

Blockchain und Distributed-Ledger-Technologie: Transformation der Finanzwelt

Oft in den Nachrichten figuriert, wird Blockchain die Finanzmärkte stark verändern und die Branche in allen Bereichen revolutionieren.

Elementum Metals: 25/02/2021

25/02/2021



Begleitend zu unserem Webinar über den aufstrebenden Blockchain-Sektor, haben wir einige der Fragen unseres Publikums beantwortet, die technische Anfragen, Vergleiche und Kontraste und sogar den Einfluss von Internet-Memes umfassten.

Haben Sie eine weitere Frage an unser Team? Nutzen Sie unsere Kontaktseite, um sich mit uns in Verbindung zu setzen.

Was sind die Unterschiede zwischen öffentlichen, privaten und permissioned Blockchains?

Öffentliche Blockchain: Ist eine Blockchain, bei der jeder mitmachen und sich an den Aktivitäten des Blockchain-Netzwerks beteiligen kann. Diese Blockchains sind dezentralisiert, was bedeutet, dass keine einzelne Einheit die Kontrolle über das Netzwerk hat. Beliebte Beispiele sind Bitcoin und Ethereum.

Private Blockchain: Eine Blockchain, die es nur autorisierten Mitgliedern erlaubt, dem Netzwerk beizutreten. Der Betreiber hat das Recht, die notwendigen Einträge in der Blockchain zu überschreiben, zu bearbeiten oder zu löschen. Hier gibt es eine Zentralisierung. Beispiele sind Ripple und Hyperledger.

Permissioned/Hybrid Blockchain: Hat Eigenschaften von privaten und öffentlichen Blockchains. Sie werden aufgrund ihrer Fähigkeit, verschiedenen Benutzern im Netzwerk bestimmte Berechtigungen zuzuweisen, immer beliebter. Dies variiert von Plattform zu Plattform, und viele sind viel kleiner als die etablierteren Namen.

Die Investitionsthese hinter dezentralem Finanzwesen ist sehr solide - beispielloses

Geld drucken durch die Zentralbanken wird wahrscheinlich zu einer Entwertung führen, und ein nicht-fiat-Wertaufbewahrungsmittel ist ein großartiger Weg, um sich dagegen zu schützen. Meine Frage ist - warum Blockchain? Welche Vorteile hat sie gegenüber anderen sicheren Zahlungsnetzwerken? Im Fall von Bitcoin scheint es klobig - energieintensiv, verbissene Geschichte (Schwarzmarkt), und die Tatsache, dass jede Transaktion von jedem auf der Welt verifiziert werden muss, scheint ineffizient?

Eine großartige Frage, die sich aus mehreren Komponenten zusammensetzt. Erstens: Warum sollte man Blockchain für Zahlungen verwenden? Blockchain ist unveränderlich, demokratisch, dezentralisiert und in einem Code geschrieben, der nicht verändert werden kann. Das gibt ihr einen unangreifbaren Vorteil gegenüber anderen sicheren Zahlungsnetzwerken (Stripe, Apple Pay etc.), die grundsätzlich zentralisiert sind. Wenn ich eine Zahlung über eines dieser Unternehmen tätige, wird diese Transaktion von diesem einen zentralisierten Unternehmen überprüft, genehmigt und verwaltet. Dies kann mit Sicherheitsrisiken (ein einziges zentralisiertes Ziel für Hacker), höheren Kosten (eine einzige zentralisierte Stelle kann Gebühren auf Transaktionen erheben) und undemokratisch (ein einziges zentralisiertes Unternehmen kann seine eigenen Bedingungen festlegen) verbunden sein.

Blockchain hingegen erlaubt es, die Infrastruktur von Grund auf aufzubauen. Das bedeutet, dass Sie die Wirtschaft und die Geldversorgung einmal zu Beginn entwerfen und definieren, und niemand kann später zusätzliches Geld "drucken" - das hilft bei dem von Ihnen erwähnten Vorteil der "Wertaufbewahrung". Bitcoin hat versucht, dies zu tun (es hat einen begrenzten Vorrat von 21 Millionen Bitcoins, die gemined werden können), aber wie Sie sagen, ist es mit vielen Ineffizienzen verbunden, nicht zuletzt mit dem intensiven Energieverbrauch, der für das Mining der Münzen erforderlich ist (siehe Frage 4, unten, für mehr dazu). Jede Transaktion, die von anderen Nutzern verifiziert werden muss, sollte jedoch nicht als eine dieser Ineffizienzen betrachtet werden, sondern eher als eine Stärke des Systems - es umgeht die Notwendigkeit einer zentralisierten (und daher anfälligen und potenziell teuren) Plattform, die anderen sicheren Zahlungssystemen innewohnt.

Während es Ihr gutes Recht ist, die Schwarzmarkt-Geschichte von Bitcoin anzumerken, ist dies eher ein Spiegelbild der Aktivitäten von frühen Anwendern als ein Zeichen von Schwächen - nur wenige würden argumentieren, dass physische Währung völlig abgewertet werden sollte, weil sie in der Vergangenheit für ruchlose Zwecke verwendet wurde.

Was könnte es also noch geben? Neue Blockchain-basierte Zahlungskonzepte tauchen auf, sowohl für Groß- als auch für Massenzahlungen, einige sind dezentral, andere eher zentralisiert. Beispiele hierfür sind:

- Ripple: wird für dezentrale Interbanken- und grenzüberschreitende Zahlungen

verwendet, wickelt weltweit Transaktionen in 3 -5 Sekunden ab und wickelt 1.500 Transaktionen pro Sekunde mit XRP ab.

- Diem (ex-Libra für den Einzelhandel): Ein zugelassenes Blockchain-Zahlungssystem, das von Facebook vorgeschlagen wurde.
- CBDCs (Central Bank Digital Currencies): Diese entstehen auf der ganzen Welt, wobei China die weltweit erste digitale Zentralbankwährung, bekannt als DCEP, eingeführt hat, die eine digitale Version des Yuan ist und durch Yuan-Einlagen in Chinas Zentralbank gesichert ist.

Zusammenfassend haben Sie also recht, wenn Sie sagen, dass Bitcoin ein klobiges System mit einigen offensichtlichen und zunehmend bekannt gewordenen Nachteilen ist (es bleibt abzuwarten, ob sie behoben werden können). Die Technologie, die Bitcoin zugrunde liegt, d.h. die Blockchain, ermöglicht jedoch eine weitaus größere Effizienz als andere, vertrauere Zahlungssysteme, die in den letzten zwei Jahrzehnten oder so entwickelt wurden.

Was ist der Unterschied zwischen dem "proof of stake consensus", der anscheinend in neuen Blockchains / Kryptowährungen verwendet wird, und dem für bitcoin verwendeten ("proof of work")?

Der Proof of Work (PoW) Mechanismus wird verwendet, um die Bitcoin Blockchain zu sichern und einen Konsens zu schaffen. Er funktioniert, indem alle Knoten (Teilnehmer/Geräte) im Netzwerk mathematische Algorithmen lösen (um Transaktionen als legitim zu verifizieren), wobei der erste Knoten, der eine Lösung findet, belohnt wird (die Miner-Belohnung ist eine Anzahl von Bitcoins). PoW bietet weitere Sicherheitsvorteile für Blockchain, da es die Erstellung eines neuen Blocks auf ca. 10 Minuten verlangsamt, was bedeutet, dass ein Hacker, der einen Block manipulieren will, den PoW jedes Blocks im System erneut durchführen muss, was aufgrund der Größenordnung fast unmöglich ist. Die mit PoW verbundenen Negative sind jedoch wie folgt:

- i. Aufgrund der Mining-Belohnungen entstehen immer größere Mining-Firmen, die riesige Mengen an Strom verbrauchen (kürzlich wurde weithin berichtet, dass das Bitcoin-Mining so viel Energie verbraucht wie ganz Argentinien).
- ii. Um die Chancen einer erfolgreichen Mine zu erhöhen, schließen sich Miner in "Mining-Pools" zusammen, was die Blockchain tatsächlich zentralisierter macht und damit den dezentralen Ethos des Unterfangens untergräbt.

In Online-Foren wurde 2011 ein neuer Algorithmus namens Proof of Stake (PoS) vorgeschlagen, bei dem stattdessen ein Wahlverfahren verwendet wird, bei dem ein Knoten zufällig ausgewählt wird, um den nächsten Block zu validieren. Anstelle von Minern werden Validatoren verwendet, die neue Blöcke prägen/schmieden. Um ein Validator zu werden, muss der Knoten eine bestimmte Anzahl von Münzen als Einsatz hinterlegen (stellen Sie sich das wie eine Kautions vor). Je mehr Sie "einzahlen", desto höher ist die Chance, dass Sie ein Validator werden. Dies ist fairer als PoW, da PoW diejenigen begünstigt, die Skaleneffekte in Bezug auf ihr Mining-Kapital/Energie haben, während die Eintrittsbarrieren bei PoS vergleichsweise niedriger sind. Um sicherzustellen, dass korrekte

Validierungen stattfinden, verlieren Validierer einen Teil ihres Einsatzes, wenn sie betrügerische Transaktionen genehmigen. Solange dieser Verlust größer ist als ihre Belohnung, hält der Konsens durch die Preismotivation an. Schließlich ist PoS dezentraler, da es keine Mining-Pools mehr gibt und es billiger ist, einen Knoten innerhalb der PoS-Blockchain einzurichten.

Die mit PoS verbundenen Negative sind jedoch wie folgt:

- i. 51% Angriffe: Im Gegensatz zu PoW, wo Sie 51 % des Netzwerks erwerben müssen, müssen Sie für PoS 51 % der Marktkapitalisierung der Währung erwerben, was für Kryptowährungen mit kleiner Marktkapitalisierung relativ einfach sein könnte.
- ii. PoS-Algorithmen sind nicht vollständig zufällig, da es vom Einsatz der Validierer abhängt (der reichere Personen begünstigen kann).

Im Moment ist PoS noch nicht verbreitet, obwohl erwartet wird, dass das System in Ethereum 2.0, das 2021 erscheinen soll, verwendet wird.

Irgendein Kommentar zu Tesla und der Entscheidung, Bitcoin statt einer anderen Form von digitalen Assets zu kaufen? Ist es reine Spekulation?

Aus der Perspektive des Unternehmens Tesla könnte es eine Folge der negativen Zinsen und des Treasury-Managements sein, das nach Wegen sucht, wie man die Vermögensverteilung diversifizieren kann. Aus einer Musk-Perspektive ist es schwer zu sagen, was seine tiefste Motivation war. Er investierte sowohl in Bitcoin als auch in Dogecoin, was zu Preissteigerungen bei beiden Kryptowährungen nach seiner Ankündigung der Käufe auf Twitter führte.

Musk sitzt auf einem besonderen Platz, er kann Technologien und Konzepte ausprobieren, die zu einer positiven Marktresonanz führen, unabhängig von jeglichen wirtschaftlichen oder geschäftlichen Gründen. Die Analysten von Wedbush Securities haben geschätzt, dass Tesla bereits \$1 Milliarde Gewinn aus seinen Bitcoin-Investitionen gemacht hat. Das Unternehmen ist auf dem besten Weg, im Jahr 2020 mehr mit seinen Bitcoin-Investitionen zu verdienen als mit dem Verkauf von Elektroautos.

Was die Wahl von Bitcoin und Dogecoin gegenüber anderen Kryptowährungen angeht, sind die Dinge weniger klar. Bitcoin ist bei weitem die größte und offensichtlichsste Wahl, vielleicht deshalb als geringeres Risiko wahrgenommen, während Musk selbst oft ein Image als in die Online-Kultur eingesteckt kultiviert hat - Dogecoin, nachdem zunächst aus Internet-Memes geboren (sowie mit einer Marktkapitalisierung gut in die Milliarden) könnte als ein Teil davon interpretiert werden. Es ist jedoch erwähnenswert, dass er nicht die einzige hochkarätige Persönlichkeit ist, die die Kryptowährung öffentlich unterstützt: behauptete Einträge von Musikern Gene Simmons und Snoop Dogg haben ebenfalls dazu beigetragen, das Interesse zu steigern.

Wie hoch ist die Marktkapitalisierung von Decentralized Finance-Protokollen?

Ab Februar 2021 beträgt die Marktkapitalisierung 45 Milliarden USD.

Wie unterscheidet sich die Rolle von Distributed-

Ledger- Technologie (DLT) im Kapitalmarkt von traditionellen Börsen?

Traditionelle Börsen stellen eine bilaterale, sequenzielle Art der Kommunikation und des Informationsaustauschs dar. DLT hat bereits begonnen, die Wertschöpfungsketten der Kapitalmärkte neu zu strukturieren, indem sie traditionelle Annahmen verändert und Vertrauen ohne menschliche Eingriffe schafft.

DLT kann einen Mehrwert für die Kapitalmärkte schaffen durch:

- i) Gemeinsame Informationen für alle Teilnehmer - Reduzierung der Abstimmungskosten
- ii) Intelligente Verträge - Eliminierung des Kontrahentenrisikos
- iii) Unveränderlicher Audit-Trail - verbesserte Regulierung
- iv) Digitalisierte Prozesse - Ermöglichung der reinen Automatisierung

Die meisten traditionellen Rollen in Kapitalmärkten wie Broker, Börsen und Verwahrer werden auch in einem DLT-Kapitalmarkt weiter bestehen. Es werden jedoch neue Rollen in Verbindung mit den traditionellen Rollen erforderlich sein. Das folgende Diagramm veranschaulicht dies:

```
{"id": "set-36", "enabled":true, "values":{"type": "glideimage", "images": ["page_images::blockchain-environment.png"], "align": "center", "width": "50"}}
```

Quelle: Tokentrust AG

Zu den geänderten Funktionen, Eigenschaften und Entitäten gehören:

- Depotbanken, die über Tresore für digitale Vermögenswerte verfügen, in denen sie private Schlüssel aufbewahren, die für den Zugriff auf Krypto-Wallets und damit auf Vermögenswerte erforderlich sind.
- **Digital Asset Vault**, die Software, die von Verwahrern gekauft wird, um die Speicherung privater Schlüssel zu ermöglichen.
- **Asset Tokenizer**, der durch die Bereitstellung von Smart Contracts rechtskonforme Prozesse ermöglicht, um Finanzinstrumente im Namen des Emittenten zu tokenisieren.
- **Digital Asset Registrar**, der den Konsens zwischen den verschiedenen Interessengruppen erleichtert und das Digital Asset Registry durch die Validierung aller Transaktionen auf der Plattform verwaltet.
- **Gatekeeper**, der den Zugang zur Plattform über KYC/AML-Prüfungen gewährt/einschränkt.
- **Cash on Ledger Issuer**, die die Smart Contracts verwalten und Fiat-Transaktionen über die Bank initiieren und Cash on Ledger-Transaktionen validieren.
- **Cash Tokenizer**, der die Infrastruktur zur Ausgabe von 100% besichertem Bargeld auf dem Ledger für die On-Chain-Abwicklung (Lieferung vs. Zahlungsabwicklung) bereitstellt.

Ein Beispiel aus der Praxis ist die thailändische Börse, die eine Plattform für die Tokenisierung und den Austausch von Vermögenswerten auf Basis von DLT entwickelt. Informationen angepasst von hier.

Welche Rolle spielen von der Zentralbank ausgegebene digitale Währungen (CBDC) für die Tokenisierung der Kapitalmärkte?

Die Tokenisierung adressiert den Bedarf an einem dominanten neuen Format zur Darstellung von Vermögenswerten und Rechten, was zu größerer Flexibilität und Liquidität führt. Da Zentralbankgeld für große Transaktionen weiterhin bevorzugt wird, bleiben CBDCs ein vielversprechendes Medium für den Token-basierten Austausch. Sie funktionieren ähnlich wie die Hartwährungen, jedoch mit digitalen Möglichkeiten. CBDCs können den Bargeldumlauf ergänzen und als Alternative zu Kartenzahlungen dienen. Darüber hinaus können sie diversifizierte Zahlungsformate ermöglichen und den Tausch von Token in Zentralbankgeld erlauben, was weiteres Vertrauen in die Tokenisierung schafft. Schließlich erleichtern CBDCs direkte Zahlungsbeziehungen, wodurch die Notwendigkeit von Intermediären reduziert wird und somit die hohen Transaktionskosten, die wir traditionell auf den Kapitalmärkten sehen, deutlich gesenkt werden.

Zusammengestellt von Jay Kumar, NTree International, für Metal.Digital.

Melden Sie sich für unsere Artikel an

ABONNIEREN