DeFi.jetzt

- 3 -
DeFi 301

mit Thor Alexander, Ralf Knobloch & Mario

Mögliche Anwendungsfälle für DeFi

- Tokenisierung der analogen Welt durch NFT’s (z.B. Immobilien, Quadratzentimeter Mona Lisa, Fahrpreise auf km-Basis)
- Dezentrale Börsen (Tausch Asset1 gegen Asset2)
- Hypothek (Maker-DAO-Stablecoin)
- Standardisierte Kreditaufnahme und Kreditgewährung ohne manuelle Interaktion
- Custody = Depotverwahrung
- Wenn-Dann-Geschäftslogiken, z.B. DEX, Atomic Swaps, Trading/Arbitraging, Versicherungen, zeitgesteuertes Sperren von Token (Sperrfristen)

Einige Hauptmerkmale von DeFi

- DeFi-Anwendungen benötigen keine Vermittler und andere Schiedsrichter-Techniken.
- Der Code legt einen oder wenige Abläufe fest. Die Nutzer von DeFi müssen dem Code vertrauen. Eine Prüfung ist nur durch gute Programmierer möglich. Rechtsanwälte und Gerichte können den Code nicht lesen bzw. verstehen.
- Kostengünstiger, schneller, meist einfacheres dezentrales Finanzsystem trotz zentral gesteuerter Token.
- Alle Regeln sind intrinsisch! (Niemand kann gegen die Regeln verstoßen.)
- Für alle Nutzer gelten die gleichen Regeln
  (keine Korruption, keine Benachteiligung Einzelner, weniger Betrug).
- Einfacher Zugang für Personen ohne Bankkonto.
- Global verfügbar
  (Da das traditionelle Finanzsystem darauf angewiesen ist, dass die Vermittler Gewinne erzielen, fehlen ihre Dienstleistungen in der Regel an Standorten mit einkommensschwachen Gemeinschaften.)

Was passiert, wenn DeFi sich durchsetzt?

- DeFi konzentriert sich auf den Aufbau von Finanzdienstleistungen, die vom traditionellen finanziellen und politischen System getrennt sind.
- Das Ergebnis ist ein offeneres Finanzsystem.
- Keine Zensur, keine Diskriminierung.
- Große zentralisierte Organisationen haben wenig bis keine Macht über die Open-Source-Community und den Einzelnen.
- Effizienteres Finanzsystem

Warum gibt es DeFi?

- Traditionelle Finanzdienstleistungen werden täglich auf der ganzen Welt genutzt
- Sie alle enthalten einen Single Point of Failure / Intermediär
- Funktionalität basiert auf Vertrauen ins System
- → DeFi ist der Versuch, ein neues, dezentrales, vertrauensloses, demokratisches und offenes Finanzsystem auf Basis auf Blockchainbasis zu schaffen, indem der "Mittelsmann" ausgeschaltet und die Macht an die Teilnehmer zurückgegeben wird
- (Außerdem kann man Geld machen!)

Die sechs Bestandteile des trad. Finanzsystems

- Geld ($, €, ...)
- Finanzinstrumente (Aktien, Hypotheken, Versicherungspolicen, ...)
- Finanzmärkte (Aktienmarkt, Anleihenmarkt, ...)
- Finanzinstitute (Banken, Versicherungen, NYSE, ...)
- Aufsichtsbehörden (SEC, BaFin, ...)
- Zentralbanken (FED, EZB, ...)

Die vier Bestandteile des DeFi-Systems

- Geld (BTC, ETH, Stablecoins, ...)
- Finanzinstrumente (Aktien, Hypotheken, Versicherungspolicen, ...)
- Finanzmärkte (Kryptomarkt als Ganzes)
- Finanzinstitute (Dezentrale Börsen, [CEX])
- ~~Regulierungsagenturen~~ (keine)
- ~~Zentralbanken~~ (keine)

Vorteile dezentraler Strukturen in DeFi

- Token-/Geldmengenerweiterung ist transparenter (Wie viel Euro druckte die EZB gestern ./. wie viel BTC sind gestern erzeugt worden)
- Kein zentral gesteuerter Zins
- Spielregeln werden nicht im Laufe des Spiels geändert; wenn doch Abstrafung, möglich (Wettbewerb der Währungen/Assets)
- Offen, global, neutral, zensurresistent, unveränderlich, transparent

Welche Ökosysteme erlauben DeFi?

- Ethereum
- Binance Smart Chain
- Polkadot
- Solana
- Tron
- EOS
- Cardano
- Ethereum Classic
- ...

#DeFi

- Passives Einkommen durch:
  - Staking und Mining
  - Geld leihen und verleihen
  - Farming
- Trading
- Orakeln
- Finanzprodukte aus der alten Welt (Versicherungen, tokenisierte Dinge, ...)

Geld borgen und verleihen in DeFi (Borrowing/Lending)

- Ermöglicht durch sog. Liquiditätsprotokolle
- Benutzer können Krypto an das Protokoll verleihen und erhalten dafür eine Rendite (APY)
- ermöglicht es dem Nutzer, einen überbesicherten Kredit zu nehmen, ohne eine vertrauenswürdige Partei → beseitigt Barrieren beim Zugang zu Kapital
- → LTV (loan to value ratio) liegt zwischen 50% - 80%
- beseitigt die Notwendigkeit, Ihre Kryptoassets zu verkaufen, wenn Sie Geld benötigen
- Renditen zwischen 0% - 10%
- Kreditzinsen zwischen von 0% - 25% (für AAVE)

Farming

- Durch Smartcontracts automatisiertes Borgen und Verleihen
- Komplexe Strategien generieren Rendite, indem sie zur Verfügung gestellte Kryptoassets durch verschiedene Protokolle bewegen, immer auf der Suche nach dem höchsten Gewinn
- Strategien können von der Gemeinde vorgeschlagen und gewählt werden
- Erhebliche finanzielle Risiken sind involviert, daher nur für fortgeschrittene Nutzer empfohlen
- Für Nutzer mit viel Kapital und Risikoaffinität geeignet
- Renditen von 0 % bis zu 200.000 % pro Jahr

Mining 1

- Blockchain-Netzwerke basieren auf Vertrauen in Code+Rechenleistung.
- Transaktionen werden in Blöcken gebündelt und veröffentlicht.
- Ein Großteil der Rechenleistung wird als Arbeitsbeweis (PoW = Proof of Work) und ein kleiner Teil zur Verifikation der Transaktionen verwendet.
- Zweck des Arbeitsbeweises
  -> Spamschutz
  -> Steuerung der Blockzeit (in welchen Zeiteinheiten werden neue Blöcke veröffentlicht)
  -> Urkapitalistisches Entlohnungsmodell (Erster bekommt komplette Belohnung)
- Motivation: Belohnung durch Kreierung neuer Münzen und Einbehalten von freiwillig gegebenen Transaktionsgebühren
- Wichtigkeit fürs Netzwerk: Einhaltung der Regeln, Chronist (Welche Transaktion passierte wann)

Mining 2

- Drei Gruppen bestimmen in Blockchain-Ökosystemen:
  - Entwickler entscheiden über die Regeln
  - Miner entscheiden über die Historie
  - Käufer/Verkäufer, Spekulanten, Zahlungsdienstleister und Börsen entscheiden über den Preis
- Solo-Mining ./. Pool-Mining (Mining-Pools)
- BTC ist aufgrund PoW das sicherste Netzwerk und aufgrund seiner Geldmengenerweiterung gemäß Stock2Flow-Ratio so hart wie Gold
- PoW-Blockchains:
  - BTC & Forks (Chain-Forks wie BCH, BSV, BTG, BTD)
  - BTC-Software-Forks: LiteCoin, Dash, Monero

Staking (PoS = Proof of Stake, DPos = Delegierter PoS)

- Wie Mining, aber Arbeitsbeweis wird durch Geldnachweis ersetzt
- Mehr Geld - mehr Chancen, den nächsten Block zu minen und die Belohnung (neue Münzen und Transaktionsgebühren) zu erh.
- Basis vieler weiterer Beweise (Proof of Importance, Proof of Relevanz etc.)

PoA = Proof of Authority

- In Testnetzwerken verwendete Regelung, wer neue Blöcke erstellen darf
- Ausgewählte Autoritäten (Unis; Unternehmen, die maßgeblich im echten Ökosystem Geld verdienen)
- Es gibt keine Belohnung mit Geldwert, sondern wertlose Testnetzmünzen.
- Ziel ist das Netzwerk am Laufen zu halten und das echte zu simulieren.
- Bei ETH gibt es mehrere Testnetzwerke mit untersch. Autoritäten

Orakel

- Miner+Knotenrechner können nur Infos im eigenen Ökosystem sehen.
- Orakel erlauben den Blick in andere Welten (auf ökosystemfremde Daten).
- Man kann Orakeln nicht zwangsläufig vertrauen.
- Alle Miner & Knotenrechner (Nodes) benötigen zur Prüfung von Smart Contracts in Blocks+Transaktionen die selben Daten, um zu den gleichen Ergebnissen zu kommen.
- Maschinengesteuert ./. Sozialgesteuert
- Software-Orakel, Hardware-Orakel, Menschliche Orakel
- Mechanismen zur Integritätsprüfung von Orakeln, z.B. Orakel-Pools
- Marktplatz für Orakel(-daten)

Dezentrales Traden auf einer DEX

- CEX ./. DEX
- DEX = Dezentrale Börse
- Keine Abhängigkeit von einer einzelnen Entität.
- Keine Notwendigkeit, die Hoheit über die Token abzugeben.
- Der Handel erfolgt direkt aus der Wallet heraus.
- Nachteil hoher Transaktionsgebühren bei gesteigerter Netzwerkauslastung.
- Beispiele: Uniswap, Sushiswap, Bisq
- Meta-DEX / Aggregatoren: 1inch

Probleme und Risiken

- Vergessene Passwörter
- Falsch geschickte Transaktionen
- Hacks und Exploits
  (Smart contracts/Protokolle, Endgerätesoftware)
- Rugpulls
- Frontrunning
- Erpressung
- ...

Wie fängt man an und was braucht man?

- Funktionierende, stabile Internetverbindung
- Kapital in Form von Kryptowährungen (ETH, BTC, ...)
- Eine Wallet (Browser: MetaMask; Mobile: Argent)
- Zeit / Nachforschung / Praxis
- Gesteigerte Risikoaffinität