FAQ

Hier finden Sie Antworten auf häufig gestellte Fragen zur jeweiligen Moduldokumentation sowie zu Funktionen, Inhalten und Anwendungen.

- BTC-Empfängeradressen erklärt

BTC-Empfängeradressen erklärt

Was ist der Unterschied zwischen einer klassischen Empfängeradresse und einer Silent Empfänger Adresse?

Empfängeradresse
Die Empfängeradresse ist die klassische Form, Bitcoin an eine andere Person oder ein Unternehmen zu senden. Sie funktioniert ähnlich wie eine Kontonummer im Bankwesen: Der Sender trägt die Adresse ein, und der gewünschte Betrag wird dorthin übertragen. Solche Adressen werden von Wallets erzeugt und können öffentlich weitergegeben werden, zum Beispiel auf Rechnungen, Webseiten oder in Zahlungsanfragen. Da Bitcoin-Transaktionen grundsätzlich in der Blockchain nachvollziehbar sind, kann eine mehrfach verwendete Adresse von Dritten eingesehen und mit Zahlungseingängen verknüpft werden. Aus diesem Grund empfehlen viele Wallets, für jeden Zahlungseingang eine neue Adresse zu verwenden.

Silent Payment Adresse

Die Silent Payment Adresse ist eine moderne Alternative zur klassischen Empfängeradresse und wurde entwickelt, um die Privatsphäre beim Empfang von Bitcoin zu verbessern. Statt eine sichtbare Empfangsadresse weiterzugeben, wird ein öffentlicher Schlüssel verwendet, aus dem kompatible Wallets automatisch für jede Zahlung eine neue, individuelle Empfangsadresse ableiten. Dadurch erscheint auf der Blockchain nicht dieselbe Adresse mehrfach, was Rückschlüsse auf Zahlungseingänge erschwert. Silent Payments eignen sich besonders für Nutzer, die regelmäßig Zahlungen empfangen oder ihre Finanzdaten besser schützen möchten. Voraussetzung ist, dass die verwendeten Wallets diese Funktion unterstützen.

Klassische Bitcoin-Empfängeradressen

Klassische Bitcoin-Adressen dienen als öffentliche Zieladressen für den Empfang von BTC. Es gibt drei Hauptformate:

Format	Präfix	Beispiel	Beschreibung
P2PKH	`1...`	`1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`	Legacy-Adresse, veraltet, hohe Gebühren
P2SH	`3...`	`3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy`	Für Multisig oder Scripts
Bech32	`bc1q...`	`bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh`	Native SegWit (P2WPKH), niedrige Gebühren

Format	Präfix	Beispiel	Beschreibung
Taproot	`bc1p...`	`bc1p5cyxnuxmeuwuvkwfem96l0hu32k6sd59k5u2dd`	P2TR (seit 2021), Grundlage für BIP-0352

Diese Adressen sind **öffentlich sichtbar** und jede Transaktion an diese Adresse ist in der Blockchain **direkt zuordenbar**.

Silent Payment Empfangsadressen (BIP-0352)

Silent Payments sind ein besonders **datenschutzfreundlicher Adresstyp**, bei dem:

- keine wiederverwendbare BTC-Adresse veröffentlicht wird,
- jede Zahlung automatisch auf einer neuen Zieladresse eingeht,
- der Empfänger Zahlungen durch Scan der Blockchain erkennt – ohne Onchain-Verknüpfung.

Aufbau:

Silent Payments nutzen keinen klassischen Bitcoin-Adress-String, sondern einen sogenannten **Scan-PubKey** (auch: **x-only Public Key**). Dieser wird in folgendem Format veröffentlicht:

> silent:pubkey=f3c1d4b8e5a1c0d2b7f98ab3d378ff45a56739c0d59d3e49d23e89dd1b35c3af

- Der Schlüssel besteht aus 32 Byte und wird hexadezimal kodiert (64 Zeichen).
- Alternativ verwenden viele Wallets das kompaktere Format mit **sp1...**-Präfix (Bech32m-kodiert).
- Beide Formate sind gleichwertig – die Unterstützung hängt von der verwendeten Wallet ab.

Für den Empfänger:

- Veröffentlicht **nur** seinen Scan-PubKey (z. B. in einer der beiden Varianten).
- Erkennt eingehende Zahlungen durch regelmäßiges Scannen der Blockchain.
- Nutzt dazu eine Silent Payments-kompatible Wallet (z. B. Cake Wallet, Dana Wallet, SilentPay).

Für den Sender:

- Muss eine Wallet mit **Silent Payments-Sendeunterstützung** verwenden.
- Die Zieladresse wird automatisch berechnet und **regulär als Taproot-Zahlung** durchgeführt.

- Aktuell unterstützte Wallets: u. a. SilentPay, Dana Wallet, Cake Wallet, BitBox02 (nur senden).

Unterschiede im Überblick

Merkmal	Klassische BTC-Adresse	Silent Payment Adresse
Sichtbarkeit in Blockchain	Öffentliche Adresse	Zieladresse ist nur für Empfänger erkennbar
Format	`1...`, `3...`, `bc1q...`	`silent:pubkey=...`
Wiederverwendung	Sollte vermieden werden	Kann **dauerhaft** veröffentlicht werden
Datenschutz	Schwach	**Sehr hoch**
Wallet-Kompatibilität	Weit verbreitet	Aktuell nur in Spezialwallets

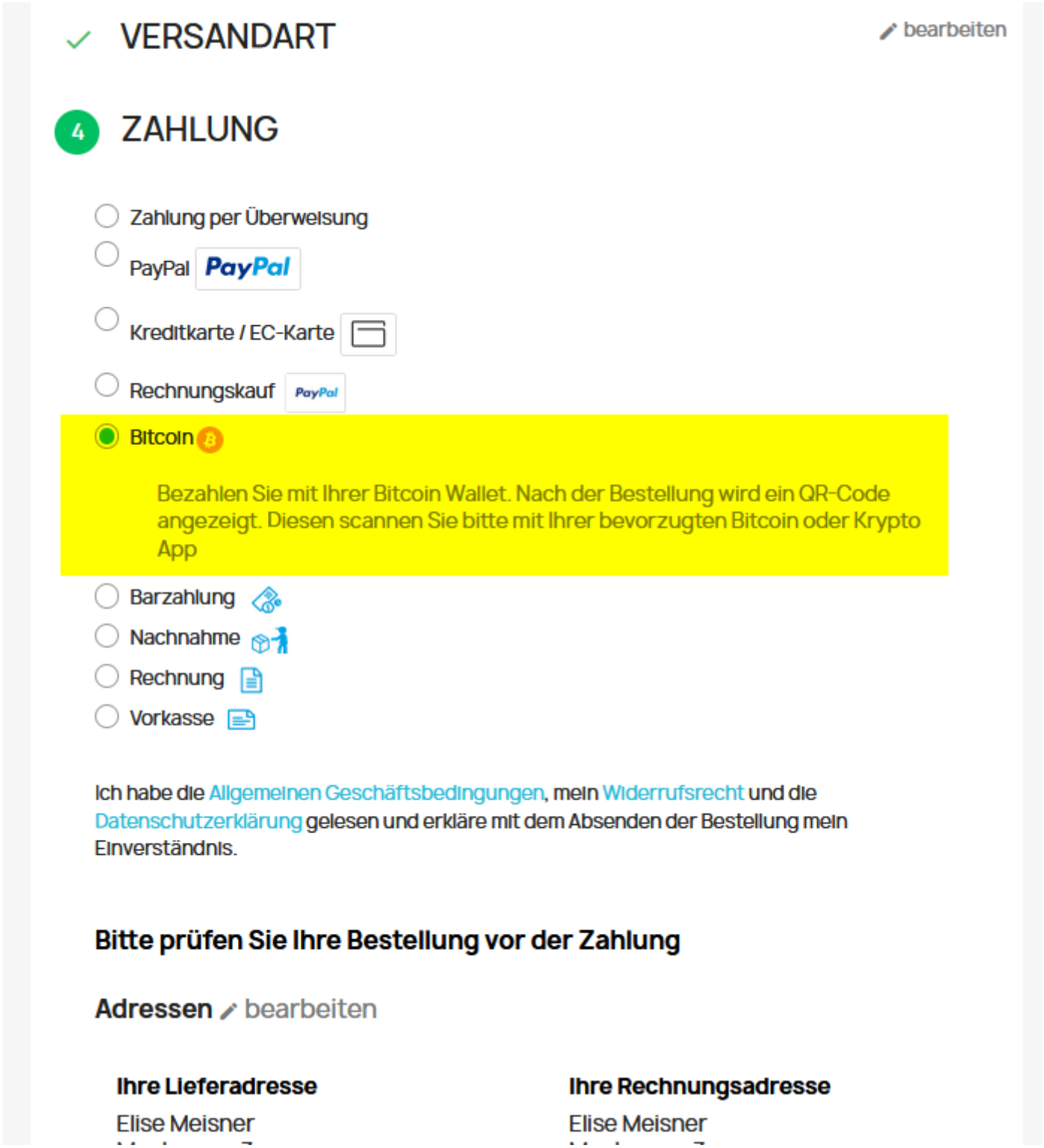
Silent Payments erhöhen die Privatsphäre erheblich, ohne neue Coins oder zentrale Dienste einzuführen.
Sie basieren auf Taproot und sind vollständig **Bitcoin-kompatibel**, benötigen aber passende Wallets zur Nutzung.

Silent Payments – Wallet-Kompatibilitätstabelle

Wallet	◫◫ Empfangen	◫◫ Senden	Plattform	Hinweise
BitBox02	▯ Nein	▯ Ja	Hardware (Desktop App)	Nur Senden unterstützt (ab Firmware 9.21.0 / App 4.45.0)
BlueWallet	▯ Nein	▯ Nein	Android / iOS	Keine Taproot- oder SP-Unterstützung
Cake Wallet	▯ Nein	▯ Nein	Android / iOS	Kein SP-Fokus
Calke Wallet	▯ Ja	▯ Ja	Android (F-Droid)	Privacy-fokussiert, gute QR/Export-Tools
Dana Wallet	▯ Ja	▯ Ja	Android / Desktop (FOSS)	Aktive SP-Unterstützung, manuell installierbar über F-Droid
Electrum	▯ Nein	▯ Nein	Desktop	Kein offizieller SP-Support
Ledger Live	▯ Nein	▯ Nein	Desktop / Mobile	Kein SP-Support, Taproot vorhanden

Wallet	□□ Empfangen	□□ Senden	Plattform	Hinweise
Samourai Wallet	□ Nein	□ Nein	Android	Fokus auf CoinJoin, kein BIP-352
Shakesco Wallet	□ Ja	□ Ja	CLI / Dev Tool	Für technisch versierte Nutzer, CLI-basiert
SilentPay Wallet	□ Ja	□ Ja	Android (GitHub Build)	Open Source, vollen BIP-352 Support
Silentium Wallet	□ Ja	□ Ja	PWA (Browser)	Modernes Webinterface mit vollständigem SP-Support
Sparrow Wallet	□□ Bald	□□ Bald	Desktop	SP-Funktion in Entwicklung (teils via Script nutzbar)
Trezor	□ Nein	□ Nein	Hardware (Web App)	Kein Taproot-Support in Core → kein SP
Wasabi Wallet	□ Nein	□ Nein	Desktop	Fokus auf CoinJoin, kein SP geplant

Zahlung mit Bitcoin und QR-Codes auf der Bestellbestätigungsseite



Sollten beide Adressen im Modul konfiguriert sein, werden auf der Seite der Bestellbestätigung auch beide QR-Codes angezeigt:



Standard Bitcoin Zahlung

Jetzt mit Bitcoin zahlen!



Silent Payments

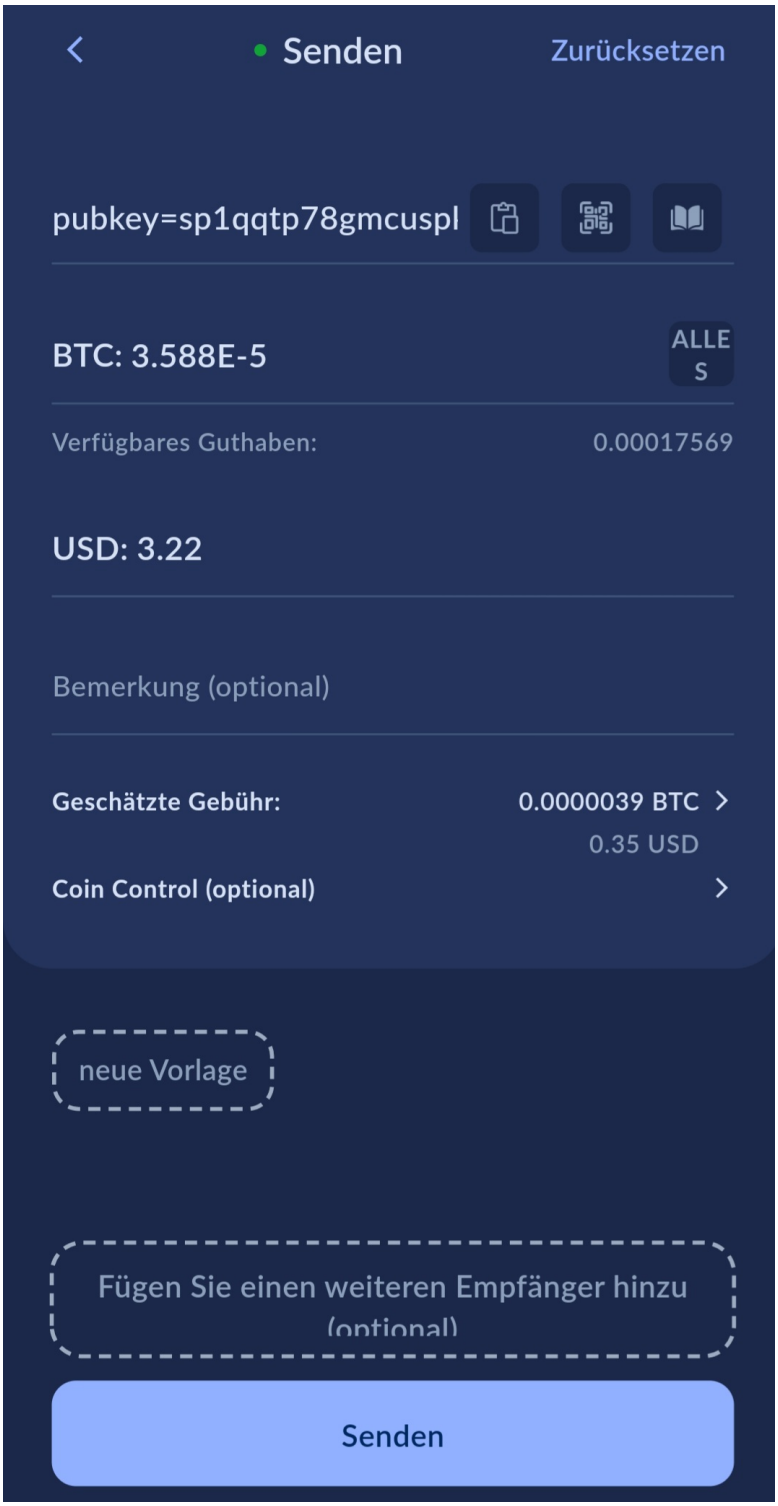
(Bitcoin Zahlungen für maximale Privatsphäre)

Jetzt mit Silent Payments in Bitcoin bezahlen!

Scanne den QR-Code mit einer Silent-Payment-kompatiblen App (BitBox02, Cake-Wallet, Dana, SilentPay,...)

Betrag in BTC	**0,00286679 BTC**
Betrag in SATS	286679 SATS
Betrag in EUR	215,71 €
Wechselkurs EUR/BTC	75.244,54
Wechselkurs BTC/EUR	0,00001329
BTC-Empfänger-Adresse	bc1qf5f4qzvf0hsc4pjzss7mt6ndska4fc4l4vx0v4
BTC-Silent-Payment-Adresse	sp1qqtp78gmcuspksr7u70uudvvkthpcs0thstskc4yk4ewnm30zwaxfcqlkvqxjmmvugqxqt804rqfd0zz995xuxpxwlkwuyngylpexw3jhc5va9dfy

In der Regel erkennt die Wallet beim Scannen des QR-Codes automatisch den Betrag (hier Dana Wallet für Android):


Senden
Zurücksetzen
pubkey=sp1qqtp78gmcuspl
BTC: 3.588E-5
ALLES
Verfügbares Guthaben:
0.00017569
USD: 3.22
Bemerkung (optional)
Geschätzte Gebühr:
0.0000039 BTC
0.35 USD
Coin Control (optional)
neue Vorlage
Fügen Sie einen weiteren Empfänger hinzu (optional)
Senden