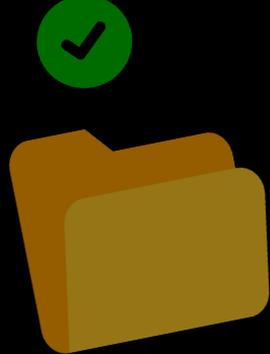


₿6,15

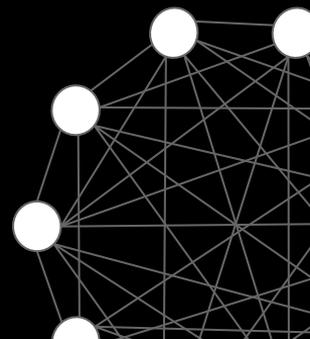
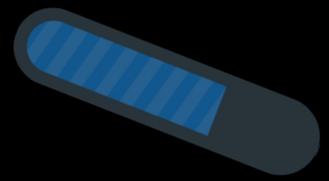


@anilsaidso

Bitcoin

Terminologie

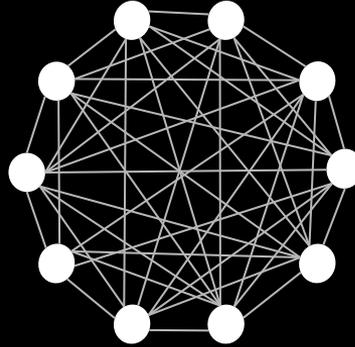
Übersetzt von: @BitsKnowledgeDE
www.bitsofknowledge.de



₿6,15

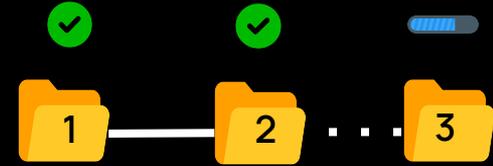
Bitcoin

Geld



Das Netzwerk

Verbundene Knoten



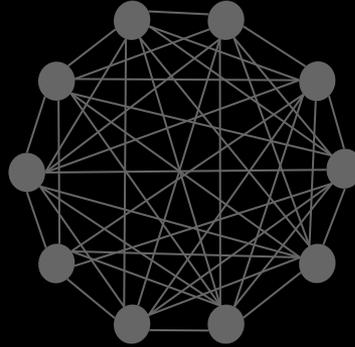
Die Blockchain

Verbundener Nachweis
verifizierter Transaktionen

₿6,15

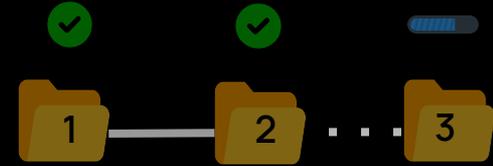
Bitcoin

Geld



Das Netzwerk

Verbundene Knoten



Die Blockchain

Verbundener Nachweis
verifizierter Transaktionen

von 21M
maximalen
Einheiten

₿6,15

=15.000.000
satoshis

Bitcoin

Verrechnungseinheit

nativ auf der Bitcoin-Blockchain

Übersetzt von: @BitsKnowledgeDE
www.bitsofknowledge.de



100.000.000
sats

1 BTC

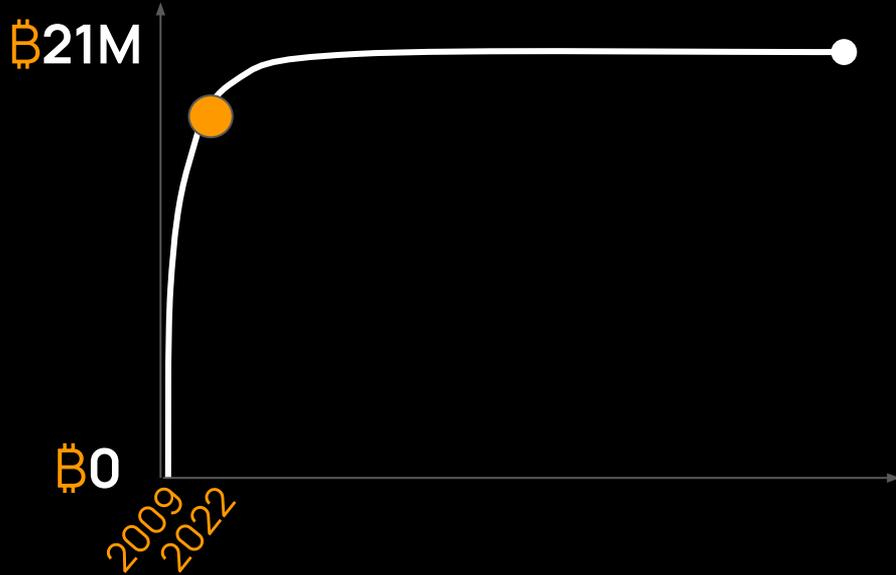
Satoshi

Ein Bitcoin ist in
100 Millionen
kleinere Einheiten
namens satohis
(oder sats) teilbar.



Endlicher Bestand

Die maximale Anzahl an Bitcoin, die jemals existieren wird, sobald alle gemined wurden.



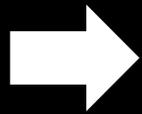
Emissions -Zeitplan

Vorprogrammierter
Zeitplan zur
Ausschüttung neuer
Bitcoin.

₿50

₿25

₿12.5



₿6.25

₿3.125

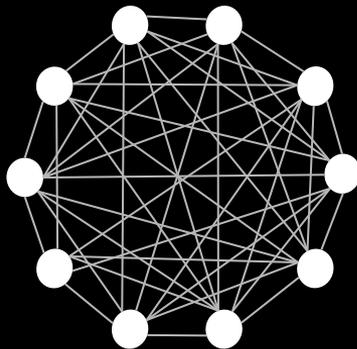
Halvening

Alle 210.000 Blöcke (~4 Jahre) wird die Rate neu ausgeschütteter Bitcoin um 50% reduziert.

Bitcoin 6.15

Bitcoin

Geld



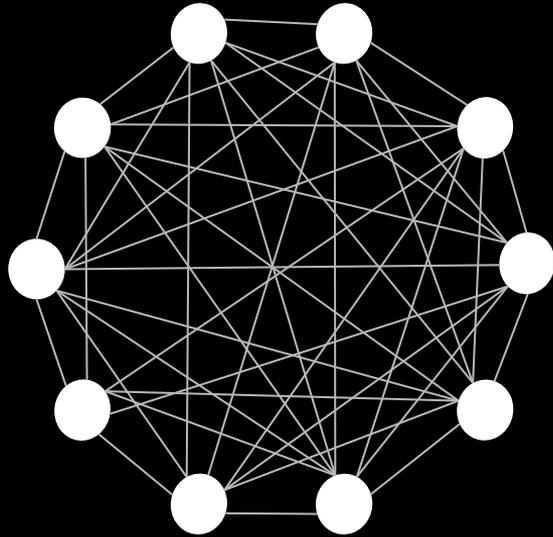
Das Netzwerk

Verbundene Knoten



Die Blockchain

Verbundener Nachweis
verifizierter Transaktionen



Bitcoin's Netzwerk

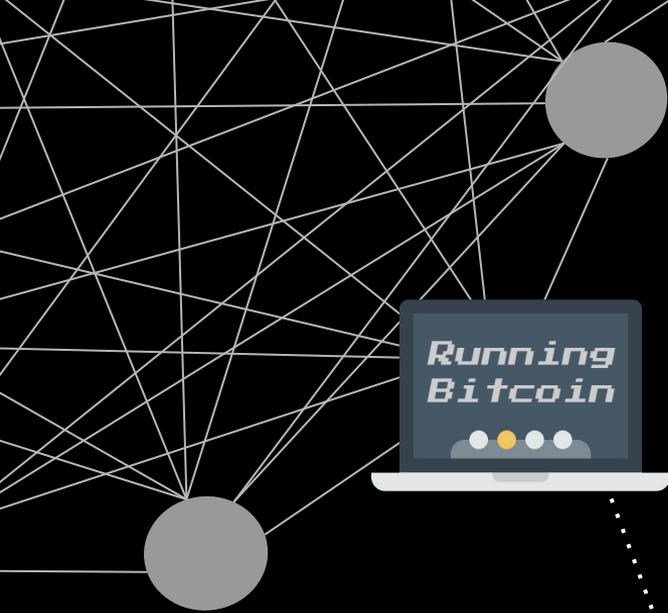
Verbundene Knoten,
die einem gemeinsamen
Regelsatz folgen.

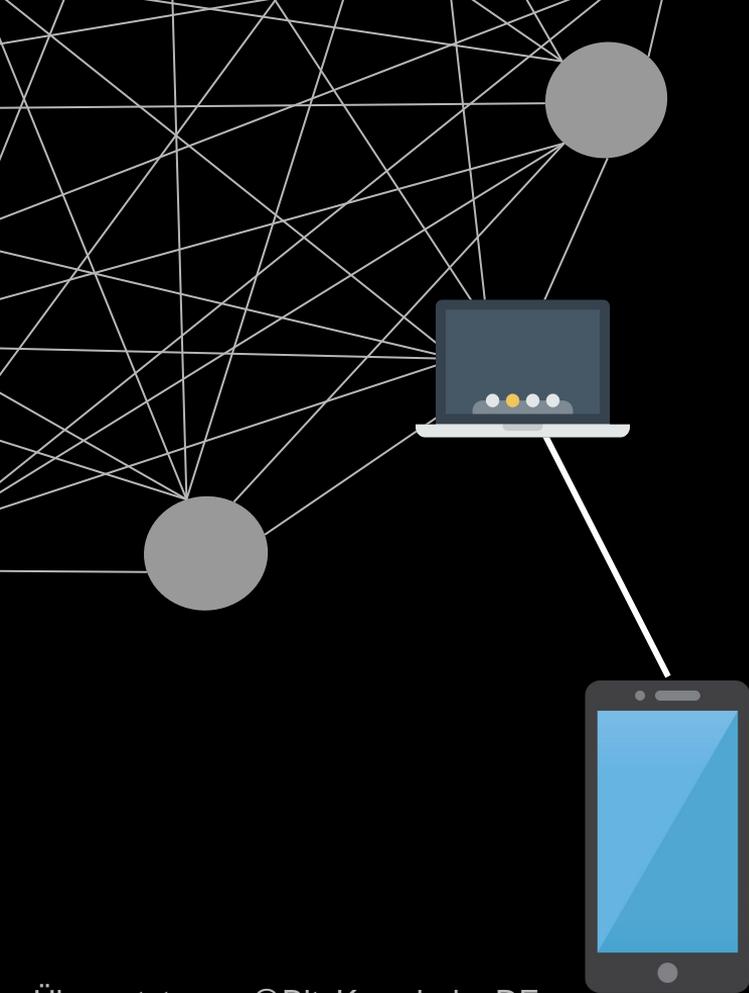


Bitcoin Core 22.0

Die *Bitcoin* *Software*

Open-source
Software, die das
Regelset
festschreibt





Light client

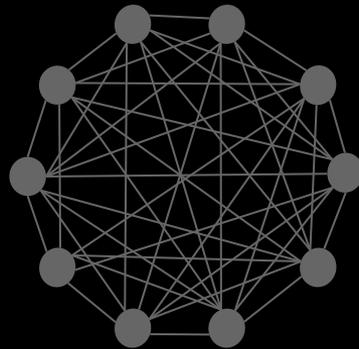
Verbindet sich mit einer Full node, um mit dem Netzwerk zu interagieren.

Speichert nur einen Teil der Historie, um Speicherplatz zu sparen

Bitcoin 6.15

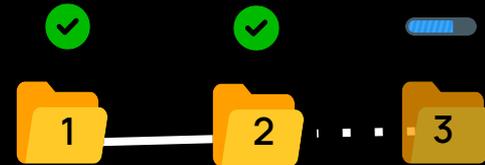
Bitcoin

Geld



Das Netzwerk

Verbundene Knoten



Die Blockchain

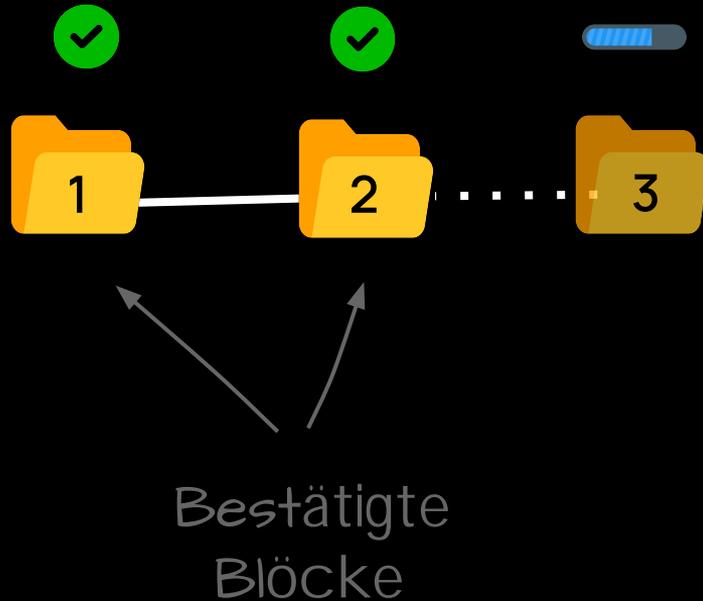
Verbundener Nachweis
verifizierter Transaktionen



— Tx 1
— Tx 2
— Tx 3

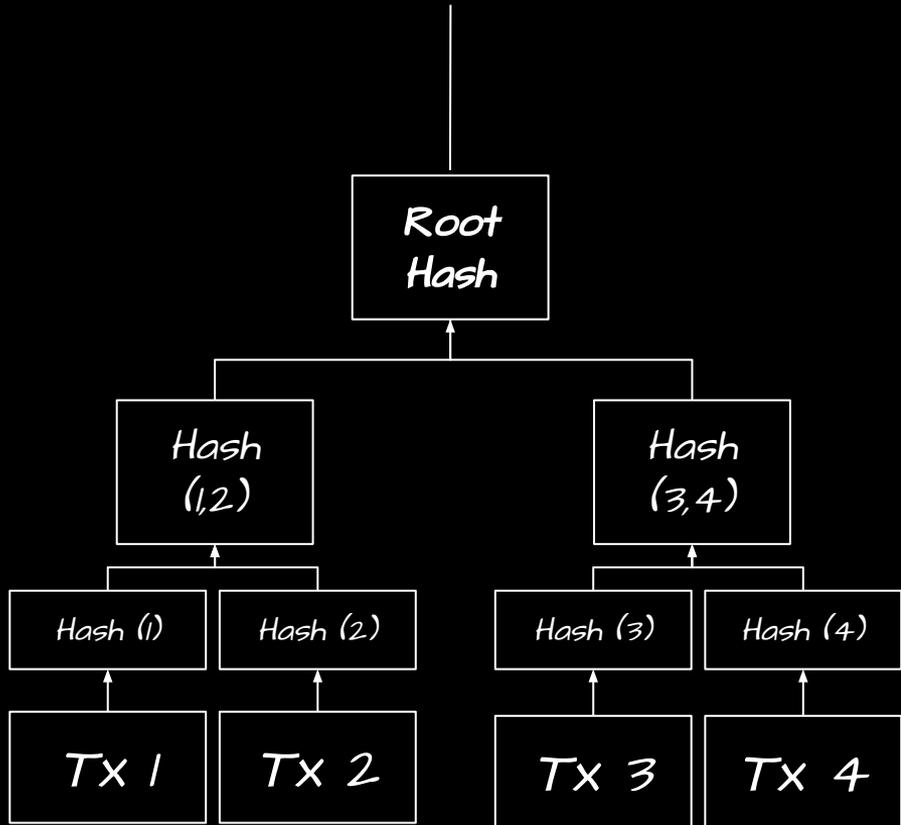
Block

Stapel an
bestätigten
Transaktionen mit
Zeitstempel



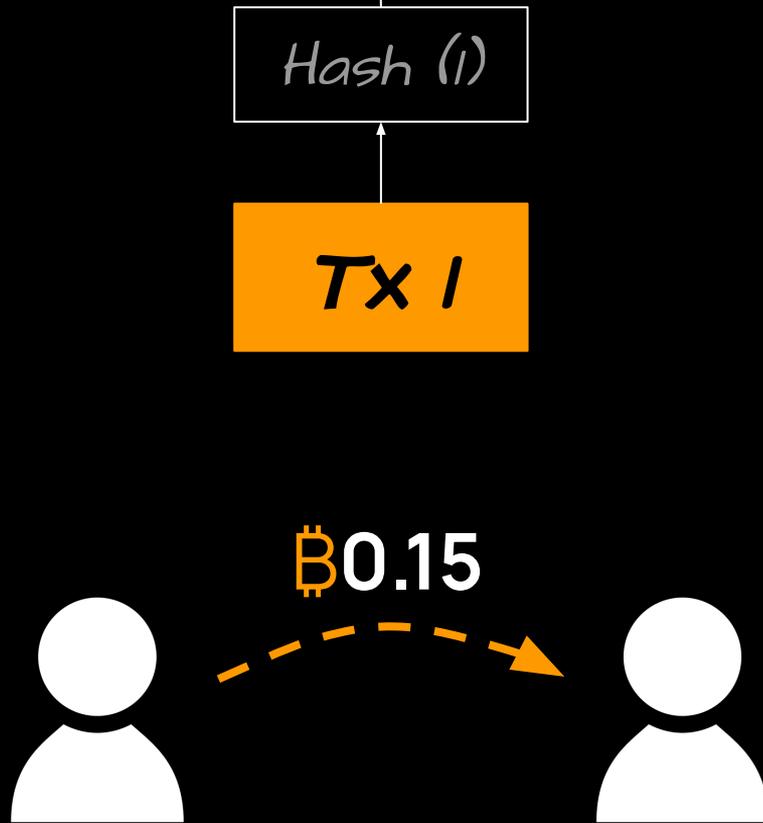
Bitcoin's Blockchain

Sequenziell
verbundene Blöcke
Historische Aufzeichnung
aller bestätigten
Transaktionen



Merkle tree (Hash-Baum)

Datenstruktur, die dabei hilft, Speicherplatz zu reduzieren und einfach Transaktions-Echtheit zu beweisen



Transaktion

Eigentumsübertrag von
Bitcoin zwischen
Netzwerk-Teilnehmern
Kryptografisch unterschrieben
vom Absender



Lightning Grundlagen



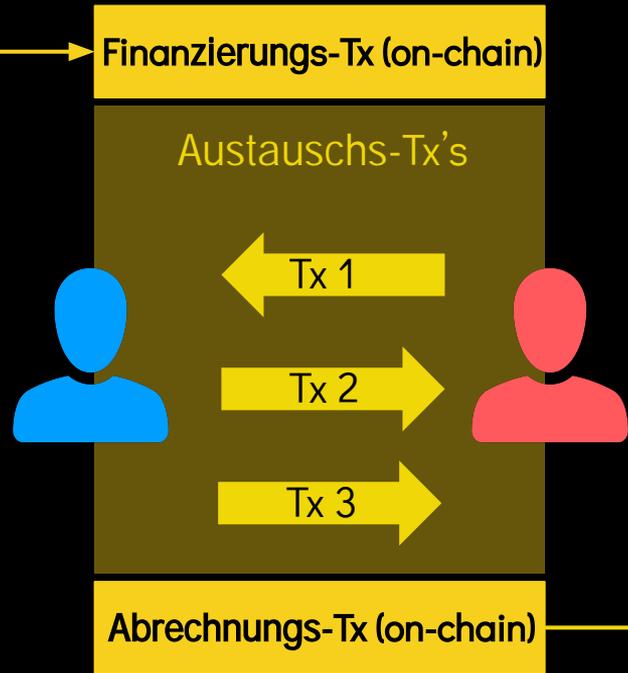
Lightning Netzwerk

Protokoll, das Skalierbarkeit via sofortiger off-chain Bezahlung ermöglicht.



Off-chain Transaktionen

Lightning-Transaktionen sind wie eine konstante Rechnung zwischen zwei Teilnehmern, deren Bilanz letztendlich auf der Bitcoin-Hauptchain abgerechnet wird.



Lightning Netzwerk

Das LN-Protokollpaket besteht aus **fünf** Ebenen.

Zahlungs-Ebene

Routing-Ebene

P2P-Ebene

Nachrichten-Ebene

Netzwerkverbindungs-Ebene

Zahlungs-Kanal

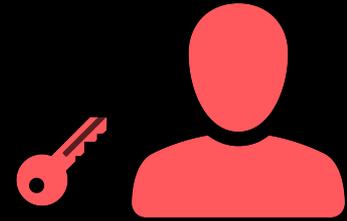
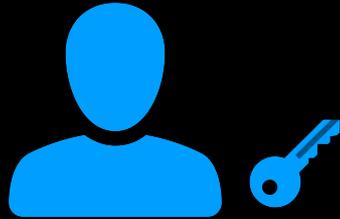
Finanzielle Beziehung
zwischen zwei Parteien



Gesamte Kanal-Kapazität:
150.000 sats

Multi-Signatur

Ein Zahlungskanal benötigt die Signaturen beider Teilnehmer (2-von-2) zum Öffnen und finalen Abrechnen auf der Bitcoin-Blockchain.



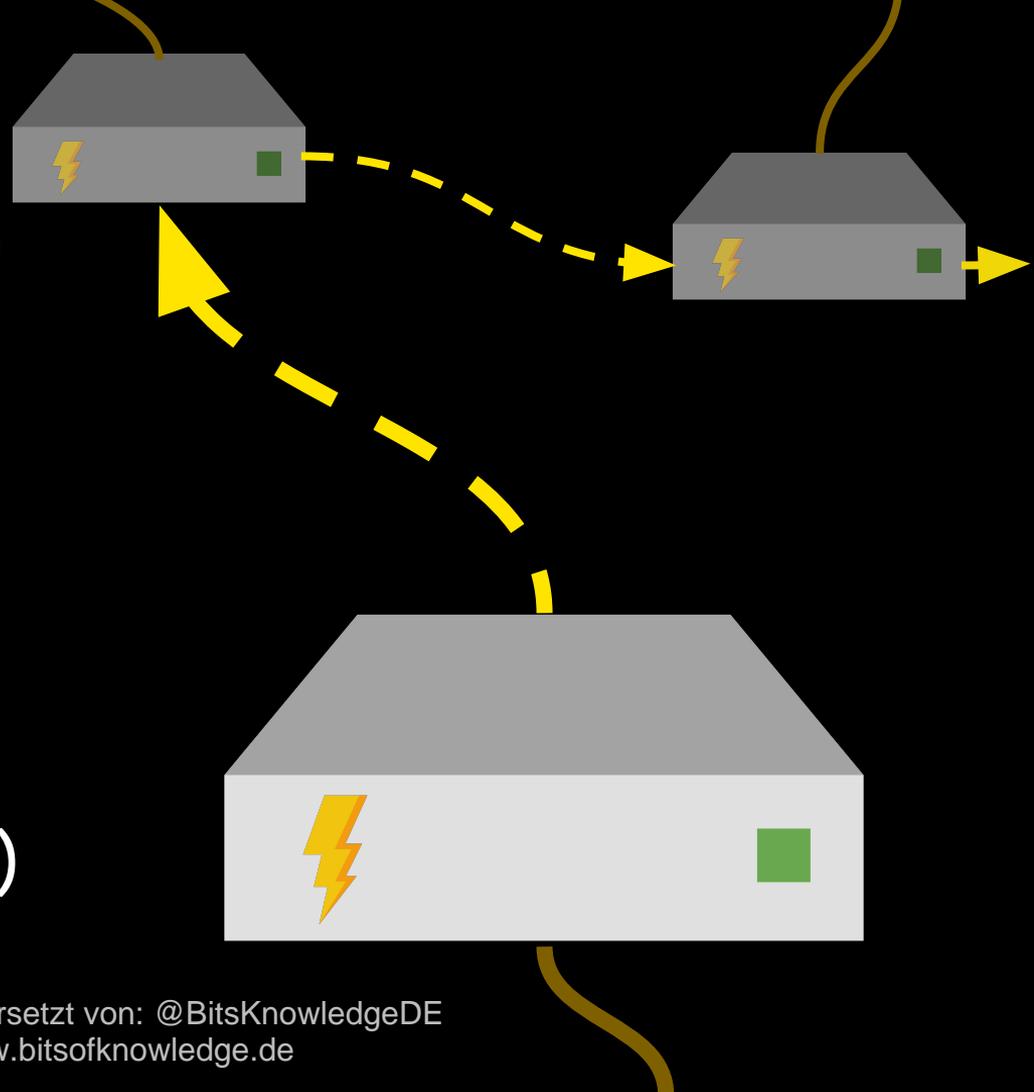
Bilanz:
150.000 sats

2 von 2

Zahlungs- Weiterleitung

(Routing)

Lightning-Zahlungen passieren off-chain, deswegen müssen alle Zahlungen zu ihrem Ziel weitergeleitet (geroutet) werden.



Lightning Wallet

Eine Lightning-Wallet ist **immer online**. Sie sollte nicht benutzt werden, um große Summen zu halten.

Lade deine Lightning-Wallet nur mit Beträgen auf, die du vorhast, in naher Zukunft auszugeben.





Anil

@anilsaidso 

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