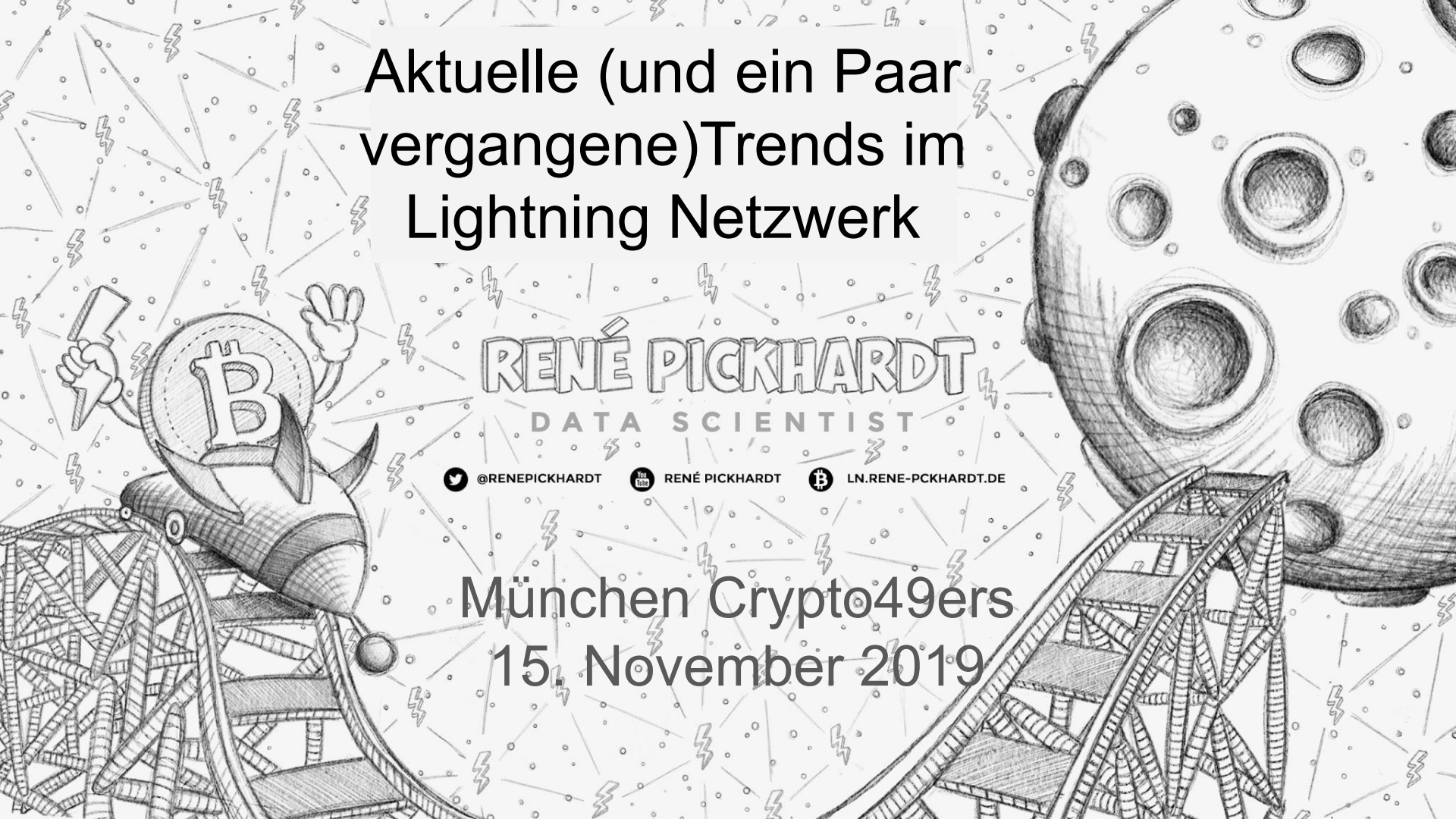
Aktuelle (und ein Paar vergangene)Trends im Lightning Netzwerk



RENÉ PICKHARDT

DATA SCIENTIST

@RENEPICKHARDT RENÉ PICKHARDT LN.RENE-PCKHARDT.DE

München Crypto49ers

15. November 2019

Rene (zu einer Bankkauffrau):

"Was wäre wenn ich dir sage, dass ich Kleinstbeträge von Geld in Bruchteilen von Sekunden um die halbe Welt schicken kann, so dass sie sicher bei der empfangenden Person im Säckel sind?"

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Bankkauffrau:

"Das wäre unglaublich nützlich!

Doch mit dem Giralverkehr ist das unmöglich, weil der teuer und langsam ist!

Also schöner Traum lieber Rene..."

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

We had no idea that this would turn into a global and public infrastructure.

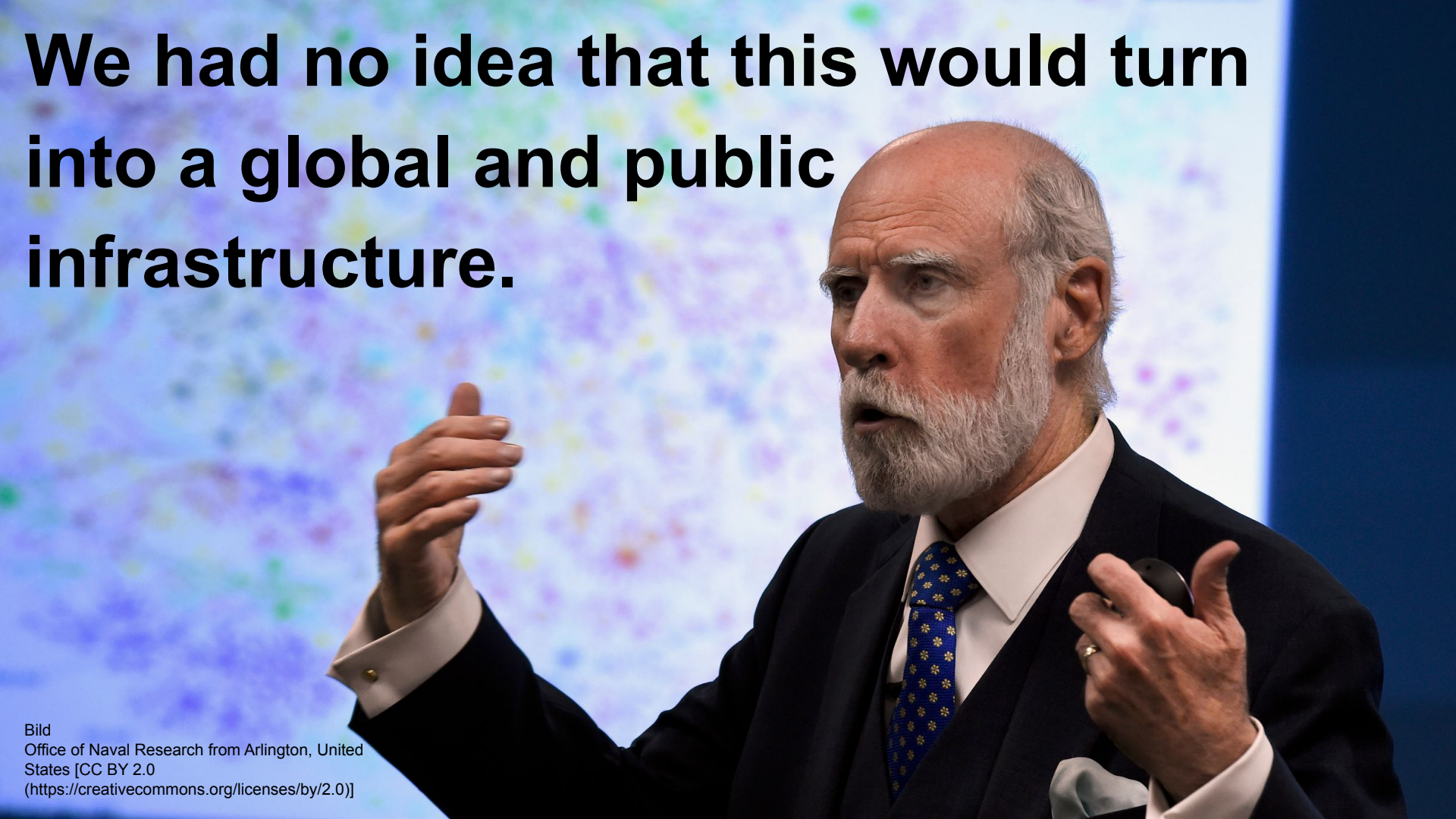


Bild
Office of Naval Research from Arlington, United States [CC BY 2.0 (https://creativecommons.org/licenses/by/2.0)]

Was ist das Lightning Netzwerk?

- Ein kluger Mechanismus Bitcoin zu verwenden
  - Ermöglicht unbegrenzt viel Zahlungen mit Bitcoin
  - Bitcoins werden off-chain außerhalb der Bitcoin Blockchain übertragen
  - Sicherheit und Vertrauen vom Bitcoin Netzwerk geerbt
- Smart Contracts bilden Zahlungskanäle
  - Echtzeit Zahlungen
    - Keine Bestätigungen
    - Direkter Transfer von Wert
  - Niedrige Gebühren
  - Microzahlungen (im Gegenwert von Bruchteilen eines Euro cents!)
- Zahlungskanäle lassen sich zu einem Netzwerk zusammenschließen
  - Knoten können beim Routen nicht stehlen
  - Router können nicht sehen wer wen bezahlt
- Die eierlegende Wollmilchsau durch die Bitcoin "to the mooooon" geht?
  - Klingt fast so. Mal schauen...

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Bitcoin und Blockchains können nicht skalieren

- Bitcoin Transaktionen benötigen ~200 Byte
- 1 Bitcoin Block kann ca. 5000 Transaktionen speichern
  - (1 MB = 1'000'000 Byte → 1 MByte / 200 Byte/tx = 5'000 tx)
- Skalierung durch Veränderung der Blockchain?
  - Kürzere Blocktime
  - Größere Blöcke
  - Beides funktioniert nicht bzw. nur begrenzt.
- Übrigens Funfact über Skalierbarkeit (https://de.wikipedia.org/wiki/Skalierbarkeit):
  - In der Elektronischen Datenverarbeitung bedeutet Skalierbarkeit die Fähigkeit eines Systems aus Hard- und Software, die Leistung durch das Hinzufügen von Ressourcen – z. B. weiterer Hardware – in einem definierten Bereich proportional (bzw. linear) zu steigern.
- Bitcoin hat von Tag 1 an die Schwierigkeitsanpassung
  - Mehr hardware —> mehr Hashrate —> gleich viel Blöcke —> gleich viel Transaktionen
  - Per Definition skaliert Bitcoin nicht.
  - So viel zu Satoshis Vision! Gruß an die BSV und BCH Fraktionen (:

License: CC-BY-SA 4.0

Eigenschaften von Zahlungskanälen

- 2 Partner teilen sich einen Kanal
  - 2-2 Multisig Adresse
  - Jede Seite hält einen Private key
- Öffnenen und Schließen
  - Reguläre Bitcoin Transaktion
  - Braucht Bestätigungen
  - Kann sehr teuer werden
- Kapazität
  - Der Betrag auf der Multisig Adresse
- Balance
  - Eine signierte "Commitment Transaktion" vom 2-2 Multisig wallet codiert die Balance der Partner
- Ohne Vertrauen
  - Signierte Commitment Transaktion hat einen smart contract, der sie rückziehbar machen lässt.
  - Ein Partner kann den Kanal ohne Hilfe der Gegenseite schließen.

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Ein Netzwerk von Zahlungskanälen ...

- Routing
  - Zahlungen können über Teilnehmer des Netzwerk durch einen Pfad von Kanälen versendet werden
- Ohne Vertrauen
  - Router können auf grund von Hashed Time Locked Contracts (HTLCs) kein Geld stehlen
- Privatsphäre
  - Pakete werden ähnlich zu TOR via Onion Routing verschickt
- Günstig
  - Bislang sind die Gebühren für das Routing quasi umsonst
  - Grenzkosten zum Erstellen eines Kanals sind Onchain fees geteilt durch payments im Kanal
    - Werden bei beliebig vielen Routingvorgängen beliebig klein
- Schnell
  - Weiterleiten von Paketen ist nur durch Datenübertragungsrate im Internet begrenzt
- Zufällig
  - Pfade finden ist ein zufälliger Prozess, der mehrere Versuche benötigen kann

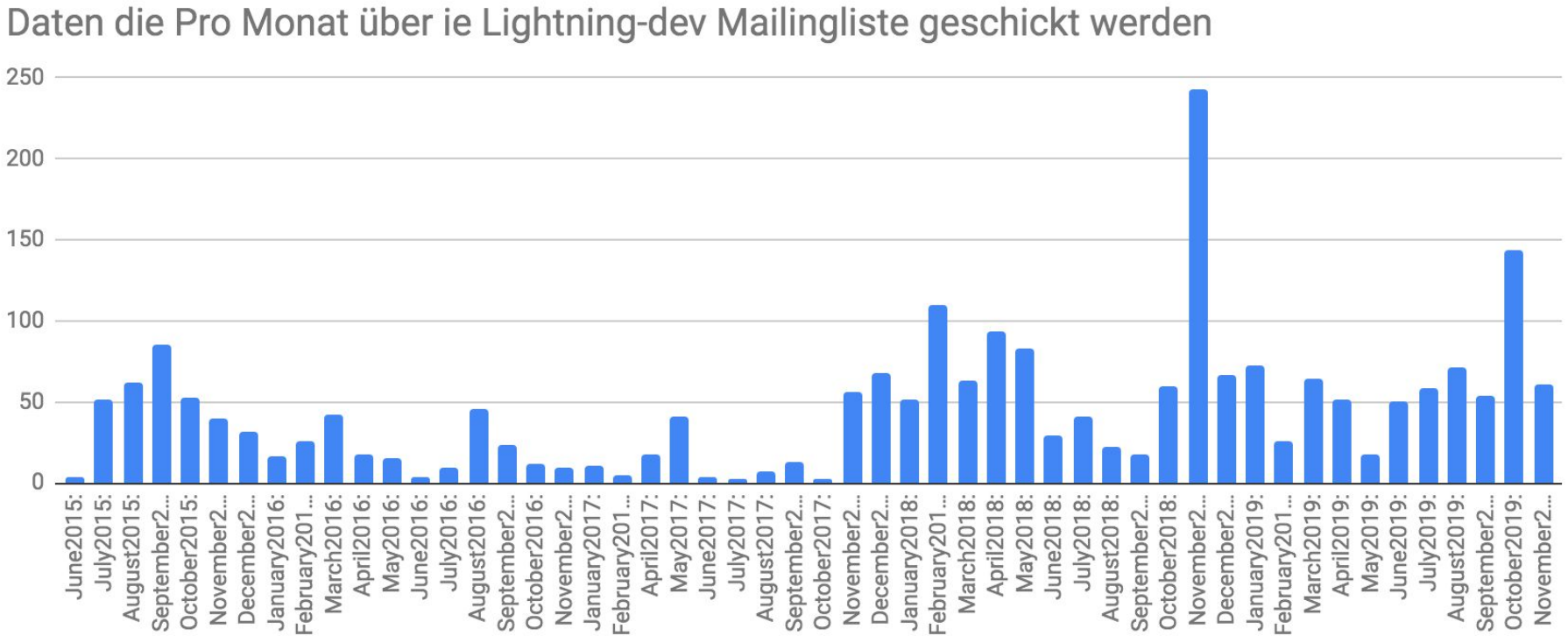
License: CC-BY-SA 4.0

Die eierlegenden Wollmilchsau? Nein, denn...

- Path finding
  - Völlig unklar ob aktuelle Strategien ausreichen werden oder Vorschläge helfen werden
- Backups
  - Lightning Nodes lassen sich mehr schlecht als recht backupen.
- Hotwallet risk
  - Es gibt keine Möglichkeit das Lightning Netzwerk als Cold Wallet zu betreiben
  - Zwang meistens online zu sein
- DoS Attacks
  - Vor allem SPAM
  - Aber auch htlcs
- Probing attacks
  - Privatsphäre kann durchaus ausspioniert werden
- Keine garantierte Geschwindigkeit
  - Zahlungsvorgang kann - ohne Erfolgsgarantie - Stunden dauern und nicht abgebrochen werden
- Sicherheit z.T. ungeklärt

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Nur eine Graphik die relevant ist (:



Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de


TO THE
MOOOON!

Es war ja doch keine eierlegende Wollmilchsau

- Path finding
  - Völlig unklar ob aktuelle Strategien ausreichen werden oder Vorschläge helfen werden
- Backups
  - Lightning Nodes lassen sich mehr schlecht als recht backupen.
- Hotwallet risk
  - Es gibt keine Möglichkeit das Lightning Netzwerk als Cold Wallet zu betreiben
  - Zwang meistens online zu sein
- DoS Attacks
  - Vor allem SPAM
  - Aber auch htlcs
- Probing attacks
  - Privatsphäre kann durchaus ausspioniert werden
- Keine garantierte Geschwindigkeit
  - Zahlungsvorgang kann - ohne Erfolgsgarantie - Stunden dauern und nicht abgebrochen werden
- Sicherheit z.T. ungeklärt

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Pathfinding ist ein sehr aktives Research Thema

- Nicht nur meine geplante PhD Thesis
- Multipath payments (AMP)
  - Für BOLT 1.1. geplant
  - Mit Boomerang vorschlag sehr viel versprechend
    - Braucht eltoo + Schnorr
- JIT Routing
  - Funktioniert in BOLT 1.0 allerdings nicht ökonomisch für router
    - Lässt sich durch backward kompatible Protokoländerungen fixen
    - Welche?
- ZmnSCPxj's arbeiten zu Permuteroute und Real Time Strategy games.

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Backups ohne Risiko werden kommen

- Eltoo Channels
  - Brauchen bitcoin Fork
  - BIP 118
- Keine Sorge mehr alte Backups einzuspielen
  - Aber: Altes Backup zu meinen Ungunsten könnte so bleiben
- Aktuell mehr schlecht als rechte Lösungen
  - Static channel Backup
  - Datenbank replikation
  - RAID auf Festplatten ebene
- Watchtower services?

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Hot Wallet Risk ist ein prinzipielles Problem

- Konsequenz aus der Deseignentscheidung die Smart Contracts über Time Locks zu regeln
- Kann aber besser werden
  - Hardware Wallet kommen
    - Routen von Bezahlen trennbar
  - Access Control Knowhow wird über Zeit kommen
- Außerdem Backups und Eltoo ermöglichen längere Offline Zeiten
- Wenig Development / scheint akzeptiert zu werden.

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

DoS Attacks bleiben Vorerst ein Problem

- 1 Million channel challenge und Verbesserungen am Gossip Protokol
- HTLCs
  - Maximales HTLC limit konfigurierbar
  - P2 Contract und Tap
- Up - front Payments

Probing attacks schränken die Privatsphäre ein

- Schwieriges Dilemma
  - Die starke privatsphäre ermöglicht auch Angreifern viel Privatsphäre
- Auch hier werden up-front Payments helfen
- BOLT 1.1 empfiehlt, dass nodes gelegentlich proben um inaktive Kanäle zu schließen

Garantierte Geschwindigkeit - Service Level

- Cancelable & Stuckless Payments
  - Adaptor Signaturen
  - BIP Schnorr
- Escrow Services
- Mehr Privatsphäre durch Payment Decorrelation als Nebeneffekt
- Sehr starke Protokoll Veränderung.
  - Zahlungskanal und Routing werden neu gebaut
  - Nicht für BOLT 1.1 geplant

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Sicherheit kommt über

- Erfahrung
- Tests
- Zeit
- Mehr Developer*innen
- Mehr Nutzer*innen

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Mehr neue Features

- Splicing
  - Die Möglichkeit die Kapazität von Zahlungskanälen zu ändern
- Dual funded channels
  - 2 Knoten können gemeinsam Bitocins zum Zahlungskanal bringen
- Rendezvous Routing
  - Empfänger kann sich verstecken
- Trampoline Payments
  - Experten Netzwerk für Routing, so dass Mobile Clients keine kompletten Wege finden müssen.

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Was braucht es auf technischer Ebene

- Eltoo channels für das Backup Problem
  - Schnorr signaturen
  - Sighash noinput
  - Bitcoin hardfork!
- Payment Punkte / Secrets für Service Level agreements und garantiert schnelle Zahlungen
  - Schnorr Signaturen
  - Adaptor Signaturen
  - Bitcoin Hardfork
- Großteile des Lightning Netzwerkes müssten neu geschrieben werden

Author: Rene Pickhardt License: CC-BY-SA 4.0 https://ln.rene-pickhardt.de

Liebe Grüße an den Architekt (:

Bild
Office of Naval Research from Arlington, United States [CC BY 2.0 (https://creativecommons.org/licenses/by/2.0)]

Über Rene Pickhardt

- Unabhängiger open source Lightning Network Entwickler
  - Autopilot
  - JIT-Routing
  - Kleinere Patches für Sicherheitsbugs
- Co-Autor Mastering the Lightning Network (O'Reilly) mit Andreas Antonopoulos und Olaoluwa Osuntokun
- Data Science Consultant
  - Auch für Bitcoin / Lightning Netzwerk
- Diploma in pure Mathematics
- Lightning Network Lehrer
  - Youtube Kanal
  - Lehrer für die chaincodelabs Lightning Residency 2019 (Mit Christian Decker, Fabrice Drouin & Alexander Bosworth)
  - Lehrer für die blockchain training conference des C4
  - Hauptautor des Lightning Netzwerk Wikipedia Artikels

License: CC-BY-SA 4.0

Copyright notice

- This slide deck is openly licensed with a creative commons license CC-BY-SA-4.0.
  - The full license text can be found at: https://creativecommons.org/licenses/by-sa/4.0/legalcode
- You are
  - free to
    - Share
    - Remixe
  - As long as you
    - Link to the original work
    - State my Name and Website
    - Mark changes in your derivative work
    - Use the same license for your derivative work
- Screenshots in this slide deck are taken by me but the design of the websites might be protected by copyright
- This slide deck uses parts of the lightning-rfc which is licensed as CC-BY (the lightning developers)
  - The full license text can be found at: https://creativecommons.org/licenses/by/4.0/legalcode
- The graphics from the backup slides are taken from https://en.bitcoin.it/wiki/Transaction and are Public Domain

Thanks to Marietheres Viehler (aka journalspiration) for the design of the title slide.

About this slide deck

The purpose is to help spreading education about the Lightning Network Protocol so that the technology will be adopted more quickly by more people. This shall be my contribution to the Bitcoin / Lightning Network Community.

It is partially created from https://commons.wikimedia.org/wiki/File:Introduction_to_the_Lightning_Network_Protocol_and_the_Basics_of_Lightning_Technology_(BOLT_aka_Lightning-rfc).pdf. To the best of my knowledge the original file is the most comprehensive work making an introduction to the BOLT standard.

The slides are part of my effort to create a book about the lightning network. You can follow that effort at: https://github.com/lnbook/lnbook or you can support the effort at my fundrasing pages at: https://tallyco.in/s/lnbook or at: https://www.patreon.com/renepickhardt or at 1GZx8tWgDd21Rd8b1QdMrzdZGHgyfVkzaD part of this effort also consists of creating video tutorials and teaching materials on my Youtube Channel over at: https://www.youtube.com/user/RenePickhardt

This work was funded (sorted by amount of contribution from top to bottom) by: Me personally, fulmo.org, everyone who contributed to the above mentioned fundraiser and George Danzer.

Thank you to the lightning developers and people in various telegram groups for helpful discussions