

@anilsaidso

BITCOIN

IRRTÜMER



Diese Äußerung ist
umstritten!

"Bitcoin ist ein radikaler Bruch mit der Vergangenheit, deswegen hilft das Verständnis über die Funktionsweise des bisherigen Geldes nicht dabei, Bitcoin zu verstehen.

Wenn überhaupt, ist es hinderlich.

Die Leute, die Bitcoin am wenigsten verstehen, sind Währungsökonominnen.

Sie kriegen es nicht in ihre Köpfe."

—Andreas M. Antonopoulos

" es sollte verboten werden."

—Joseph Stiglitz

" Die Volatilität von Bitcoin macht es für die meisten Unternehmen unattraktiv, ihn anstelle von Bargeldreserven zu halten."

—Steve Hanke

"Bitcoin hat sich auf eine Billion Dollar an Marktkapitalisierung hochgearbeitet, die Rendite erinnert an das Drucken von Falschgeld,"

—Jeffrey Sachs



DIE 3 TÖPFE DER KRITIK

SPEKULATIV /
UNFAIR

- BLASE
- ZU VOLATIL
- UNBESICHERT
- WIRD GEHORTET
- ZENTRALISIERTER BESITZ

VERSCHWENDERISCH /
NUTZLOS

- VERALTET
- ENERGIE-INTENSIV
- LANGSAM
- TEURE GEBÜHREN
- VOM INTERNET ABHÄNGIG

GEFÄHRLICH /
BETRUG

- VON KRIMINELLEN GENUTZT
- PONZI-/PYRAMIDENSYSTEM
- REGIERUNGS-VERBOT
- INFLATIONS-BUG
- KOPIERBAR

IS NE BLASE

Bitcoin wurde schon oft als Blase bezeichnet, von vielen Leuten, über viele Jahre.

Obwohl der Bitcoin-Preis viele starke Rückgänge erlebt hat, die diese Bezeichnung rechtfertigen würden, geht der Gesamttrend spektakulär nach rechts oben.

Kritikern, die nach jedem Marktzyklus den *Tod* Bitcoins ausrufen, gehen dankenswerterweise die Vergleiche aus, die als das entlarvt werden, was sie sind — **falsch.**



Volatilität ist subjektiv. Die Erwartung, dass der Bitcoin-Preis sich in irgendeinem ausgedachten Bereich bewegt, ist haltlos.

Bitcoin wird rund um die Uhr in fast jedem Land der Welt gehandelt. Es gibt keine Anmelde-Bedingungen, Bank-Feiertage, Sicherheitssysteme, oder Rettungspakete. Es ist ein wahrhaft freier Markt. Jegliche Volatilität ist das Ergebnis von Käufern und Verkäufern, die in Echtzeit miteinander verhandeln, ganz ohne die Einmischung von Regierungen.

Bitcoin ist auf dem besten Weg, der primäre globale Wertespeicher des Informations-Zeitalters zu werden. Der Glaube, dass er auf dieses Ziel linear ansteigt, ist verrückt.

Mit wachsender Adoption wird Bitcoin immer risikoärmer, weiteres Wertsteigerungspotenzial wird kleiner, und die Volatilität geringer.



ZU VOLATIL!

UNBESICHERT

UNBESICHERT



Das Konzept von *besichertem Geld* ist ein Widerspruch an sich, denn dann wäre das, was es *besichert*, ja das eigentliche Geld.

Geld leitet einen Teil seines Werts von Seltenheit ab. Bitcoin braucht keine Besicherung durch andere seltene Dinge, weil er inherent absolut selten ist. Da er unabhängig verifizierbar und kontrollierbar ist, ist Bitcoin völlig frei von Gegenpartei-Risiko. Es gibt nicht irgendwo eine Drittpartei, der vertraut werden muss, irgendwelche Rohstoffe oder Wertgegenstände zu halten und zu sichern. Wenn überhaupt, wird in Zukunft wahrscheinlich Bitcoin die Besicherung sein.

" Letztendlich ist Bitcoin von etwas besichert, und es ist das Einzige, das jede Form von Geld besichert: die Glaubwürdigkeit seiner monetären Eigenschaften."

—Parker Lewis

SELTENHEIT
TEILBARKEIT
BEWEGLICHKEIT
HALTBARKEIT
ERKENNBARKEIT

ER WIRD **OBSOLET** WERDEN

Bitcoin repräsentiert die einmalige Entdeckung von absoluter Knappheit. Er ist ein einzigartiges Ereignis, wie die Entdeckung des Feuers, der Elektrizität oder der Mathematik. Mit Bitcoin um diese Eigenschaft zu konkurrieren, ist sowohl unlogisch als auch unmöglich.

Es gibt keine Steigerung von absoluter Knappheit.

Die Kritik zu Bitcoins aktuell wahrgenommenen Einschränkungen oder Nachteilen nimmt an, dass ein Zusammenspiel zwischen Sicherheit und Anreizstrukturen nicht existiert oder dass Bitcoins aktueller Zustand nicht schon jetzt immense Vorteile für Millionen von Nutzern bringt.

Als ein exponentiell wachsendes, frei zugängliches Netzwerk, das über 99.98% der Zeit seit mehr als einem Jahrzehnt online ist, Billionen von Dollar an Wert überträgt und von Milliarden Dollar an Hardware gesichert ist, ist es für Bitcoin zu diesem Zeitpunkt unwahrscheinlich, dass es als das dominante digitale Geld- und Zahlungsnetzwerk abgelöst wird.

“ Es gab noch nie ein Beispiel für ein Hundert-Milliarden-Dollar schweres Monster-Digitalnetzwerk, das noch bezwungen wurde, nachdem es die dominante Position erreicht hat.”

—**Michael Saylor**



AUSUFERNDER ENERGIEVERBRAUCH

Bitcoin ist global verfügbares, hartes und zensur-resistentes Geld aufgrund seines "Proof of Work"-Mechanismus.

Für geschätzt 4 Milliarden Menschen, die aktuell unter irgendeiner Form von autoritärem Regime leben, bietet Bitcoin eine Möglichkeit, Werte zu versenden, zu erhalten, zu sparen and zu transportieren.

Frag dich selbst—wie hoch ist die Menge an Energie, die so ein monetäres Netzwerk verbrauchen darf? Und viel wichtiger: Wieso bist du die richtige Person, das zu beurteilen?

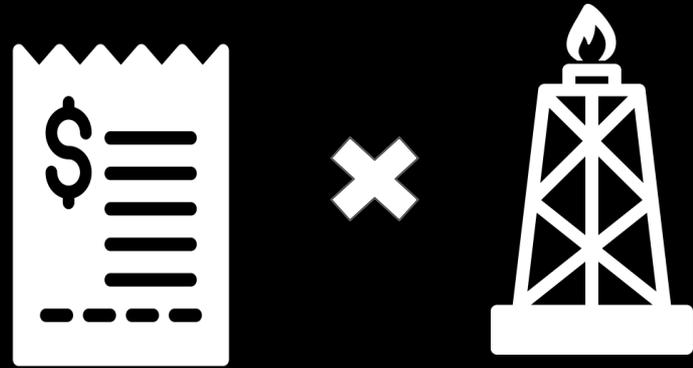
“Stell dir eine topografische Karte der Welt vor, aber mit den lokalen Elektrizitätskosten als Variable für die Berge und Täler. Bitcoin als Verbraucher hinzuzufügen, ist wie ein Glas Wasser über die 3D-Karte zu schütten – es fließt in die Täler und ebnet sie. Denn Bitcoin ist ein globaler Käufer für Energie zu einem festen Preis.”

—Nic Carter



MONETARISIERUNG ÜBERSCHÜSSIGER ENERGIE

Bitcoin-Mining bietet eine höchst mobile Abnahmemöglichkeit für Energie, die in Regionen ohne aktuelle lokale Nachfrage oder Transportmöglichkeiten vorhanden ist. Durch die Verwendung lokaler Mining-Anlagen können Bitcoin geschürft werden. Diese können dann zur weiteren Wertsteigerung gehalten oder in den hoch liquiden, globalen, freien Markt verkauft werden.



“Den Markt auf die atomare Ebene zu bringen ist sehr mächtig.”

—**Marty Bent**

INTERNET-ABHÄNGIG

Die Gefahr, aufgrund von Infrastruktur-Ausfall, Naturkatastrophen oder absichtlichen Unterbrechungen Zugang zum Internet zu verlieren, ist eine berechtigte Sorge. Glücklicherweise gibt es verschiedene Möglichkeiten, Bitcoin offline oder über andere Telekommunikationskanäle zu übertragen.

Im Fall von on-chain-Transaktionen muss eine signierte Transaktion lediglich eine einzige Node erreichen, um an das gesamte Netzwerk für die Einbeziehung in einen zukünftigen Block durch die Miner gesendet zu werden. Ein paar der unterschiedliche Methoden, um die Übertragung auf ein mit dem Internet verbundenes Gerät zu erreichen, sind..

.. via SMS, durch Weiterreichen eines physischen Wallets, das einen einmalig benutzbaren, manipulationssicheren Private Key enthält, oder über das Empfangen neuer Blöcke per Satellit.



BITCOIN OFFLINE VERSENDEN

SATELLIT
(BLOCKSTREAM)



**KURZWELLEN-
RADIO**



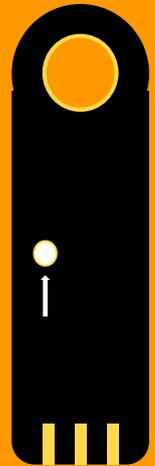
SMS



**MESH
NETZWERK**



**PHYSISCHES
WERKZEUG**

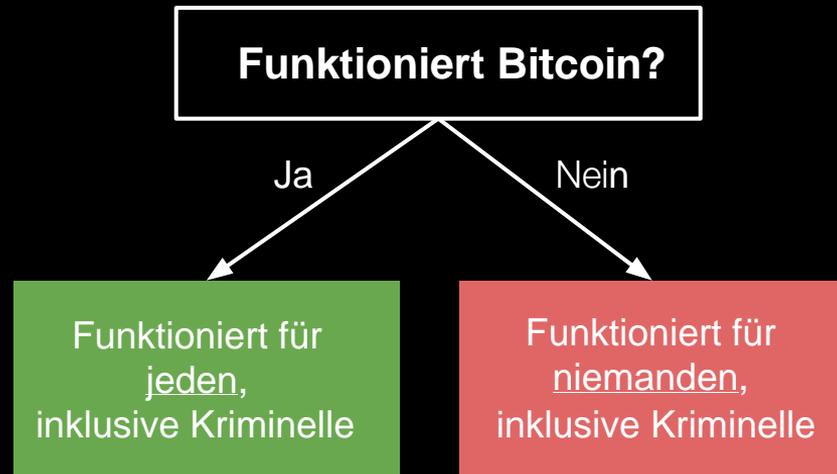


ERLEICHTERT VERBRECHEN

Bitcoin ist ein neutrales Netzwerk zur Übertragung von Wert. Es hat keine intrinsischen Überzeugungen, Meinungen oder moralischen Werte. Menschen geben Bitcoin Bedeutung durch seine Verwendung.

Das Argument, dass Bitcoins Eigenschaften zu einem Netto-Anstieg an kriminellen Aktivitäten geführt haben, hält einer genauen Prüfung nicht stand.

Kriminalität entsteht nicht durch den Zugang zu neuen Werkzeugen, sondern durch individuelle Umstände.



Quelle: *Bitcoin Is Not For Criminals* (2019)

“Es ist nichts inherent Kriminelles an den Werkzeugen, die für Verbrechen verwendet werden. Trotz krimineller Verwendung ist niemand für das Verbot von Straßen, dem Internet, Briefpost, etc.”

—Parker Lewis

PONZI-SCHEMA

Bitcoin als Ponzi-Schema zu bezeichnen, zeigt sowohl mangelndes Verständnis von Bitcoin als auch von der Definition eines Ponzi-Schemas.

Ein Kernelement eines Ponzi ist ein **überdurchschnittliches Wertversprechen** für Investoren. Als frei zugängliches Netzwerk hat Bitcoin keine zentrale Autorität, die so ein Versprechen geben könnte. Noch viel fundamentaler, Bitcoin ist kein Investmentprodukt, es ist **Geld** in sich selbst.

Außerdem, im Gegensatz zu den undurchsichtigen Investmentprodukten, die ahnungslosen Privatanlegern beworben werden, ist Bitcoins Code open-source und seine Umlaufmenge unabhängig zu jeder Zeit verifizierbar.



LANGSAM

Die Abwicklung einer Bitcoin-Transaktion auf der Haupt-Chain ist nicht das Gleiche, wie einen Taco mit der Kreditkarte zu bezahlen. Selbst dann, auch wenn es so aussieht, als wär die Zahlung sofortig, läuft sie tatsächlich durch mehrere Gegenparteien, bevor sie nach mehreren Tagen der Bearbeitung ins Bankkonto des Händlers gebucht wird. Mit Bitcoin versendest du keine Schuldscheine.

Du schickst hartes Geld **direkt** zum Empfänger, ohne Mittelsmänner oder Zensurrisiko, und mit der Sicherheit der Zahlungsfinalität, sobald die Transaktion bestätigt wurde.

Sechs Blöcke klingen plötzlich gar nicht mehr nach so einer langen Zeit.



"Der richtige Vergleich wäre zwischen Bitcoin und der nationalen Notenbank; als Herausgeber der Währung und als Clearing-Mechanismus."

—**Parker Lewis**

"Bitcoin für alltägliche Käufe zu nutzen, ist wie einen Concorde-Jet die Straße entlang zu fahren, um Lebensmittel einzukaufen: eine absurd teure Verschwendung eines beeindruckenden Werkzeugs."

—**Saifedean Ammous**

KORRUMPIERBARE UMLAUFMENGE

Sich für ein gemeinsames Set an Regeln entscheiden. Jeder kann den Code forken und seine eigenen Regeln hinzufügen, aber niemand wird diese Version benutzen.

Bitcoin's Anziehungskraft kommt von seinem unkorruptibaren Bestand, der durch seinen dezentralen Konsens erreicht wird, in dem jeder Knotenpunkt des Netzwerks jede Transaktion, die jemals im Bitcoin-Netzwerk getätigt wurde, verifiziert.

“Glaubt mir, jemand kriegt es hin, mehr Bitcoin zu erschaffen. Wenn sie dir sagen, dass es Regeln gibt, dass sie es nicht tun können, glaubt ihnen nicht. Wenn der Anreiz groß genug ist, werden schlimme Dinge passieren.”

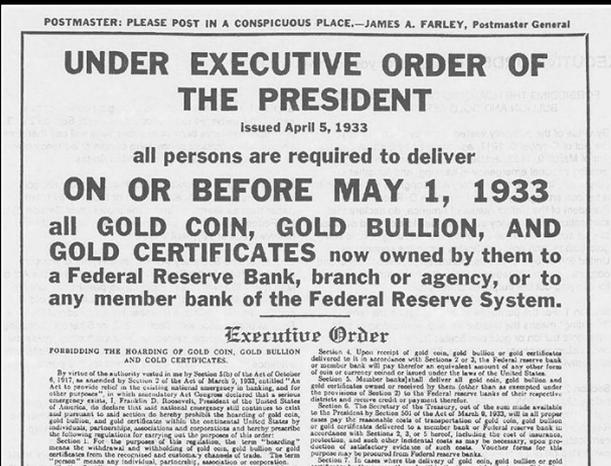
—Charlie Munger

ES WIRD VERBOTEN

Um fair zu sein: Bitcoin kann verboten werden. Aber die Durchsetzung dieses Verbots ist aussichtslos. Das liegt daran, dass Bitcoin Geld in reine Information verwandelt hat (ein Private Key ist einfach eine zufällige 256-bit Zahl). Bitcoin zu verbieten würde bedeuten, die Erstellung zufälliger Zahlen zu verhindern. Viel Glück dabei, das zu erreichen!

“ Bitcoin zu verbieten ist nicht viel anders als der Versuch, Mathematik zu verbieten. Es wird nur seinen Nutzen zeigen und weitere Menschen anziehen.”
—Saifedean Ammous

Auch wenn Bitcoin-Transaktionen auf der Blockchain sehr transparent sein können, sind die Standorte der Private Keys, die den Zugriff darauf verwalten, größtenteils unbekannt. Außerdem ist die Infrastruktur, die erforderlich ist, auf das Bitcoin-Netzwerk zuzugreifen, trivial, solange grundlegende Computer-Hardware vorhanden ist.



KONZENTRIERTER BESITZ

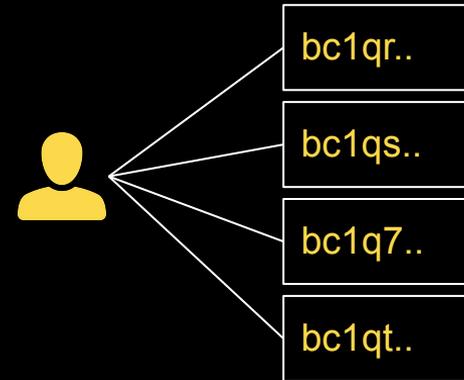
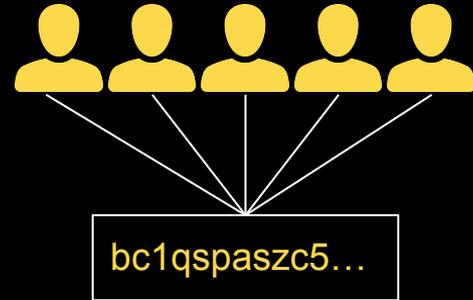
Wie oft hast du die gleiche, alte Aussage gehört:

“ Ein paar Wallets besitzen den Großteil aller Bitcoin!”

Das stimmt, aber eine wichtige Klarstellung fehlt. Das sind in der Regel Wallets von Börsen, jede mit Millionen von Kunden. In einer idealen Welt würden die Menschen ihre Bitcoin nicht auf den Börsen lassen, aber das ist ein Thema für einen anderen Tag.

Auf einer einzigen Bitcoin-Adresse können Bitcoin liegen, die mehreren Menschen gehören und ein einzelner Nutzer kann mehrere Wallets besitzen. Tatsächlich gehört zu den besten Möglichkeiten, die eigene Privatsphäre zu schützen, dass man für jede neu eingehende Transaktion eine neue Adresse generiert.

Viele Nutzer, eine Adresse



Ein Nutzer, viele Adressen

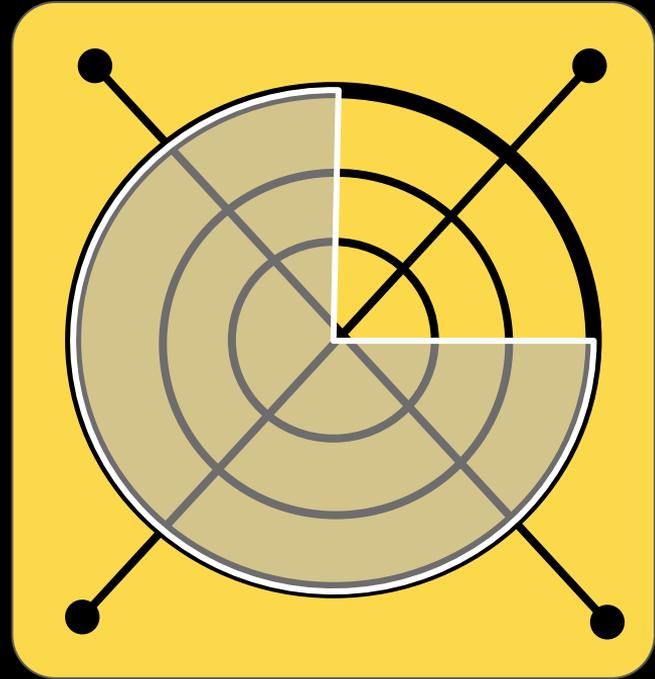
ZENTRALISIERTES MINING

Die Vorstellung einer Bedrohung, dass Mining-Pools zusammenarbeiten, um irgendwie das Netzwerk zu sabotieren, Transaktionen zu zensurieren, oder Bitcoin doppelt auszugeben, kommt vom mangelnden Verständnis des Anreizmechanismus für Miner und ihre Kontrolle über das Netzwerk und die Blockchain.

*"Eine Mehrheit der hashing power **kann nicht***

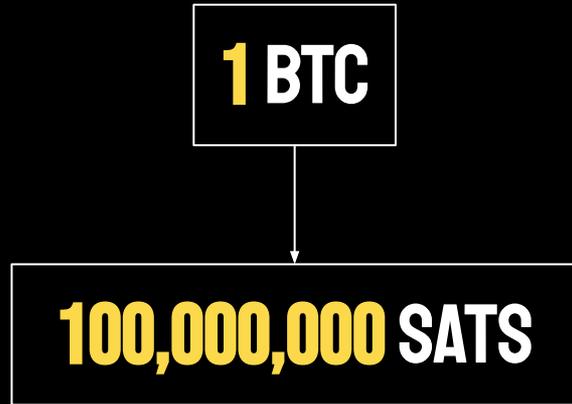
- dir die Coins nehmen, die du schon besitzt*
- die Regeln von Bitcoin verändern*
- dir schaden, ohne sich selbst zu schaden"*

—**Jimmy Song**



ZU TEUER

Bitcoin's Stückpreis mit dem von anderen Assets (z.B. 1 Bitcoin zu 1 Unze Gold) zu vergleichen, zeigt die **Einheiten-Befangenheit (unit bias)**. Es ist korrekter, die gesamte Marktkapitalisierung von Bitcoin mit der von anderen Assetklassen zu vergleichen. Außerdem ist ein einzelner Bitcoin in **100 Millionen kleinere Einheiten** (Satoshis) teilbar. Die Maxime lautet: "Du kannst auch einen Bruchteil eines Bitcoins kaufen!"



UNERSCHWINGLICHE TRANSAKTIONSgebÜHREN

Bestätigte Transaktionen auf Bitcoin's Haupt-Layer bieten eine Gewissheit über ihre Endgültigkeit, die im klassischen Finanzsystem nicht erreicht werden kann.

Deswegen können Transaktionsgebühren zu bestimmten Zeiten sehr teuer sein, aber das Bitcoin-Netzwerk bleibt eine unglaublich effiziente und zuverlässige Verrechnungsebene für höherwertige Transaktionen.

Kleinere Transaktionen (inkl. Mikrotransaktionen) finden immer mehr auf einer zweiten Ebene (z.B. Lightning, Liquid oder föderierte Side-Chains) statt, wo die Gebühren bei Weitem günstiger sind als alles, was sich eine traditionelle Bank leisten könnte.



*"Zwischen Oktober 2010 and Juli 2021 lagen die durchschnittlichen täglichen Transaktionsgebühren bei etwa **0.02%** des Transaktionswertes."*

—Saifedean Ammous

(The Fiat Standard)

ES WIRD GEHORTET

Ein Argument, das in der Zeit billiger Schulden wieder auflebt, besagt, dass ein Geld mit festgelegtem Bestand zum *Horten* anregt, bei dem Besitzer ihre Bitcoin nicht in der Wirtschaft verwenden, sondern nur die Hände in den Schoß legen und der Wertsteigerung zusehen.

Es gibt ein paar Probleme mit dieser Logik, allem voran, dass sie ein Verhalten demonisiert, das man als *Sparen* bezeichnet (Überschuss an Einkommen > Ausgaben).

Sparen in Horten umzudeuten ist wie dafür zu plädieren, dass man von Gehalt zu Gehalt leben sollte. Jedes sinnvolle Investment braucht vorher gespartes Kapital (zumindest war das die Logik, bevor die Banken angefangen haben, Geld in die Existenz zu leihen).



" Das Halten von Geld dient der Absicherung gegen zukünftige Unsicherheiten.

Ja, auch das Halten von Bitcoin bedeutet, Bitcoin zu nutzen. Alle Bitcoin werden immer von irgendwem gehalten, durch Zahlungen ändert sich lediglich der Besitzer."

—Pierre Rochard

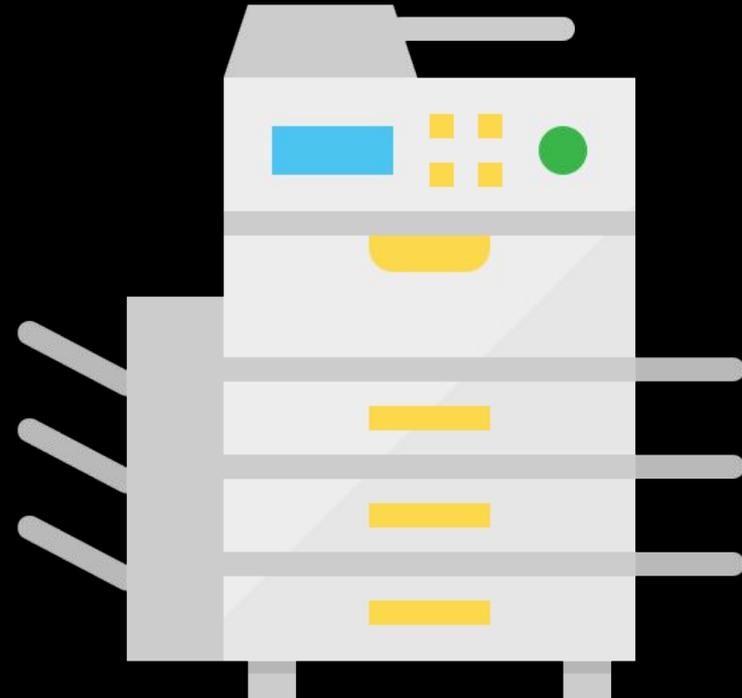
KANN KOPIERT WERDEN KOPIERT

Kritik: Bitcoin ist nicht selten, denn es gibt tausende andere Kryptowährungen da draußen und außerdem kann jeder den Bitcoin-Code kopieren und seine eigene Version erstellen.

Bitcoin ist ein open-source Protokoll zum Übertragen von Wert. Ja, jeder kann es forken oder versuchen, eine identische Kopie zu starten. Aber du kannst nicht alle Entwickler, Miner & hash power, die Benutzer, Node-Betreiber oder darauf aufbauende Produkte mitnehmen. Bitcoin zieht Menschen und Ressourcen genau wegen seiner Transparenz und dem strikten Entwicklungsprozess an.

" Open-source ist im Großen und Ganzen eine Leistungsgemeinschaft. Du hast ein Schwarmbewusstsein, das Lösungen baut. Du bekommst die gesamte Überprüfung, die sich direkt in Sicherheit übersetzt. Bitcoin Core ist wahrscheinlich die mit am intensivsten überprüfte Codebase der Welt."

—@BTCSchellingPt



DIE REISE EINES BITCOINERS

Es braucht wenig Talent, um sich **100 Gründe** auszudenken, wieso Bitcoin scheitern wird.

Aber es braucht ehrliche Neugier, um diese Gründe unabhängig und systematisch zu entkräften, einen nach dem anderen, von Grund auf.

Auf diese Weise werden Bitcoiner **geschmiedet**.



GRAHAM'S UNEINIGKEITS-HIERARCHIE

Übernommen aus 'How to Disagree' (2008) von Paul Graham

Übersetzt von: @BitsKnowledgeDE
www.bitsofknowledge.de

Beweise gegen ein Argument finden, von dem du glaubst, dass es fehlerhaft ist und dann erklären, **wieso** es fehlerhaft ist.

Den **umgekehrten** Fall beschreiben mit wenig oder keinem Beweis.

Den **Charakter** des Gegenüber angreifen

Den **zentralen Punkt** widerlegen

Widerlegung

Gegenargument

Widerspruch

Auf den Ton antworten

Ad Hominem

Beschimpfen

Den zentralen Punkt des Gegenüber erfolgreich **identifizieren**, bevor man dagegen argumentiert.

Widerspruch **plus** Argumentation und/oder Beweis. Direkt auf das ursprüngliche Argument bezogen.

Gereizt reagieren auf einen **Ton**, den andere als neutral empfinden

Die **unterste** Form der Uneinigkeit.

DIE **VIER** KRITIKER VON BITCOIN

laut Alex Gladstein

“Du könntest eine Ausnahme sein, aber praktisch alle Bitcoin-Kritiker fallen in eine dieser 4 Kategorien:”

Der Salty Hater

“ Du hast vor Jahren von Bitcoin gehört, aber nie gekauft und bist deswegen salty.”

Der Verzweifelte Staatist

“ Du denkst, Geld kann nur vom Staat erschaffen werden, deswegen zerbricht Bitcoin deine Weltanschauung.”

Der Unehrlliche Intellektuelle

“ Du hast dir nicht die Arbeit gemacht, Bitcoin zu verstehen und wünschst dir deshalb, dass es einfach wieder verschwindet.”

Der Gefangene der Versickerten Kosten

“ Du hast in einen Altcoin investiert und hast das Gefühl, Bitcoin kritisieren zu müssen, um diese Lebens-Entscheidung zu rechtfertigen.”



 @anilsaidso

Danke fürs Lesen!

Poste ein Review auf Gumroad und hilf dabei, Bitcoin FUD zu reduzieren, indem du dafür sorgst, dass andere die Slides finden.

*Du darfst alle Folien gratis mit Urheber-Kennzeichnung für nicht-kommerzielle lehrende Zwecke nutzen

Hi! Und vielen Dank, dass du auch die letzte Folie liest.

Ich bin Bits of Knowledge und habe die Arbeit von Anil ins Deutsche übersetzt. Besuch gerne bitsofknowledge.de/anilsaidso für alle Übersetzungen.



@BitsKnowledgeDE