

VŠB TECHNICKÁ
UNIVERZITA
OSTRAVA

VSB TECHNICAL
UNIVERSITY
OF OSTRAVA



www.vsb.cz

Bolt Card – Moderní přístup k platbám přes Bitcoin Lightning

Jakub Růžička

VŠB – Technická univerzita Ostrava

jakub.ruzicka.st@vsb.cz

14. dubna 2025

- 1 Úvod do Bolt Card
- 2 Technické detaily
- 3 Ekosystém Bolt Card
- 4 Bezpečnost
- 5 Případové studie a využití
- 6 Závěr

Co je Bolt Card?

- Bezpečná NFC karta pro okamžité platby přes Lightning Network
- Vytvořena komunitou kolem LNBits
- Podporuje offline i online platby přes Bitcoin Lightning
- Funguje podobně jako běžné bezkontaktní platební karty (např. Visa, Mastercard)

Proč vznikla Bolt Card?

- Usnadnit používání Lightning Network pro běžné uživatele
- Odstranit nutnost používání mobilních aplikací pro každou platbu
- Zjednodušit UX plateb v Bitcoinu
- Nabízí alternativu k tradičním platebním metodám

Jak Bolt Card funguje?

- 1 Karta obsahuje NFC čip (např. NTAG424)
- 2 Přiložením ke čtečce se spustí HTTP požadavek
- 3 Čtečka získá informace o účtu (LNURLw nebo LNURLp)
- 4 Platba se odešle přes Lightning Network

Vrstvy Lightning Networku 1/2

1. Base Layer – Bitcoin Blockchain

- On-chain transakce (pomalejší, dražší, bezpečné)

2. Second Layer – Lightning Network (LN)

- Rychlé, levné off-chain platby
- Uzly, platební kanály, směrování

Vrstvy Lightning Networku 2/2

3. Application Layer – Aplikační vrstva nad LN

- **LNbits** – správa multiuživatelských peněženek, pluginy
- **Bolt Card, LNURL, Lightning peněženky**
- Propojuje vývojáře, podniky a koncové uživatele

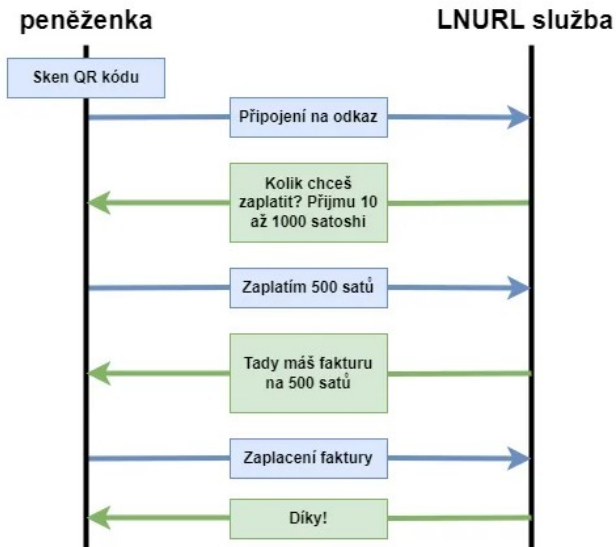
4. Experimental Layer – Budoucí a rozšířené koncepty

- Fedimint, RGB, Taro, LSATs
- Tokenizace, anonymita, přístupové systémy

LNURL protokol

- LNURL je protokol pro přenos platebních instrukcí přes HTTP
- Bolt Card používá variantu LNURLw (withdraw) nebo LNURLp (pay)
- Tato URL adresa je bezpečně uložena v NFC čipu

Ukázka jak funguje LNURL



Co potřebujeme k provozu?

- Lightning Node (např. LND, Core Lightning)
- LNBits server – pro generování LNURL a správu účtů
- Authme nebo LNURL-Auth – pro bezpečné přihlašování
- NFC čtečka a writer (např. Flipper Zero, ACR122U)

Vývojové nástroje a kompatibilita

- LNBits plugin: boltcard
- NFC čipy: NTAG213, NTAG424 (doporučen)
- Mobilní aplikace: Bolt Card App, BlueWallet (s LNURL), Wallet of Satoshi
- Open-source: vše dostupné na GitHubu

Bezpečnost Bolt Card

- Karta neobsahuje privátní klíče
- Autorizace se děje přes backend (LNBits)
- Využívá HMAC ověřování (v NTAG424) – zabrání spoofingu
- Možnost nastavit denní limity a blokace

Možné útoky a obrana

- **Replay attack:** zabráněno pomocí unikátního tokenu na každé použití
- **Skimming:** čip lze zamknout nebo používat jen pro čtení
- **Ztráta karty:** karta nemá přímý přístup k financím – vše je spravováno serverem

Reálné použití Bolt Card

- Konference (např. Bitcoin 2023) – platby za merch, jídlo
- Kavárny a restaurace přijímající LN
- Integrace s NFC čtečkami na Raspberry Pi

Výhody vs. nevýhody

Výhody

- Jednoduchost
- Rychlost (okamžitá platba)
- Bez potřeby aplikace
- Open-source

Nevýhody

- Závislost na backendu
- Nutnost vlastní infrastruktury
- Ztráta karty = nutnost deaktivace

Shrnutí a budoucnost Bolt Card

- Bolt Card přibližuje Lightning Network běžným lidem
- Nabízí UX srovnatelné s tradičními kartami

Literatura a odkazy



LNBits. *Bolt Card Plugin*. Dostupné na:
<https://github.com/lnbits/boltcard>



Bolt Card Guide. *Complete Setup Tutorial*. <https://boltcard.org>



Kryptoanarchista - Co je to LNURL?

Děkuji za pozornost

Jakub Růžička

VŠB – Technická univerzita Ostrava

jakub.ruzicka.st@vsb.cz

14. dubna 2025