Bitcoinová peněženka pro pokročilé uživatele

Jakub Dvořák | mobilní multisig peněženka s hardwarovou peněženkou Trezor

Vedoucí práce: RNDr. Filip Zavoral, Ph.D. | Katedra softwarového inženýrství | MFF UK | 2026

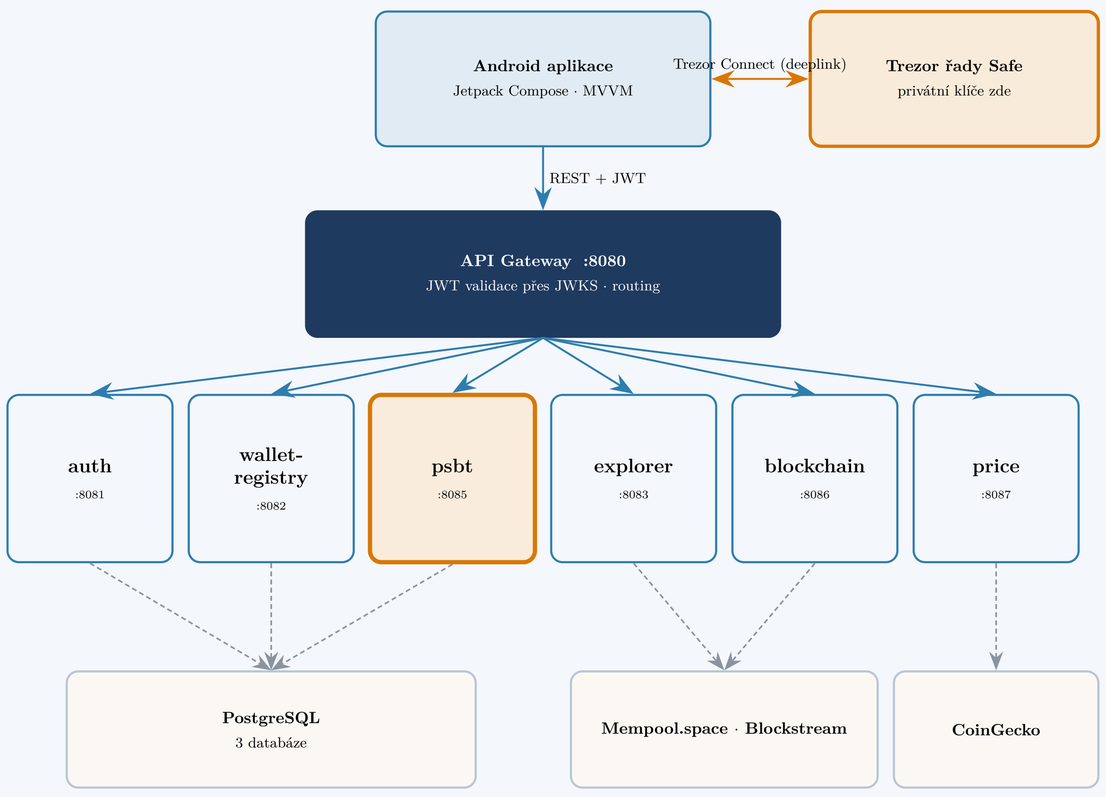
Motivace a mezera na trhu

Pokročilá správa Bitcoinu kombinuje tři techniky. **Hardwarová peněženka** drží klíče izolované na zařízení, **multisignature M-of-N** vyžaduje k utracení souhlas více klíčů a **coin control** umožňuje ruční výběr UTXO pro nižší poplatky a lepší soukromí. Na desktopu to vše zvládá Sparrow Wallet; **na Androidu ale žádná aplikace nespojuje všechny tři s přímou integrací Trezoru** nezávislou na cizí cloudové službě. Tuto mezeru práce zaplňuje.

Peněženka	Android	Multisig	Coin ctrl	Trezor přímo
Sparrow	✗	✓	✓	✓
Trezor Suite	✓	✗	✓	✓
Electrum mobil	✓	✗	✗	✗
BlueWallet	✓	✓	✓	✗
Nunchuk ~	✓	✓	✓	✓
Naše řešení	✓	✓	✓	✓

~ Nunchuk vyžaduje vlastní cloudovou službu a placené předplatné; BlueWallet integruje HW jen ručním přenosem PSBT souborů, ne přímo.

Architektura systému



API Gateway a šest mikroslužeb (Kotlin/Ktor)

- **API Gateway** :8080 — jediný vstup, validuje JWT přes JWKS a směruje požadavky
- **auth** :8081 — vydává RS256 JWT, identitu odvozuje z Trezor fingerprintu
- **wallet-registry** :8082 — derivace adres, parser deskriptorů, cosigneři
- **psbt** :8085 — tvorba, koordinace a broadcast PSBT, jádro celé práce
- **explorer** :8083 — agregace zůstatku, historie a UTXO
- **blockchain** :8086 — proxy na Mempool.space a Blockstream
- **price** :8087 — směnný kurz BTC na fiat z CoinGecko

Každá služba běží v samostatném kontejneru a má vlastní databázi; celkem tři instance PostgreSQL orchestrované přes Docker Compose.

Z čeho se skládá PSBT — BIP-174

GLOBÁLNÍ

`UNSIGNED_TX` kostra nepodepsané transakce — vstupy, výstupy, verze, locktime; dokument začíná magic bajty `0x70736274ff`

VSTUP × n

`WITNESS_UTXO` částka + scriptPubKey utráceného výstupu
`NON_WITNESS_UTXO` celá předchozí transakce; Trezor fw 2.3.1+ ji vyžaduje i pro nativní SegWit
`WITNESS_SCRIPT` multisig skript — klíče seřazené dle BIP-67
`BIP32_DERIVATION` odvozovací cesta veřejného klíče cosignera
`PARTIAL_SIG` dílčí podpisy cosignerů, sbírá se práh M

VÝSTUP × n

`BIP32_DERIVATION` cesta change adresy — Trezor díky tomu pozná change jako vlastní výstup, ne jako cizí platbu

Zajímavá implementační řešení — vlastní přínos

- **BIP-67 řazení podpisů na úrovni *odvozených* klíčů**, nikoli podle pořadí xpub — chybné umístění dá platný, ale *sítí odmítnutý* podpis.
- **`NON_WITNESS_UTXO` i pro nativní SegWit** — Trezor firmware 2.3.1+ ho vyžaduje jako mitigaci *SegWit fee útoku* dle BIP-143, ačkoliv PSBT pole je jen volitelné.
- **Korektní odhad poplatku pro multisig:** k 41 B režie vstupu se přičte witness — M podpisů (73 B) a N klíčů (34 B) — který SegWit (BIP-141) účtuje čtvrtinovou vahou. Pro 2-of-3: $41 + \lfloor(5 + 73 \cdot 2 + 34 \cdot 3)/4\rfloor = 104$ vB na vstup, nikoli 68 vB jako u singlesig; podcenění srazí poplatek pod cíl.
- **Prevence opakování change adres** napříč rozpracovanými PSBT — ochrana soukromí proti klastrování adres.
- **Robustní deeplink:** odpověď se ověřuje jednorázovým `requestId` ze SecureRandom; podpis jiným zařízením či passphrase se pozná přes fingerprint a vede k auto-logoutu; stav se obnoví i po zabití procesu.

Bezpečnostní model

- **Bezklíčový koordinátor:** backend drží jen veřejné `xpub` a indexy adres, **nikdy klíče**. I jeho kompromitace odhalí jen veřejná data. *Návrh této architektury je vlastní přínos.*
- **Ověření adresy na Trezoru** funkcí *Show On Trezor* — obrana proti podvržení adresy kompromitovaným klientem.
- **Autentizace:** RS256 JWT ověřované přes JWKS; refresh tokeny single-use s race-safe rotací, v databázi jen jejich SHA-256 otisk.

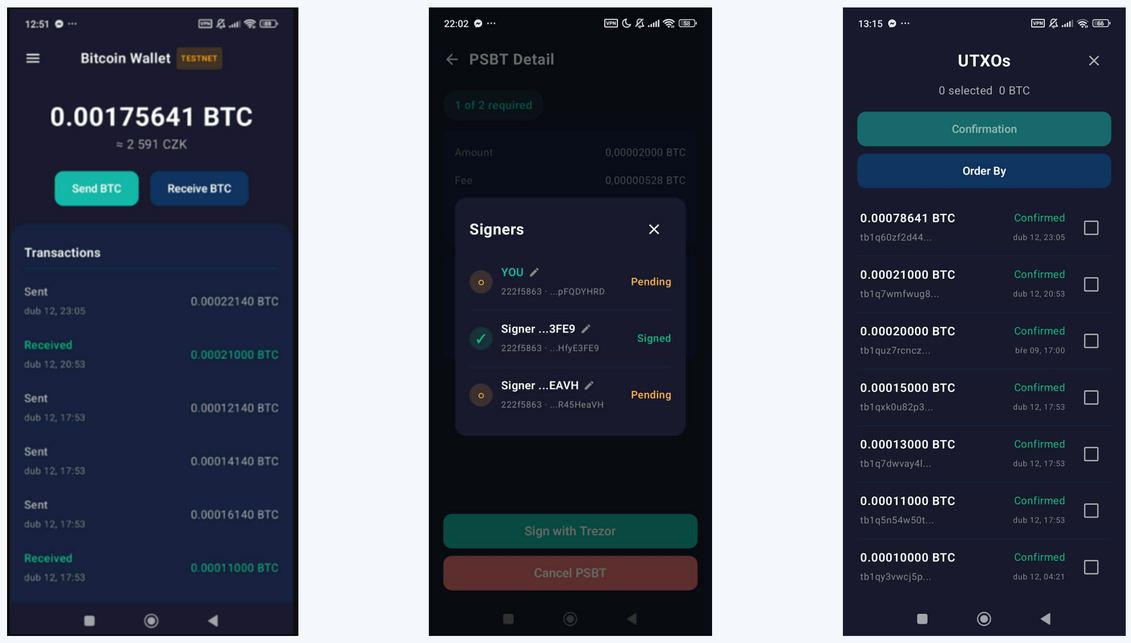
Ověření a testování

140 jednotkových testů napříč pěti moduly: konstrukce a kódování PSBT, witness skript a odhad vsize **parametrizované přes celý rozsah M-of-N** od 1-of-2 až po 15-of-15; derivace adres proti oficiálním vektorům BIP-84 a BIP-173; parser deskriptorů; race-safe rotace refresh tokenů; retry logika.

End-to-end na testnet4 s reálným Trezorem: kompletní singlesig i multisig tok od importu deskriptoru přes koordinaci podpisů až po broadcast, dále coin control a ověření adresy; **interoperabilita ověřena proti Sparrow Wallet**.

Standardy: BIP-32/39, **BIP-48/67**, BIP-84/141/143/173, **BIP-174**, BIP-380/383, BIP-125. **Frontend:** Jetpack Compose, knihovna `hummingbird` pro animované UR QR a ZXing.

Ukázky aplikace



Dashboard | stav podpisů multisig PSBT | coin control

Závěr | Zdrojový kód

Plně funkční Android aplikace, která zaplňuje mezeru v ekosystému — mobilní multisig s přímou integrací Trezoru a bez cizí cloudové služby. Backend nikdy nedrží privátní klíče, přesto plnohodnotně koordinuje multisig přes PSBT.

Dále: přímá USB komunikace s Trezorem; TLS a audit před produkcí; Taproot dle BIP-86; podpora dalších HW peněženek.

Zdrojový kód:

GitLab MFF UK + příloha v SIS