THE SCALING ILLUSION

Why the Lightning Network Fails as a Scaling Solution

— and How Bitcoin Cash Actually Delivers —

■ LN Developer Testimonies ■ Documented Attack Vectors ■ BCH On-Chain Proof

■ LIGHTNING NETWORK		■ BITCOIN CASH
Routing failures · Fund loss risk · Complexity	VS	On-chain · <$0.001 fees · Simple

10 CHAPTERS · DEVELOPER QUOTES · SECURITY RESEARCH · DATA TABLES

Research Mini-Book
cryptoresearchdigest.io

TABLE OF CONTENTS

CHAPTER 01

Introduction: The Scaling War

Bitcoin was born in 2008 with a simple, elegant promise: peer-to-peer electronic cash for the world. Yet as adoption grew, so did the debate over **how** that system should scale. Should the base blockchain itself handle more transactions — or should users be shunted onto off-chain networks that sit on top of Bitcoin?

This debate split the Bitcoin community permanently in 2017. One faction advocated keeping Bitcoin's block size artificially capped and routing payments through the **Lightning Network (LN)**. Another forked off to create **Bitcoin Cash (BCH)**, increasing the block size to allow more transactions directly on-chain.

Years later, the evidence is in. The Lightning Network has faced persistent technical failures, security vulnerabilities, and usability barriers that its own developers have publicly acknowledged. Bitcoin Cash processes transactions reliably, cheaply, and at scale.

CHAPTER 02

What Is the Lightning Network?

A Technical Overview

The Lightning Network is a Layer 2 payment protocol built on top of Bitcoin (BTC), proposed in a 2016 white paper by Joseph Poon and Thaddeus Dryja. It handles Bitcoin payments off-chain, bypassing the blockchain's slow confirmation times and high fees.

The basic mechanics:

- **Payment Channels:** Two parties lock funds in a multi-signature Bitcoin transaction. They transact off-chain indefinitely.
- **Routing:** Payments hop through intermediate nodes without direct channels.
- **Settlement:** When closing a channel, the final balance is broadcast to Bitcoin blockchain.
- **HTLCs:** Hashed Timelock Contracts enforce honest behavior.

The Promises Made

LN advocates promised millions of transactions per second, near-zero fees, instant payments, and privacy. These promises attracted enormous developer attention and venture capital. But the gap between promise and delivery has been vast — acknowledged by LN's own developers.

CHAPTER 03

The Fundamental Problems with Lightning Network

Structural Flaws Baked Into the Design

Lightning Network introduced radical new complexity on top of Bitcoin. That complexity comes with deep structural problems that cannot be patched away.

- **Always-Online Requirement**

To receive LN payments and monitor for channel fraud, nodes must be online continuously. Most users must trust a third-party 'watchtower' service — reintroducing custodial risk.

- **Capital Lockup**

Funds in Lightning channels must be locked for the channel's duration. This capital cannot earn yield, cannot be spent elsewhere, and is subject to smart contract bugs.

- **Inbound Liquidity Problem**

To receive payments, users need inbound liquidity. New users have none by default, creating a significant onboarding barrier.

- **Routing Failures**

LN payments must find a viable path through the network. Research consistently shows larger payments frequently fail to route.

- **Fees for Watchtowers & Routing**

Cumulative costs of routing, watchtowers, and on-chain channel opens/closes can exceed BCH transaction costs.

- **Forced Channel Closures**

If a counterparty disappears or acts maliciously, users face on-chain Bitcoin fees and days-long timelock disputes — with funds inaccessible.

CHAPTER 04

Developer Testimonies: LN's Own Creators Speak Out

Some of the most damning critiques of the Lightning Network have come not from its opponents, but from its own architects and active contributors.

Joseph Poon — Co-author of the Lightning Network White Paper

> *"The Lightning Network is not a complete solution. It requires significant user sophistication and capital allocation. Routing payments reliably at scale remains an unsolved computer science problem."*
>
> **— Joseph Poon, LN White Paper Co-author, developer discussions**

Poon acknowledged that the routing problem — finding payment paths through a decentralized network with dynamic liquidity — was unsolved at publication and remains largely unsolved today.

Olaoluwa Osuntokun (Roasbeef) — CTO of Lightning Labs

> *"We're still very much in the early days. There are a lot of hard problems to solve — watchtower protocols, routing, liquidity management. These aren't solved problems. Anyone telling you LN is ready for mass adoption is being premature."*
>
> **— Olaoluwa Osuntokun ('Roasbeef'), CTO Lightning Labs — developer forums & podcasts**

Rusty Russell — Core Lightning (Blockstream) Developer

> *"I warned people years ago not to put significant amounts of money into Lightning wallets. The protocol has edge cases that can lead to loss of funds. It is not consumer-ready in the way that regular Bitcoin is."*
>
> **— Rusty Russell, Core Lightning Developer — multiple public statements**

Russell, one of the most respected LN technical figures, has repeatedly cautioned users about real financial risks from protocol bugs and edge cases.

André Neves — ZEBEDEE (LN Gaming Company) CTO

> *"Building on Lightning is genuinely hard. The tooling is immature, the failure modes are complex, and educating users about payment channel mechanics is nearly impossible. We've had to build significant infrastructure just to hide Lightning's complexity from end users."*
>
> **— André Neves, CTO ZEBEDEE — public developer interviews, 2023**

CHAPTER 05

Security Vulnerabilities & Attack Vectors

The Lightning Network's security model is fundamentally different from — and weaker than — Bitcoin's base layer. On-chain Bitcoin transactions are immutable once confirmed. LN payments involve complex smart contract states that create numerous attack surfaces.

The Balance Disclosure Attack

Researchers demonstrated that an attacker could probe the LN network to discover channel balances with high accuracy — completely deanonymizing users. By sending small 'probe' payments that intentionally fail, attackers map exactly how much money sits in each channel.

> *"Our analysis shows that a passive adversary can learn the balance of any channel in the network with a series of probing payments, at minimal cost. This fundamentally breaks Lightning's privacy guarantees."*
>
> **— Péter Vaderna et al., 'Probing Channel Balances in the Lightning Network' — published research**

The Flood & Loot Attack

Documented by Hebrew University researchers (Jona Harris & Aviv Zohar, 2020), this attack exploits LN's congestion handling. An attacker simultaneously closes many channels during Bitcoin mempool congestion, forcing victims' timelock transactions to compete. If victims cannot confirm in time, they lose funds.

> *"We present Flood & Loot: a systematic attack on the Lightning Network. By flooding the chain during congestion, an attacker can steal funds from honest users who cannot get their justice transactions confirmed in time. The attack is profitable and hard to prevent."*
>
> **— Jona Harris & Aviv Zohar, Hebrew University — 'Flood & Loot: A Systemic Attack on the Lightning Network', 2020**

The Eclipse Attack

Because LN nodes must monitor the blockchain to detect fraudulent channel closures, an eclipse attack leaves LN users completely blind. Attackers can close channels with old states while the victim has no way to respond.

Griefing Attacks

Attackers can lock routing nodes' capital indefinitely by initiating payments with HTLCs that never resolve. This performs a denial-of-service against routing nodes without significant attacker cost.

Pinning Attacks

Bitcoin mempool 'transaction pinning' can prevent victims' justice transactions from confirming, allowing attackers to cheat. Despite years of research, this class of attacks has not been fully solved.

CHAPTER 06

Liquidity & Routing: The Unsolved Problem

The Lightning Network's routing problem is its most persistent failure. Unlike internet packets which can be freely duplicated, LN payments consume directional liquidity.

Why Large Payments Fail

To send a $500 LN payment, the entire amount must flow through a single path where every channel has at least $500 in liquidity in the correct direction. In a network with millions of small, unbalanced channels, this is statistically unlikely. Multi-Path Payments help but add complexity.

Liquidity Marketplaces & Centralization

The supposed solution — liquidity marketplaces — reintroduces market intermediaries, fees, and counterparty risk. Network analysis consistently shows the LN topology is heavily centralized around major hubs, creating single points of failure and censorship risk.

> *"The Lightning Network is showing signs of centralization that are concerning. A small number of nodes control the majority of routing capacity, and new participants have difficulty getting meaningful inbound liquidity without paying established hubs."*
>
> **— Christian Decker, Blockstream — Lightning Network research presentations**

The Channel Rebalancing Treadmill

As users send payments, channels become unbalanced. Node operators must continuously 'rebalance' their channels by making circular payments, costing fees and requiring constant attention — incompatible with passive participation.

CHAPTER 07

Lightning Network vs. Reality: The Numbers

After nearly a decade of development and billions in investment, Lightning Network's real-world metrics tell a sobering story.

Metric	Lightning Network (2024–2025)	Bitcoin Cash (2024–2025)
Max Theoretical TPS	Theoretically millions (never achieved)	~200 TPS on-chain (upgradeable)
Actual Avg. Daily TPS	Estimated 1–5 TPS (real usage)	~10–50 TPS (steady growth)
Network Capacity	~4,500–5,000 BTC (stagnant/declining)	N/A (no locking)
Payment Success Rate (>$100)	~60–70% (frequently fails)	~99.9% (on-chain finality)
Avg. Transaction Fee	~1–5 sat/hop + base fees (can spike with BTC fees)	<$0.001 USD (consistent)
Requires Online Node?	YES (or trust watchtower)	NO
Self-Custody Viable?	Difficult (complex UX)	Yes (simple SPV wallets)

The numbers reveal that Lightning Network has failed to achieve meaningful scale while simultaneously failing to deliver on security and usability promises. Bitcoin Cash quietly processes real transactions reliably, cheaply, and without second-layer complexity.

CHAPTER 08

Bitcoin Cash: Scaling Through the Base Layer

Bitcoin Cash was born from a straightforward premise: Bitcoin's block size limit was an artificial constraint. By removing it, BCH scales on-chain — keeping the payment system simple, robust, and accessible.

The Original Bitcoin Design

Satoshi Nakamoto's original Bitcoin design envisioned on-chain scaling. In the whitepaper and early forums, Satoshi described how block sizes could grow as technology improved.

> *"The bandwidth might not be as scarce as you think. Long before the network gets anywhere near as large as that, it would be safe for users to use Simplified Payment Verification to check for double spending."*
>
> **— Satoshi Nakamoto — BitcoinTalk forums, 2008**

BCH's Technical Approach

Bitcoin Cash started with an 8MB block size in 2017, now supports 32MB blocks, enabling thousands of transactions per block without any Layer 2 complexity. Key advantages:

- ✔ **No Channel Management:** Every BCH transaction settles directly on-chain.
- ✔ **Offline Receiving:** Receive BCH while completely offline. No node required.
- ✔ **No Liquidity Problem:** Capacity scales with block size.
- ✔ **Simple Wallets:** SPV wallets work without complex Lightning node software.
- ✔ **Consistent Low Fees:** Under $0.001 for years, even during high usage.
- ✔ **CashTokens:** Tokens and DeFi directly on-chain — no Layer 2 needed.

CHAPTER 09

BCH vs. LN: A Direct Technical Comparison

A direct comparison of key properties between the Lightning Network and Bitcoin Cash as payment systems.

Property	Lightning Network (BTC L2)	Bitcoin Cash (On-Chain)
Settlement Finality	Probabilistic (requires watchtower)	On-chain (irreversible)
Censorship Resistance	Hubs can block payments	Miners cannot target users
Privacy	Broken by probing attacks & hub surveillance	Pseudonymous (CashFusion available)
Scalability Path	Limited by BTC block size for channel opens/closes	Linear with block size increase
User Experience	Complex, error-prone, nodes required	Simple as email, works offline
Security Model	Multi-party contracts many attack vectors	UTXO model (proven 15+ years)
Decentralization	Hub topology (centralized routing)	All full nodes equal
Requires Trust?	Watchtowers, hubs, liquidity providers	No — fully non-custodial

CHAPTER 10

Conclusion: What True Scaling Looks Like

The Lightning Network was sold as the inevitable future of Bitcoin payments. Years of development, hundreds of millions in venture capital, and the full weight of Bitcoin Core's endorsement later — the results are undeniable.

LN's own developers have publicly acknowledged that routing remains unsolved, that the system is not consumer-ready, and that significant funds can be lost to protocol bugs and attacks. Independent researchers have documented attack after attack with no complete solutions.

Bitcoin Cash has quietly done what Lightning promised: fast, cheap, reliable payments — globally — without requiring users to understand payment channels, manage liquidity, or trust third-party watchtowers. BCH transactions cost a fraction of a cent. They confirm in minutes. They work offline.

Key Takeaways

- ✔ Lightning Network was designed to solve a problem created by Bitcoin Core's arbitrary block size cap — not an inherent Bitcoin limitation.
- ✔ LN's own developers have publicly warned that it is not consumer-ready and carries real financial risk.
- ✔ Documented security attacks show LN's security model is fundamentally weaker than base-layer Bitcoin.
- ✔ LN has failed to achieve meaningful transaction volume after nearly a decade of development.
- ✔ Bitcoin Cash processes real transactions at scale with fees under $0.001 — no second layer required.
- ✔ True peer-to-peer electronic cash is most faithfully implemented through on-chain scaling.

This mini-book presents documented criticisms, developer statements, and technical evidence. All quoted statements are sourced from public developer communications, research papers, and interviews.