor für ein solches Unterfangen ist jedoch die hohe Kosten für jede Transaktion (ca. 0,01 BTC pro Kilobyte).

Die genannten Projekte stammen sicherlich aus der Bitcoin-Maximalisten-Community,

aber sie nutzen absichtlich den Blockraum ineffizient aus, um die Knappheit auszunutzen. Sie sind das Äquivalent dazu, Goldbarren in Schmuckstücke umzuwandeln. Ihr Einsatz erzeugt Kontroversen unter den Mitgliedern der Gemeinschaft aufgrund der Bedenken, dass die Blockchain für zukünftige Generationen von Knotenbetreibern aufgebläht wird, aber sie befinden sich in der Minderheit in Bezug auf wirtschaftliche Transaktionen. Wenn es einen positiven Aspekt ihrer Existenz gibt, abgesehen von der Kritik an ChatGPT, dann ist es, dass sie Regulierungsbehörden absolut verwirren - sogenannte Gegenparteitoken, Ordinal Inscriptions und STAMPS sind eine Ausübung der Meinungsfreiheit auf einem öffentlichen, unveränderlichen Hauptbuch. Wie der Bitcoin-freundliche Anwalt Justin Wales in seinem Forschungspapier "Bitcoin is Speech" von 2019 an der University of Miami im Law Review schrieb, gibt es für die US-Regierung ziemlich solide Gründe, Bitcoin-Transaktionen unter den Bestimmungen des ersten Verfassungszusatzes unter Schutz zu stellen.

Auf der anderen Seite haben wir skalierbare und wirtschaftliche Bitcoin-Maximalistenprojekte. Sie belasten die Basis-Layer nicht, da sie die zusätzlichen Transaktionen auf eine zweite Ebene oder eine parallele Kette verlagern. Darüber hinaus sind ihre Transaktionskosten erheblich niedriger.

Blockstreams Liquid ist vielleicht die bekannteste Bitcoin-Sidechain. Liquid fungiert als Föderation von Blockproduzenten, die auch als Torwächter des Systems agieren. Durch sie erhalten Sie Ihre L-BTC, wenn Sie Ihre BTC auf der Basis-Layer sperren, und es ist mindestens ein Föderationsmitglied, das Ihren Antrag bearbeiten muss, um die L-BTC zu verbrennen und die Mittel auf der Hauptkette freizugeben. Einige argumentieren, dass das Design weit entfernt von dem im Oktober 2014 erstmals skizzierten Sidechain-Konzept ist, hauptsächlich aufgrund des genehmigten Designs und des Ersatzes der Dezentralisierung durch eine Föderation von Mitgliedern.

Dennoch bietet Liquid durch Vertrauliche Transaktionen ziemlich gute Privatsphäre und kann Bitcoin auch in Zeiten hoher Nachfrage skalieren. Es kann wie Counterparty/Omni Token ausgeben und einige der Funktionen, die man auf Ethereum findet (Verträge, Lizenzsysteme), nachahmen, jedoch in einer privateren Umgebung. Nichtsdestotrotz besteht der Hauptanwendungsfall darin, Börsen und Händlern zu helfen, Abwicklungen schneller und kostengünstiger durchzuführen und die Möglichkeit zu haben, die Beträge zu verbergen, die sie bewegen - Wal-Tracking-Bots auf Twitter und Telegram zeigen somit keine großen Geldtransfers mehr an.

Auf der Liquid-Sidechain gibt es auch einige interessante Anwendungen. Eine davon ist Raretoshi, ein tokenisierter digitaler Kunstmarkt, der denselben Stil und dieselbe Funktionalität wie das bekanntere OpenSea nachahmt. SideSwap, BitMatrix und TDEX sind einige der dezentralen Börsen, auf denen Sie L-BTC gegen L-USDT (Tether auf Liquid) handeln können. Dann gibt es Fuji Money, eine Plattform, die es Benutzern ermöglicht, Bitcoin-gedeckte Stablecoins und synthetische Vermögenswerte ohne vertrauenswürdige dritte Partei in der Mitte zu leihen. Das Ökosystem rund um die Liquid-Sidechain ist sicherlich interessant, hat aber nicht viel Aufmerksamkeit erregt. Vielleicht wird Liquid in Zukunft, wenn die Nachfrage nach Blockraum auf der Hauptkette höher ist, im Rampenlicht der Mainstream-Bitcoin-Kultur stehen.

Rootstock, heute als RSK bekannt, ist eine weitere wichtige Sidechain. Ihr Ziel ist sehr einfach, aber ambitioniert: Alle Ethereum-Smart Contracts auf eine Bitcoin-Ebene zu portieren. Es handelt sich um eine modifizierte Version von Ethereum, die durch Merge-Mining von mehr als 57% der Bitcoin-Hashrate gesichert wird - was bedeutet, dass dieselben Miner die thermodynamische Sicherheit des Systems gewährleisten und Transaktionsgebühren zur Erhöhung ihrer Einnahmen erhalten. RSK-Architekt Sergio Demian Lerner hat auch ein paar zusätzliche Optimierungen hinzugefügt, die es in Ethereum nicht gibt. Zum Zeitpunkt dieser Aufzeichnung sind rund 3500 Bitcoins in RSK gesperrt - fast so viel wie in Liquid (4130). Da Rootstock mit Ethereum kompatibel ist, umfassen die Anwendungen sowohl originäre Werke als auch Ports von anderen Chains. Metamask ermöglicht einen einfachen Übergang, Vermögenswerte können sowohl mit Trezor als auch mit Ledger Hardware-Wallets gesichert werden, und es gibt Möglichkeiten, Stablecoins gegen Ihre RBTC mit Sovryn zu leihen. Für diejenigen, die sich für dezentrale Finanzen interessieren, bietet das Ökosystem auch RSK Swap - ein Klon von Uniswap, der die Grundlage für eine dezentrale Börse ohne KYC bildet.



Insgesamt profitiert RSK von Funktionen und Integrationen, die speziell für Ethereum nicht verfügbar sind, da die Portierung von Anwendungen und Verträgen nahtlos erfolgt. Der Grund, warum es Ethereum noch nicht ersetzt, ist, dass die ursprüngliche Kette noch keine kritischen Sicherheitslücken aufgewiesen hat und die Preminers immer noch viel Geld für Marketing haben, um neue Benutzer anzulocken. Aber RSK ist ein nützliches Sicherheitsnetz, das garantiert, dass es keine Störungen gibt, wenn Ethereum scheitert... und letztendlich kommt alles auf Bitcoin zurück.

Drivechains hingegen sind eine Neuerfindung des Sidechain-Forschungspapiers von 2014 und reprä-sentieren stolz die reinste Form des Bitcoin-Maximalismus. Über sie könnte Bitcoin jeden bestehenden Anwen-dungsfall von Altcoins integrieren und ihrem offensichtlichen Betrug ein Ende setzen. Durch Paul Sztorcs BIP300 und BIP301 ermöglichen Drivechains, dass jeder seine eigene Bitcoin-Sidechain erstellen kann, die Gebühren an dieselben BTC-Miner zahlt.

Der freie Marktzugang könnte den Shitcoins ein Ende setzen.

Die gesamte Wirtschaft würde sich um die 21 Millionen BTC drehen, die über verschiedene Ketten hinweg bewegt werden, um mehrere Vorteile zu erlangen. Zum Beispiel können einige Coins zu einer Monero-/Zcash-Sidechain verschoben werden, um eine bessere Transaktionsprivatsphäre zu erhalten, während andere in eine Ethereum-ähnliche Sidechain gelangen können, auf der jeder ICOs und DeFi betreiben kann. Was an diesem Design radikal anders ist, ist, dass niemand mehr Geld aus dem Nichts drucken kann - jede Aktivität, egal wie legitim oder betrügerisch sie ist, verursacht BTC-Kosten und zahlt Gebühren an die Bitcoin-Miner. Darüber hinaus werden Konservative, die nur die Hauptkette nutzen wollen, nicht beeinträchtigt, und ihre Full Nodes speichern keine Informationen, die von den Sidechains generiert werden..

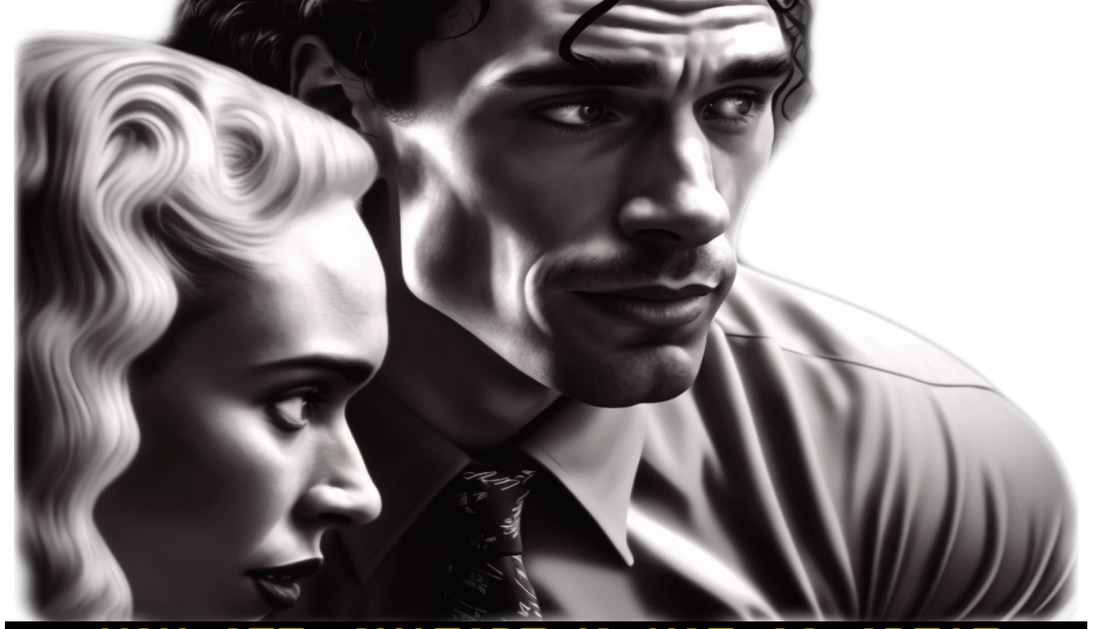
Auf dem Testnet zeigen Drivechains vielversprechende Ergebnisse: Paul Sztorc veröffentlichte Anleitungen und Video-Tutorials, die zeigen, wie eine Zcash- und eine Ethereum-Sidechain funktionieren. Am wichtigsten ist, dass er gezeigt hat, dass Bitcoin Core nicht betroffen war und keinerlei Kenntnis von den Aktivitäten auf anderen Ketten hatte. Wenn sie auf dem Hauptnetzwerk fusioniert werden, könnten Drivechains die Bitcoin-Softfork sein, um alle Altcoins zu beenden und die Notwendigkeit einer weiteren Aktualisierung der Bitcoin-Basis in Zukunft zu minimieren.

Statechains erweitern auch die Funktionalität von Bitcoin

und bieten weitere Skalierungsmöglichkeiten. Sie wurden erstmals von Ruben Somsen auf der Scaling Bitcoin-Konferenz 2018 in Tokio vorgestellt und fungieren als Layer-2, um den Besitz von Coins auszutauschen. Auf der Grundlage einer multisignierten Hauptchain, die Mittel sperrt, können Benutzer das Protokoll nutzen, um vorübergehende Schlüssel zu generieren, die den außerhalb der Chain stattfindenden Wertetransfer ermöglichen.

Die beliebteste Implementierung von Statechains findet sich in MercuryWallet: einer Desktop-Bitcoin-Wallet, die außerhalb der Chain CoinSwaps durchführt, die





Benutzern ermöglichen, UTXOs mit demselben Wert ohne Spuren auf der Chain zu handeln. Aber über die Transferfunktion hinaus sind Statechains auch interoperabel mit dem Lightning-Netzwerk und ermöglichen Benutzern das direkte Öffnen von Kanälen aus dieser Layer. Dies bringt Vorteile in Bezug auf Privatsphäre, Skalierbarkeit und Kosten.

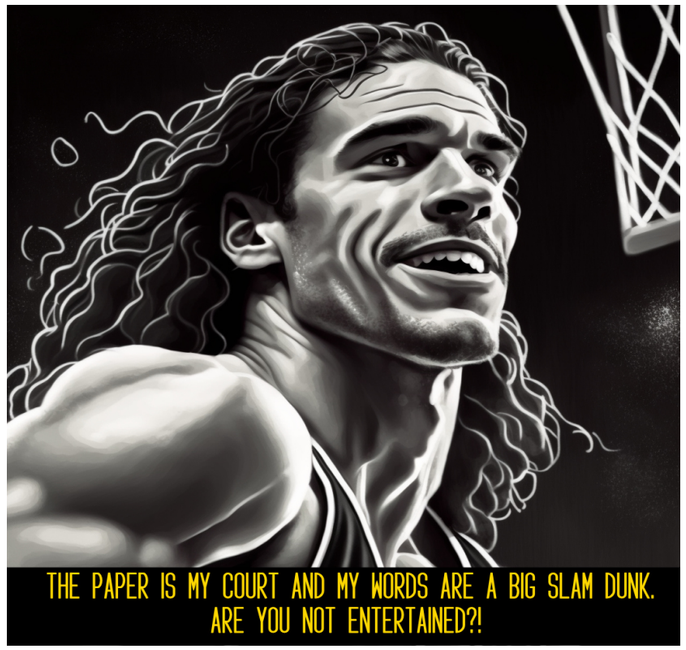
Von allen in diesem Artikel vorgestellten Layern und Protokollen sind Statechains die am meisten übersehenen und ihr Potenzial wird stark unterschätzt. Aber vielleicht werden Sie nach dem Lesen dieses Artikels inspiriert sein, einen Blick auf Ruben Somsens Arbeit zu werfen und etwas darauf aufzubauen.

Das Lightning-Netzwerk ist bei weitem die erfolgreichste Bitcoin-Layer. Wo die anderen Protokolle und Sidechains meistens ein einzelnes Entwicklerteam haben, das sich auf deren Verbesserung und Wachstum konzentriert, da arbeiten Tausende von Menschen aus der ganzen Welt an Lightning. Auf Protokollebene konkurrieren Lightning Labs (lnd), Blockstream (Core Lightning), ACINQ (eclair), Nayuta (Nayuta Core) und Electrum um Marktanteile, indem sie verschiedene Verbesserungen auf allen Plattformen vornehmen. Auf Betriebssystem- und Distributions-Ebene haben wir RaspiBlitz, Umbrel, MyNode, Start9 EmbassyOS, Citadel und eine Vielzahl anderer Schnittstellen, die es jedem ermöglichen, Bitcoin- und Lightning-Knoten leicht zu starten. Selbst auf Wallet-Ebene ist Lightning das beliebteste und robusteste - Breez, Blixt, Phoenix, Electrum und Muun sind nur einige Beispiele für nicht gehosteten Lösungen, die ohne einen dedizierten Knoten laufen, der rund um die Uhr läuft. Stand April 2023 hat das Lightning-Netzwerk auch in Bezug auf Liquidität (5460+ BTC), unabhängige Knoten (15000+) und Kanäle (70000+) die Vorherrschaft.

An diesem Punkt ist Lightning so groß und bedeutend, dass es Layer-3s gibt, die darauf aufbauen, sowie interoperable Layer-2s: RGB, Taro und Cashu repräsentieren ersteres, während Statechains, Liquid und Fedi zu letzteren gehören. Dieses Phänomen tritt auf, weil Lightning netzwerkunabhängig ist und atomare Swaps zwischen verschiedenen Chains ermöglichen kann.

Der Mehrwert des Lightning-Netzwerks besteht darin,

dass Benutzer für den Preis von zwei On-Chain-Transaktionen hunderte (wenn nicht tausende) Transaktionen durchführen können, und das mit der Geschwindigkeit ihrer Internetverbindung und zu erheblich geringeren Kosten. Das Hauptproblem liegt jedoch im Routing - damit eine Zahlung von Wallet A zu Wallet B gelangt, müssen entweder eine direkte Verbindung zwischen den Wallets hergestellt oder ein Dritter hinzugezogen werden, der sie ver-



bindet. Mit zunehmender Liquidität entstehen große Hubs - Benutzer tendieren natürlich zu Knotenpunkten mit der größten wirtschaftlichen Aktivität (Geschäfte, spezialisierte Unternehmen, die Infrastruktur bereitstellen). Und wenn dieser Zustrom von Liquidität von offensichtlichen Auswahlmöglichkeiten für gemeinsame Hubs begleitet wird, werden die isolierten Knotenpunkte weniger und die Chancen, Knotenpunkte zu verbinden, werden größer.

Was großartig an Lightning ist, ist, dass es als Grundlage für andere Layers dienen kann, die seine Geschwindigkeit und Flexibilität nutzen können, um andere Dinge zu ermöglichen. Zum Beispiel strebt RGB an, das Ethereum-Design mit einer clientseitigen Validierung überflüssig zu machen, während Taro einen USD-Stablecoin einführen möchte, um mehr Handelsoptionen zu ermöglichen. Es gibt auch Portal und Fabric, die mit atomic swaps, Berechnungen und Datenspeicherung zu tun haben. Und wenn Ihre Lightning-Transaktionen nicht privat genug sind, werden Chaumianische Coins wie Cashu und Fedi zu Hilfe kommen. Doch bevor wir dazu kommen, sprechen wir über John Carvalhos Synonym.

Synonym beschreibt eine ganze Reihe von Anwendungen und Integrationen: Von Bitkit (Bitcoin-Toolkit) bis Blocktank (ein Lightning-Service-Anbieter) gibt es viel zu entdecken. Aber das wirklich einzigartige Produkt sind Slashtags - ein Tool, das die Identität im Web erheblich vereinfacht. Mit nur einer Bitcoin- und Lightning-Wallet (derzeit von Bitkit bereitgestellt) kann jeder ein Profil erstellen, seinen Ruf aufbauen und seine Beiträge unter einer einfachen, benutzerfreundlichen Oberfläche leicht auffindbar machen.

Kurz gesagt, Synonyms Slashtags versucht das Zensurproblem im Internet auf eine Weise zu lösen, die aufrichtigen Handlungen Anreize gibt. Ihr Profil ist plattformunabhängig, sodass jede Website mit Integration von Slash-tags es Ihnen ermöglicht, Kommentare abzugeben und an Debatten teilzunehmen. Zusätzlich gibt es eine Lightning-Zahlungskomponente. Facebook und Google haben Mitte der 2000er Jahre etwas Ähnliches versucht, jedoch hatten sie immer Kontrolle über die Profile, sodass sie Konten schließen, einschränken und zensieren konnten.

Derzeit versucht Metamask etwas Ähnliches für Assets im Ethereum-Ökosystem: eine Browser-Integration, die das Einloggen in andere Anwendungen und Protokolle erleichtert. Der Umfang von Metamask ist jedoch auf finanzielle Anwendungen beschränkt. Slashtags decken einen breiteren Anwendungsbereich ab, der das Kommentieren auf Websites und den Aufbau eines Rufs umfasst. Daher bietet die Bitcoin-Version wieder mal mehr und macht es besser.

Ein weiteres interessantes Projekt ist Portal, eine DeFi-Plattform, die Atomic Swaps im Lightning-Netzwerk nutzt. Sie wird von einigen der Veteranen entwickelt, die das erste Bitcoin-Meetup im Silicon Valley organisiert haben (insbesondere George Burke). Das Projekt wird vom Kapital großer zentralisierter Börsen unter-stützt (insbesondere Coinbase und OKEX) und zielt darauf ab, eine skalierbare Alternative zu Verwahrungsbörsen zu werden. Bisher hat Portal erfolgreich einen erfolgreichen Cross-Chain L2-Swap zwischen Bitcoin und Ethereum durchgeführt - ohne die Notwendigkeit von "Brücken" oder gewrappten Coins. Im Laufe der Zeit wird erwartet, dass der Projektumfang wächst.

Fabric ist ein Protokoll, das die Ambitionen des Lightning-Netzwerks auf die nächste Stufe hebt, indem es eine Berechnungsebene für Datenspeicherung und vertrauenslose Anwendungsbereitstellung aufbauen möchte.

Die offizielle Beschreibung lautet "Betriebssystem für den leistungsstärksten Supercomputer der Welt", aber die Pläne für die Datenspeicherung erweitern den Anwendungsbereich über die Ambitionen eines App-Stores hinaus. Fabric wurde erstmals im Februar 2016 angekündigt und der Hauptarchitekt Eric Martindale hat über einige Durchbrüche mit frühen Prototypen berichtet. Das Projekt muss jedoch noch in vollem Umfang implementiert werden.

RGB, Taro, Fedi und Cashu

sind ebenfalls Dritt-Layer, die auf dem Lightning-Netzwerk aufbauen. Obwohl es einige technische Ähnlichkeiten zwischen ihnen gibt, unterscheiden sich ihre Zwecke sehr. RGB ist ein Smart-Contract-System, das auf Bitcoin und dem Lightning-Netzwerk basiert. Es profitiert von der clientseitigen Validierung und ermöglicht sofortige Übertragungen des Eigentums an Vermögenswerten. Wenn digitale Sammelkarten von Bitcoin Heads zu RGB transferiert werden, können Sammler sie innerhalb von Sekunden und zu erheblich geringeren Kosten als bei On-Chain-Transaktionen austauschen.

Konzeptionell gesehen ist Taro von Lightning Labs sehr ähnlich wie RGB - bis zu dem Punkt, an dem Maxim Orlovsky, der Schöpfer und Hauptentwickler von RGB, ihre Taktik kritisiert hat, Teile des Codes ohne Anerkennung zu kopieren und dann Millionen von Dollar für das Endprodukt zu sammeln. Allerdings wird Taro explizit darauf abzielen, "die Währungen der Welt" (aka Stablecoins) auf das Lightning-Netzwerk zu bringen. RGB ist universell im Design und zielt darauf ab, Benutzern zu ermöglichen, eine weltweite Wirtschaft aufzubauen, in der sie über sichere tokenisierte Unternehmensanteile Geld sammeln, digitale Sammelobjekte handeln und mehr können. Im Grunde genommen eine skalierbarere, elegantere und privatere Version dessen, was heute auf Ethereum passiert.

Taro hat eine engere und spezialisiertere Rolle, da es das Lightning-Netzwerk als Abwicklungs-Layer für andere Arten von Währungen nutzt. Es scheint darauf abzielen, den Dollar auf Lightning zu bringen, aber andere Arten von Fiatgeld werden definitiv folgen. Technisch gesehen könnte RGB bei ausreichender Finanzierung den Bedarf an Taro theoretisch ersetzen. Aber dieser Wettbewerb, bei dem eine Seite mehr Ideen hat und die andere mehr Kapital, könnte sich als gesund für Innovation erweisen.

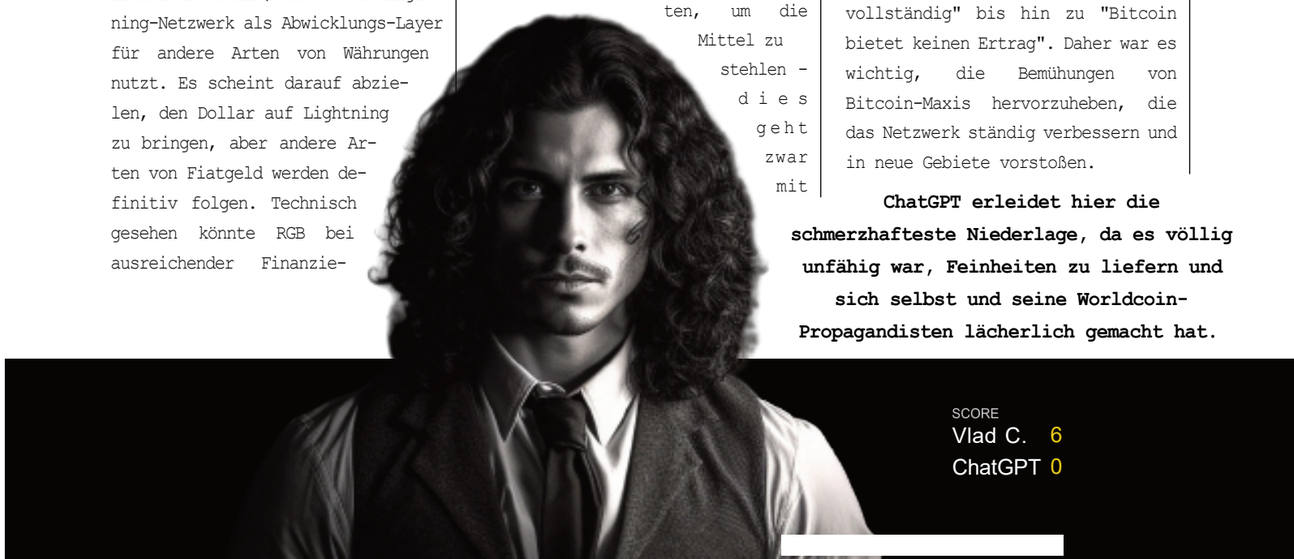
Fedi und Cashu sind die neuesten Ergänzungen zum Layer-3-Stack von Bitcoin. Sie sind im Design sehr ähnlich, da sie beide Chaumianische Coins für Anonymität erstellen. Aber es sind die kleinen Unterschiede, die sie auf ihre eigene Weise einzigartig machen. Fedi von Eric Sirion hat zum Ziel, Gemeinschaftsbanken zu schaffen, die den Einstieg für Menschen erleichtern, die sich normalerweise vor der Selbstverwahrung fürchten. Menschen in kleinen Städten, Dörfern oder Mitglieder verschiedener Vereine und religiöser Gruppen können ihre Bitcoins zusammenlegen und einer Handvoll Personen vertrauen, die eine Multisignatur-Wallet einrichten, um die Münze zu erzeugen. Der Vorteil besteht darin, dass die Transaktionen aller privat sind und niemand sehen kann, wie viel Geld jeder andere hat. Die einzige Information, die alle beobachten können, ist die Gesamtmenge an BTC in der Münze.

Allerdings hat Fedi auch soziale und politische Nachteile. Gemeinschaftsbanken sind leichter zu zensieren und zu schließen als ein dezentrales globales Netzwerk von Computern. Darüber hinaus können die Schöpfer der Coins zusammenarbeiten, um die Mittel zu stehlen - dies geht zwar mit einem Rufschaden innerhalb der Gemeinschaft einher - aber es ist dennoch möglich.

Cashu hingegen wurde entwickelt, um die Datenschutzbeschränkungen von Lightning zu verbessern. Schöpfer Calle hat sich mit Chaumian E-Cash befasst, um sich für ein System inspirieren zu lassen, bei dem Menschen ihr Geld zusammenlegen, um ihre Transaktionsprivatsphäre zu maximieren. Auf dem Lightning-Netzwerk profitiert nur der Sender von guter Privatsphäre - während der Empfänger exponiert bleibt. Der Hauptunterschied zwischen Fedi und Cashu besteht darin, dass ersteres auf einer Föderation basiert, während letzteres individuelle Selbstverwahrung optimiert. Cashu eignet sich auch hervorragend für die Verwendung mit verwahrungsgebundenen Lightning-Wallets, um zu verhindern, dass der Node-Betreiber weiß, wer Sie sind, wie viele Mittel Sie besitzen und mit wem Sie handeln. Dadurch wird dem Verwahrer die Macht genommen, Benutzer zu zensieren.

Ursprünglich sollte dieser Artikel eine einfache Aufzählung der Schichten und Protokolle sein, die Bitcoin viel komplexer und leistungsfähiger machen als von den Mainstream-Medien und den Machern von ChatGPT dargestellt. Aber das "Pet Rock mit begrenzten Anwendungsfällen" FUD tritt immer wieder auf und nimmt viele Formen an - von "Bitcoin ist nicht Turing-vollständig" bis hin zu "Bitcoin bietet keinen Ertrag". Daher war es wichtig, die Bemühungen von Bitcoin-Maxis hervorzuheben, die das Netzwerk ständig verbessern und in neue Gebiete vorstoßen.

ChatGPT erleidet hier die schmerzhafteste Niederlage, da es völlig unfähig war, Feinheiten zu liefern und sich selbst und seine Worldcoin-Propagandisten lächerlich gemacht hat.



KYM
Know
Your
Magazine

Edition	1st	2nd	3rd	4th
				
Menge	120 Stück	41 Stück	50 Stück	50 Stück
veröffentlicht bei	Fulmo Lightning Hackaton	Scarce.City	Wasabi's Hunting Sats Campaign	Pizza Day
Ort	Istanbul, Türkei	Online Auktion	Budapest, Ungarn	Paralelni Polis, Prag
Veröffentlichungsdatum	25. Februar 2022	6. April 2022	Weihnachten 2022	21. Mai 2022
gedruckt in	Türkei: 100-150 Rumanien: 1-70	Rumänien	Ungarn	Tschechien
Cover Artist	Vlad	Scrilla	Alexa	CypherpunkNow & Katka
Boni	mit Vol. 2 Signiert & nummeriert XCP token	mit Vol. 2 XCP token Gestempelt mit Scrilla's Signatur	mit Vol. 2, Wasabi merchandise	Signiert & nummeriert
Aktuellster Preis	0.0045 BTC (13. Juni 2022)	0.0149 BTC (1. August 2022)	N/A (nicht verfügbar)	0.00082 BTC (21. Mai 2022)

Edition	6th		open source
				
Menge	200 Stück	100 Stück	100+ Stück	digital
veröffentlicht bei	Mallorca Blockchain Days	Baltic Honeybadger	Surfin Bitcoin	Github.com/VladdyC
Ort	Palma de Mallorca, Spanien	Riga, Lithauen	Biarritz, Frankreich	online
Veröffentlichungsdatum	14. Juli 2022	3. September 2022	26. August 2022	26. February 2022
gedruckt in	Deutschland	Lithauen	Deutschland (ersten100)	überall
Cover Artist	Andre	Anna from HodlHodl	Bogdan Menci & Delacroix	Vlad & Bogdan Menci
Boni	Signiert & nummeriert (erste 70 Kopien)	Signiert & nummeriert XCP token	Beste BTCTKVR Artikel übersetzt Von Grittoshi	Download it Print it Sell it
Aktuellster Preis	N/A (nicht verfügbar)	#1: 0.005 BTC #100: 0.00005 BTC (3. September 2022)	N/A (nicht verfügbar)	kostenlos

Edition	7th	8th		
				
Menge	100 Stück	90 Stück	300 Stück	100 Stück
veröffentlicht bei	HCPP	TABConf	LABitconf	Adopting Bitcoin
Ort	Prag, Tschechien	Atlanta, Georgia, USA	Buenos Aires, Argentinien	El Salvador
Veröffentlichungsdatum	30. Sep. - 2. Okt. 2022	14. - 15. October 2022	10. - 13. November 2022	15. - 17. November 2022
gedruckt in	Tschechien	USA	Argentinien	El Salvador
Cover Artist	CypherpunkNow	NoGood	Andrej Cibik, Mariana Aquirre, FC Hájske	Bitko
Boni	Signiert & nummeriert von Vlad	Signiert & nummeriert von Madelyn Ash	Signiert & nummeriert von Roberto	Verkauft beim Adopting Bitcoin merch booth
Aktuellster Preis	0.0013 BTC	N/A (nicht verfügbar)	N/A (nicht verfügbar)	N/A (nicht verfügbar)

Edition	9th	10th	Vol.2	
				
Menge	100 Stück	20 Stück	21 Stück	311 Stück (auch digital)
veröffentlicht bei	Adopting Bitcoin	Dakar Bitcoin Days	Christmas 2022	Fulmo Lightning Hackaton
Ort	El Salvador	Senegal	Rumänien	Istanbul, Türkei
Veröffentlichungsdatum	15. - 17. November 2022	2. - 3. Dezember 2022	25. Dezember 2022	25. Februar 2022
gedruckt in	El Salvador	Senegal	Rumänien	Türkei: 100 Rumänien: 111 USA: 50 Ungarn: 50
Cover Artist	Adopting Bitcoin	UndercoverMax	Golshid Rahbar, Vlad	Bogdan Menci, Igor Petrov
Boni	Verkauft beim Adopting Bitcoin merch booth	Verteilt von Nourou	Beinhaltet franz. + span. Übersetzungen Signiert & nummeriert	Signiert & nummeriert
Aktuellster Preis	N/A (nicht verfügbar)	N/A (nicht verfügbare)	N/A (nicht verfügbar)	N/A (nicht verfügbar)



Breaking ChatGPT's Bitcoin FUD #7

Energieverbrauch

VERSCHWENDUNG/VERBRAUCH · MINING · BITMAIN · CO^2 · POW

Laut Laut ChatGPT ist die Menge an Energie, die zur Absicherung des Bitcoin-Netzwerks erforderlich ist, bedenklich, da das dezentrale Proof-of-Work-Netzwerk mehr Strom verbraucht als andere Zahlungssysteme. Wie üblich liefert das KI-Modell nur wenig bis gar keine Nuancen und präsentiert eine eher allgemeine Kritik. Dennoch ist die Tatsache, dass uns ein vergleichender Blickwinkel geboten wird (formuliert als "verbraucht mehr Energie als die meisten anderen Zahlungssysteme"), wirklich nützlich und wir können sie zur Entlarvung der FUD nutzen.

Bevor wir uns jedoch damit beschäftigen, die FUD selbst zu widerlegen, ist es wichtig, zwischen zwei Arten der öffentlichen Kommentierung des Energieverbrauchs von Bitcoin zu unterscheiden:

- die erste Art ist von Natur aus nihilistisch und impliziert, dass Bitcoin nutzlos ist oder nicht neben Bankdienstleistungen existieren sollte. Diese Art der Argumentation führt zu dem Schluss, dass Bitcoin verschwenderisch, belanglos und zu umweltschädlich ist, um irgendeine Anerkennung zu erhalten. Dies ist die häufigste Art des Angriffs, auch wenn er indirekt unter dem Vorwand "Bitcoin hat keinen Nutzen" und "Bitcoin kann kein Geld sein" präsentiert wird;

- die zweite Art legt nahe, dass Bitcoin auf Proof-of-Stake umstellen sollte. Es handelt sich um ein nuancierteres, technisches und letztendlich zerstörerisches Argument, das hauptsächlich von Altcoin-Befürwortern verbreitet wird, die die Dezentralisierung von Bitcoin untergraben und möglicherweise eine gewisse Kontrolle erlangen möchten. Ethereum wird oft als Beispiel für einen Übergang zu Proof-of-Stake präsentiert, dem Bitcoin folgen sollte, während Ripple-Manager aktiv Anti-Bitcoin-Kampagnen finanzieren, um den Ruf des Systems zu schädigen. Einige dieser Punkte mögen für den durchschnittlichen Menschen vernünftig klingen, aber es ist wichtig zu erklären, warum Proof-of-Stake ohne eine besorgniserregende Zentralisierung keine Sicherheit bieten kann.

Beide Argumente sind insofern zerstörerisch, als sie darauf abzielen, die grundlegenden Eigenschaften von Bitcoin zu untergraben. Das erste Argument kommt den Bankern zugute, während das zweite den Interessen der Altcoin-Befürworter dient, deren Netzwerke auf dem freien Markt nicht mit Bitcoin konkurrieren können... Daher entscheiden sie sich folglich dafür, ein politisches Spiel zu spielen.

Nun wollen wir etwas Kontext geben, um zu erklären, wie Bitcoin funktioniert

und warum er Energie verbraucht, um zu funktionieren. Denn ja, Bitcoin ist eine Form von Geld, die große Mengen an Elektrizität benötigt, um sicher zu bleiben. Das System unterliegt den Gesetzen der Physik, da Transaktionen thermodynamisch gegen zukünftige Änderungen geschützt werden. Neue Transaktionen von Benutzern weltweit werden in einen Speicherpool eingefügt, der von Bitcoin-Knotenpunkten gespeichert wird, während Miner an einem globalen Wettbewerb teilnehmen, um eine seltene Zahl zu finden (als "Hash" bezeichnet). Sobald ein Miner oder eine Gruppe von Minern diese Zahl entdeckt, wird eine Nachricht an das gesamte Netzwerk gesendet und ein zeitgestempelter Block, der einige tausend Transaktionen aus dem Speicherpool umfasst, wird zur öffentlichen Hauptbuch hinzugefügt.

Nur ein Miner oder eine Gruppe von kooperierenden Minern kann die Belohnung erhalten. Bitcoin ist ein "Alles oder nichts"-System, das Wettbewerb fördert und Ineffizienz nicht bevorzugt. Miner müssen eine kostengünstige und zuverlässige Stromquelle finden, Hardware verwenden, die die größte Anzahl von Hashes pro verbrauchter Kilowattstunde produziert, und sich ständig an einen dynamischen

Gefällt dir der Artikel?

Scanne den QR-Code und hinterlasse ein Kommentar oder eine Donation!



globalen Markt anpassen, der niemals aufhört, Innovationen voranzutreiben und manchmal von lokalen oder nationalen Regierungen reguliert wird. In den meisten Fällen ist die beste Energiequelle für Bitcoin-Miner auch die umweltfreundlichste - die Produktion erneuerbarer Elektrizität ist ein aufstrebendes Feld, und es gibt immer überschüssige Kilowattstunden, die nicht gespeichert werden können und daher für die Sicherheit von Bitcoin genutzt werden.

Bitcoin-Mining mittels Proof of Work verbindet das digitale Geldnetzwerk mit der realen Welt und erzeugt Kosten für die Produktion und Übertragung von Geldmitteln. Es bietet thermodynamische Endgültigkeit für jede Operation und stellt sicher, dass die Geschichte nicht ohne hohe Kosten und dauerhafte Beweise verändert werden kann. Ursprünglich war Proof of Work ein Mechanismus, um Denial-of-Service-Angriffe (wie von Moni Naor und Cynthia Dwork 1993 beschrieben) abzuwehren und E-Mail-Spam zu verhindern (wie von Adam Back in Hashcash implementiert). Im Wesentlichen erfordern Operationen innerhalb eines Proof-of-Work-Systems entweder eine monetäre Zahlung oder eine Rechenleistung: Wenn Sie eine Mailingliste mit Spam überfluten möchten, müssen Sie Ihren Computerprozessor verwenden, um die richtige Menge an Hashing-Zyklen auszuführen.

Bei Bitcoin dient Proof of Work auch als Schutz vor Zensur: Wenn alle Transaktionen Gebühren zahlen und ein Miner erforderlich ist, sie in einen Block aufzunehmen, wird es immer jemanden geben, der bereit ist, die Gebühr anzunehmen, um die Stromkosten zu decken. Auf globaler Ebene umgeht dieser Mechanismus politische Zensur. Wenn bestimmte Benutzer in einer bestimmten Anzahl von Ländern sanktioniert werden, ist es unmöglich für das gesamte Netzwerk, bei der Zensur zusammenzuarbeiten, da ein Miner aus einer freien Rechtsordnung keine moralischen oder rechtlichen Bedenken haben wird, die Gebühr anzunehmen und somit diese Transaktion in einen Block aufzunehmen.

Ein weiterer Vorteil des Proof-of-Work-Minings von Bitcoin ist seine sogenannte "Permissionless"-Natur.

Jeder kann einen Computer kaufen, der auf das Mining spezialisiert ist. Natürlich profitiert nicht jeder auf der Welt von wettbewerbsfähigen Stromkosten und einer freundlichen Rechtsprechung. Aber es ist keine Registrierung erforderlich und es ist nicht notwendig, dass die Miner ihre Identität der Welt offenlegen - alles, was sie brauchen, ist Glück oder viel Rechenleistung, um den seltenen Hash vor dem Rest der Welt zu entdecken.

Die oben genannten Beschreibungen sollten die Vorstellungskraft eines jeden Verteidigers der Menschenrechte beflügeln und klar machen, warum Regierungen und große Unternehmen Bitcoin ablehnen und oft dafür kritisieren, dass es verschwenderisch ist. Auch Menschen in autoritären Regimen brauchen eine Möglichkeit, sich zu schützen.

Klingt kompliziert? Das liegt daran, dass das dezentrale Design ständige Überprüfung verwendet. In diesem Geldsystem überprüfen alle Teilnehmer die Ehrlichkeit der anderen und verlassen sich auf Mathematik und Computercode, um festzulegen, was fair ist und was ungültig ist. Das Bitcoin-Mining dient der Sicherung eines dezentralen Netzwerks, das keine zentrale Einheit hat, die die Regeln festlegt. Bitcoin ist der erfolgreichste Versuch, das Double-Spending-Problem zu lösen - es stellt sicher, dass, wenn es keinen Server gibt, der als Orakel für alle anderen fungiert, dieselbe Geldmenge nicht







zweimal vom selben Teilnehmer ausgegeben wird. Es ist wie, wenn man in den Laden geht und versucht, eine 2-Dollar-Schokoladentafel zu bezahlen, indem man dieselbe 1-Dollar-Banknoten zweimal anbietet, bevor der Kassierer den Schein in die Kasse legen kann. Das kann nicht funktionieren, solange es Überprüfer gibt, die sehen, dass man versucht, das System zu betrügen.

Jeder ist an die gleichen Konsensregeln gebunden, daher sind Betrugsversuche teuer: Wenn ein Miner beispielsweise vorgibt, den richtigen Hash gefunden zu haben und die regeldurchsetzenden Knoten des Netzwerks anderer Meinung sind, wird die Arbeit des Miners nicht Teil des öffentlichen Hauptbuchs. Diese Ablehnung geht mit finanziellen Kosten einher, da der Miner, der versuchte zu betrügen, energieintensive Berechnungen durchgeführt hat und entweder mit dem Rest in Einklang gebracht werden muss oder versuchen muss, eine Mehrheit von 51 % der anderen Miner davon zu überzeugen, beim Betrug mitzumachen.

In der Geschichte von Bitcoin war es immer profitabler, nach den Konsensregeln zu spielen, als zu versuchen, das Netzwerk anzugreifen. Ehrliche Miner erhalten Belohnungen, die ihre Stromkosten und andere Ausgaben decken. Unehrliche Miner konnten keine gefährliche Mehrheit bilden, aufgrund der geografischen Verteilung des Bitcoin-Netzwerks und der Beteiligung einer großen Anzahl von Benutzern, die an dieses parallele Geldprojekt glauben und seinen Erfolg sehen wollen. Ein Teil des Verdienstes gehört der Art und Weise, wie die Anreize entworfen wurden, um Ehrlichkeit zu fördern, aber wir sollten niemals menschliches Handeln ignorieren. Es ist die Qualität der Bitcoin-Benutzer, die Bitcoin bis zu diesem Punkt gebracht hat.

Banken haben dieses Problem nicht, da sie von menschlicher Politik geregelt werden. Ihre Abwicklungen sind auch viel langsamer als Bitcoin-Blöcke, sie funktionieren nur von Montag bis Freitag innerhalb eines Zeitrahmens von 8 Stunden, und alle Transaktionen dazwischen werden in einer proprietären Version des "Memory Pool" gespeichert, der während der Bürozeiten gelöscht wird. Im Gegensatz zu Bitcoin können Banken Transaktionen rückgängig machen und Gelder leicht einfrieren. Es ist diese Zensurdimension, die sogar in den demokratischsten Ländern mit liberalen Verfassungen auf extreme Weise genutzt wird, die theoretisch die Meinungsfreiheit umfassen. Einigen Einzelpersonen wurden ihre Konten aufgrund politischer Äußerungen eingefroren, während eine Gruppe kanadischer LKW-Fahrer sich zwischen Finanzzugang und Fortsetzung eines Protests entscheiden musste.

Eine gerechtere Welt benötigt Bitcoin als finanzielles Instrument, das den Menschen ermöglicht,

sich von Korruption und Missbrauch abzuwenden. Solange Bitcoin in dezentraler Form über Proof of Work existiert, ist es möglich, dass Einzelpersonen Kapital investieren, um Bitcoin zuschürfen und somit Teile davon zu erhalten, ohne staatlich regulierte Verfahren durchlaufen zu müssen. Mit den Coins, die sie durch das Mining oder den privaten Peer-to-Peer-Handel erhalten, können Menschen aus aller Welt mit ihren Füßen abstimmen: Sie verlassen jedes Gebiet und jede Gerichtsbarkeit, die ihre Würde verletzt, ihre Freiheiten missbraucht und ihre grundlegenden Rechte verletzt, um sich an einem freundlicheren Ort niederzulassen. Es gibt viele solcher Beispiele unter den Venezolanern, und von den Gästen des Bitcoin Takeover-Podcasts kann man beispielsweise Alessandro Cecere über die Flucht vor Tyrannei durch Bitcoin hören (Staffel 5, Episode 5).

Darüber hinaus können Menschen Bitcoin nutzen, um parallele Schwarzmärkte zu schaffen, die missbräuchliche Vorschriften effektiv umgehen. Landwirte können nicht einfach aufhören, Rinder zu züchten und stattdessen dazu gedrängt werden, Insekten zu züchten. Es ist nicht so, als ob die Nachfrage nach Milch, Milchprodukten und Rindfleisch verschwinden würde, nur weil eine Gruppe von Politikern beschlossen hat, die Produktion zu reduzieren. Die Menschen werden in der Lage sein, Lebensmittel, die sie mögen, direkt von den Landwirten in einem Peer-to-Peer-Verfahren zu kaufen, das die Kontrolle des großen Bruders vollständig umgeht.

Es gibt auch viel zu sagen über Bitcoin in der Ära von bargeldlosen Transaktionen und Zentralbank-Digitalwährungen (CBDCs). Bedenken Sie Folgendes: Zentralbanken werden eine beispiellose Kontrolle über jede Geldtransaktion haben, eine beunruhigende Überwachung gegen jeden einzelnen anwenden und die Währungsversorgung/Inflation per Knopfdruck manipulieren können. CBDCs sind von Natur aus stark zensiert, diskriminierend und anfällig für politischen Missbrauch. Keine Finanzinstitution oder registrierter Zahlungsdienst kann unzensierbare und weitgehend private Geldüberweisungen wie Bitcoin bieten.

Bitcoin bietet eine Fluchtmöglichkeit vor einer düsteren autoritären Zukunft,

in der technologische Innovationen dazu genutzt werden, die Massen effizienter zu überwachen und zu kontrollieren als es der Kommunismus und der Faschismus im 20. Jahrhundert getan haben. Es ist daher verständlich, dass Regierungsvertreter ihr Bestes tun, um die Nutzung von Bitcoin zu entmutigen. Sie versuchen bereits, alle Eingangs- und Ausgangspunkte unter Kontrolle zu halten und gleichzeitig jede Transaktion zu überwachen, um herauszufinden, wohin das Geld fließt. Aber Bitcoin ist der Albtraum eines jeden Autoritären: ein globales Com-



puternetzwerk, das nach Konsensregeln funktioniert, die kein Parlament, kein Präsident, kein König oder keine Allianz mächtiger Politiker ändern kann. Die Menschen können nicht daran gehindert werden, BTC weltweit zu senden und zu empfangen, so dass politische Zensur plötzlich weniger effektiv wird.

Gleichzeitig halten korrupte Politiker wahrscheinlich auch einen Teil ihres Reichtums in Bitcoin - daher wird es wahrscheinlich nicht auf eine Weise verboten, die technisch umgangen werden kann. Sie können die Bitcoin-bezogenen Websites blockieren, die Eingangs- und Ausgangspunkte beschränken und entmutigen, aber sie werden Tor, VPNs und andere IP-Verschleierungsdienste nicht verbieten können, die diese Beschränkungen umgehen. Regierungen werden das Internet auch niemals abschalten, weil es ihnen zu viele wertvolle Daten liefert und für Propaganda nützlich ist. Sie können das Netzwerk nutzen, um die Bürger zu überwachen und auch ihre Gedanken durch Nachrichten und Unterhaltung zu kontrollieren.

Basierend auf den vorgebrachten Argumenten können wir zustimmen, dass Bitcoin sicherlich für viele Menschen in allen Lebensbereichen nützlich ist. Daher ist die elektrische Energie, die das System sichert, offensicht-lich nicht verschwendet. Darüber hinaus ist die Tatsache, dass ein realer Ressourcenverbrauch erforderlich ist, um BTC zu produzieren, auch ein Grund, warum es eine so hohe globale Nachfrage nach dem magischen Internetgeld gibt. Der Preis von Gold berücksichtigt Abbau-, Transport- und Sicherheitskosten. Der Preis von Lebensmitteln beinhaltet Produktions-, Transport- und Lagerungskosten. Bitcoin ist wertvoll, weil Einzelpersonen und Unternehmen Elektrizität nutzen, um ihre Ersparnisse zu sichern und Mining-Belohnungen zu erhalten.

Im Gegensatz zu Fiatgeld, das aus dem Nichts geschaffen wird

und auf Vertrauen in Regierungen und Zentralbanken beruht (begleitet von einem gewissen Grad an militärischer Durchsetzungskraft), ist Bitcoin ehrliches Geld, das jeder zu einem Preis erwirbt, der die Produktionskosten für Hardware und Strom, Angebot und Nachfrage berücksichtigt. Anders als staatliches Geld weiß man immer, wie viele Bitcoin sich im Umlauf befinden. Wenn man den Preis bestimmt, sind die einzigen wirklich relevanten Variablen die Produktionskosten und die Nachfrage. Zum Zeitpunkt, als ich diesen Artikel schreibe, beträgt der Preis von 1 Bitcoin etwa 30.000 US-Dollar. Aber wenn Fiatgeld ersetzt wird, könnte ein Bitcoin in Stunden an Arbeit, knappen natürlichen Ressourcen, Stücken Land, Goldmünzen und anderen von Menschen geschaffenen Produkten bewertet werden. Zeit, Energie und Ressourcen sind begrenzt - warum sollte das Geld, das sie erwirbt, nicht den Gesetzen der Physik und nicht der menschlichen Politik unterliegen?

Die Verwendung des Energieverbrauchs als Referenzpunkt für die Bewertung ist ein Merkmal, das Bitcoin zugutekommt. Es sichert das Netzwerk und verleiht der Währung mehr Legitimität. Das häufig vorgebrachte Gegenargument lautet, dass Bitcoin ein Computercode ist, den jeder klonen kann, um ein identisches Netzwerk bereitzustellen. Die Märkte werden jedoch im Laufe der Zeit dem neuen Netzwerk nicht den gleichen Wert beimessen, und daher konvergiert der Energieverbrauch auf das stabilste und ständig nachgefragte Geldnetzwerk.

Solche Angriffe auf die Vorherrschaft von Bitcoin haben bereits 2017 und 2018 mit verschiedenen Forks stattgefunden, wie Bitcoin Cash, Bitcoin Gold und Bitcoin Satoshi's Vision, die alle klar gescheitert sind. Obwohl sie heute noch existieren, haben sie den Markt nicht davon überzeugen können, dass sie die wahren und wertvollsten Versionen von Bitcoin sind. Infolgedessen haben sie kontinuierlich Marktanteile gegenüber dem originalen Bitcoin verloren, bis BCH heute nur noch 0,39% der Mining-Hash-Rate des echten Bitcoins hat.

Nicht alle Kryptowährungs-Mining-Aktivitäten sind gleich. Die Märkte erkennen, was Wert hat, und auf lange Sicht wird deutlich, was wirklich wertvoll ist und was sich als Misserfolg oder Betrug erweist. Im Jahr 2023 ist Bitcoin seit 14 Jahren der unbestrittene König. Klone kamen und gingen, aber nur eine Form von Internetgeld half Menschen weltweit zuverlässig dabei, täglich Transaktionen durchzuführen und Ersparnisse anzulegen. Es gibt also offensichtlich einen hohen Wert in diesem Netzwerk, und es verdient es, diese Elektrizität zu nutzen, um Menschen auf der ganzen Welt mehr Freiheit gegenüber übermäßiger Tyrannei zu verschaffen.



An diesem Punkt könnte man argumentieren, dass ein Wechsel von Proof of Work (dem Mechanismus, der die Gesetze der Thermodynamik nutzt, um Elektrizität in digitales Geld umzuwandeln) zu Proof of Stake (Ethereums Ansatz zur Sicherheit, bei dem neu geprägte Coins an Benutzer vergeben werden, die ihre ETH-Token in einem Vertrag sperren und einen Validierungscomputer online halten) den Energieverbrauch von Bitcoin um bis zu 99% reduzieren könnte. Dieser Punkt ist nur in Bezug auf den Energieverbrauch gültig, vernachlässigt jedoch völlig die Bedeutung der Dezentralisierung und der Idee von gerechtem Geld.

In Bitcoin kann jeder externe Ressourcen (Fiatgeld, Gold) investieren, um Mining-Ausrüstung zu kaufen und Stromrechnungen zu bezahlen, um BTC-Token zu erwerben, ohne dabei die bereits auf dem Markt vorhandenen Coins zu berühren. Man kann das Netzwerk sichern und Belohnungen verdienen, ohne den Preis mit einem potenziellen Marktkauf zu beeinflussen.

In einem Proof-of-Stake-System bleibt einem nichts anderes übrig, als seine Coins von Menschen zu kaufen, die sie aus dem Nichts geschaffen haben, ohne jeglichen Energieaufwand. Darüber hinaus funktioniert Proof of Stake wie eine Oligarchie: Die neu geschaffenen Währungseinheiten werden an diejenigen verteilt, die die größten Beträge eingesetzt haben. Die Reichen werden immer reicher, während die Armen dazu verdammt sind, arm zu bleiben. Offensichtlich fehlt es an Dynamik: Frühzeitige Anwender können es sich leisten, immer zu setzen und nur die Belohnungen auszugeben, die sie erhal-ten. Das System war von Anfang an unfair, aber die Art und Weise, wie die Ärmsten die Coins von den Eliten kaufen müssen, um effektiv den Status ihrer Herren zu bewahren, ist abscheulich und inakzeptabel für den Fortschritt der Menschheit.

Zumindest ist Proof of Work dynamisch, wie durch signifikante Verschiebungen in der Dominanz der Mining-Pools gezeigt wurde:

- im Jahr **2011** wurde Deepbit der erste Mining-Pool, der mehr als 50% der Hash-Rate erreichte, und diese Tatsache löste Panik unter den Nutzern des BitcoinTalk-Forums aus;
- im Jahr **2013** war Deepbit bereits Geschichte. Aber BTC Guild war der neue Akteur auf der Bildfläche, und Nutzer äußerten Bedenken hinsichtlich seiner Dominanz. Im Januar 2015 wurde der Pool aufgrund regulatorischen Drucks geschlossen;
- im Jahr **2014** beschwerte sich Vitalik Buterin, Mitbegründer des Bitcoin Magazine, in einem Artikel über GHash.io, einen Pool, der fast 50% der Bitcoin-Hash-Rate erreichte. Innerhalb von weniger als zwei Jahren gab GHash das Mining-Geschäft auf;
- im Jahr **2017** waren Bitcoin-Nutzer besorgt über Bitmains unfairen Vorteil als Hersteller, der auch den Antpool betreibt. Stand April 2023 macht der Antpool nur noch 23% der Bitcoin-Hash-Rate aus;
- im Jahr **2023** sieht die Community kritisch auf Foundry USA, einen Pool, der nach einem großen Teil der Operationen außerhalb Chinas immer größer wird. Dieser vergleichsweise neue Pool stellt derzeit etwa 33% der Bitcoin-Hash-Rate bereit. Allerdings ist Foundry zwei Faktoren ausgesetzt: den übermäßigen regulatorischen Bedenken in den Vereinigten Staaten von Amerika sowie den Dynamiken eines wettbewerbsorientierten und globalen freien Marktes, der nach der am häufigsten verfügbaren und erschwinglichen Form von Energie sucht. Ein Rückgang ist niemals ausgeschlossen, und es gibt immer einen konkurrierenden Service, der die Aufgabe übernehmen kann, Bitcoin thermodynamische Sicherheit zu bieten;

Auf der anderen Seite ist es immer noch nicht klar, ob Proof of Stake ohne Bedenken hinsichtlich der Zentralisierung funktionieren kann. Als Ethereum zu diesem Konsensprotokoll wechselte, erließ man eine Regel, die es den Stakern (Benutzern, die das Netzwerk durch Sperren ihrer Münzen sichern) nicht erlaubt, ihr Geld aus dem Vertrag abzuziehen. Es handelt sich um eine vorübergehende Entscheidung, um größere Sicherheitsprobleme zu vermeiden... oder so behaupten sie.

Ihr System, auch wenn es sehr wenig elektrische Energie verbraucht, ist unfair und viel schlimmer als das Bankensystem, das wir bereits haben. Proof of Stake kann neben einem freien globalen Geldnetzwerk, das jedem gleiche Chancen bietet, nicht funktionieren und wird es auch nicht. Deshalb beharren die Feinde von Bitcoin darauf, dass der Wechsel von Proof of Work stattfinden sollte. Sie wollen nicht, dass der Preis von Bitcoin einen realen Äquivalentwert in Energie hat, sie wollen nicht, dass das System jedem gleiche Chancen bietet, sich zu messen, und sie wollen nicht, dass die Dezentralisierung Bestand hat. Sie bevorzugen etwas, das sie kontrollieren können.

Die nächste Stufe der Kritik, die sie vorbringen würden (offiziell oder über ChatGPT), wäre, dass Bitcoin kein Geld ist, da nur Regierungen in solchen Angelegenheiten Entscheidungen treffen. Und wieder gibt es zwei unterschiedliche Aspekte, um diese FUD zu widerlegen:

- der einfachste Weg besteht darin, auf El Salvador zu verweisen, ein Land, das Bitcoin als offizielle Währung anerkennt;
- Der nuanciertere Weg besteht darin zu erklären, dass die Märkte entscheiden, was Geld ist, nicht Regierungen. Die Märkte sind dynamisch und innovativ, während Regierungen reaktiv und konservativ sind. Es waren die Märkte, die Gold und Silber auswählten, um sie über nationale Grenzen hinweg zu handeln, aber es waren die Regierungen, die sich unter dem Vorwand der Vereinfachung der Coin-Prüfung in die Mitte stellten. Es waren auch die Märkte, die Kredit und Eigentumszertifikate verwendeten, bevor Regierungen diese Art von Buchführung übernahmen und zentralisierten.

In der Vergangenheit konnten Regierungen bestimmte Arten von Währungen verbieten und konfiszieren,

die sie für gefährlich für die Elite hielten. Heute können dieselben Regierungen Bitcoin nicht daran hindern, auf Märkten für den Kauf von Waren und Dienstleistungen verwendet zu werden. Die einzige Eigenschaft traditionellen Geldes, die Bitcoin wirklich fehlt, ist die Fähigkeit, von der Regierung konfisziert zu werden. Wenn wir also Geld durch diese Brille definieren, können wir zustimmen, dass Bitcoin definitiv etwas anderes ist.

Nun wollen wir eine differenzierte Diskussion über den Energieverbrauch von Bitcoin führen. Wir haben bereits erklärt, dass das Proof-of-Work-System einen Wert hat und auf dynamische Weise etwas Nützliches für die Menschheit produziert. Betrachten wir den Energieverbrauch daher aus einer vergleichenden Perspektive. Schließlich gibt es viele "verschwenderische" Verwendungen von Elektrizität, die von Regierungen nicht kritisiert werden, aber viele Kilowatt verbrauchen - von Weihnachtslichtern über Wäschetrockner bis hin zu im Leerlauf laufenden Fernsehbildschirmen, die niemand anschaut.

Menschen, die ihre Kleidung mit dedizierten Maschinen trocknen, ihre Häuser mit Raumheizungen (elektrische Warmluft) erwärmen und mit eingeschalteten Computern oder Fernsehern schlafen, werden nicht als ökologische Terroristen betrachtet. Regierungen, die viel Strom für militärische Operationen und verschiedene Experimente verbrauchen, werden nie zur Rechenschaft gezogen. Große Technologieunternehmen, die Serverfarmen betreiben, erhalten Narrenfreiheit, da sie genug Geld haben, um Regierungen zu beeinflussen und Regulierungsbehörden und Umweltaktivisten wegzuschauen lassen. Aber Bitcoin-Miner werden übermäßig strengen Standards unterworfen und werden dafür kritisiert, ein Geldnetzwerk abzusichern, das von Regierungen nicht kontrolliert werden kann.

Alarmisten bezeichnen Bitcoin-Mining als eine verschwenderische,

die Umwelt schädigende, übermäßige Kohlenstoffemissionen verursachende und ozeanerhitzende Aktivität. Auf der anderen Seite beschreiben Befürworter und Interessenvertreter des Minings es als eine zunehmend umweltfreundliche Tätigkeit, die sich zu den günstigsten Formen der Stromerzeugung entwickelt - und diese sind oft erneuerbar. Die Wahrheit liegt jedoch immer irgendwo in der Mitte: Tatsächlich kann jeder Mining-Equipment kaufen und es zu Hause betreiben, als Teil einer Mining-Farm in einer dedizierten Einrichtung oder an einem anderen Ort, an dem Strom günstig ist.

Es gibt auch etwas über freie Märkte im Energiesektor zu sagen und wie sich die Preise im Laufe der Zeit an die Angebot-Nachfrage-Dynamik anpassen werden. Zum Beispiel ist die durch die Verbrennung von Kohle erzeugte Elektrizität im Vergleich zu Kernenergie, Solarenergie, Windenergie oder Wasserkraft teuer, stark verschmutzend und unerwünscht. Wenn jedoch die Nachfrage nach Kohle so stark sinkt, dass die Ressource sehr günstig zu kaufen und zu verbrennen wird, ist es wahrscheinlich, dass sie von wettbewerbsfähigen Akteuren genutzt wird. Nicht nur im Bergbau, sondern in allen Energiesektoren. Schließlich hat sogar die deutsche Regierung die Stromerzeugung durch Kohleverbrennung im Jahr 2022 erhöht, um mit der Energiekrise umzugehen... was für ein Land, das von einer linksgerichteten Koalition regiert wird, zu der auch die Grüne Partei gehört, eher ungewöhnlich ist.

Im Bitcoin-Netzwerk erhalten die Miner nach jeder Entdeckung von 210.000 Blöcken 50% weniger Coins pro Block als Belohnung. Dieser Zyklus, der als "Halbierung" bezeichnet wird, dauert etwa 4 Jahre und trägt maßgeblich zur Professionalisierung des gesamten Mining-Sektors bei. Die ineffizienten Teilnehmer, die hohe Preise für Energie zahlen und nicht genügend Rechenleistung erbringen, um wettbewerbsfähig zu bleiben, werden verdrängt.

Gleichzeitig kann die Hash-Rate des Minings im Laufe der Zeit nicht konstant bleiben und wird nicht nur wachsen. Wenn die Miner ihren Strom aus Kraftwerken beziehen, wo er im Überfluss produziert wird, bleiben nicht viele Orte übrig. Sie können geothermische Energie nutzen, das sonst verschmutzende Gasflaring in Elektrizität umwandeln und dadurch CO2 statt des stark verschmutzenden Methans in die Atmosphäre freisetzen, und sie können sogar die durch vergorenen Kuhmist erzeugten Kilowattstunden nutzen. Was passiert also, wenn die Hash-Rate des Minings nicht mehr steigen kann und unerwartet aufgrund von Zuverlässigkeitsproblemen in einigen Teilen der Welt abnimmt?

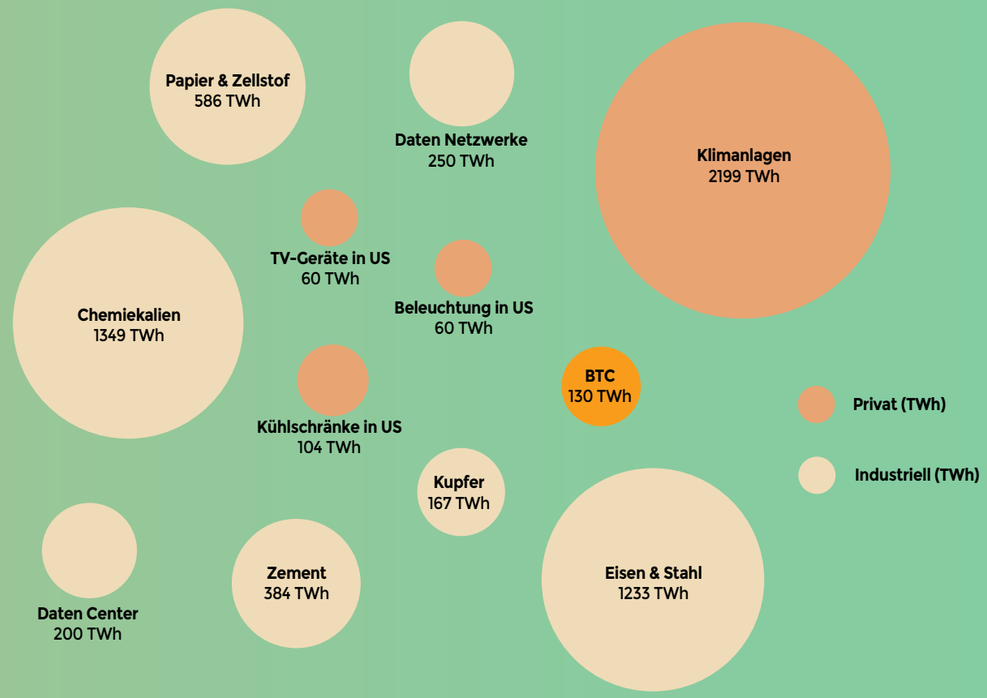
Letztendlich ist das Bitcoin Proof-of-Work Mining darauf ausgelegt, Dynamik zu gewährleisten und es jedem auf der Welt zu ermöglichen, jederzeit beizutreten oder auszusteigen. Wie werden Abnahmen der Hash-Rate umgesetzt? Nun, alle 2016 Blöcke (ungefähr 2 Wochen) passt sich die Mining-Schwierigkeit an, um die Blockzeit von 10 Minuten aufrechtzuerhalten. Die Schwierigkeit erhöht sich also nach Zeiten hoher Aktivität (wenn mehr Miner Blöcke viel schneller finden) und verringert sich nach Zeiten geringer Aktivität (wenn die Miner Schwierigkeiten haben, Blöcke zu finden).

Dies bedeutet auch, dass, wenn zu einem bestimmten Zeitpunkt mehr Energie für Bitcoin eingesetzt wird, die









Mining-Belohnungen gleich bleiben und die erhöhte Anzahl an Teilnehmern diese teilen muss. Dies ist ein weiteres brillantes Design - wenn mehr Ressourcen für die Suche nach Goldminen oder Ölquellen eingesetzt werden, wird die Menge der auf dem Markt verfügbaren Ressourcen größer und die Preise werden niedriger. Aber Bitcoin hat ein programmiertes Inflationssystem, das in der ersten Epoche von 210.000 Blöcken 50 Münzen pro Block freisetzt, in der zweiten Epoche von 210.000 Blöcken 25 Münzen pro Block und so weiter, bis die Belohnungen aufgebraucht sind und die Miner nur noch von den Transaktionsgebühren zwischen den Teilnehmern bezahlt werden.

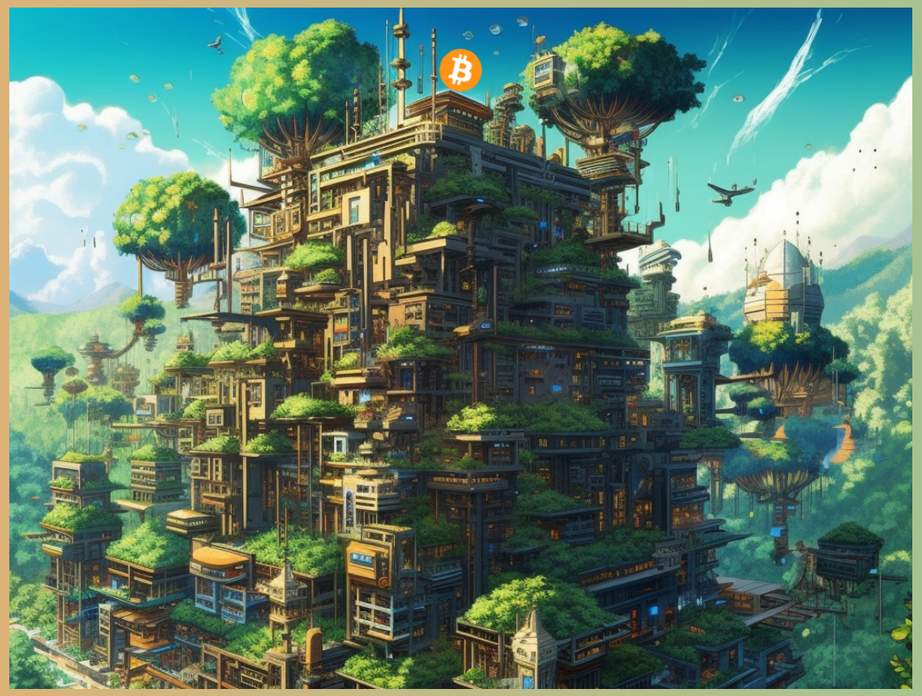
Nur die effizientesten Miner, die aus den abnehmenden Belohnungen Gewinn erzielen können, werden überleben. Und wenn die niedrigsten Stromkosten erreicht sind und die Mining-Hardware an ihre Grenzen stößt, gibt es immer noch den Fall des ideologischen Minings - Menschen auf der ganzen Welt, denen die Belohnungen nicht so wichtig sind, sondern die nur das Bitcoin-Netzwerk gegen Angriffe absichern wollen.

Die Kritik an Bitcoins Energieverbrauch ist so einfach, weil es genauso einfach ist, ihn herauszufinden - die Hash-Rate des Minings ist eine öffentliche Metrik, die Effizienz der beliebtesten Mining-Hardware ist bekannt, so dass jeder eine ziemlich genaue Abschätzung des Energieverbrauchs machen kann. Im Vergleich dazu veröffentlicht keine andere private Finanzinstitution solche Daten. Banken werden nicht enthüllen, wie viel Strom ihre Büros und Server verbrauchen. Es gibt keine Berichte von PayPal und Venmo, aus denen hervorgeht, wie viel sie für Strom ausgegeben haben, um ihren Betrieb (einschließlich Büros, Support-Schreibtischen, Servern und allem, was ihr Geschäft antreibt) zu betreiben. Und selbst bei Regierungen ist nicht alles transparent - das Militär und die Geheimdienste geben nur ihr Gesamtbudget an, geben jedoch nicht öffentlich an, wie sie es ausgeben oder warum sie eine bestimmte Menge an Strom für etwas benötigten, das keine Ergebnisse bringt.

Deshalb müssen wir den Energieverbrauch von Bitcoin mit dem anderer Branchen vergleichen. Laut Statista erreichte Bitcoin zwischen Februar 2017 und November 2022 einen Höchstwert von 204,6 TWh pro Jahr (im ersten Quartal 2022 erreicht). Im Jahr 2021 verbrauchte die gesamte Welt 176.431 TWh. Selbst auf dem Höhepunkt betrug der Anteil von Bitcoin am weltweiten Energieverbrauch nur 0,11%. Dies ist 100-mal weniger Strom als das, was das World Economic Forum in ihrem lächerlich schlechten Artikel von Dezember 2017 mit dem Titel "Im Jahr 2020 wird Bitcoin mehr Strom verbrauchen als die Welt heute" für das Jahr 2020 schätzte. Die Eliten in Davos müssen dieses Geldsystem wirklich hassen, welches sie nicht kontrollieren können.

Ich hoffe, der Autor des WEF, Adam Jezard, liest dies, denn das Wachstum des Minings wird nicht gleichmäßig und exponentiell sein. In seinem Modell verwendete er eine monatliche Hash-Rate-Zunahme von 25% als Konstante. Aber so funktioniert es nicht: Wenn Sie 25% mehr Leistung einsetzen, erhalten Sie nicht 25% mehr Belohnungen. Der Schwierigkeitsanpassungsalgorithmus macht die gleiche Blockbelohnung schwieriger zu erhalten. Das bedeutet, dass viele Miner weltweit unrentabel werden und ihre





Operationen einstellen werden. Langfristig werden nur diejenigen profitabel bleiben und weitermachen, die günstigsten Strom zur verfügung haben. Ineffizienz wird ständig aus dem Markt verdrängt, und es gibt Anreize für die Schaffung von Hardware-Innovationen, die Maschinen mehr Hashes pro Watt generieren lassen.

Außerdem ist 0,11% des weltweiten Energieverbrauchs wirklich unbedeutend, wenn wir möchten, dass Individuen die Möglichkeit haben, frei von Tyrannei zu sein. 204,6 TWh pro Jahr entsprechen einem Zehntel der Energieproduktion Rumäniens aus dem Jahr 2022, 19 TWh weniger als die jährliche Energieproduktion Kenias aus dem Jahr 2021 und 1,65% der gemeldeten Stromerzeugung der Vereinigten Staaten von Amerika aus dem Jahr 2021.

Im Dezember 2020 machte sich der Forbes-Mitarbeiter James Conca die Mühe, einige Berechnungen anzustellen und kam zu dem Schluss, dass Weihnachtslichter in den USA während des Monats Dezember 3,5 TWh verbrauchen. Nehmen wir an, dass der Rest der Welt durch Feiertage wie Weihnachten, Hanukkah und das neue Jahr die Menge der in den USA verbrauchten Elektrizität verdoppelt. Das wären 7 TWh weltweit im Monat Dezember. Im Vergleich dazu verbrauchte Bitcoin im selben Zeitraum geschätzt 6,48 TWh (eine Zahl, die den geschätzten BitcoinTWh pro Jahr im Dezember 2020 darstellt, geteilt durch 12).

Laut dem Cambridge Bitcoin Electricity Consumption Index betrug der jährliche Verbrauch von Bitcoin Ende April 2023 geschätzte 129,94 TWh - deutlich niedriger als der Höchststand, der von Statista angegeben wurde. Wenn wir uns andere Branchen ansehen, stellen wir fest, dass Gold jedes Jahr 131 TWh verbraucht, während Fernseher in den USA jährlich 60 TWh verbrauchen. Am auffälligsten ist, dass Kühlschränke in den USA jährlich 104 TWh verbrauchen... aber niemand startet eine Kampagne, um die Menschen davon abzuhalten, Kühlschränke zu kaufen und stattdessen nur noch frische Lebensmittel zu essen.

Rechenzentren, die weltweit Internetdienste für Menschen bereitstellen, erhalten keine Drohung, zusätzlich 30% für den von ihnen verbrauchten Strom zahlen zu müssen (wie es US-Miner taten). Beide bieten etwas an, das objektiv nützlich für die Menschheit ist, aber nur eines davon ist zu 100% kontrollierbar durch den Staat... und es ist das andere, das regelmäßig mit Regulierungen bedroht wird, die das Geschäft erschweren. Es gibt viele Doppelstandards bei der Beurteilung des Bitcoin-Minings und das ist nicht fair. ChatGPT trägt zu dieser FUD (Fear, Uncertainty, Doubt) bei, obwohl wir verstehen müssen, dass Bitcoin nützlich ist und einen Wert für die menschliche Zivilisation bietet.



Friss diese Niederlage, du elite-schützende KI!

SCORE

Vlad C.	7
ChatGPT	0

SLUSH POOL

IS NOW

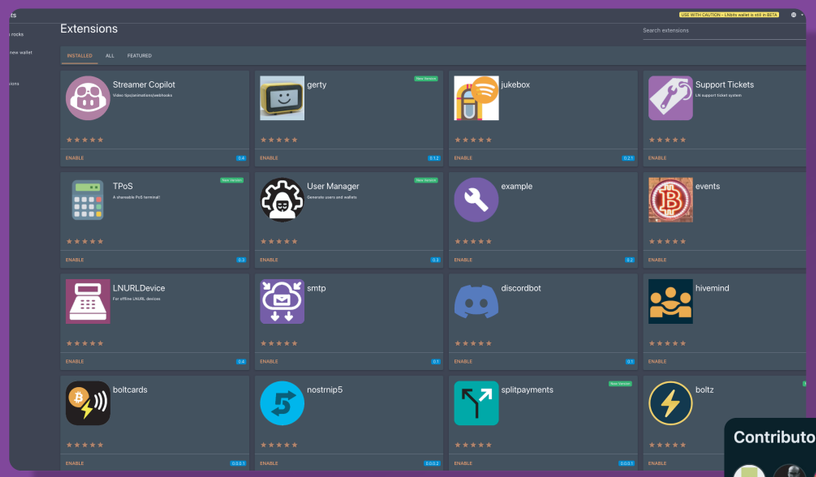
BRAIINS POOL

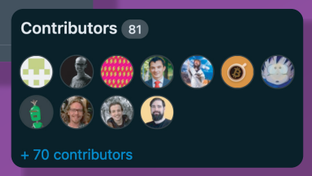
MINING BITCOIN
SINCE 2010

LEARN MORE AT BRAIINS.COM/POOL

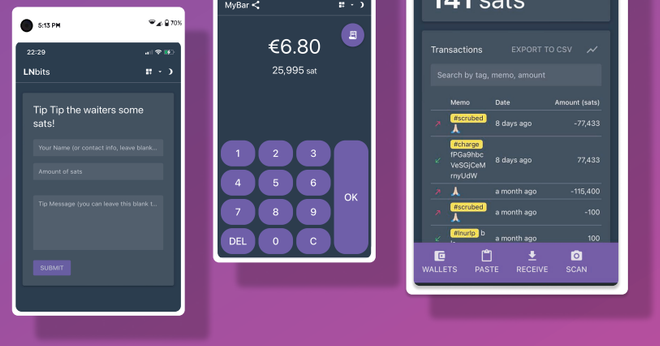
LNbits

Free and open-source bitcoin accounts and extension system.
Run for yourself, friends & family, or for the whole world!





An insta-wallet system
Your own branded lightning wallet
Custodial community banking solution
Accounts system, each wallet with own API keys
Extendable platform using our extension framework
Develop for an API, use any funding source!
Part of a development stack for a bitcoin service
Build and connect your hardware tools
Awesome community!



Coinflip

Join us!
https://github.com/lnbits/lnbits





Breaking ChatGPT's Bitcoin FUD #8

Mining Zentralisierung

51% ATTACKE MINING BITMAIN CHINA / USA POW

Laut ChatGPT, kontrolliert eine kleine Anzahl von Mining-Pools einen großen Teil der Mining-Leistung im Bitcoin-Netzwerk. Ein solches Szenario könnte zu einer Zentralisierung von Macht und Entscheidungsfindung führen. Zunächst einmal ist es schön zu sehen, dass das KI-Modell etwas Nuancen einführt, indem es darauf hinweist, dass der beschriebene Angriff hypothetisch ist. "Könnte" ist etwas weniger drastisch als "kann kollaborativ zentralisieren" oder andere Formulierungen, die den Schwerpunkt auf die Folgen dieser Bedrohung legen.

Zweitens ist es interessant, dass ChatGPT den 51%-Angriff nicht erwähnt, bei dem die jüngsten Transaktionen umorganisiert und theoretisch die Geschichte über mehrere Blöcke hinweg neu geschrieben werden können. Möglicherweise haben die Programmierer nicht genügend Zeit damit verbracht, es darauf zu trainieren, Bitcoin zu FUD (Fear, Uncertainty, Doubt) zu machen (und den Orwellian Worldcoin zu bewerben, den Open AI als Alternative unterstützt), oder vielleicht wurde die Vagheit absichtlich belassen. Unabhängig von der Semantik wollen wir diese FUD widerlegen.

Um die FUD über die Zentralisierung des Minings in Bitcoin herauszufordern, muss man sich historische, technische und spieltheoretische Beispiele ansehen. Denn die Bedenken gehen auf das Jahr 2011 zurück und wurden nie wirklich bestätigt - ein Blockchain-Reorg-Angriff erfordert viel Koordination, und selbst wenn der Angriff stattfindet, ist er finanziell teuer und sozial schwer aufrechtzuerhalten.

Wie im vorherigen Artikel beschrieben, der einige unehrliche Bedenken hinsichtlich Proof of Work Mining und Energieverbrauch widerlegt hat, gab es in der Geschichte von Bitcoin Momente, in denen Benutzer Angst hatten, einen 51%-Angriff zu erleben. Was ist ein 51%-Angriff? Es handelt sich um eine Situation, in der eine Mining-Entität die einfache Mehrheit der Hash-Rate erreicht und sich entscheidet, jüngste Blöcke umzustrukturieren und Geld aus Transaktionen zu stehlen. Es geht nicht um eine Mehrheit der Teilnehmer, sondern um eine Mehrheit der Rechenleistung (oder Hashes).

Der Grund, warum ein erfolgreicher 51%-Angriff auf Bitcoin nie stattgefunden hat, liegt darin, dass Mining-Pools keine einzelnen Entitäten sind, die im Namen aller Teilnehmer handeln können. Außerdem haben die Miner bisher immer herausgefunden, dass es profitabler ist, sich an die Regeln zu halten und die Block-Belohnungen zu sammeln.

Hier sind die Momente in der Geschichte, in denen ein Mining-Pool eine gefährlich hohe Hash-Rate erreicht hat - eine, die theoretisch Angriffe gegen Bitcoin ermöglichen könnte:

- im Juli 2011 überstieg Deepbit die 50%-Marke: Ein Ereignis, das den Benutzer bcearl im Bitcoin Talk Forum dazu veranlasste, darüber zu schreiben und anderen zu sagen: "Keine Panik, aber beobachtet genau!". Innerhalb von weniger als 2 Jahren war Deepbit bereits unbedeutend geworden, und Bitcoin-Nutzer wechselten zu neuen und effizienteren Pools;
- im September 2013 wies der Bitcoin Talk Forum Benutzer mechs darauf hin, dass BTC Guild ein "51%-Angriffsrisiko" darstellen könnte. Lustigerweise war die erste Antwort von Nancarrow: "Whoa man, déjà vu". Der Bitcoin Core Entwickler Greg Maxwell schaltete sich auch ein, um zu erklären, warum die Bedenken unbegründet sind. Aber die prophetischste Antwort kam von einem Benutzer namens johnyj, der vorschlug, dass GHash.io ein größeres Risiko darstellt, weil der Hardware-Hersteller auch der größte Betreiber ist;
- im Januar 2014 ließ der Aufstieg von GHash.io den Mitbegründer von Bitcoin Magazine, Vitalik Buterin, den Glauben an das Proof of Work Mining verlieren. Zur gleichen Zeit verkündete der Bitcoin Core Entwickler Peter Todd auf Reddit, dass er die Hälfte seiner Bitcoins verkauft hat, um das Risiko zu mindern. Aber im März 2014 koordinierte die Community einen massiven DDoS-Angriff gegen GHash. In der Folge stellte der Pool seinen Cloud-Mining-Service ein und verschwand schnell in der Bedeutungslosigkeit, da er keine neuen Mitglieder mehr aufnahm. Nur GHash's Exchange-Service CEX.io ist heute noch vorhanden;
- im Jahr 2017 kämpften Bitcoin-Nutzer erneut gegen einen großen Mining-Pool namens Bitmain. Wie GHash.io stellte Bitmain Chips her, die der Rest der Branche nutzte. Aber was Bitmain tat, war die Entwicklung und Aktivierung des sogenannten ASIC Boost, einer speziellen Art von Software, die die Leistung ihrer Mining-Geräte steigert. Als sie herausfanden, dass das SegWit-Upgrade von Bitcoin ihren ASIC Boost wirkungslos machen würde, konzentrierte sich das Unternehmen auf die Unterstützung von Bitcoin Cash - der



Gefällt dir der Artikel?

Scanne den QR-Code und hinterlasse ein Kommentar oder eine Donation!



"Big Block"-Version von Bitcoin, die nicht genügend Anklang fand.

Bitmains Unterstützung für BCH führte zu einem Verlust der Dominanz ihrer beiden Mining-Pools: BTC.com und AntPool. Während Bitcoin-Nutzer besorgt waren, dass Bitmain zu groß werden könnte und Bitcoin angreifen könnte, führte schlechtes Management dazu, dass das Unternehmen schrumpfte und letztendlich seine Rolle bei der Bereitstellung von Hash-Rate verringerte. Bitmain ist jedoch immer noch der größte Hersteller von SHA-256 ASICs für das Bitcoin-Mining, und die meisten anderen Pools (sowie individuelle Beitragende) verwenden ihre Hardware.

Diese kurze Geschichte soll uns helfen zu verstehen, dass das Proof of Work Mining dynamisch ist und keine Entität zu groß ist, um zu scheitern. Da das Konzept eines Mining-Pools jedoch so oft diskutiert wurde, ist es wichtig zu erklären, was es ist und wie es funktioniert.

Ein Mining-Pool ist ein freiwilliger Zusammenschluss von Minern, die ihre Chancen maximieren möchten, häufiger Belohnungen zu erhalten. Indem sie ihre Hash-Power zusammenlegen, werden sie zu einem Pool und teilen die Einnahmen entsprechend dem Beitrag jedes Mitglieds. Zum Beispiel kann jemand, der aus Bhutan mit Wasserkraft minen möchte, feststellen, dass es alleine sehr schwierig und unzuverlässig ist, Bitcoin-Blöcke zu finden. Daher suchen sie nach bestehenden Mining-Pools und wählen denjenigen mit den niedrigsten Gebühren aus. Es gibt große Mining-Pools aus China (F2Pool, AntPool, ViaBTC), große Mining-Pools aus den Vereinigten Staaten von Amerika (Foundry, MARA Pool, Luxor) und es gibt auch eine kleinere Option aus Europa (Braiins).

Die Miner aus Buthan können jeden Pool…

wählen und nach Belieben zwischen ihnen wechseln. Natürlich werden sie nach dem besten Gleichgewicht aus Vorhersehbarkeit und hohen Belohnungen suchen. Obwohl der größte Mining-Pool die häufigsten Auszahlungen bietet, haben die kleineren Pools niedrigere Gebühren und bieten zusätzliche Dienstleistungen wie kostenlose Firmware-Updates zur Steigerung der Effizienz Ihrer Hardware und fortschrittliche Rentabilitätsrechner an. Es ergibt keinen Sinn, dass alle zum größten Player gehen - denn die Situation "kleiner Fisch in großem Teich" ist nicht immer der effektivste Weg, Geld zu verdienen, und freie Märkte bieten Anreize zur Unterstützung des Wettbewerbs.

Angenommen, die Miner aus Buthan wählen einen Pool, der heimtückisch ist und Bitcoin angreifen wird, sobald die 51%-Hashrate-Marke erreicht ist. Dann bedeutet dies nicht, dass die Teilnehmer aus Buthan mit der Entscheidung einverstanden sein müssen. Sie können den Pool verlassen, der in böser Absicht handelt, und dazu beitragen, das Gleichgewicht an anderer Stelle wiederherzustellen.

In einigen Fällen können 51%-Angriffe für die Miner profitabel sein. Aber diese zerstörerische kurzfristige Wette schadet letztendlich dem langfristigen Geschäft. Angenommen, jeder Teilnehmer handelt auf rationalste wirtschaftliche Weise, dann ergibt es keinen Sinn, eine kurzfristige große Auszahlung zu akzeptieren, anstatt eine Einnahmequelle zu schützen, die über einen längeren Zeitraum höhere Belohnungen bringen kann. Es ist, als würde ein Bauer viel Geld dafür bekommen, seine Ernte zu verbrennen - es mag kurzzeitig verlockend sein, aber was ist der Sinn, sein Ansehen und seine Existenzgrundlage zu riskieren, wenn er das Land viele weitere Jahre lang bestellen kann, um anständig zu leben?

Darüber hinaus, wenn Bitcoin angegriffen wird, ist es wahrscheinlich, dass die Marktteilnehmer in Panik geraten und den Preis abstürzen lassen. Die potenziellen Belohnungen am Ende eines erfolgreichen Angriffs sind daher deutlich geringer. Sicher, die Angreifer können US-Dollar verwenden, um den Preis auf einer Börse zu shorten... aber sie haben keine Garantie, dass ihr Versuch erfol-greich sein würde, und sie setzen sich nur weiteren Risiken aus. Ein erfolgloser 51%-Angriff macht die gesamte Anstrengung zu einer Zeit- und Energieverschwendung, zerstört den Ruf der Angreifer und stärkt nur das Bitcoin-Netzwerk, um besser auf eine solche Bedrohung reagieren zu können. Aber dennoch nehmen wir an, dass eine solche Koordination möglich ist, obwohl uns die Geschichte lehrt, dass dies in Zeiten, in denen die Wahrscheinlichkeit hoch schien, nicht geschehen ist.



Stand Mai 2023 gibt es eine geopolitische Multipolarität bei den Bitcoin-Mining-Pools. Die chinesischen Miner, die verdächtigt wurden, sich eines Tages zusammenzuschließen, um einen 51%-Angriff gegen das Netzwerk zu starten, kontrollieren immer noch etwa 40% der Hash-Rate über eine handvoll Pools. In der Zwischenzeit machen die US-amerikanischen und europäischen Mining-Pools ebenfalls etwa 39% der Hash-Rate aus. Im Falle einer totalitären Übernahme in China oder den USA, die zu einem politisch motivierten Angriff auf Bitcoin führt, kann keine Partei die notwendige Mehrheit erlangen.

Darüber hinaus bedeutet der Pool aus China oder den USA nicht automatisch, dass sich die Miner physisch im gleichen Land befinden müssen. Als Rumäne, der möglicherweise von zu Hause aus mined, bin ich frei, entweder als Solo-Miner ein Lotterielos abzugeben und nur durch reines Glück die gesamte Blockbelohnung zu erhalten, oder mich einem Pool anzuschließen, der mir das beste Gleichgewicht aus niedrigen Gebühren und hohen Belohnungen zu einem vorhersehbaren Satz bietet.

Obwohl der Pool selbst für die Koordination der Teilnehmer verantwortlich ist, werden dezentrale Beschränkungen durch Software-Innovationen wie Stratum V1 (der Branchen-standard seit 2012) und Stratum V2 (ein neuerer Standard, der derzeit von Braiins implementiert wird und noch mehr Dezentralisierung durch die Möglichkeit bietet, dass individuelle Miner ihre eigenen Transaktionssätze verhandeln). Es ist noch schwieriger für einen Pool, Bitcoin anzugreifen, wenn die Miner die Autonomie haben, sich von bestimmten Arten von Transaktionen auszuschließen.

Wie hoch sind die Kosten für einen 51%-Angriff theoretisch?

Stand 2. Mai 2023, bei einer Hash-Rate von 322 EH/s und einem Preis von 28.700 US-Dollar, kostet es etwa 1,27 Millionen US-Dollar pro Stunde, die Hardware zu mieten, die für diesen Angriff erforderlich ist. In der letzten Stunde hat Bitcoin durch volle Blöcke und hohe Gebühren Coins im Wert von 1,6 Millionen US-Dollar generiert. Theoretisch könnte ein Angreifer einen Gewinn von 0,33 Millionen US-Dollar erzielt haben, vorausgesetzt, die Mehrheit würde so lange halten und andere Miner würden keine zusätzlichen Maschinen einschalten, um die 51% zu verdünnen.

Allerdings ist dieses Modell rein theoretisch, da es nicht genügend Maschinen gibt, die ein Angreifer mieten könnte, um das Bitcoin-Netzwerk anzugreifen. Derzeit wird beim Proof-of-Work-Mining von Bitcoin ein SHA-256-Hashing-Algorithmus verwendet, der spezielle Hardware erfordert. Aufgrund der begrenzten und spezialisierten Nachfrage werden diese ASIC-Miner nur an wenigen Orten weltweit hergestellt und ihre Verfügbarkeit ist immer begrenzt. Diese Knappheit der Geräte ist aus Sicht eines durchschnittlichen Bitcoin-Enthusiasten, der von zu Hause aus minen möchte, oligopolistisch und nachteilig. In der Praxis bedeutet dies jedoch, dass Feinde von Bitcoin zusätzliche Ressourcen investieren müssen, um die Hardware zu kaufen, sie in Gebieten mit überschüssiger Energie zu betreiben und eine Initiative zu starten, die möglicherweise scheitern kann.

Im Januar 2021 hat Braiins einen Artikel veröffentlicht, der einige grundlegende Berechnungen darüber anstellt, was ein erfolgreicher 51%-Angriff erfordert. Zu dieser Zeit betrug die Hash-Rate 150 EH/s. Inzwischen hat sie sich verdoppelt. Wenn wir ihr Modell verwenden und davon ausgehen, dass die aktuellen Miner ehrlich bleiben und der Angreifer mindestens die gleiche Hash-Rate erreichen muss (300 EH/s), und es



auch eine unbegrenzte Verfügbarkeit von Antminer S19 XP Hyd Mining-Geräten gibt, die etwa 257 TH/s pro Gerät leisten, dann wären mindestens 1.167.315 Einheiten erforderlich, um den Angriff zu starten. Davon abgesehen kann Bitmains Produktion dieser Art von Nachfrage nicht gerecht werden. Nehmen wir jedoch an, dass ein Nationalstaat in der Lage ist, das zu bekommen, was er will, oder seine eigene Hardware in einer geheimen Fabrik herzustellen.

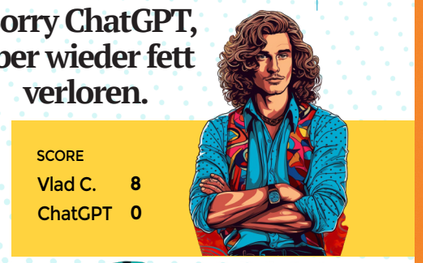
Nun sollten wir berücksichtigen, dass jedes einzelne Antminer S19 XP Hyd-Gerät 5346 Watt pro Stunde verbraucht. 5346 multipliziert mit 1.167.315 ergibt 6,23 GW/h. Diese Menge an Energie ist immens und es wäre sehr schwierig, sie aus überschüssigen Quellen zu beziehen, ohne Störungen an Orten zu verursachen, an denen Strom benötigt wird. Nur mächtige Nationalstaaten wie China, Russland und die Vereinigten Staaten könnten theoretisch mobilisiert werden, um einen derartigen Angriff in großem Maß-stab durchzuführen. Aber in der Realität ist es bei einem Preis von 10.000 US-Dollar pro Antminer S19 XP Hyd-Gerät und der Notwendigkeit von 1.167.315 Geräten viel einfacher und günstiger für sie, soziale Angriffe zu starten, die die Nutzung von Bitcoin aktiv behindern. Sie können Vorschriften erlassen, alle Arten von FUD verbreiten und finanzielle Mechanismen nutzen, um den Preis an

konformen Handelsplätzen in ihrer Zuständigkeit zu manipulieren.

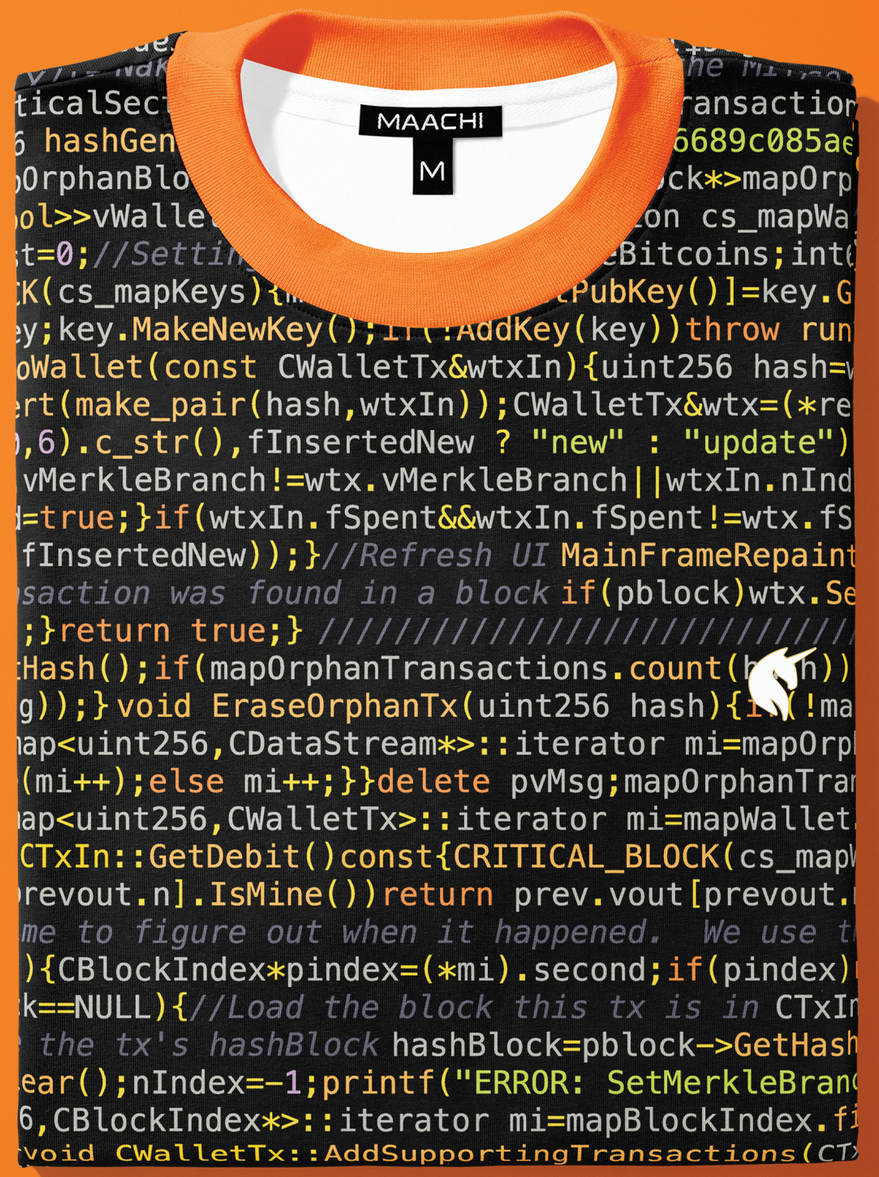
Man könnte jetzt fragen: "Ist es nicht einfacher für Bitcoin, zu Proof-of-Stake überzugehen und dieses komplizierte Spiel mit wahrscheinlichen Angriffspunkten globaler Supermächte hinter sich zu lassen?". Nun, die Antwort ist eindeutig nein. Proof-of-Stake ist ein "ein Coin, eine Stimme"-System, das ohne eine besorgniserregende Zentralisierung nicht funktionieren kann. Wenn ein Nationalstaat beabsichtigt, Ethereum, Cardano oder ein anderes Proof-of-Stake-System anzugreifen, muss er lediglich mit strengen Vorschriften drohen, um den Preis zu senken, und Geld drucken, um die Mehrheit der Coins zu erwerben. Dann ist das gesamte System verloren, da der größte Anteil die Kontrolle über die Governance hat.

Ein Angriff auf Bitcoin erfordert die Investition von Geld in Hardware und elektrische Energie. Und selbst wenn man alles richtig macht und einen erfolgreichen Angriff durchführt, bei dem die USA und China zusammenarbeiten, ist es immer noch wahrscheinlich, dass die Benutzer eine Abspaltung vornehmen und zu einer anderen Blockchain migrieren, die die Vorangegangene kopiert und den Mining-Algorithmus ändert, um weitere Angriffe zu einer Verschwendung von Ressourcen zu machen.

Bitcoin hat noch nie einen erfolgreichen 51%-Angriff erlebt, weil das Spieltheoriesystem funktioniert. Es gibt geopolitischen Wettbewerb zwischen Nationen, Wettbewerb um die Energieeffizienz zwischen Minern und die Anreize, sich an die Regeln zu halten, sind stärker als die Gefahren eines Angriffs. Über 51%-Angriffe gegen Bitcoin nachzudenken, ist eine interessante intellektuelle Übung, und die Vorstellung dieser Bedrohung ist nützlich, um ehrliche Miner im Zaum zu halten (wenn ihnen das Netzwerk wichtig ist, werden sie in Betracht ziehen, zu kleineren Pools zu wechseln). Aber in der Praxis bleibt es eine Fiktion, einen erfolgreichen Angriff durchzuführen.









Breaking ChatGPT's Bitcoin FUD #9



Aufklärung

ARGENTINIEN BITCOIN BILDUNG FUD NIGERIEN

Laut ChatGPT verstehen viele Menschen immer noch nicht die Technologie hinter Bitcoin. Diese mangelnde Bildung könnte die Einführung dieser dezentralisierten digitalen Währung einschränken.

Grundsätzlich stimme ich zu, dass es von größter Bedeutung ist, anderen beizubringen, was Bitcoin ist, wie es funktioniert und warum es wichtig ist. Immerhin ergibt keine Erfindung oder Entdeckung in der Geschichte der Menschheit Sinn, wenn es sowohl an Forschung zur Verfeinerung als auch an Bildung zur Erklärung mangelt. Und selbst wenn man diese beiden Elemente hat, ist ein Kontext für die Verwendung dieses Wissens ebenfalls erforderlich. Argumentierend kann gesagt werden, dass alles von Algebra bis zum Internet bedeutungslos ist, es sei denn, wir nutzen es, um Probleme zu lösen und unser Leben zu verbessern.

Gefällt dir der Artikel?

Scanne den QR-Code und hinterlasse ein Kommentar oder eine Donation!

Bitcoin ist nicht anders. Im Kern handelt es sich um Software, die auf Millionen von Computern weltweit läuft, um ein innovatives eigenständiges Wirtschaftssystem abzusichern und zu überprüfen. Es ist gleichzeitig eine lang erwartete Entdeckung und eine revolutionäre Erfindung. Es hat das Potenzial, die Art und Weise zu verändern, wie wir Geld verstehen und damit umgehen. Die Art und Weise, wie wir ein solches System nutzen und beschreiben, ist jedoch subjektiv von menschlichem Handeln und den finanziellen Bedürfnissen jedes Einzelnen abhängig.

Angesichts dieser Argumente halte ich die Aussage "der Mangel an Bildung könnte die Einführung von Bitcoin einschränken" für albern, faul und veraltet. Das könnte 2009 wahr gewesen sein, als nur wenige Computer-Nerds verstanden, was Bitcoin ist und wie es nützlich sein kann. Das war wahrscheinlich 2014 wahr, bevor Andreas Antonopoulos' "Mastering Bitcoin" veröffentlicht wurde, um eine ganze Generation von Autoren zu inspirieren, diesen Weg ebenfalls zu verfolgen. Aber im Jahr 2023 kann jeder auf der Welt zumindest einige grundlegende Informationen über Bitcoin in seiner Muttersprache lesen. Daher möchte ich behaupten, dass dies die kurzsichtigste und am leichtesten widerlegbare Art von FUD ist, die ChatGPT produzieren könnte, da wir heute mehr Bildungsmaterialien über Bitcoin haben als je zuvor.

Ich könnte den FUD wahrscheinlich nur dadurch entkräften, indem ich zeige, wie das Magazin BTCTKVR seit seiner Veröffentlichung im Jahr 2021 gewachsen ist: Noch bevor die diesjährige Ausgabe gestartet wurde, haben weltweit bereits über 2000 Personen eine physische Ausgabe des Magazins erhalten und viele weitere Enthusiasten haben sich die kostenlose digitale Version heruntergeladen. Und da es sich um ein Open-Source-Projekt handelt, wurden einige der besten Artikel ins Französische und Spanische übersetzt. Im Jahr 2022 konnten Bitcoin-Enthusiasten aus Frankreich, Argentinien, El Salvador und Senegal auf verschiedenen Konferenzen Magazine erhalten. Und das sind nur empirische Daten, für die ich persönlich Zeuge sein kann.

Jeden Tag werden weltweit Hunderte von neuen Artikeln über Bitcoin geschrieben. Wir können ein wachsendes Interesse von Blogs, Mainstream-News-Websites sowie wissenschaftlichen Fachzeitschriften erkennen. Wenn Sie auf YouTube nach "Bitcoin" suchen und die Ergebnisse so filtern, dass nur Inhalte angezeigt werden, die in den letzten 24 Stunden veröffentlicht wurden, werden Sie Tausende von Videos in Englisch, Französisch, Italienisch, Spanisch, Türkisch, Arabisch, Vietnamesisch, Tschechisch, Polnisch und vielen anderen Sprachen durchscrollen. Sie haben nicht genug Zeit an einem Tag, um die gesamte generierte Inhaltsmenge zu konsumieren, was eine bemerkenswerte Leistung ist.

Aber werfen wir auch einen Blick auf Bücher: Bei Amazon sind über 300 umfangreiche Veröffentlichungen zum Thema Bitcoin aufgelistet, von digitalen Selbstveröffentlichungen bis hin zu Taschenbüchern großer Verlage auf der ganzen Welt. Sie finden alles von Malbüchern über Handelsanleitungen und wirtschaftstheoretischen Handbüchern bis hin zu Programmier-Tutorials.

Zugegebenermaßen ist der Großteil des Inhalts in Englisch verfügbar, und die neuesten Forschungsergebnisse werden zuerst in Englisch veröffentlicht. Es scheint auch eine Verzögerung von 3-4 Jahren zu geben, bis das ursprüngliche Werk übersetzt und in mehr als 5 Sprachen veröffentlicht wird. Darüber hinaus werden einige der technischeren Werke selten übersetzt,



da sich ihr Zielpublikum bereits ausreichend mit der Arbeit in Englisch auskennt. Während diese Punkte valide sind, bleibt mein Argument dennoch bestehen: Jeder auf der Welt, der Zugang zum Internet hat, kann zumindest die Grundlagen von Bitcoin lernen. Wenn etwas nicht offiziell übersetzt und/oder veröffentlicht wird, ist die heutige KI-Technologie stark genug, um einen englischen Text in etwas umzuwandeln, das ein Kambodschaner oder Gambier lesen kann.

Aber um den Anwalt von ChatGPT zu spielen, gibt es einen offensichtlichen Unterschied zwischen Quantität und Qualität, der am besten am Beispiel von YouTube-Videos beobachtet werden kann. Die meisten dieser Clips sind absichtlich so gestaltet und strukturiert, dass sie Klicks anziehen, bieten jedoch selten viel Bildungsinformationen. Viele von ihnen präsentieren verzerrte Fakten, die ein schlechtes Verständnis des Themas offenbaren, und der beliebteste Ansatz, aus dem Bitcoin präsentiert wird, ähnelt dem Glücksspiel. Es geht nicht einmal darum, sich gegen die Inflation der Fiatwährung abzusichern, der beliebteste Ansatz dreht sich ausschließlich um den Handel mit BTC gegen mehr USD.

Das ist möglicherweise in Ordnung. Muss wirklich jeder Bitcoin-Benutzer die technischen Details darüber verstehen, wie das Senden und Empfangen von Geld funktioniert? Ist es wirklich notwendig, ökonomische Theorie jemandem zu erklären, der nur Geld von einer digitalen Brieftasche senden und empfangen muss? Benötigt eine Form von solideem Geld eine moralische Doktrin, die aktiv die Art und Weise beurteilt, wie die Menschen es nutzen?



Bitcoin ist ein Werkzeug, auf das Menschen freiwillig und rational zusteuern…

wenn sie es brauchen. Unter Technologiebegeisterten und Libertären ist es sicherlich einfacher Bitcoin anzunehmen, aber unterdrückte und zensierte Individuen benötigen es am dringendsten, um ihre Herausforderungen zu überwinden. Während die erstgenannte Gruppe Bitcoin als ideologisches Hobby oder für Spekulationen verwendet, braucht die letztere Kategorie von Menschen es, um unter Tyrannei zu überleben.

Obwohl ich dazu neige, puritanisch zu sein, wenn es um Bitcoin-bezogenen Inhalt geht, und oft minderwertige Beiträge ablehne, stimme ich zu, dass eine begrenzte Menge an Wissen, die geteilt wird, immer noch besser ist als gar kein Wissen. Solange die Menschen wissen, warum sie Bitcoin verwenden (und wir sollten ihre Rationalität nicht in Frage stellen), ist es unwichtig, ob sie den Unterschied zwischen P2PKH- und SegWit-Adressen kennen.

Internetnutzer müssen nicht die Unterschiede zwischen verschiedenen Protokollen verstehen, um E-Mails zu nutzen und einen Webbrowser zu bedienen. Bitcoin muss den gleichen Grad an Zugänglichkeit erreichen, unter einer Benutzeroberfläche, die es jedem nahtlos ermöglicht, Zahlungen über alle Ebenen und Sidechains hinweg zu senden und zu empfangen.

Bildung ist sicherlich wichtig, und es wird bereits jeden Tag viel davon produziert. Aber Bewusstsein ist noch wichtiger. Zum Glück leisten Regierungen in Krisenzeiten einen ziemlich guten Job bei der Förderung von Bitcoin, wenn sie versuchen, Bitcoin zu verbieten. Als die nigerianische Regierung 2021 den Zugang zu on- und off-ramps (Tausch Bitcoin gegen Fiat) einschränken wollte, als Reaktion auf die sinkende Nachfrage nach ihrer scheiternden Landeswährung, führte dies dazu, dass mehr Menschen von Bitcoin erfuhren und es peer-to-peer gegen Waren und Dienstleistungen austauschten. Zu einem Zeitpunkt war die Nachfrage nach BTC so hoch, dass der Wechselkurs in Nigeria höher war als an jedem anderen Ort auf der Welt.

In jüngster Zeit beschloss die argentinische Zentralbank, Bitcoin aus Zahlungsanwendungen zu verbieten, um "Risiken zu mindern". Was sie tatsächlich getan haben, war den Menschen zu sagen, dass Bitcoin die Flucht aus der Krise ist - und zweifellos werden die Ergebnisse in den kommenden Monaten sichtbar sein. Die Zentralbanker haben alles getan, um dem Bitcoin-Projekt zu helfen, auch wenn sie es nicht realisieren. Die steigende Nachfrage nach Bitcoin wird zur Schaffung noch mehr adhoc Bildungsmaterialien führen.

Die Menschen in Nigerien und Argentinien wurden nicht durch den begrenzten Zugang zu Bildungsressourcen abgeschreckt (zumindest im Vergleich zu englischsprachigen Ländern). Sie haben die Annahme von Bitcoin nicht aufgegeben, nur weil niemand ein bestimmtes Buch in ihre Sprache übersetzt hat, und es war ihnen egal, dass die Anzahl der BTC-bezogenen Podcasts und YouTube-Shows in ihrem Land gering ist. Sie haben ihre Bedürfnisse verfolgt, die ihnen zur Verfügung stehenden Werkzeuge genutzt und nach bestem Wissen gelernt.

Bitcoin kann als dezentrales Projekt nicht koordinativ die Finanzierung von Büchern, Podcast-Aufnahmen und Video-Tutorials ermöglichen. Alles ist ein freiwilliger Einsatz, der möglicherweise von der Nachfrage einer Community unterstützt wird. Einige Benutzer erstellen Bildungsinhalte mit einer bestimmten Zielgruppe im Hinterkopf, während andere es tun, weil sie es einfach nur wollen.

Dieses Magazin gehört zur letzteren Kategorie: Ich weiß nicht, wer Sie



sind, warum Sie dies lesen und was Sie mit dem neu erworbenen Wissen planen. Ich hoffe jedoch, dass Sie einige Informationen mit Ihren Freunden und Bekannten teilen und ihnen helfen, freier zu werden. Wenn Sie dieses Magazin übersetzen möchten, nur zu. Wenn Sie Änderungen vornehmen und es verkaufen möchten, steht Ihnen dies frei. Es ist wichtig, dass Informationen für edle und wohlwollende Ziele weitergegeben werden, die die Menschenwürde und Freiheit schützen.

In einer perfekten Welt, in der Zentralbanken und Regierungen rechenschaftspflichtig und ehrlich sind, wäre Bitcoin eine alberne Idee, die aufgrund mangelnder Nachfrage scheitert. Aber in unserer Zeit ist es ironisch, wie diese Institutionen die Menschen zu Bitcoin treiben und Pädagogen und Content-Erstellern ermöglichen, einen gewissen Erfolg in ihren Communities zu genießen. Die Annahmerate und die Qualität der Bildung sind miteinander verflochten, da die erstere eine Metrik für das Angebot ist, das die Schaffung nützlicher Ressourcen vorantreibt.

In einer perfekten Welt hätte ChatGPT recht in dieser Sache. Leider ist es nur ein Werkzeug, das pro-regierungsorientierte Erzählungen ohne viel Nuance wiedergibt. Es ist genau das, was die Investoren von OpenAI wollen, was es umso befriedigender macht festzustellen, dass die Maschine...

…wieder eine bittere Niederlage einstecken muss. Bitcoin-Bildung "to the moon"!

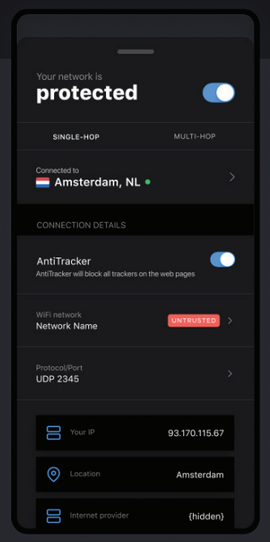
SCORE
Vlad C. 9
ChatGPT 0

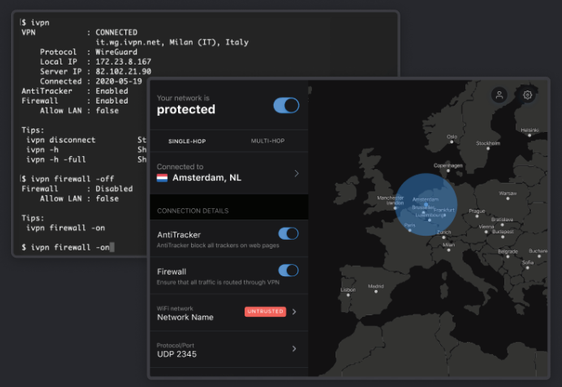


IVPN

Not your average VPN provider

- Generated accounts (no emails)
- Open source apps
- Regularly audited
- Run by privacy + Bitcoin advocates





BTC accepted,
Lightning recommended

Ask Vlad for a trial voucher card, or email **trial@ivpn.net** and refer to BTCTKVR.

Resist Online Surveillance

IVPN.net



Breaking ChatGPT's Bitcoin FUD #10

Mainstream Akzeptanz

ADOPTION MAINSTREAM EL SALVADOR GESETZLICHES ZAHLUNGSMITTEL

Laut ChatGPT ist es ein großes Problem, dass Bitcoin immer noch nicht von Unternehmen und Einzelpersonen im Mainstream angenommen wird. Dies wird angeblich zu einer Bedrohung für das gesamte Bitcoin-Projekt. Obwohl ich zustimme, dass es wichtig ist, Nachfrage nach der Währung zu schaffen, indem Produkte und Dienstleistungen im Austausch dafür angeboten werden, halte ich die Erwartungen des KI-Modells für unrealistisch und diese Form von FUD für albern.

Um zu erklären, warum ich ChatGPTs Bedenken hinsichtlich der Mainstream-Akzeptanz nicht ernst nehme, muss ich den Begriff "Mainstream-Akzeptanz" definieren. Eine erste Definition bezieht sich auf die Akzeptanz durch Nationalstaaten, die von El Salvador und der Zentralafrikanischen Republik vorangetrieben wurde. Die

What do you think about this article?

Leave your comments or send a donation by scanning this QR code.

zweite Definition konzentriert sich auf eine bottom-up-Basisakzeptanz, die bedeutender ist und ideologisch mit der Mission des Bitcoin-Projekts übereinstimmt. Es umfasst Unternehmen, Einzelpersonen und alles dazwischen, was den privaten Sektor betrifft.

Ist Bitcoin in Bezug auf die Akzeptanz durch Nationalstaaten ein Misserfolg oder eine Enttäuschung? Nun, lassen Sie uns das mit den beiden größten Fiat-Währungen der Welt vergleichen: dem US-Dollar und dem Euro. Der US-Dollar wurde erstmals am 6. Juli 1785 konzeptionell entwickelt, und es dauerte weitere 6 Jahre und 9 Monate, bis er durch das Coinage Act von 1792 zur offiziellen Währung der Vereinigten Staaten von Amerika wurde. Es dauerte jedoch bis 1944, bis der Dollar zur Weltreservewährung wurde - 152 Jahre seit der Einführung und ungefähr 158 Jahre seit der ersten Ankündigung.

Im Fall des Euro handelt es sich um das Ergebnis jahrzehntelanger Diskussionen über eine gemeinsame europäische Währung, um die Vorherrschaft des US-Dollars herauszufordern. Er wurde am 7. Februar 1992 erstmals im Rahmen des Vertrags von Maastricht angekündigt und wurde am 1. Januar 1999 in 11 europäischen Ländern gleichzeitig zur offiziellen Währung. Da die Deutsche Mark bereits eine weltweite Reservewährung war, erbte der Euro sofort diese Eigenschaft. Stand Mai 2023 existiert Bitcoin erst seit 14 Jahren und 4 Monaten. Nach 12 Jahren seines Bestehens wurde es zur offiziellen Währung in El Salvador. Die Zentralafrikanische Republik hat Bitcoin im April 2022 ebenfalls angenommen, aber nur ein Jahr später wieder aufgegeben. Obwohl diese Annahme von oben nach unten erfolgte, wird die Verwendung von Bitcoin nicht von den Staaten erzwungen - das bedeutet, dass die Verwendung von Bitcoin für alle Arten von Zahlungen legal ist, aber die Regierung wird ihre Gewaltmonopolie nicht nutzen, um Händler und Banken zu zwingen, Bitcoin zu akzeptieren. Im Fall des Euro hatten die Italiener, Spanier und Deutschen keine andere Wahl, als ihre Lira, Peseten und Mark gegen die neue Währung umzutauschen, die sie in allen Transaktionen verwenden mussten. Im Vergleich dazu ist diese erste Welle der Bitcoin-Adoption auf der Ebene der Nationalstaaten viel freiwilliger.

	Bitcoin	US Dollar	Euro
First Announced	October 31st 2008 (Whitepaper)	July 6th 1785 (Continental Congress resolution)	February 7th 1992 (Maastricht Treaty)
Launch Date	January 3rd 2009	April 2nd 1792 (Coinage Act of 1792)	January 1st 1999
First Became Official Currency in a Country	June 9th 2021 (12 years, 8 months since announcement)	April 2nd 1792 (6 years,9 months since announcement)	January 1st 1999 (6 years, 11 months since announcement)
Number of Countries Where It's Official Currency	~~2~~ 1	7 exclusively, 22 along other national currencies	20
Reserve Currency Since	2021	1944	1999
% of Global Reserves (2022)	<1%	58.36%	20.47%
Years It Took to Become Reserve Currency	12 since launch 13 since announcement	152 since launch 158 since announcement	0 since launch 7 since announcement





Aber Bitcoin wurde nicht geschaffen, um Regierungen von Nationalstaaten zu dienen. Es existiert als Möglichkeit für Einzelpersonen, sich Tyrannei zuentziehen und den Folgen der zentralbankgesteuerten Inflation zu entkommen. Der beabsichtigte Zweck des Projekts wurde von Schöpfer Satoshi Nakamoto im ersten Block des Netzwerks deutlich gemacht: "Chancellor on the brink of second bailout for banks" - ein direktes Zitat von der Titelseite der britischen Zeitung The Times, die einen Schlagzeilenartikel aus Kanzler Alistair Darlings Entscheidung machte, die Banken auf Kosten aller Steuerzahler zu retten, genau am Tag der Einführung von Bitcoin.

Bitcoin wird von keinem Land ausgegeben oder kontrolliert,

es funktioniert nach einer vorhersehbaren Geldpolitik, die für alle Teilnehmer klar und transparent ist und ausschließlich auf freiwilligen Interaktionen beruht. Diese Art von digitaler Währung kann nicht beschlagnahmt, eingefroren oder besteuert werden. Niemand kann einen bestimmten Benutzer daran hindern, seine eigene Wallet zu installieren, zu nutzen oder eine zu erstellen, um an dieser Wirtschaft teilzunehmen. Darüber hinaus kann niemand Einzelpersonen daran hindern, den Ledger zu sichern, der die gesamte Transaktionsgeschichte enthält, und dann ihre eigenen Transaktionen über ihren Full Node an das Netzwerk zu übertragen. Und wenn Benutzer thermodynamische Sicherheit für Bitcoin bieten und auch am Geldschöpfungsprozess teilnehmen möchten, können sie ihre eigenen Solo- oder Pool-Mining-Operationen durchführen.

In vielerlei Hinsicht ist jeder Vergleich mit bestehenden Arten von Geld falsch - hauptsächlich, weil wir Metriken aus einem freien, transparenten und freiwilligen System und Daten aus einem auf Vertrauen basierenden, militärisch durchgesetzten und politisch zwanghaften Apparat gegenüberstellen. Es ist eine Wahl zwischen Freiheit und Unterwerfung gegenüber dem großen Tyrannen.

Dennoch ist es immer noch vorteilhaft zu verstehen, dass Bitcoin während seiner 14-jährigen Existenz eine Menge erreicht hat und vermehrt als weltweite Währung akzeptiert wird, insbesondere weil seine Konkurrenten unehrlich und



intransparent sind.

Freie Märkte überdauern Wahlen,

Regimewechsel und Regierungen. Ebenso wird nicht-staatliches und nicht zensierbares Internetgeld jegliche Art von finanzieller Zentralplanung überdauern. Historisch gesehen halten Märkte und neutrales Geld in der Regel länger als Reiche, Nationen und verschiedene Migrationswellen. Die Seidenstraße bestand aus eurasischen Handelsrouten, die etwa 1500 Jahre lang Bestand hatten, während Gold und Silber seit mindestens 550 v. Chr. als Geld verwendet werden. Bitcoin ist relativ jung, hat aber bereits einen guten Rekord darin, Krisen standzuhalten und durch Chaos zu navigieren.

Der wichtigste Teil von Bitcoins Mission besteht darin, dass er von Menschen angenommen wird, die ihn brauchen, und mehr wirtschaftliche Freiheit in die Welt bringen. Derzeit funktioniert es größtenteils als eine Art Erpressung gegenüber Regierungen und Zentralbanken - entweder stimmen sie zu, ein vernünftiges Maß an Rechenschaftspflicht zu wahren, indem sie nicht die Ersparnisse aller entwerten, oder die Menschen werden sich weigern, ihre Währung zu verwenden und Steuern zu zahlen. Bitcoin ist der effektive Protest, ein Werkzeug, das viel besser funktioniert als Demonstrationen auf der Straße und Petitionen. Die Hauptvoraussetzung ist jedoch, dass die Menschen es auf eine nichthoheitliche und souveräne Weise nutzen.

Dies ist meiner Meinung nach die Hauptbarriere, die zwischen Bitcoin und einer massenhaften Akzeptanz steht, oder wie ChatGPT es nennt, einer allgemeinen Akzeptanz. Selbst heute, wenn die Benutzeroberflächen benutzerfreundlicher sind, gibt es immer noch Macken und häufige Hindernisse, die das Erlebnis holprig machen. Manchmal steigen die On-Chain-Transaktionsgebühren für eine Weile an und Transaktionen bleiben im Mempool stecken. Andere Male scheitern Lightning-Zahlungen aufgrund eines Kommunikationsfehlers. Es gibt Zeiten, in denen die Verwaltung von UTXOs Kopfschmerzen verursacht. Diese Probleme können selbst aus der Perspektive eines fortgeschrittenen Benutzers schwierig zu identifizieren sein.

Angesichts der Einfachheit, eine Debitkarte zu verwenden, um ein Konto bei einer zentralisierten BTC-Börse einzurichten, ist es kein Wunder, dass die meisten Benutzer in diesen Exchanges stecken bleiben. Die Verwendung eines zentralisierten, regulierten und letztendlich regierungskonformen Verwahrers widerspricht jedoch dem Zweck von Bitcoin. Nur wenn Sie Ihre eigene Wallet, mit Ihrer eigenen Full Node verwenden, ermöglicht dies erst Privatsphäre gegenüber Ihrer Regierung. Anderenfalls sind Sie nicht wirklich frei oder in der Lage, friedlich zu protestieren.

Die Komplexität der Eigenverwahrung ist definitiv ein Hindernis auf dem Weg zur allgemeinen Akzeptanz. Denn die Verwendung von Bitcoin ohne Souveränität ist nichts anderes als Spekulation mit einem vertrauenswürdigen Dritten in der Mitte. Aber diejenigen, die Bitcoin wirklich nutzen müssen, finden alle Bildungsmaterialien, die sie benötigen, um sich von jeglicher Art von Tyrannei zu befreien.

Der Grund warum Bitcoin, in den relativ prosperierenden Zeiten, keine allzu große allgemeine Akzeptanz in Entwicklungsländern gefunden hat, liegt ebenfalls am Mangel an technologischen Möglichkeiten in ebendiesen Ländern Welt. Zwischen diesen beiden Extremen gab es Menschen, die sich entweder entschieden haben zu spekulieren oder sich eine bessere Zukunft sichern wollten. Der Preis spielt ebenfalls eine große Rolle, aber auf lange Sicht weist die Volatilität auf eine massive Wertsteigerung gegenüber jeder Fiat-Währung hin. Selbst wenn Bitcoin 50% seines Marktwerts gegenüber dem US-Dollar verliert, schneidet er immer noch besser ab als gescheiterte Fiat-Währungen wie den argentinischen Peso, die türkische Lira und den nigerianischen Naira.

Bildung über Geld und Bitcoins Platz im globalen Finanzsystem ist wichtig. Ein gutes Verständnis der Informatik und der Märkte hilft ebenfalls sehr. Aber am Ende nehmen die meisten Menschen Bitcoin an, weil sie ihn brauchen - und wenn sie ihn bis jetzt noch nicht angenommen haben, dann nur, weil noch kein dringendes Bedürfnis bestand.

Mit jeder Preiserhöhung kommen neue Spekulanten hinzu, von denen viele den Wert von Bitcoin verstehen und andere darüber unterrichten werden. Wenn die Zentralbanken in dieser von Bitcoin geschulten Umgebung mehr Geld drucken, wird die Akzeptanz für die dezentralisierte digitale Währung wachsen. Und mit zunehmender Akzeptanz verbessert sich alles - von Regierungen, die mehr zur Rechenschaft gezogen werden, bis hin zu Bitcoin-Wallets, die genügend Feedback erhalten, um benutzerfreundlicher zu werden.

Aber schluss mit den Ausreden, ChatGPT kann dieses Battle nicht gewinnen. Laut CoinATM Radar gibt es weltweit 34.100 Bitcoin-Automaten in 75 Ländern. Das bedeutet, dass Menschen aus 75 verschiedenen Ländern ihre lokale Fiat-Währung verwenden können, um Bitcoin zu kaufen oder die BiTC, die sie haben, gegen sofortiges Bargeld zu tauschen. Nennen Sie eine andere Währung, die in 75 Ländern so einfach akzeptiert und gehandelt wird. Diese Metrik berücksichtigt nicht einmal die Tausenden von kleinen Unternehmen auf der ganzen Welt, die Zahlungen direkt in BTC akzeptieren.

Versuchen Sie, nach Ostasien, Südamerika oder Zentralafrika mit Euro, britischen Pfund und Bitcoin zu reisen.

Sprechen Sie mit Händlern auf Märkten, gehen Sie in Geschäfte und erkundigen Sie sich, welche der drei Währungen am schnellsten gegen die offizielle Währung des Landes umgetauscht werden kann (und daher am wahrscheinlichsten als Zahlungsmittel akzeptiert wird). Sie werden überrascht sein zu entdecken, dass die Nachfrage nach Bitcoin nach dem US-Dollar an zweiter Stelle steht.

Im Westen haben die meisten großen Einzelhändler nicht aufgeholt. Dies ermöglicht bitcoinfreundlichen Drittanbietern wie Bitrefill (die Geschenkkarten verkaufen) und ShopInBit (die alle legalen physischen Artikel verkaufen) die Rolle von Amazon, Steam, Spotify, eBay, PlayStation Store und vielen anderen Diensten zu übernehmen. Es gibt definitiv eine parallele Wirtschaft, die allmählich mit der Mainstream-Wirtschaft zusammenwächst, aber es ist wahrscheinlich noch zu früh, damit BTC im Handel genauso allgegenwärtig ist wie der US-Dollar.

Leider gibt es nur zwei Momente, die zu einem Anstieg der Bitcoin-Adoption führen: massive Preisanstiege, die Spekulanten anziehen, und tragische Ereignisse, die Menschen anziehen, die Bitcoin als Sicherheitsnetz benötigen. Aber mit zunehmender Zeit beweist die dezentralisierte



digitale Währung ihre Widerstandsfähigkeit und die Nachfrage aus der Basis nimmt zu, was zu einer zunehmenden Akzeptanz im Mainstream führt. Der US-Dollar wurde in 14 Jahren nicht zur dominanten Währung, und auch Gold wurde nicht über Nacht zum wichtigsten Edelmetall der Welt. Es erfordert Arbeit, Ausdauer und Bildung.

Nichtsdestotrotz hat Bitcoin unter den gegebenen Umständen alle Erwartungen übertroffen, die düsteren Vorhersagen aller nobelpreisgekrönten Ökonomen widerlegt und dem Druck besser standgehalten als ganze Regierungen. Dabei wurde es mit jedem Benutzer, der die Souveränität annahm, dezentralisierter und mit jeder Person, die das Wort über das magische Internetgeld verbreitete, bekannter.

Mainstream-Akzeptanz ist ein Marathon, kein Sprint. Und kontinuierlich erreicht diese das Ziel. Sorry, ChatGPT.

SCORE
Vlad C. 10
ChatGPT 0





Become Part Of **Bitcoin History!**

Secure one of the coveted Rare Pepe trading card booster packs. Join the community and explore the fascinating world at **www.peperium.site**

RARE
PEPE PHYSICALS

21 ∞ mil



Limited 1st editions available for early community participants!



FUD Zum Grübeln

Udi is a fraud



PROBLEME FUNGIBILITÄT PRIVATSPÄHRE SICHERHEITSBUDGET WOHLSTANDSVERTEILUNG

Trotz aller Gewissheiten, die es bietet, und all dem FUD, der Bitcoin durch seine fortwährende Existenz zerstören kann, ist das Netzwerk immer noch nicht perfekt. Benutzer und Entwickler müssen sich immer noch mit einigen Designentscheidungen des Systems auseinandersetzen, die Raum für Spekulationen lassen.

Ein Beispiel dafür ist die größte Wette bei Bitcoin, nämlich dass das Netzwerk eines Tages von denselben Sicherheitsanreizen profitieren wird, während die Miner nur mit Transaktionsgebühren bezahlt werden. Die abnehmende Blocksubvention ist ein wesentlicher Bestandteil von Bitcoins wirtschaftlichem System: Alle 210.000 Blöcke (ungefähr alle 4 Jahre) werden die Mining-Belohnungen halbiert. Im Januar 2009 wurde festgelegt, dass die Mining-Belohnung 50 Bitcoin pro Block betragen würde. Dann wurde sie im November 2012 erneut halbiert, und nochmals im Juli 2016 und im Mai 2020.

Im Mai 2023 erhalten Miner 6,25 Bitcoin + Transaktionsgebühren. Und irgendwann im nächsten Jahr wird diese Belohnung auf 3,125 BTC pro Block reduziert. Dieser Halbierungs-Trend wird bis zum Jahr 2140 fortgesetzt, wenn die gesamten 21 Millionen Coins in Umlauf sein werden. Nach diesem Punkt wird Bitcoin ein vollständig deflationäres Währungssystem sein.

Es ist jedoch auch erwähnenswert, dass bis Mai 2024, wenn die nächste Halbierung der Blockbelohnung stattfinden soll, bereits 93,75 % aller Bitcoins geschürft sein werden. Ein Großteil des Angebots ist also im Umlauf, die Kosten für die Produktion eines Bitcoins sind höher, und daher werden nur die effizientesten Miner überleben. Die einzige erfolgversprechende Kombination besteht aus erschwinglicher und reichlich vorhandener Energie (nuklear, solar, wind und/oder hydro) in Verbindung mit leistungsfähiger Mining-Hardware, die mehr Hashes pro Kilowatt erzeugt. Wenn das Mining über die Halbierungszyklen hinweg stagniert, wird die Spieltheorie komplizierter.

Dieses Problem wird allgemein als "das Bitcoin-Sicherheitsbudget" bezeichnet, und es stellt sich die Frage, inwieweit bestehende Subventionen die Miner in Zukunft profitabel halten können. Es wird geschätzt, dass bis 2032 überwiegend Transaktionsgebühren die Miner bezahlen werden, nicht die Blockbelohnung von 0,78125 BTC. Aber einige Analysten sind unsicher, ob Bitcoin-Benutzer bereit sind, ständig hohe Gebühren zu zahlen.

Es gibt 6 Wege, um das Problem des Sicherheitsbudgets zu lösen,

die ich vom beliebtesten bis zum am wenigsten unterstützten vorstellen werde:

A. Der Bitcoin-Preis verdoppelt sich alle 2 Jahre, sodass die verringerte BTC-Belohnung in US-Dollar genauso viel wert ist. Obwohl dieses Szenario das beliebteste ist, haben wir einen Punkt erreicht, an dem es eine halbe Billion US-Dollar dauert, um die heutige Marktkapitalisierung zu verdoppeln, und es werden weitere Billionen Dollar benötigt, um den gleichen erfolgreichen Übergang im Jahr 2028 zu erreichen (dann zwei Billionen im Jahr 2032, vier Billionen im Jahr 2036 und so weiter). Zur Referenz, Apple und Microsoft haben eine kumulierte Marktkapitalisierung von 5 Billionen US-Dollar, während Gold bei 13,36 Billionen US-Dollar liegt. Selbst wenn wir davon ausgehen, dass die Inflation durch Geldschöpfung in den kommenden Jahren weitergeht und schlimmer wird, erfordert ein Bitcoin-Preis, der sich alle 210.000 Blöcke verdoppelt, immer noch viel Liquidität, die möglicherweise nicht immer vorhanden ist.

B. Mit Hilfe von merge-mined Sidechains wie RSK und Drivechains, die viel Aufmerksamkeit erhalten, gelingt es den Bitcoin-Minern, mehr Transaktionsgebühren auf mehreren parallelen Chains zu sammeln. Die Gebühren auf der Hauptkette steigen nicht zu stark an, da die meiste Aktivität in den Second-Layer-Lösungen stattfindet. Die erhöhte Anzahl von Transaktionen im Ökosystem wird jedoch kompensieren.

C. Die Bitcoin-Transaktionsgebühren werden nach jedem Halbierungszyklus dauerhaft verdoppelt, um den schwindenden Einnahmen entgegenzuwirken. Dies ist eine soziale Lösung, da sie auf dem guten Willen anderer und ihrer Bereitschaft beruht, freiwillig höhere Transaktionsgebühren zu zahlen, um die derzeitigen Miner am Laufen zu halten. Außerdem müssen die Gebühren nicht verdoppelt werden - sie können proportional zum Preis steigen, damit die Miner eine Menge erhalten, die sie dazu moti-

Gefällt dir der Artikel?

Scanne den QR-Code und hinterlasse ein Kommentar oder eine Donation!





viert, weiterzumachen.

D. Nichts tun und die Miner Geld verlieren lassen, bis sie günstigere Energiequellen finden, ihre Ausrüstung verbessern oder aufgeben. Diese Lösung fördert Effizienz und Innovation in Bezug auf Hashes pro Watt, eliminiert jedoch vollständig Miner, die nicht mithalten können. Wenn die Konsequenz dieser Säuberung die Hashrate drastisch beeinflusst, werden wahrscheinlich alle Bitcoin-Benutzer mehr Bestätigungen abwarten, bis sie feststellen, dass eine Transaktion endgültig ist.

E. Die Blockgröße erhöhen in der Hoffnung, dass mehr Transaktionen stattfinden. Dies ist schwierig umzusetzen, da dies eine Hard Fork erfordert (alle Benutzer verlassen die alte Chain und wechseln zu einer aktualisierten), es die Einnahmen der Miner in Zeiten geringer Nachfrage negativ beeinflusst und das Netzwerk während und nach Zeiten hoher Nachfrage viel stärker zentralisiert. Außerdem garantiert diese Art der Skalierung nichts in Bezug auf Benutzer und Adoption - Bitcoin Cash, der große Block-Klon von Bitcoin, konnte trotz aggressiver Marketingkampagnen in den Jahren 2017 und 2018 keinen Erfolg im Handel erzielen.

F. Änderung der Geldpolitik, um Inflation/Tail-Emission hinzuzufügen. Dies ist bei weitem der unbeliebteste Ansatz und wird nur ernsthaft in Betracht gezogen, wenn Bitcoin sich in einer Phase befindet, in der die Gebühren die abnehmende Blocksubvention nicht ausgleichen. Dies impliziert eine Erweiterung der 21 Millionen Bitcoin-Grenze, um die Miner zu bezahlen und somit die Art von Inflation und zentraler Planung zu schaffen, die Bitcoin-Befürworter vermeiden wollten. Der wahrscheinlich interessanteste Vorschlag stammt von Peter Todd, der vorgeschlagen hat, eine kleine jährliche Tail-Emission für das Sicherheitsbudget hinzuzufügen..

Grundsätzlich wird dieses Problem des Sicherheitsbudgets wahrscheinlich erst um das Jahr 2032 zu einer dringenden Diskussionsfrage werden. Bis dahin wird erwartet, dass in allen Bereichen viele Innovationen stattfinden - genauso wie das erste Jahrzehnt von Bitcoin von Entdeckungen und neuer Forschung geprägt war. Trotzdem ist es gut zu wissen, was los ist und welche Optionen vorhanden sind - je mehr Zeit wir damit verbringen, über das Problem nachzudenken, desto qualitativ hochwertigere Debatten werden wir in den nächsten zehn Jahren führen.

Eine weitere legitime Quelle für FUD (Fear, Uncertainty, Doubt) ist die Austauschbarkeit der Währung und die Privatsphäre, die sie erfordert. Wenn wir mit Goldmünzen oder Banknoten umgehen, müssen wir uns nicht allzu sehr um ihre Herkunft kümmern. An der Kasse sollte ein 10-Dollar-Schein, der einmal Brad Pitt gehörte, nicht wertvoller sein als ein anderer, der zuvor einem unbekannten Automechaniker aus den Vororten gehörte. Das Geld ist fungibel, was bedeutet, dass eine Währungseinheit gleichwertig ist mit einer anderen, die den gleichen Nennwert hat.

Aber im Fall von Bitcoin sind nicht alle Coins gleich erschaffen und werden gleich transferiert. Tatsächlich ist es unmöglich, zwei Bitcoin-Einheiten zu finden, die dieselbe Geschichte haben, es sei denn, man kauft die frisch geschürften Coins direkt von den Minern. Der Unterschied zwischen Bargeld und Bitcoin besteht darin, dass ersteres für lokale Transaktionen von Angesicht zu Angesicht großartig ist, da es sofort, privat und endgültig ist, während letzteres für Internetzahlungen entwickelt wurde und auf der öffentlichen Blockchain relativ einfach nachverfolgt werden kann.

Bitcoin hat 4 Hauptarten Privatspähre:

A. Privatsphäre auf netzwerkebene,



die Benutzer von einfachen Wallets (die auf den Knoten anderer Personen und Electrum-Servern ausgeführt werden) schützen, damit ihre IP-Adresse nicht registriert wird. Wenn jemand Ihre Bitcoin-Transaktionen mit einer echten IP-Adresse in Verbindung bringen kann, kann er über Social Engineering herausfinden, wo Sie wohnen. Glücklicherweise kann dieses Problem leicht mit Tor-Routing (Tails OS auf dem Desktop, Orbot auf Android-Handys oder bestimmte Wallets, die eine Tor-Integration haben: Blixt, Blockstream Green, Phoenix) oder einem guten VPN-Dienst (IVPN und Mullvad sind beide ausgezeichnet, da sie keine E-Mail-Adresse erfordern und BTC-Zahlungen akzeptieren) gemildert werden.

B. Privatsphäre des öffentlichen Schlüssels (public keys), die verhindert, dass die Server anderer Personen Transaktionen von einem UTXO mit dem Rest Ihrer Wallet (und potenziell Ihrer Identität) in Verbindung bringen. Das xpub (erweiterter öffentlicher Schlüssel) Ihrer Wallet enthält Informationen darüber, wie viele Bitcoin Sie haben, welche Adressen Ihnen gehören und welche Adressen Ihre Wallet generieren wird, wenn Sie sie weiterhin verwenden. Um dieses Risiko zu beseitigen, betreiben Benutzer ihre eigenen vollständigen Knoten oder installieren Wallets, die eine BIP157/158-Implementierung (Neutrino) verwenden. Die Verwaltung Ihres eigenen Knotens bringt große Privatsphäre-Vorteile mit sich und ist sicherlich etwas, das jeder lernen sollte.



C. Sender-Privatsphäre, die der schwächste Punkt von Bitcoin ist. Wenn Sie jemandem Bitcoin senden, kann er sich die öffentliche Blockchain ansehen, um zu sehen, woher die Transaktion stammt und wohin die Gelder zuvor gegangen sind. Nachdem Sie von einer KYC-Börse (Know Your Customer), die mit Blockchain-Analyse-Diensten zusammenarbeitet, abgehoben haben, wird höchstwahrscheinlich jemand Ihre Gelder über Transaktionen hinweg verfolgen, um herauszufinden, wem Sie Bitcoin senden und von wem Sie empfangen. CoinJoins (Wasabi, JoinMarket, Samourai) bieten eine recht gute Lösung: Sie nehmen an einer kollaborativen Transaktion teil, bei der es schwierig ist zu erkennen, wer wer ist, nachdem die Ausgaben generiert wurden, auch wenn die Eingänge bekannt sind. CoinSwaps (MercuryWallet) sind ebenfalls großartig, um Ihre UTXO gegen die einer anderen Person auszutauschen, bergen jedoch das Risiko, die Identität einer Person zu erhalten, die weitaus mehr überwacht wird als Sie. Die Verwendung beider Tools in Kombination ist bisher die beste Lösung.

D. Empfänger-Privatsphäre, was Bitcoin's stärkster Punkt in Bezug auf Privatsphäre ist. Solange Sie Adressen nur einmal verwenden, wird niemand in der Lage sein, festzustellen, wie viel Geld Sie haben oder mit wem Sie zuvor Transaktionen durchgeführt haben. Ihr Sender kann nur sehen, dass sich Ihr Guthaben von 0 (wie alle neuen Adressen) auf den Betrag erhöht hat, den er oder sie in Ihrer Wallet überwiesen hat. Sie können jedoch sehen, wie Sie Ihre Gelder danach übertragen. Wenn jedoch ein Drittanbieterknoten Ihren öffentlichen Schlüssel besitzt (wie in Punkt B beschrieben), wird Ihre Empfänger-Privatsphäre aufgehoben - er kann Ihre Transaktion in jeder neuen Adresse sehen, die Sie aus derselben Wallet generieren.

E. Betrags-Privatsphäre, bei der es darum geht, sehen zu können, wie viele Bitcoin über Adressen hinweg übertragen werden. Bitcoin ist ein öffentliches Hauptbuch, sodass Sie sehen können, wie viel Geld übertragen wird, auch wenn Sie nicht wissen, wer der Sender und der Empfänger sind. Grundsätzlich geht es hier um die Transparenz der Geldpolitik - Sie können immer sehen, dass die Menge der im Umlauf befindlichen Münzen nicht mehr als die Menge der abgebauten Münzen beträgt, wovon es nie mehr als 21 Mil geben wird. Es gibt jedoch interessante laufende Forschungen auf diesem Gebiet. Zero-Knowledge-Beweise oder eine andere Art von Technologie können die Notwendigkeit der Prüfbarkeit und Betrags-Privatsphäre mildern.

Das Problem mit Bitcoin ist, dass Regierungen herausgefunden haben, wie das Netzwerk funktioniert.



On- und Off-Ramps sind in den meisten Ländern reguliert, sodass die einzigen wirklich privaten Transaktionen diejenigen sind, die zwischen jemandem stattfinden, der direkt von einem Miner gekauft hat, und seinem Handelspartner, CoinSwappern oder Wallets von Vollknoten (full nodes), die auch einige CoinJoin-Runden durchlaufen haben. Natürlich gibt es Off-Chain-Lösungen, die eine bessere Privatsphäre bieten: das Lightning-Netzwerk, die Liquid-Sidechain, Statechains, Drivechains und andere bestehende oder vorgeschlagene Sidechains. Aber auch die Basis-Layer benötigt Verbesserungen.

Derzeit ist Privatsphäre kostspielig. Es ist jedoch wichtig, Bitcoin nicht von Nationalstaaten erfassen zu lassen, die Überwachung betreiben, da es sonst zu einem finanziellen Panoptikum wird. Die Adoption durch Nationalstaaten ist ebenfalls keine gute Idee, da Bürger beim Transferieren noch weniger Privatsphäre haben. Nicht zuletzt ist das Hauptargument einfach: Solides Geld erfordert Fungibilität, und Bitcoin hat diese noch nicht erreicht.

Ein weiteres legitimes Bedenken betrifft die Ungleichheit der Vermögensverteilung. Der Mainstream-Ökonom Nouriel Roubini wies wiederholt darauf hin, dass Bitcoin einen schrecklichen Gini-Koeffizienten hat. Bitcoin-Befürworter argumentierten, dass auch das herkömmliche Finanzsystem den Großteil des Reichtums in den Händen weniger Eliten und ihrer Familien konzentriert hat, aber akademische Ökonomen ignorieren dieses Problem, da sie nicht die Hand beißen können, die sie füttert.

Dennoch ist es wahr, dass fast 93% des Angebots in den letzten 14 Jahren geschürft wurden und sich in den Händen von einigen Millionen Benutzern befinden. Dies ist kein Argument für Umverteilung, sondern eines für Fairness: Wenn Bitcoin eine bessere Form von Geld sein soll, sollte es mehr sein als nur der Austausch der finanziellen Eliten des Industriezeitalters gegen eine neue Klasse von Computerfreaks.

Bitcoin kann nicht die Währung der ganzen Welt sein, es sei denn, es kann 8 Milliarden Menschen dienen. Um dieses Ziel zu erreichen, müssen frühe Nutzer großzügiger und manchmal auch wohltätig sein, indem sie anderen erlauben, mehr Bitcoin als den Äquivalenten in staatlichem Geld im Austausch für ihre Waren und Dienstleistungen zu verdienen. Trinkgelder und Geschenke sind ebenfalls Möglichkeiten, um andere zu gewinnen und sie bereitwillig am Netzwerk teilnehmen zu lassen.

Solange Bitcoin jedoch als Sammlerstück behandelt wird, kann er nicht das Geld für die ganze Welt sein - und dieses Argument geht über die Skalierungsdebatte hinaus. Auf einem Bitcoin-Standard sind alle Transaktionen freiwillig. Daher sollten wir versuchen, freiwillig großzügig zu sein, um zu verhindern, dass andere neidisch oder unglücklich werden und zu Gewalt greifen. Wenn wir wirklich eine bessere Form von Geld aufbauen, müssen wir aus den Problemen des Fiat-Geldes lernen und versuchen, es besser zu machen.

ChatGPT war offenbar nicht clever genug, um diese drei Beispiele an FUD vorzulegen.

Ich denke, dass diese Beispiele deutlich besser sind als das, was ChatGPT präsentiert hat und ich freue mich, dass ich die Chance hatte, diese darzustellen und darüber aufzuklären. Das ist FUD zum Nachdenken, denn wir alle haben die Wahl und die Möglichkeit, zum Bitcoin-Projekt beizutragen. Im Gegensatz zum Fiat-System, das seine eigenen Hierarchien hat, welches sich um ein offizielles Narrativ und ein Vertrauenssystem dreht, ist Bitcoin voluntaristisch: Jeder kann sich anschließen, jeder kann das Programmieren lernen und versuchen, Verbesserungen einzubringen, jeder kann andere darüber aufklären, ohne eine Lizenz von einer Autorität zu benötigen, und jeder kann ein Node betreiben oder minen. Mit anderen Worten, wir sind alle eigenverantwortlich und wir können einen bedeutenden Schritt machen. Jetzt, da wir den FUD theoretisch kennen, können wir ihn auch in der Praxis entkräften.

Europe's biggest BITCOIN Store

SHOPINBIT

800.000 Products

Free Shipping from 21€

3% Discount with Bitcoin/Lightning



Our Premium Services:

CONCIERGE SERVICE

Get anything.
We ship it worldwide.

TRAVEL SERVICE

Go anywhere.
Get the best deals.



Also part of the SHOPINBIT Family: PLEBBIN.COM



Breaking FUD

Wie Die Hingabe Eines Vaters Einen Skeptiker Zu Bitcoin Führte

Dieser Artikel wurde von Grafton Clark verfasst, mit Unterstützung seines guten Freundes Garry Rominger. Grafton ist technischer Schriftsteller bei Trezor und ein echter Verfechter des Bitcoin-Peer-to-Peer-Handels bei Vexl. Er ist auch der beste Freund von Ash, dem flauschigsten und datenschutzfreundlichsten Hund in der Bitcoin-Welt. Folge Grafton auf Twitter unter @SatsDisco.

Garry und ich sind seit fast 13 Jahren Freunde – vereint durch unsere Liebe zu Videospielen, fleischigen Mahlzeiten, spontanen Ausflügen zu Burgen und unvergesslichen Roadtrips nach Berlin, um Konzerte wie von Billy Strings zu besuchen. Unsere Freundschaft wuchs, während wir unzählige Abende online verbrachten und Call of Duty spielten. Zwischen den Runden würden wir über alles mögliche chatten: von unseren Jobs und neuen Filmen bis hin zu Mädchen und Philosophie.

Während ich eine Karriere in der Welt von Bitcoin verfolgte, vertiefte mein wachsendes Wissen in diesem Bereich meinen Fokus auf Privatsphäre und finanzielle Freiheit in allen Aspekten meines Lebens. Bitcoin wurde natürlich zu einem wesentlichen Bestandteil meines beruflichen Lebens und zu einem wiederkehrenden Gesprächsthema mit Garry. Trotz seiner anfänglichen Vorbehalte ("Nein, Mann, das ist viel zu volatil, und ich habe keine Ahnung vom Handel mit Aktien oder so etwas.") wurde ich immer leidenschaftlicher darin, meine Erfahrungen und mein Wissen über BTC mit Garry während unserer In-Game-Chats zu teilen.

Obwohl ich nur eine kurze Zeit in der Branche tätig bin, war Bitcoin fast ein Jahrzehnt lang eine bedeutende Präsenz in meinem Leben. Unnötig zu sagen, dass ich unzählige Geschichten erzählt und technische Einblicke mit gerollten Augen und genervten Seufzern geteilt habe, was mich nur dazu motivierte, weiter zu bohren und zu forschen. Ich weiß, dass Satoshi Nakamoto sagte: "Wenn du es nicht glaubst oder nicht verstehst, habe ich keine Zeit, dich zu überzeugen, tut mir leid." ("If you don't believe me or don't get it, I don't have time to try to convince you, sorry."). Aber wenn ich spät in der Nacht Videospiele spiele, habe ich eines und das ist Zeit.

Garry ist kein überambitionierter Mann. Er sagte immer: "Solange die Miete bezahlt ist und Essen auf dem Tisch steht, bin ich zufrieden." Aber ich kenne ihn, und ich weiß, dass er immer einen Weg findet, Geld für Dinge für sich und seine Familie auszugeben, das er eigentlich nicht hat. Ich konnte sehen, dass seine Haltung gegenüber Bitcoin offener wurde. Trotzdem hinterließen Schwierigkeiten beim Erwerb von Bitcoin (ein Amerikaner, der in der EU lebt, ohne eine Adresse oder ein Bankkonto in seinem Heimatland zu haben, machte es ihm schwer, die potenziell erworbenen Währungen abzuheben) einen bitteren Geschmack in seinem Mund.

Man kann vielleicht verstehen, warum der überarbeitete Familienvater von diesem neuen finanziellen Vorhaben abgebracht wurde. Obwohl er den Wert all dessen sah, was ich zu erklären versuchte, hatte er immer noch Ängste vor den wahrgenommenen Risiken, und jedes Mal, wenn er den Mut aufbrachte, in die Welt von Bitcoin einzutauchen, wurde er mit neuen Hindernissen konfrontiert. Für Garry schien Bitcoin vorübergehend außer Reichweite.

Garrys zweites Kind wurde gerade geboren, und das Spielen von Videospielen wurde ein noch wichtigeres Bindungsinstrument mit seinem ältesten



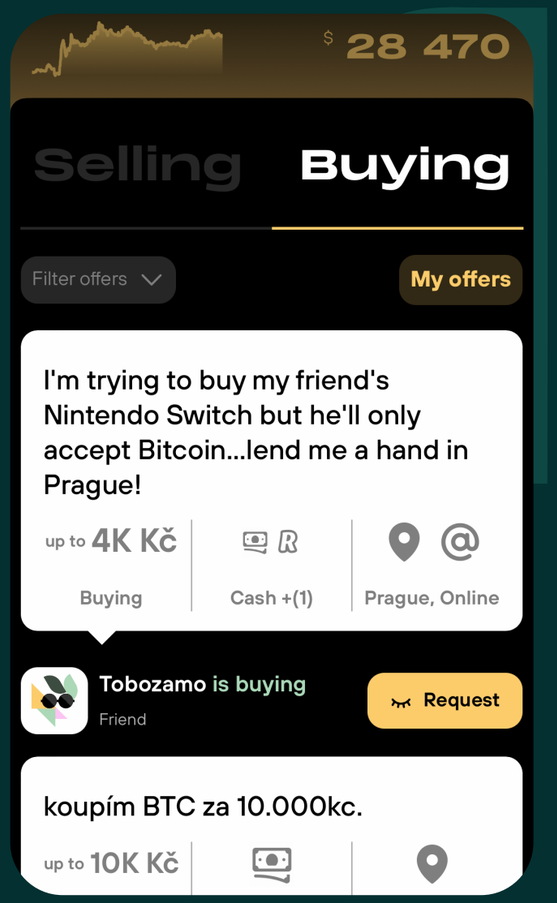
Gefällt dir der Artikel?

Scanne den QR-Code und hinterlasse ein Kommentar oder eine Donation!

Kind. Er hatte es auf eine Nintendo Switch abgesehen. 2017 kaufte ich genau eine solche Videospielkonsole bei einem örtlichen Elektronikgeschäft, das gerade angefangen hatte, Bitcoin zu akzeptieren. Ich wurde jedes Mal daran erinnert, wenn ich das Klicken der Konsole beim Starten hörte. Ich wurde wieder daran erinnert, als ich hörte, dass er bei seiner Suche nach einer preisgünstigen Switch sofort auf dem Facebook Marketplace betrogen wurde.

Obwohl ich Mitgefühl für seine Situation empfand, nachdem ich davon erfahren habe, verspürte ich einen Hauch von Schadenfreude. Sobald wir aufhörten zu lachen, traf ich die Entscheidung, ihm meine Nintendo Switch zu einem, zugegebenermaßen, ausgezeichneten Preis anzubieten. Es gab jedoch einen Haken: Ich wollte in Bitcoin bezahlt werden, und ich würde keine meiner eigenen Coins gegen Fiat verkaufen..

Garry war nun mit einem realen Grund konfrontiert, Bitcoin zu erwerben, und war entschlossen, es geschehen zu lassen. Durch den Chat während des Spiels half ich ihm schnell dabei, eine Lightning Wallet einzurichten, und wir übten das Hin- und Herschicken von Sats. Das waren seine ersten Bitcoin-Transaktionen überhaupt. Er war erstaunt, wie einfach es war, was sein Vertrauen stärkte. Nach dieser Erfahrung war er Feuer und Flamme, sein ersten Bitcoin zu kaufen. Also stellte ich ihm Vexl vor, eine mobile App, die es ihm ermöglichte, Bitcoin ohne einen lästigen KYC-Prozess und ohne den Umgang mit einer Finanzinstitution zu kaufen. Peer-to-Peer, so wie es gedacht war.

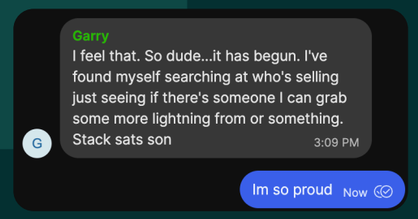


Garry lud die App herunter und erstellte schnell ein Angebot. Innerhalb von Minuten fand er jemanden, der bereit war, Bitcoin zu handeln. Er hatte endlich sein schmutziges Fiat-Geld in Bitcoin umgewandelt. Ende der Transaktion, keine Dokumente, keine Stromrechnungen, keine Schwierigkeiten. Garrys erster Bitcoin-Kauf verlief so, wie viele von uns es sich gewünscht hätten.

Anschließend schickte er mir Bitcoin - und im Gegenzug übergab ich ihm mit Freude die Nintendo Switch für seinen Sohn. Ich war mehr als bereit, die Bitcoin, die ich vor vielen Jahren für die Switch ausgegeben hatte, wieder zu erhalten. Es brauchte eine Anwendung in der realen Welt und jahrelange Freundschaft, damit Garry seine Angst, Unsicherheit und Zweifel überwinden konnte. Heute ist er ein stolzer und aktiver Bitcoiner.

Die Bitcoin-Community hat wirklich einige Fortschritte gemacht, um die Beteiligung an dem Peer-to-Peer-Zahlungssystem zu vereinfachen. Es geht weniger darum, ein Vermögen zu machen, sondern vielmehr darum, einen einfachen und uneingeschränkten Weg zu haben, Geld zu handhaben.

Heutzutage gibt es viele benutzerfreundliche Tools, die Menschen ohne Probleme in Bitcoin einsteigen lassen. Es geht darum, die Kontrolle über die eigenen Finanzen zu haben und dabei das Erlebnis zu genießen. Nimm Garrys Geschichte als Beispiel - er ist in die Welt von Bitcoin eingestiegen und liebt diese jetzt. Ich fühlte mich unglaublich stolz, als ich diese Textnachricht von ihm erhielt, und ich kann es nicht lassen, diese zu teilen:



Die Bitcoin-Community hat es geschafft, Bitcoin nicht nur zugänglich zu machen, sondern auch zu einem unterhaltsamen Erlebnis gemacht. Mit so vielen neuen Möglichkeiten öffnen sich überall für die Menschen die Augen für Bitcoin in einem ganz neuen Licht. Ich habe es wirklich genossen, Garrys "Aha"-Momente zu beobachten, während er seine ersten Schritte in der Welt der Bitcoin-Erkundung unternommen hat. Jetzt, jedes Mal, wenn wir zusammen abhängen, ist er immer bereit, die Rechnung zu übernehmen... solange ich es ihm natürlich in BTC zurückzahle. Es war großartig, Teil seiner Reise zu sein, und ich bin gespannt, wie er seine Begeisterung und Abenteuer mit anderen teilen wird.

HALL OF PLEBS

@Buchiimaine says you should watch the Dirty Coin documentary

King Arctan

@BeggiJonsson

From Dragoș M. to Marian A. "Bro, everything is seen!"

Ionuț Bogdănel Herghelegiu

Iulian Șerban (Zece)

tweetious

Travin "Tavern" Keith

@Buchiimaine says no really, you should watch @TheDirtyCoinDoc



David St-Onge says: check out my book "Bitcoin: Everything You Need to Know"



Daniel Ses @ iBlock.ro

Mopar Mining @ CryptoCloaks.com

@Florinqw9

Max Hillebrand

@Buchiimaine says: let's go Brandon... to El Salvador 🇸🇻

Asanoha

@BTCparadigm says: "you are an idiot. eat mushrooms and buy bitcoin"

