

KVANTOVÉ POČÍTAČE & BITCOIN.

Tomáš Sušánka · Trezor CTO

PROČ JE KVANTOVÝ POČÍTAČ PROBLÉM?

Z VEŘEJNÉHO KLÍČE ROVNOU PRIVÁTNÍ.

Veřejný klíč

Veřejná informace. Dnes z něj privátní klíč nikdo nespočítá.



Shorův algoritmus

Kryptograficky relevantní kvantový počítač řeší diskretní logaritmus v polynomiálním čase.



Privátní klíč

Podpis, utracení, hotovo. Žádný brute force, žádné hesla.

Platí to pro ECDSA i Schnorra stejně — obojí stojí na stejné křivce. **Hashe naopak drží:** Grover dává jen odmocninové zrychlení, takže SHA-256 zůstává bezpečný — včetně těžby.

KLÍČ ZA HASHEM.

SegWitová adresa neobsahuje veřejný klíč, ale jeho hash. Shorův algoritmus tedy nemá s čím pracovat — dokud z té adresy neutrátíš. Nejstarší a nejnovější outputy tuhle ochranu nemají.

SegWit

P2WPKH · BC1Q...

veřejný klíč



HASH160



v blockchainu

Klíč je skrytý. Odhalí se až podpisem.

P2PK

2009 · 1A1ZP1EP...

veřejný klíč



v blockchainu

Klíč je v řetězci od roku 2009. Včetně coinů, které se už nikdy nepohnou.

Taproot

P2TR · BC1P...

veřejný klíč



v blockchainu

Klíč je vidět od první přijaté transakce.

Hash ale není řešení, jen odklad. Ve chvíli utracení je klíč veřejný a útočník má okno, než transakce potvrdí.

KDO JE VIDĚT.

01

P2PK a staré coiny

U prvních outputů je veřejný klíč přímo v blockchainu. Včetně coinů, které se už nikdy nepohnou.

Nikdo je nezachrání

02

Znovupoužité adresy

Jednou utratím, veřejný klíč je venku. Kdo na stejnou adresu přijímá dál, nechává zůstatek odhalený.

Vlastní volba

03

Taproot

P2TR má veřejný klíč v outputu jako takovém. Elegantní pro Schnorra, nepříjemné pro kvanta.

P2TR

04

Každá transakce v mempoolu

Ve chvíli podpisu je klíč veřejný. Útočník má desítky minut na to, aby transakci přebil vlastní.

Okno na jeden blok

PROČ DĚLAT BITCOIN ODOLNÝ VŮČI KVANTOVÝM POČÍTAČŮM?



NAP.EDU · ZPRÁVA NATIONAL ACADEMIES O KVANTOVÝCH POČÍTAČÍCH

KLÍČOVÉ ZJIŠTĚNÍ 1

NEPANIKAŘTE.

„Vzhledem k současnému stavu kvantových počítačů a nedávnému tempu pokroku je vysoce nepravděpodobné, že v příští dekádě vznikne kvantový počítač schopný nabourat RSA 2048 nebo srovnatelné kryptosystémy s veřejným klíčem založené na diskretním logaritmu.“



NAP.EDU • ZPRÁVA NATIONAL ACADEMIES O KVANTOVÝCH POČÍTAČÍCH

KLÍČOVÉ ZJIŠTĚNÍ 10

PANIKAŘTE.

„I kdyby byl kvantový počítač schopný dešifrovat dnešní šifry víc než dekádu daleko, riziko takového stroje je dost vysoké — a čas potřebný na přechod na nový bezpečnostní protokol dost dlouhý a nejistý — na to, aby byla prioritizace vývoje, standardizace a nasazení postkvantové kryptografie **klíčová** pro minimalizaci šance na bezpečnostní katastrofu a ztrátu soukromí.“

STAVÍ SE — VELMI VELMI POMALU.

2016

IBM

5

QUBITŮ

IBM Q Experience — první kvantový procesor veřejně dostupný přes cloud.

2018

GOOGLE

72

QUBITŮ

Bristlecone — první seriózní krok k odolnosti proti chybám. Přesnost hradel zůstává úzkým hrdlem.

2021

IBM

127

QUBITŮ

Eagle — první procesor přes 100 qubitů, mimo dosah přímé klasické simulace.

2022

IBM

433

QUBITŮ

Osprey — počty qubitů se rok po roce zdvojnásobují podle veřejné roadmapy IBM.

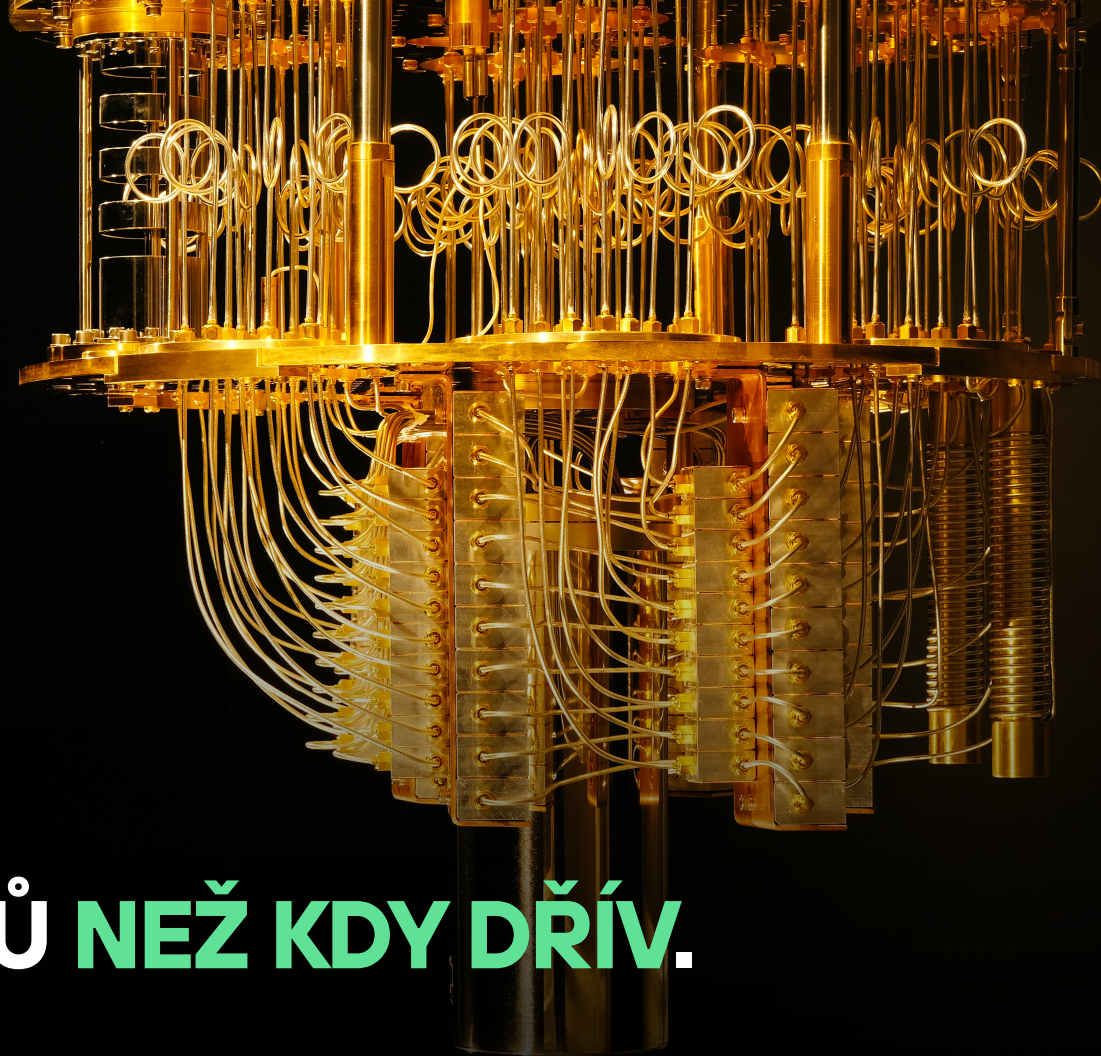
2023

IBM

1,121

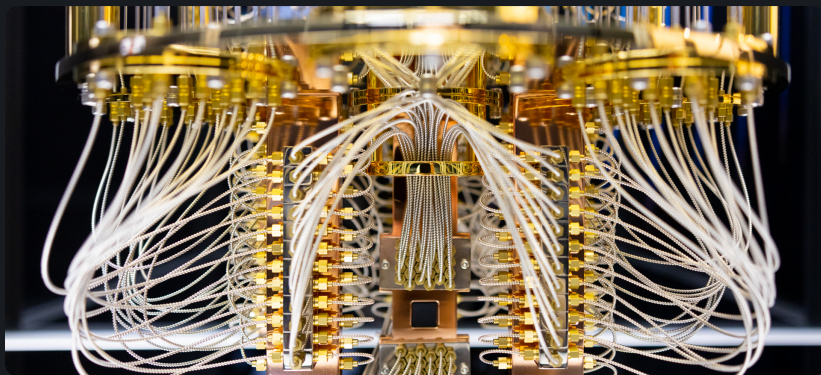
QUBITŮ

Condor — první za hranicí 1 000 qubitů. Chybovost zůstává hlavní překážkou.



ČÁST I · PROČ ANO

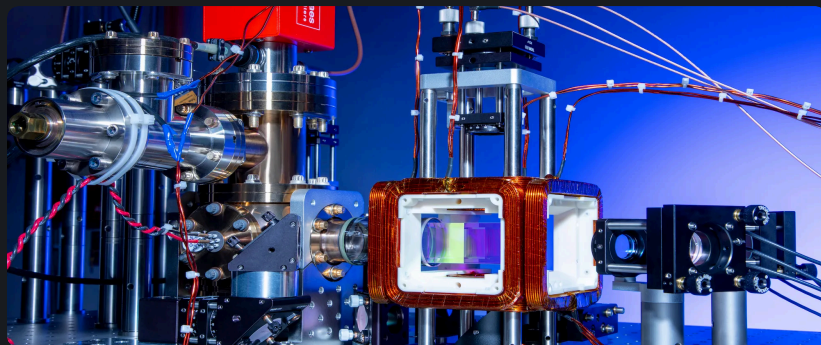
VÍC PŘÍSTUPŮ NEŽ KDY DŘÍV.



Supravodivé

GOOGLE · IBM · RIGETTI

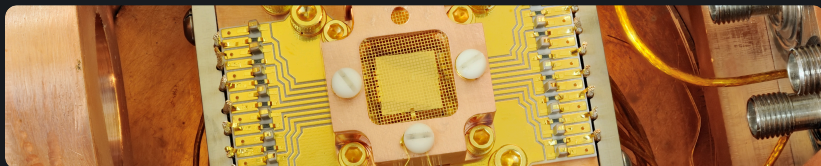
Supravodivé obvody chlazené téměř k absolutní nule. Dnešní lídři v počtu qubitů.



Neutrální atomy

ORATOMIC · QUERA · ATOM COMPUTING

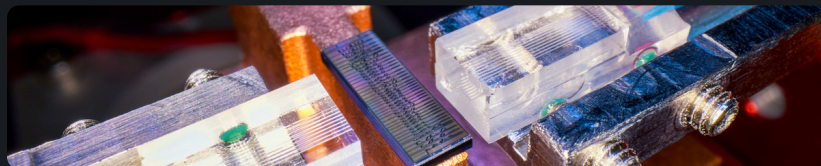
Jednotlivé atomy držené v optických pinzetách. Překonfigurovatelná pole — základ práce Oratomicu o 10K qubitech.



Zachycené ionty

IONQ · QUANTINUUM · HONEYWELL

Ionty držené v elektromagnetickém poli a ovládané lasery. Nejvyšší přesnost hradel ze všech platforem.



Fotonické

PSIQUANTUM · XANADU

Fotony jako qubity ve vlnovodných obvodech. Pokojová teplota — potenciál škálování ve standardní čipové výrobě.

ČÁST I · PROČ ANO

CÍL SE ZMENŠUJE.

~~10M~~



500K



10K

qubitů — starý odhad na zlomení
ECDSA. Vypadal nedosažitelně
daleko.

qubitů — práce Googlu z roku
2026. Supravodivý přístup. 20×
méně.

qubitů — Oratomic 2026.
Architektura neutrálních atomů a
3 roky. Další 50× méně.



MÁME UŽ POST- KVANTOVÉ ALGORITMY

CO TO VŮBEC JE.

Postkvantová kryptografie běží na klasickém počítači. **Jen stojí na jiném matematickém problému** — takovém, na který Shorův algoritmus nefunguje.

DÁVNÁ HISTORIE

RSA

Bezpečnost z faktorizace velkých čísel. První cíl, na který Shor v roce 1994 mířil — a důvod, proč se o kvantech vůbec mluví.

1977 · padne

DNES

Eliptické křivky

Bezpečnost stojí na diskretním logaritmu. To je přesně problém, který Shorův algoritmus řeší rychle.

ECDSA · Schnorr · padne

CESTA 1

Mřížky

Najít nejkratší vektor ve vícedimenzionální mřížce. Kvantový počítač tu žádnou zkratku nemá. Malé klíče, rychlé podpisy.

ML-DSA · FN-DSA

CESTA 2

Hashe

Bezpečnost jen z hashovací funkce, kterou už Bitcoin používá. Nejkonzervativnější volba — za cenu velkých podpisů.

SLH-DSA · SHRINCS

Nejsou to nové myšlenky. Hashové podpisy popsal Lamport v roce 1979 — stáří něčeho o dekádu víc, než má samotný Shorův algoritmus.

CO UŽ JE STANDARD.

STANDARDIZOVÁNO

ML-DSA

FIPS 204 · 2024 · mřížkové (Dilithium)

SLH-DSA

FIPS 205 · 2024 · hashové (SPHINCS+)

LMS / XMSS

NIST SP 800-208 · 2020 · stavové hashové

JEŠTĚ NE

FN-DSA

FIPS 206 se stále dopisuje · Falcon

SHRINCS

Draft specifikace · Blockstream Research

SQLsign · Falcon^{WS} · Raccoon-G

Akademické návrhy · roky výzkumu před sebou

Standard NIST ale není konsensus Bitcoinu. Žádné z těchto schémat zatím nemá v Bitcoinu přijatý BIP.

CO DÁL V BITCOINU

CO UDĚLAT DÁL V BITCOINU.

01

Nové PQ adresy

Shodnout se na BIP-360 a Pay-to-Merkle-Root — nový formát adres — a doplnit opkódy pro postkvantová podpisová schémata. Adresa i slovník, který za ní stojí.

P2MR · ML-DSA · SLH-DSA · SHRINCS

02

Umožnit migraci

Povolit dobrovolný přechod na kvantově odolné adresy.

Volba uživatele

03

Připravený stav

Uživatelé postkvantovou kryptografií používat nemusí. Mohou si vybrat, kterou možností budou utrácet.

Dvojitý commitment

Dnes

Tradiční
kryptografie



Tradiční podpis

Po soft forku

Tradiční

NEBO

PQ
neaktivní



Tradiční
podpis

beze změny

Kvantum přichází

Tradiční

NEBO

PQ



PQ podpis

PQ cena až tady

JENŽE KTERÝ POST- KVANTOVÝ ALGORITMUS?

Blockstream Research, květen 2026. Optimalizované hashové podpisy — a návrh opkódu OP_CHECKSHRINCS, který s postkvantovým Bitcoinem počítá už dnes.

PROPUSTNOST ROZHODUJE.

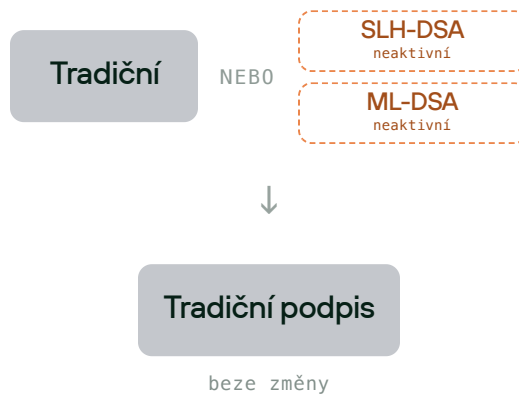
SCHÉMA	PODPIS	PROPUSTNOST	POZNÁMKA
Schnorr dnešní Taproot	64 B	6,5 tx/s	Dnešní základ, se vším — včetně BIP-32.
ML-DSA level 3	3 309 B	~0,5 tx/s	Propustnost se láme a BIP-32 mizí.
SLH-DSA level 1	7 856 B	0,36 tx/s	Konzervativní předpoklady, nejvyšší cena.
SLH-DSA rozpočet 2^40 podpisů	5 792 B	0,48 tx/s	Stačí snížit rozpočet podpisů na klíč.
SHRINCS compact cesta	580 B	až 3,0 tx/s	Vyžaduje ale stav — a ten musí někdo držet.

Blockstream Research, květen 2026. Průměrná transakce, dnešní limit bloku.

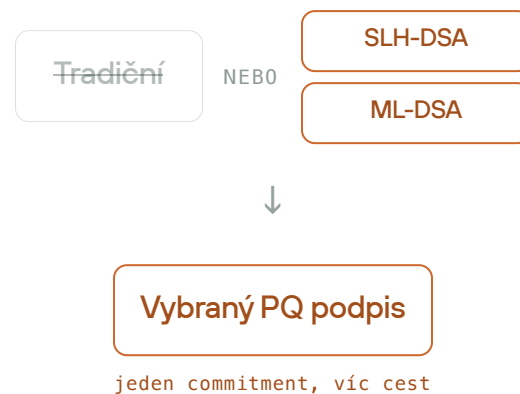
Dnes



Po soft forku



Kvantum přichází



SHRINCS.

Jeden veřejný klíč, dvě cesty podpisu. **Stav nikdy neopustí zařízení** — a to je přesně to, co hardware wallet umí a mobil ne. Když se přístroj ztratí, nové zařízení automaticky přepne na bezstavovou cestu.

580 B

Stavová cesta

Rychlý podpis, nejmenší data — dokud zařízení drží své počítadlo podpisů.

PRIMÁRNÍ ZAŘÍZENÍ

~4 336 B

Bezstavový fallback

Vždy dostupný, žádný stav. Rozpočet 2^{32} podpisů — nikdo nezmáčkne tlačítko čtyři miliardy krát.

PO OBNOVĚ ZE SEEDU

Stav byl naším problémem — tady je z něj výhoda. C++ implementace, draft specifikace i demo na Liquidu už existují; nasadit to jde přes Taproot v2 nebo BIP-360.

ZVLÁDNOU TO HARDWARE WALLETY?

Malé MCU, pár set kilobajtů RAM, žádná plovoucí čárka a seed na papíře. Co z postkvantové kryptografie se tam vlastně vejde?

CO SE NA ČIP VEJDE.

ALGORITMUS	VEŘEJNÝ KLÍČ	PODPIS	NA HARDWARE WALLETĚ	VERDIKT
SLH-DSA SPHINCS+ · hashové	32 B	7 856 B	Potřebuje jen SHA-2, které už v čipu máme. Podpis trvá sekundy, ale nic nového neriskujeme.	V POHODĚ
ML-DSA Dilithium · mřížky	1 312 B	2 420 B	Celočíselná aritmetika, desítky milisekund. RAM na hraně u starších modelů, na nových bez problému.	V POHODĚ
FN-DSA Falcon · mřížky	897 B	666 B	Nejmenší podpisy, ale vzorkování v plovoucí čáře. Konstantní čas na MCU je otevřený problém.	OTAZNÍK
LMS / XMSS hashové · stavové	~60 B	~2–3 kB	Rychlé a konzervativní, ale je nutné držet stav. Jeden jednorázový klíč použitý dvakrát znamená ztrátu prostředků.	NE

Velikosti pro nejvyšší úroveň bezpečnosti (NIST level 1–2). Vyšší úrovně jsou 2–3x větší.

ZMĚŘILI JSME TO NA TREZORU.

VARIANTA	PODPIS	OVĚŘENÍ	PODPIS	KÓD
ML-DSA-44 Dilithium · level 2	78 ms 55 kB RAM	21 ms	2 420 B	15 kB
FN-DSA-512 Falcon · level 1	510 ms 44 kB RAM	7 ms	666 B	61 kB
SLH-DSA-128f SPHINCS+ SHA-2 · level 1	3,6 s 20 kB RAM	210 ms	17 088 B	13 kB
SLH-DSA-128s SPHINCS+ SHA-2 · level 1	75 s 10 kB RAM	75 ms	7 856 B	13 kB
ML-DSA-65 / 87 FN-DSA-1024 také	OOM nevejde se do 64 kB haldy			

Referenční implementace z PQClean, bez hardwarové akcelerace hashů. Hashovací část jde ještě výrazně zrychlit.

KDE JE SKUTEČNÝ PROBLÉM.

01

Derivace klíčů

Pro postkvantová schémata nemáme obdobu BIP-32. Bez odvozování veřejných klíčů nefunguje watch-only ani obnova účtů z xpubu.

Chybí standard

02

Stav vs. seed

Stavová schémata se s obnovou ze zapsaného seedu neslučují. Papírová záloha stav podpisů nikdy nevrátí.

LMS · XMSS

03

Secure element

Dnešní bezpečnostní čipy postkvantové podpisy neumí. Klíč tedy zůstává v MCU — a to mění model útočníka.

Zatím bez SE

04

Velikosti a UX

Podpis o 2–8 kB znamená delší přenos, větší PSBT a pomalejší potvrzování na malém displeji.

2–8 kB na podpis

**DÍKY ZA
POZORNOST.**