BITHIDE | Confidential Crypto Wallet for Business

Top Crypto Payment Solutions

Pros, Cons, Comparative Analysis

BITHIDE | Confidential Crypto Wallet for Business

Business in the Age of Crypto

For me, cryptocurrencies are not just an investment or a speculative tool, but a capacity that can hold any amount of tangible assets and seamlessly move them.

In different industries, there are both thousands of daily micro-payments and strategic transfers worth millions of dollars. Companies must manage both streams with equal efficiency: ensuring uninterrupted small-scale operations while minimizing risks in large transactions.

But the reality is clear: the more a business relies on crypto payments, **the more challenges it faces**. Security, AML, choosing the right jurisdiction, account freezes, wallet vulnerabilities, and the absence of banking secrecy on the blockchain — all of this makes processes heavy and unpredictable.

My mission is to help businesses work with cryptocurrencies effectively. That's why we are launching **a series of expert materials** where we will explore the key aspects of the crypto industry for businesses and provide actionable, practice-driven recommendations.

In our first release, we analyzed **nine leading crypto payment providers**, so you can make a well-informed choice that fits the needs and demands of your business.

Vasyl Zolochevskyi
CBDO | Blockchain & Fintech Strategist, BitHide

Key Takeways

Scale matters

In 2024, stablecoin transfers hit $27.6T, surpassing Visa + Mastercard combined.

Growth of B2B crypto adoption

Stablecoin market capitalization has reached $251.7 billion, while corporate usage has grown by 25% — mainly for cross-border payments and supply chain settlements. Today, more than 25,000 online merchants worldwide accept them.

Custodial vs. non-custodial

Custodial = convenience with third-party risk. Non-custodial = full control, but self-managed security.

Hybrid use is common

Companies often mix custodial wallets for operations and self-custody cold storage for reserves.

Security gaps cost billions

Centralized wallets remain hacker honeypots; Bybit’s $1.5B hack pushed 2025 losses past $2.17B.

Provider landscape

Options range from custodial Fireblocks, Coinbase Commerce (hybrid), B2BinPay, CoinGate — to privacy-first non-custodial BitHide, BTCPay, Wasabi.

Privacy features differ

Only some solutions (e.g., BitHide, Wasabi) add IP masking, proxy routing, or CoinJoin; others expose metadata.

Bottom line

Businesses must weigh convenience, compliance, and sovereignty — the choice defines risk exposure and operational freedom.

Introduction

According to Coinbase's June 2025 Report[1], the total stablecoin transfer volume reached $27.6 trillion in 2024 — more than the combined turnover of Visa and Mastercard. At the same time, stablecoin capitalization reached $251.7 billion[2], with a daily trading volume fluctuating between $20–25 million. All of this indicates that crypto payments have already become an essential part of the global financial system.

Much of this growth is driven by B2B use cases: cross-border transactions, payroll, and supply chain settlements. This is where cryptocurrencies deliver key advantages — speed, lower transaction costs, and independence from traditional banking rails. Nowadays, more than 25,000 merchants worldwide already accept stablecoins, and the number continues to grow.

But with this rapid adoption of cryptocurrencies in business operations come **new challenges**:

- operational processes getting out of control — from accounting and reconciliation to cash flow management;
- high servicing costs, lack of automation, and reliance on manual management slowing down scalability;
- complex integrations, frozen accounts, and wallet breaches.

It remains **unclear which crypto payment provider can address these issues comprehensively**, meet all of a business's needs, and truly support its growth and scalability.

That's why our team has prepared this report. Here, we compared and analyzed **the key players in the industry** — Fireblocks, NOWPayments, Coinbase Commerce, B2BinPay, CoinGate, BitHide, Plisio, BTCPay Server, and Wasabi Wallet — across the main criteria:

- Architecture and security
- Privacy and protection features (encryption, IP shielding, authentication and access control, transaction anonymization)
- Product capabilities (scalability, White Label, AML tools, bulk operations)
- Integration and developer experience

---

[1] "The State of Crypto: the Future of Money Is Here," n.d., https://www.coinbase.com/ru/blog/the-state-of-crypto-the-future-of-money-is-here.

[2] Barry Elad, "Stablecoin Statistics 2025: Growth, Adoption, and Regulation," CoinLaw, September 6, 2025, https://coinlaw.io/stablecoin-statistics/

The report includes both a detailed comparison for each criterion and a **full table covering all providers**. In addition, we've added a dedicated section showing which solutions are best suited for different industries.

Use this report as a practical guide to make informed, well-balanced decisions when choosing your provider.

The BitHide Team

The volume of stablecoin transfers

$27.6T
in 2024

Table of Content

Table of Content

1. Architecture and Security

Crypto payment solutions can generally be divided into two types — custodial and non-custodial. It all comes down to who controls the private keys. There are also hybrid solutions.

Custodial Wallet

Custodial

Here, a third party — such as an exchange or a payment service — is responsible for storing and managing your keys. This option is more common among beginners or companies that don't yet have experience working with cryptocurrencies.

Pros

- Maximum convenience.
- Simple setup, with the ability to restore access via password.
- Security is handled by the provider.

Cons

- The old rule applies: "Not your keys — not your crypto." With a custodial wallet, you're trusting a third party: their honesty, competence, and financial stability.
- There are risks: the provider can be hacked, go bankrupt, or freeze your account at the request of a regulator.
- Since the keys are held by the custodian, they can restrict or completely block withdrawals — for example, at the request of law enforcement or due to internal compliance rules.

In practice, these risks are not very different from traditional banking: transaction censorship and loss of control over your funds are possible — the very issues cryptocurrency was originally meant to solve. The history of major hacks and collapses, including exchange bankruptcies (such as FTX), clearly shows how vulnerable users of custodial solutions can be.

Non-Custodial Wallet

Non-Custodial (Self-Custody)

You store your own keys — the provider only supplies the software or device to use them and has no access to your assets.

Pros

- Maximum control, security, and financial sovereignty.
- Only the wallet owner has access to the private keys, so no outside party can censor transactions or seize funds.
- Independence from third-party errors or legal issues.
- Suitable for businesses that need full autonomy.
- A non-custodial wallet does not require KYC (Know Your Customer), unless you choose to implement it yourself.

Cons

- Full responsibility lies with the user.
- Losing your seed phrase or making a management mistake = loss of funds.
- Requires well-thought-out processes for secure storage and backups.

Examples of Non-Custodial Solutions

BitHide

BitHide[5] operates as a fully non-custodial, privacy-focused infrastructure for businesses that want to store and transact with crypto entirely under their own control. Unlike custodians, BitHide never has access to client private keys or signing capability. Keys are generated, encrypted, and stored locally by the client, often in isolated environments and never transmitted to BitHide's servers.

Plisio

Plisio[6] is a crypto payment gateway that functions on a **payment forwarding model.** When a customer pays a merchant via Plisio, the crypto is received by Plisio's system only momentarily and is automatically forwarded directly to the merchant's own wallet address once confirmed. This means Plisio does not retain custody of funds after the transaction. There is no long-term balance held on a Plisio account.

Plisio's service is largely "set it and forget it" with coins going straight to the user. This design makes Plisio **non-custodial** – the platform manages the transaction processing but does not store private keys or maintain custodial wallets for merchants. Thus, like NOWPayments, Plisio handles the crypto in transit but not in storage, making it a non-custodial gateway.

BTCPay Server

It is an open-source crypto payment processor[7] that merchants can run on their own server, often alongside a Bitcoin full node. It is **inherently non-custodial** – the merchant has full control of the cryptocurrency addresses and private keys.

[5] "Crypto Wallet for Business," n.d., https://bithide.io/.

[6] "Cryptocurrency Payment Gateway," Plisio, n.d., https://plisio.net/

[7] BTCPay Server Foundation, "BTCPay Server Foundation," n.d., https://foundation.btcpayserver.org/.

BTCPay can be connected to the merchant's own wallet or node. It does not require trusting a third-party service.

In summary, BTCPay Server is a fully non-custodial, decentralized payment solution. It's essentially a do-it-yourself gateway that eliminates intermediaries.

Wasabi

It is a desktop Bitcoin wallet[8] focused on privacy (CoinJoin Mixing). It is, by design, a **self-custody wallet.** Users hold their own private keys, stored encrypted on their device, unlocked by their password. Wasabi never takes custody of coins. All wallet actions are initiated and signed locally by the user. Even when participating in CoinJoin rounds via Wasabi, the user's wallet collaborates with a coordinator server, but the keys remain with the user. Thus, Wasabi Wallet is a classic **non-custodial wallet.**

[8] "Wasabi Wallet: The Privacy Focused Bitcoin Wallet," n.d., https://wasabiwallet.io/.

Hybrid Approach

Many companies use a **Hybrid Approach.** For example, keeping operational funds in a custodial service but securing large reserves in a self-custody cold wallet.

It’s important to remember that custodial platforms remain prime targets for hackers. A single successful attack can wipe out the balances of thousands of clients.

By August 2025, total losses from breaches had exceeded ≈$2.17 billion[9], with the largest share coming from the $1.5 billion Bybit hack. In that case, hackers didn’t attack the exchange directly but exploited a third-party software provider embedded in its transaction signing process.

This incident underscored a simple truth: by choosing a custodial solution, a business inherits not only the risks of the provider itself but also the vulnerabilities of its entire technical ecosystem. That’s why, when making a choice, it’s critical to weigh not just features and convenience, but also the reliability of the third-party services that underpin the system.

[9] Chainalysis Team, “2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Records,” Chainalysis, August 18, 2025, https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/.

Examples of Hybrid Solutions

Coinbase Commerce

It[10] has two modes: **Self-Managed (Non-Custodial) and Coinbase-Managed (Custodial).** In the Self-Managed Commerce mode, each merchant's commerce account is a non-custodial wallet – upon setup the merchant is given a seed-phrase, and Coinbase does not hold the private keys.

In contrast, the Coinbase-Managed Commerce plan entrusts custody to Coinbase. In this mode, Coinbase will manage the crypto on behalf of the merchant – funds can be automatically converted to fiat or transferred to the merchant's Coinbase account, and even fiat payouts to the bank are supported. It likely requires KYC and an application since Coinbase is taking on custody.

Thus, Coinbase Commerce is hybrid: default use is non-custodial (for global access and simplicity), while an enterprise merchant can opt into a fully custodial service by Coinbase for additional features like fiat settlement.

Fireblocks

It is an enterprise digital asset[11] infrastructure provider whose core offering is an MPC (Multi-Party Computation) wallet platform. In the standard Fireblocks setup, private keys are split among multiple parties (e.g., client, Fireblocks, and backup shares). So, no single party has the full key. Fireblocks' cloud MPC servers co-sign transactions with the client, enabling a secure custodial-like service where Fireblocks assists in transaction authorization without holding unilateral control.

Because of this, **Fireblocks often markets itself as not a pure custodian but rather a secure operations platform.** Clients have a level of control (policies, final approvals) while Fireblocks manages key shares and the infrastructure.

[10] "Coinbase Commerce," n.d., https://www.coinbase.com/commerce.

[11] Fireblocks, "Fireblocks | Leading Digital Asset Infrastructure," August 25, 2025, https://www.fireblocks.com/.

Fireblocks

Recently, Fireblocks also launched a Non-Custodial Wallet Solution[12] (SDK). With the Fireblocks Non-Custodial Wallet SDK, businesses can let end-users generate and store keys entirely on the user's device, and Fireblocks is removed from the key management in that flow. In summary, Fireblocks offers both: an MPC-based custody platform, a custodial service with Fireblocks co-managing assets, and developer tools for pure non-custodial wallets. Thus, its key storage model is hybrid, depending on configuration.

NOWPayments

NOWPayments

It[13] is primarily **a non-custodial crypto payment gateway.** Merchants receive payments directly to their own wallets, and NOWPayments doesn't store cryptocurrency[14], never have private keys to any of client's wallets. By design, it generates a one-time deposit address for each payment (to track and convert funds) but automatically transfers the crypto to the merchant's outcome address once received.

No private keys are held by NOWPayments under the standard flow. If needed, merchants can request a "partial custody" feature – an opt-in to let NOWPayments hold funds temporarily, but absent that, the service is non-custodial. So, NOWPayments actually have a hybrid custody model: default custody-free operations, with a custodial wallet option available on request.

[12] Fireblocks, "Embedded Wallets | Fireblocks," July 28, 2025, https://www.fireblocks.com/platforms/embedded-wallets/.

[13] NOWPayments, "Crypto Payment Gateway — the Best Solution for Accepting Cryptocurrency for Your Business," April 4, 2025, https://nowpayments.io/.

[14] NOWPayments, "Where Are My Funds Stored?," NOWPayments, April 22, 2021, https://nowpayments.io/help/about-nowpayments/about/where-are-my-funds-stored.

Final Formula

CUSTODIAL =

CONVENIENCE WITH THIRD-PARTY RISK

NON-CUSTODIAL =

CONTROL WITH SELF-MANAGED RISK

HYBRID SOLUTION =

BALANCE: DAILY OPERATIONS RUN THROUGH CUSTODIAL INFRASTRUCTURE, WHILE RESERVES AND LARGE AMOUNTS ARE STORED IN NON-CUSTODIAL COLD WALLETS.

2. Protective Technologies and Privacy

When considering crypto payment platforms, it’s important to compare their built-in security technologies and privacy features. Beyond the custody model, consider the following protective measures:

Data Encryption

AES-256

Data Encryption

Modern systems typically employ AES-256 or equivalent standards to secure data. AES-256 is approved by NIST (National Institute of Standards and Technology) and widely regarded as robust for most use cases today. Not even quantum computers can crack it within a practical timeframe.

- For example, **Fireblocks** highlights[15] infrastructure-level cryptographic protection, using MPC to split private keys across multiple nodes, and SGX hardware enclaves to isolate sensitive operations. This approach reduces the risk of key compromise by removing single points of failure.

- **BitHide** goes one step further. It uses per-user application-level encryption (based on modern ciphers such as AES-256) to protect wallet data and usage history. Each user's data is encrypted with a unique key, which significantly complicates any large-scale decryption if a single key is compromised.

[15] Fireblocks, "Crypto Enterprise-Grade Security Platform | Fireblocks," June 6, 2025, https://www.fireblocks.com/platforms/security.

For callbacks, BitHide supports an optional signing feature: in addition to standard HTTPS transport, a client-defined secret key can be used to append a hash to the callback payload for integrity verification. This feature is configurable and disabled by default, allowing businesses to decide whether to enable it based on their security policies.

- Another popular opinion, **CoinGate,** operates[16] with standard SSL/TLS encryption, and claims to protect data transfers with industry-standard methods plus multisig wallets and 2FA. In the case of **B2BinPay,** the platform offers[17] multi-layered security, including AES-based encryption, 2FA, address whitelisting, threshold controls, and user rights systems. They also undergo third-party audits.

- **NOWPayments** relies[18] on cold storage for most funds, two-factor authentication, and withdrawal whitelists, ensuring that even if one layer is compromised, attackers cannot easily access user balances. **Plisio** takes a simpler approach[19] with immediate forwarding of payments through secure HTTPS channels, which eliminates long-term custody risks.

- On the enterprise side, **Coinbase Commerce** leverages[20] the broader Coinbase infrastructure: SSL/TLS encryption, 2FA, multi-approval vault withdrawals, and industry-grade compliance audits, backed by regulatory oversight.

---

[16] Vilius Barbaravičius, “Crypto Scams Guide for Business | How to Avoid With CoinGate,” Best Bitcoin & Crypto Payment Processor, May 16, 2025, https://coingate.com/blog/post/crypto-scam-threats.

[17] “Crypto Payment Gateway & Processing | B2BINPAY,” n.d., https://b2binpay.com/en.

[18] NOWPayments, “Where Are My Funds Stored?,” NOWPayments, April 22, 2021, https://nowpayments.io/help/about-nowpayments/about/where-are-my-funds-stored.

[19] “WHMCS Cryptocurrency Payment Plugin - Plisio,” Plisio, n.d., https://plisio.net/whmcs-accept-crypto.

[20] “Coinbase Security,” n.d., https://www.coinbase.com/security.

- Finally, self-hosted solutions like **BTCPay Server** and privacy-first wallets such as **Wasabi** put the burden[21] of key management on the merchant or user. BTCPay depends on the merchant's infrastructure and HTTPS, while Wasabi routes all traffic through Tor, adds client-side encryption, and enhances privacy with CoinJoin transactions.

Summary Comparison

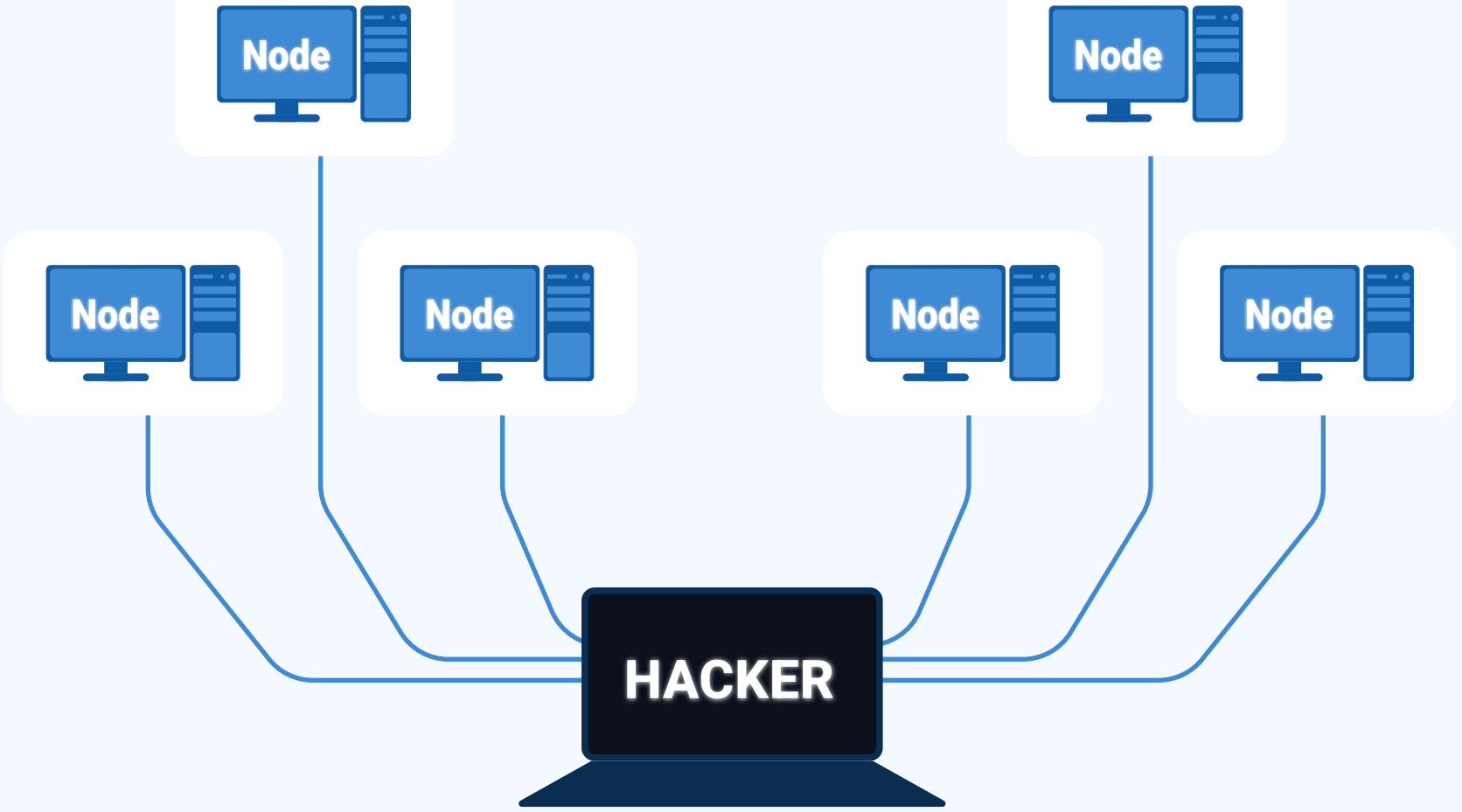
Provider	Encryption at Rest	Key Architecture	Callback Protection	Notes
Fireblocks	Yes (AES, SGX Enclave)	Distributed Via MPC	Not Specified	Hardware-Based Isolation, Policy Engine
BitHide	Yes (AES-256 and equivalents)	Self-Hosted Per-User Keys	Yes (Encrypted)	High Isolation, Self-Managed Infrastructure
B2BinPay	Yes (AES Likely)	Centralized	No	Focus On Access Controls And Audits
CoinGate	In Transit Only (TLS's)	Multisig Wallets	No	Merchant-Oriented, Simple Setup
NOW Payments / Plisio	SSL/TLS's Only	Basic Multisig	No	Suitable For Lightweight Payment Scenarios
Coinbase Commerce	Yes (AES, GCP-based)	Centralized, Coinbase Custody	No (API Webhooks Only)	Strong Regulated Entity, US-Based, Integrated With Coinbase Infrastructure
BTCPay Server / Wasabi	Self-Managed (User-Defined, optional AES)	User-Controlled Wallets (Full Node, Wasabi CoinJoin)	No (Manual Setup)	Open-Source, Privacy-First, Non-Custodial, Focus On Anonymity

[21] "BTCPay Server Documentation | BTCPay Server," n.d., https://docs.btcpayserver.org/Guide/.

IP Address Protection

IP Address Protection

Surprisingly, cryptocurrencies are not entirely anonymous. When a transaction is broadcast, the server's IP address may be visible to the connected network nodes. This metadata can be correlated with on-chain activity, potentially revealing the wallet's origin or infrastructure, and physical server location. To address this, advanced solutions implement IP-masking features to preserve operational privacy.



- For instance, BitHide's "Dark Wing"[22] technology routes wallet traffic through rotating nodes to obscure the source IP, enhancing network-level privacy without compromising functionality. It routes all wallet network traffic through a combination of Tor and VPN nodes, using dynamic IP rotation for each transaction. Because Tor alone can be blocked by the blockchain nodes, BitHide cleverly passes the traffic from Tor into VPN servers.

- Another example is Wasabi. It automatically routes[23] all traffic through Tor, so your IP remains hidden when broadcasting transactions or querying the blockchain. This applies to both direct node connections and CoinJoins. Each network request is made over a fresh Tor circuit to break likability via the IP address.

- On the other hand, BTCPay, a widely used self-hosted payment processor for merchants, isn't focused on per-transaction IP cloaking. However, it can be accessed[24] via Tor when deployed as an onion service, providing a certain level of anonymity, though the IP does not rotate by default with every transaction.

---

[22] BitHide Team, "Dark Wing Technology: Absolute Anonymity and Data Protection in Blockchain," BitHide Blog, August 22, 2025, https://bithide.io/blog/dark-wing-blockchain-anonymity/.

[23] "Network-Level Privacy | Wasabi Docs," n.d., https://docs.wasabiwallet.io/why-wasabi/NetworkLevelPrivacy.html.

[24] "Wallet FAQ | BTCPay Server," n.d., https://docs.btcpayserver.org/FAQ/Wallet/.

- By contrast, platforms like CoinGate, NOWPayments, B2BinPay, Fireblocks, Plisio, and Coinbase Commerce do not implement IP-level anonymization at all. They rely on standard HTTPS and enterprise-grade security measures but leave the IP layer visible to the network. In the end, it comes down to what matters most for your business: out-of-the-box privacy, user-level anonymity, or infrastructure sovereignty.

Summary Comparison

Solution	IP Protection	How It Works	Notes / Focus
BitHide	Yes (Dark Wing)	Routes all wallet traffic via Tor → VPN with rotating IPs for every transaction	Dynamic IP rotation, high privacy without losing functionality.
Wasabi	Yes (Tor Only)	All traffic routed through Tor, fresh circuits per request	Funds get tainted when mixed. Not compliance-friendly
BTCPay Server	Partial	Can be deployed as a Tor onion service, but the IP is not rotated per transaction	Focused on merchant use, not per-tx anonymization.
Fireblocks	No	Standard HTTPS, enterprise security	Prioritizes compliance and enterprise-grade security, not IP masking.
Coinbase Commerce	No	HTTPS, integrated with Coinbase infra	Strong regulated entity, IP metadata not hidden.
B2BinPay	No	Standard HTTPS	Focus on centralized custody and access controls.
CoinGate	No	HTTPS + Multisig wallets	Merchant-oriented, simple setup, no IP masking.
NOWPayments / Plisio	No	SSL/TLS only	Lightweight payments, no privacy at the network layer.

Authentication
& Access Control

Authentication & Access Control

Since crypto wallets handle valuable assets, strong user authentication is a MUST. At a minimum, solutions should support Two-Factor Authentication (2FA) for logins or transactions and enforce secure credentials (PIN Codes or Multi-Step Logins). Device fingerprinting is another layer some wallets use – essentially identifying and trusting specific devices or browser environments, so that an unrecognized device triggers additional verification.

Think of it like having not just one lock on your front door, but two, and if someone tries to sneak in from an unknown device, the system should immediately ask, “Wait, who are you?”.

- For example, in **BitHide**, access to the wallet is secured through a combination of login (e-mail), secret key, PIN, and fingerprint. API access exists by default, but to use it, you must have a valid API key for the specific wallet — without it, no API commands can be executed. Once an API key is issued, most non-sensitive functions (e.g., creating a new address via POST /Address/GetAddress) can be used immediately.

  However, certain sensitive operations, such as withdrawals via API, AML checks via API, or payment verification, are disabled unless explicitly enabled in the wallet’s settings. This means that even if an attacker somehow obtained an API key, they could not withdraw funds or perform AML checks unless those capabilities had been turned on by the wallet owner. When withdrawals via API are enabled, additional safeguards like network whitelisting and withdrawal rules can be applied to further limit risk.

If 2FA is enabled for the account, confirming a new device still requires access to the owner's e-mail, providing another layer of defense against unauthorized access.

- **Fireblocks** goes for a corporate-grade model with MPC approvals: no single employee or machine can push funds out, which is why it's popular with institutions. Coinbase Commerce relies on the entire Coinbase security stack, encompassing 2FA and multi-approval vaults, all within regulated infrastructure.
- By contrast, **B2BinPay** adds merchant-oriented controls like IP whitelists and role-based logins, while **NOWPayments** takes a simpler path: standard 2FA plus withdrawal whitelisting. **Plisio** minimizes the problem altogether by forwarding payments right away, so there's no big «piggy bank» to defend.

- For smaller businesses, **CoinGate** keeps things light, mostly 2FA and API separation, while **Wasabi** and **BTCPay Server** flip the script entirely. Wasabi doesn't push multifactor logins at all, because its philosophy is privacy-first: everything is routed through Tor, and security relies on the user's own key backups. BTCPay Server leaves the rules up to whoever hosts it. Run it with onion services and strict HTTPS, and you're safe. Skip those, and, well, you're basically trusting your own server hygiene.

In short, some providers give you a ready-made security stack, others hand you the keys and say, "It's your castle, defend it how you like." Overall, look for a solution that implements multifactor authentication, configurable API access controls, granular user roles, and activity logs to prevent and detect unauthorized actions. Choose a solution that makes sense for how much responsibility you want to carry yourself — and always, always keep that second lock on the door.

Summary Comparison

Solution	Authentication & Access	How It Works	Notes / Focus
BitHide	Login + Secret Key + PIN + 2FA+ Fingerprint + role-based access.	Web app secured by multi-step login, API keys required. Sensitive ops (withdrawals, AML checks) are disabled by default, but can be enabled with whitelists & rules.	Granular controls, security-first for API access.
Fireblocks	MPC + Policy Engine	Multi-Party Computation approvals, role-based governance, programmable limits	Institutional-grade, no single point of failure.
Coinbase Commerce	Coinbase Security Stack	2FA, multi-approval vaults, regulated infra	Enterprise-grade, tightly coupled with the Coinbase ecosystem.
B2BinPay	Role-Based Logins + IP Whitelists	Merchants can restrict by IP, assign roles, and control withdrawals	Merchant-oriented, compliance-aligned.
NOWPayments	2FA + Whitelisted Withdrawals	Lightweight 2FA, only trusted addresses can withdraw	Simple but effective for small ops.
Plisio	Minimal	Forwards payments directly, no funds stored	Little surface for attackers; Less flexibility.
CoinGate	2FA + API Separation	Protects logins with 2FA, keeps API and account layers apart	Lightweight controls for SMEs.
Wasabi	No 2FA (Self-Custody)	Privacy-first, all via Tor. Security depends on the user's key backups	User bears full responsibility.
BTCPay Server	Self-Configured	Depends on how the merchant deploys it (HTTPS, onion services, custom 2FA)	Full DIY. Flexible but risky if mismanaged.

Transactional Anonymization

Transactional Anonymization

Blockchain is transparent by design, so malicious actors, hackers, or even competitors can monitor addresses and analyze transaction flows, revealing wallet balances, cash flow patterns, or links between business entities. To prevent this, advanced crypto payment platforms implement privacy-preserving features that break the traceability of funds. One technique for increasing privacy is using one-time addresses and «proxy payments», where the payment flow is structured to break direct links between the payer and the final recipient.

- BitHide's Proxy Payments implement[25] this approach without mixing unrelated clients' funds or using blockchain mixers like CoinJoin. Instead, the client can choose a proxy payment, in which case a unique one-time address is generated for the transfer. This protects the client's transactions from clustering, since the addresses cannot be linked to each othe. In addition, temporary addresses are used to cover network fees on blockchains like BNB or Tron. The user sets a threshold value, and once it's reached, the temporary address is deactivated. This makes it much harder to cluster transactions by the fee-payment address.

[25] BitHide Team, "Added Proxy Payment Capability | Release 2.35," BitHide Blog, July 31, 2024, https://bithide.io/blog/release-2-35/.

This design complicates standard blockchain tracing by making it harder to directly associate a customer's deposit with the merchant's final receiving address. When evaluating providers, it's worth checking whether they rely solely on native blockchain features or add their own privacy layers (address rotation, proxy routing, custom transaction flows) to shield operational logic from external observers. For businesses handling sensitive transactions or operating in gray markets, these additional layers can be critical for reducing exposure.

- **On the other hand, Wasabi** uses CoinJoin to literally mix your coins with others, making it extremely hard to tell which output belongs to whom. It's a strong layer of privacy, though businesses sometimes avoid it because regulators can frown on «mixed» funds.

- One lesser-known legend in privacy tech is **Samourai Wallet**. We hadn't mentioned it initially because its approach went far beyond pure privacy. It offered CoinJoin via Whirlpool, «Ricochet» hops, PayNyms, and more, making it a privacy titan. But its developers were recently charged[26] with running an unlicensed money-transmitting service tied to illicit mixing, despite the wallet being strictly non-custodial. This case underscores that at a certain point, privacy features built into the product, especially those marketed toward shielding users from law enforcement, can attract legal risk.

- Back to business-focused tools: **BTCPay Server**, when self-hosted, puts address control entirely in your hands, but requires manual privacy steps like rotating addresses or running as a Tor onion to hide IPs. Platforms like **CoinGate** or **NOWPayments** generate fresh addresses per invoice but don't provide deeper cloaking. **Fireblocks** leans the other direction: built for institutional transparency and auditability, not anonymity.

[26] Cointelegraph Research, "Samourai Wallet Shutdown: Implications for Other Privacy and Self-custody Tools," Cointelegraph, June 14, 2024, https://cointelegraph.com/news/samourai-wallet-shutdown-implications-for-other-privacy-self-custody-tools.

So, when evaluating providers, consider how they handle privacy. Do they rely on underlying blockchain features? Or do they add layers (such as mixing services, address rotation, coinjoin, etc.) to protect your transactional logic from prying eyes?

Well, businesses dealing with sensitive transactions or operating in gray markets will want the latter. And as Samourai's story reminds us, leaning too far into privacy without compliance protections can land you in hot water.

3. Infrastructure and Product Capabilities

Beyond security, businesses must assess a crypto payment solution’s scalability, customization, and feature set. Key questions: Can it grow with your transaction volume?
Can it support multiple business units or brands?
Is the interface or logic adaptable to your needs?
So, here are the most important considerations regarding infrastructure and products.

Scalability
& Multi-Tenancy

Scalability & Multi-Tenancy

As crypto operations expand, the system should be able to handle increasing load and organizational complexity. Be sure to check if the platform supports multiple wallets or workspaces under a single account, and whether there are any limits on the number of addresses or transactions.

- Some solutions, like **BitHide**, offer unlimited scalability, allowing businesses to create as many wallets or workspaces as needed to segregate funds across projects, departments, or clients.

- By contrast, platforms like **NOWPayments** or **CoinGate** are designed for straightforward merchant use-cases. They’re great if you’re just plugging in a checkout button, but they usually don’t give you workspace-level isolation or advanced orchestration, so things get messy if you try to run several parallel financial flows.

- At the other end of the spectrum, **Fireblocks** takes scalability seriously with a multi-tenant custodial SaaS architecture. It lets enterprises manage hundreds of wallets with policy-driven controls, though at very high volumes, you might run into tiered pricing or API constraints.

- **B2BinPay** sits somewhere in between: multi-wallet support is there, but the depth of roles and accounts you can configure often depends on which plan or license you've bought.

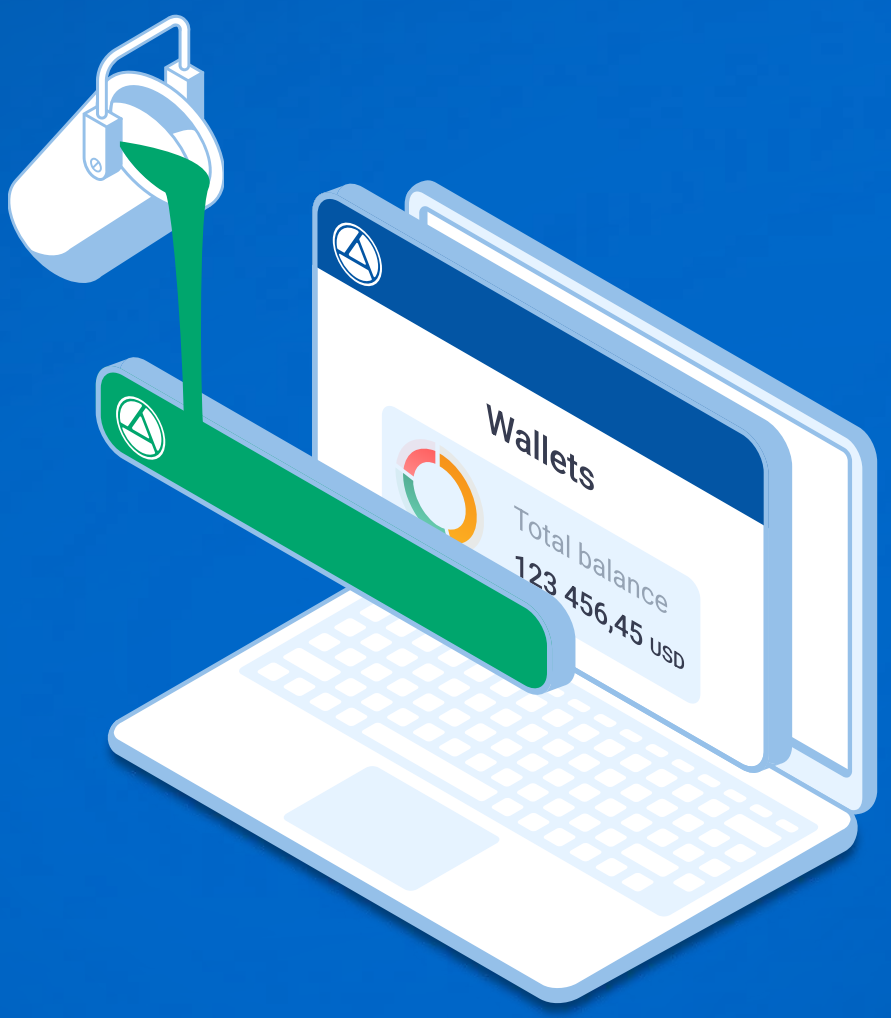
- Open-source stacks also deserve a mention here. **BTCPay Server**, when self-hosted, gives you full control to spin up unlimited merchant stores and wallets under one node, but the flipside is that scaling becomes your problem. You need the infrastructure and DevOps discipline to keep performance steady as volumes rise. However, this payment solution is limited to Bitcoin only, which restricts its use for businesses needing multi-currency support.

- And if we step into the privacy-first world, wallets like **Wasabi** don't really do multi-tenancy in the enterprise sense. They're end-user tools, not orchestration layers. Still, their design illustrates the trade-off: you can have strong privacy or strong enterprise scaling, but usually not both in the same package. The wallet also works only with Bitcoin, just like BTCPay Server.

Summary Comparison

Solution	Scalability & Multi-Tenancy	How It Works	Notes / Focus
BitHide	Unlimited wallets & workspaces	Businesses can create as many wallets/projects/ departments as needed.	Flexible fund segmentation for corporate clients, mid-market, and high-risk businesses
Fireblocks	Multi-tenant SaaS custodial infra	Hundreds of wallets with policy-driven controls; Role-based orchestration.	Enterprise-grade, but pricing/API tiers can cap scale
B2BinPay	Multi-wallet with plan-based depth	Support for multiple accounts, but role/account features depend on license tier.	Middle ground, flexible for merchants
NOWPayments	Single-merchant focus	Easy checkout button, but no workspace isolation.	Best for simple use-cases, not complex orgs
CoinGate	Limited scaling	Basic merchant layer, supports 2FA & APIs, but no enterprise orchestration.	Small business friendly
BTCPay Server	Unlimited (self-hosted), Bitcoin only	Run as many merchant stores/wallets as your infra allows.	Fully customizable, but scaling is on you
Wasabi	No multi-tenancy, Bitcoin only	Privacy-first, single-user wallet routed through Tor.	Not built for enterprise orchestration

Customizability and White-Label Options



Customizability and White-Label Options

You must also consider how much you can tailor the solution to your brand and workflow. So, what does white-label mean? White-Label capability means the provider's software can be rebranded and deployed under your own domain/branding. Some crypto payment gateways explicitly offer white-label packages. Some crypto payment gateways explicitly offer white-label packages designed for fast deployment and full brand control.

In addition, beyond branding, customizing wallets and controlling business logic are important. Can you configure how AML checks are triggered? Set up mass payout workflows or auto-withdrawal scenarios? Adjust how each wallet behaves? The most flexible platforms allow you to manage these flows fully, from custom payment pages and buttons to granular settings for every sub-wallet.The best solutions offer extensible APIs and potentially source code options, allowing for product adaptation.

- For example, **BitHide's** platform exposes a REST API and webhooks that let you build custom workflows on top of the core wallet. On the other hand, Fireblocks provides APIs, SDKs, and a comprehensive Policy Engine so that businesses can set transaction approvals, roles, limits, and governance rules programmatically, including via webhooks and embedded wallet SDKs.

- **NOWPayments** and **CoinGate**, for instance, offer lightweight APIs and plugins that are perfect if you just want to drop a payment button into your website or connect to Shopify, but you won't be scripting complex payout logic there. **B2BinPay** gives you a middle ground: API access with options for mass payouts and AML triggers, though the level of control depends on the license tier. Plisio positions itself as a simple plug-and-play solution, with APIs focused mostly on checkout integration rather than deep wallet orchestration.

- Open-source stacks show another flavor: **BTCPay Server** can be extended endlessly if you have the dev muscle, since you control the source code, but it means building features like payout automation yourself — and it only works for Bitcoin. Privacy wallets illustrate yet another trade-off: **Wasabi** bakes in Tor routing and CoinJoin automation, but it's not really meant for business logic or AML hooks. And then there's **Coinbase Commerce**, which provides polished APIs and checkout pages but with a more controlled environment – great UX, though less room for tweaking under the hood compared to Fireblocks or self-hosted setups.

So, you must look for features like custom webhooks, plugin support, or scriptable rules, which indicate you can extend or tweak the platform to fit your unique needs. This flexibility ensures the gateway can align with your business processes instead of forcing you to work around a black-box product.

User Roles and Permissions

User Roles and Permissions

It is important to mention that crypto wallets should support Role-Based Access Control (RBAC). And it deserves a chapter of its own. But shortly, this means you can create different roles (e.g., Viewer, Trader, Approver, Admin) and assign employees permissions appropriate to their job. It's a critical feature for internal security and operational efficiency, especially given the rise in phishing attacks and insider threats. The recent Coinbase breach, for example, involved a social engineering attack[27] that compromised support staff access, highlighting the need to limit permissions and isolate critical actions. That could have been contained if permissions were properly segmented.

Let's look at **BitHide** as a concrete example. BitHide supports highly flexible role-based access control, allowing businesses to configure permissions in detail and tailor them to specific workflows. There is also double transaction approval. For example, a manager can initiate a payment, but it will not be executed until it is approved by someone with the appropriate confirmation rights. At the same time, it's possible to configure roles without payment confirmation at all if the process doesn't require it. The system goes far beyond simple "view" or "transfer" rights.

[27] BitHide Team, "Coinbase Hack: How Attackers Stole Data From 70,000 Customers," BitHide Blog, August 21, 2025, https://bithide.io/blog/crypto-exchange-hack-coinbase-2025/.

Permissions can be set for: Transactions & Withdrawals, Auto-Withdrawals, Wallets, Addresses, Gas Stations, AML, Logs, Portfolio, Technical Actions, Review, and Mobile Administration. To simplify role management, BitHide also includes predefined permission templates:

Full Rights

Complete access to all actions except strictly administrative tasks (e.g., creating users, managing licenses).

No Withdrawals, No AML Checks

Blocks all types of withdrawals and manual AML address checks — suitable for analysts or those who only review transactions.

No AML Checks

User cannot initiate AML checks (manually or via auto-withdrawals); all other actions are allowed.

No Withdrawal Confirmation Rights

Users can create withdrawals but cannot approve them, ideal for separating initiation and confirmation roles.

Custom

Activated automatically when permissions are manually configured, providing full flexibility.

Fireblocks, for instance, gives enterprises a programmable Policy Engine that can enforce multi-step approvals and governance-level rules. **B2BinPay** provides multi-role structures too, but often gated by plan or license level. Coinbase Commerce and **NOWPayments** stick to lighter permission layers, offering basic access splits but not advanced approval workflows. Meanwhile, open-source options like **BTCPay Server** let you go as deep as your developers are willing to build. Maximum flexibility, but, as usual, more hands-on work.

The ability to define roles is handy if you plan to use one system across multiple departments or merchants, each of which can have its own partitioned access within the same platform. Which end you choose will define whether your system is genuinely resilient or just «formally» segmented.

Mass Operations (Bulk Payments & Automation)

Mass Operations (Bulk Payments & Automation)

In a B2B context, you also frequently need to execute mass payouts. Manually sending crypto one by one is a guaranteed way to waste time and increase the risk of errors. That's why it's important to check whether the gateway supports true bulk operations, uploading a structured table of recipients and amounts, scheduling payouts in advance, or setting up programmatic distribution.

- In **BitHide**, you can send mass payouts to a list of recipients in just a couple of clicks. The system automatically checks the list for valid address formatting and duplicates. You can also set up auto-withdrawals: once an address balance reaches the user-defined threshold, all funds are automatically transferred to one or multiple cold wallets — or any other wallets you specify.

  For payroll specifically, BitHide offers BH Mobile, a dedicated plugin designed for paying salaries in cryptocurrency. It's tailored to streamline salary processing, so finance teams can handle recurring payouts to employees with minimal friction. On top of that, BitHide's Proxy Payments can combine funds from multiple wallet addresses (or selected ones) into a single outgoing transaction.

- **Fireblocks** supports batch operations and automation, but as a custodial SaaS, high volumes can run into policy or pricing limits.

- **B2BinPay** provides mass payouts but with varying automation levels depending on the plan.

- **NOWPayments** and **CoinGate** allow bulk sends via API, though scheduling and automation are much more basic.

- **Plisio** offers simple bulk sending without deep automation.

If frequent payouts are a core part of your business rhythm, choose a platform that not only supports scheduling, limits, frequency settings, and multi-currency batches, but also offers the right mix of automation, payroll-focused tools, and privacy features to match your operational needs.

AML and Compliance Functions

AML and Compliance Functions

Reliable AML tools today are needed not only for regulatory compliance but also for protection against direct financial risks.

A single tainted transaction can result in funds being frozen or investigations that disrupt your business. For instance, only Chainalysis estimates[28] that the total value received by known illicit addresses reached at least $40.9 billion in 2024. And if that doesn't worry you, consider this: Tether's enforcement unit (in collaboration with TRON and TRM Labs) managed to freeze $126 million in USDT during 2024 alone. Meanwhile, as of mid-2025, **over $2.9 billion** worth of USDT tied to illicit activities has been blocked[29] or confiscated.

This means that businesses face a real risk of having incoming funds frozen if they originate from illicit sources, making proactive transaction screening (AML/KYT) an essential part of operational security.

---

[28] Chainalysis Team, "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized," Chainalysis, June 5, 2025, https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

[29] "Tether Acknowledged by U.S. Authorities for Freezing $1.6M Connected to Terrorism Financing - Tether.io," n.d., https://tether.io/news/tether-acknowledged-by-u-s-authorities-for-freezing-1-6m-connected-to-terrorism-financing/.

AML Solutions for Business

As a business, you need to catch tainted money at the doorstep, rather than unknowingly handling it and facing consequences later. That is not scalable nor safe in 2025's regulatory climate. A strong compliance solution will perform:

Address Screening

Checking the counterparties' wallet addresses against watchlists (OFAC Sanctions Lists, Known Scam Addresses, etc.) and risk-scoring them (e.g., risk percentage or category like "Darknet Exposure").

Transaction Monitoring

Analyzing patterns such as huge transfers, in-and-out movements, or mixing services usage.

Source of Funds Tracing

Looking at the origin of inbound crypto (how far back to a known clean source, whether it passed through mixers like Tornado Cash, etc., sometimes called KYT (Know Your Transaction).

The best systems are not one-size-fits-all but offer a compliance console to fine-tune checks and see detailed analytics. In addition, consider if the provider keeps up with AML/KYT regulations. In the last year or two, frameworks like the Travel Rule[30], MiCA[31] in Europe, etc., have introduced new requirements. A forward-looking solution will update its AML/KYC features accordingly.

[30] "The FATF Recommendations," n.d., https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

[31] "Regulation - 2023/1114 - EN - EUR-Lex," n.d., https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng.

How Providers Handle AML

Modern payment gateways typically integrate external blockchain analytics services to perform address and transaction checks, either automatically or manually.

- **Fireblocks** offers built-in transaction monitoring with policies to block or delay payouts on suspicious activity, integrating with Chainalysis[32] and Elliptic[33]. **B2BinPay** uses third-party services to screen both incoming and outgoing addresses, with options for automatic blocking triggers or manual reviews. **NOWPayments** and **CoinGate** focus on basic address screening without extended analytics or deep source-of-funds tracing.

- **BitHide**[34] includes built-in AML screening for incoming funds and counterparties' addresses, triggered automatically (e.g., on deposits above a set threshold per coin), during specific workflows like auto-withdrawals or exchanges, or manually on demand.Businesses can set rules to block or allow transfers based on risk levels and configure custom scoring ranges (e.g., Green 0–25%, Orange 26–75%, Red 76–100%, adjustable as needed).

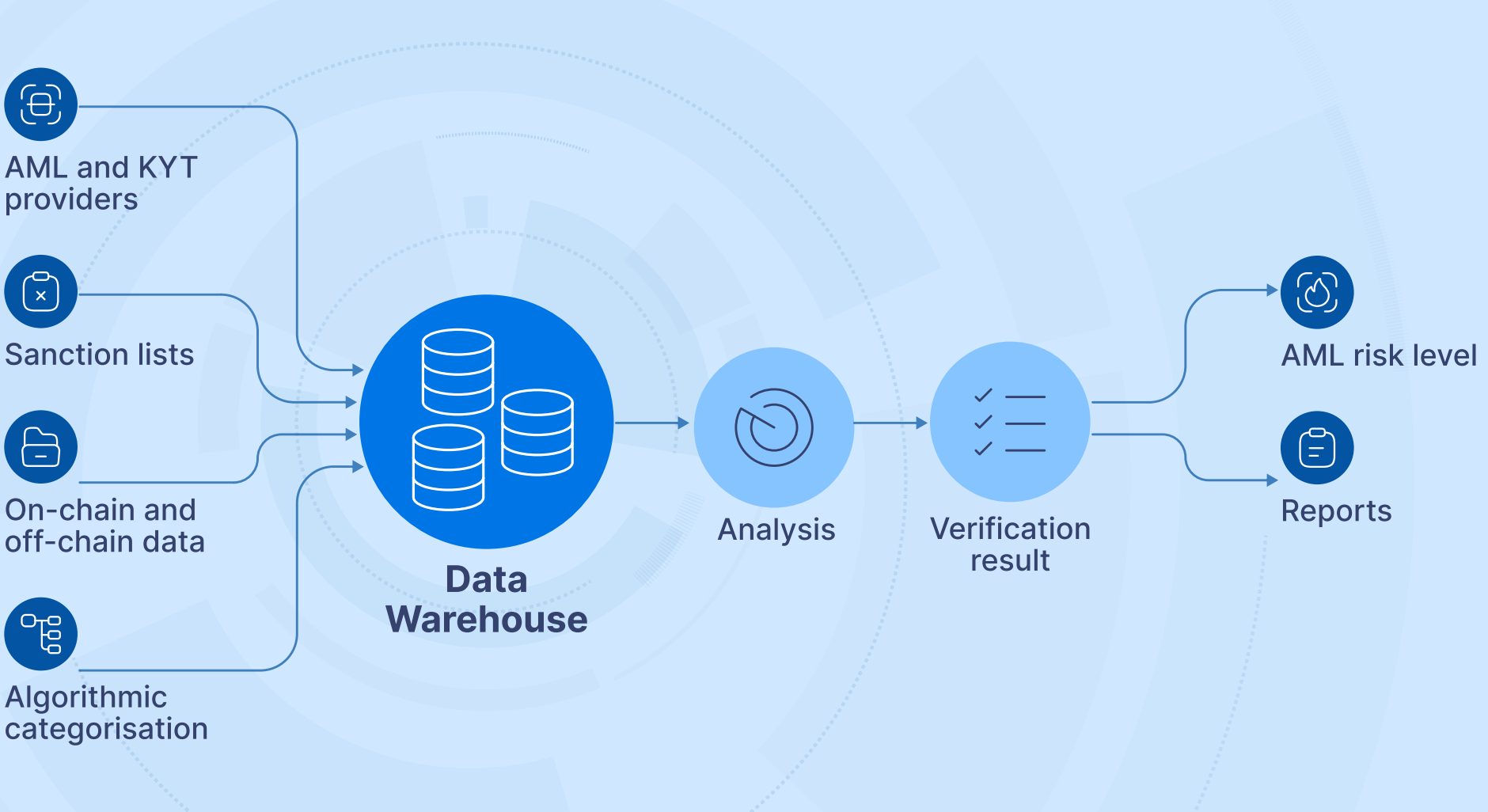
  BitHide uses the AML Data Warehouse — a centralized repository of integrated checks and reports, combining data from leading global providers to power analytics and compliance reporting. The system sources information from the same top-tier providers trusted by Binance, OKX, and Bybit, giving BitHide clients access to the exact same data that compliance teams at major exchanges rely on.

[32] Chainalysis, "The Blockchain Data Platform - Chainalysis," August 7, 2025, https://www.chainalysis.com/.

[33] London, "Blockchain Analytics & Crypto Compliance Solutions | Elliptic," n.d., https://www.elliptic.co/.

[34] "Crypto Wallet for Business," n.d., https://bithide.io/.

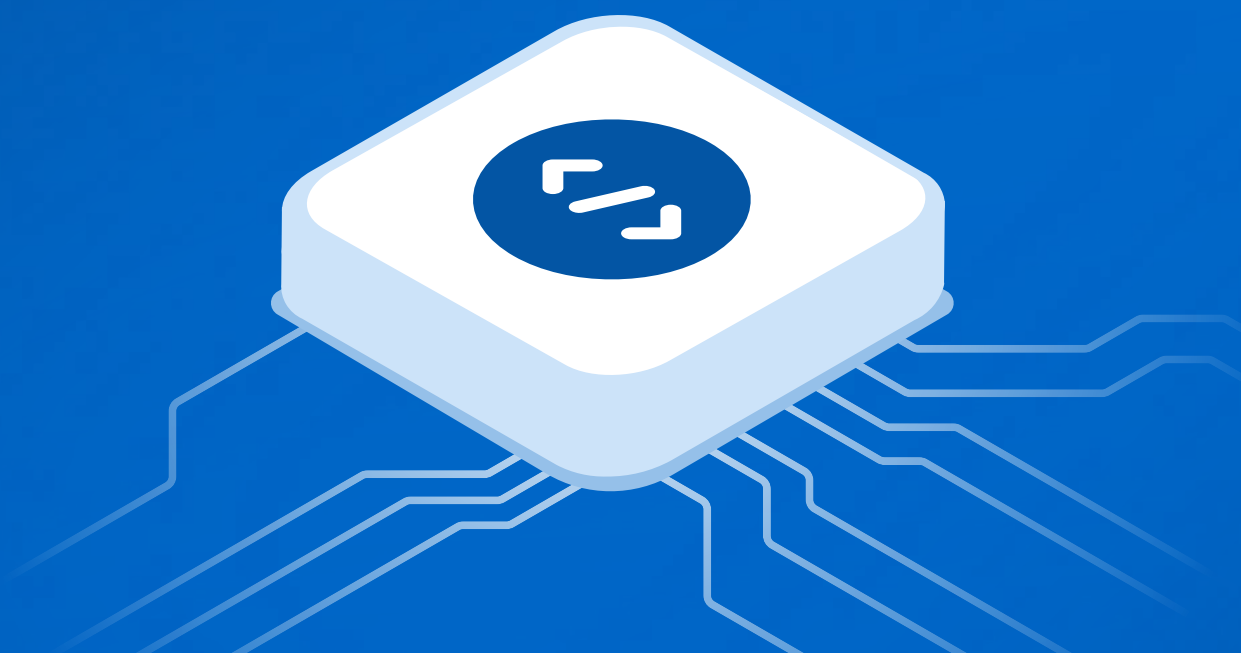
Incoming funds are always credited, but high-risk addresses are marked, affecting the wallet's overall risk rating. The system provides visual segmentation by risk level in portfolio and address views, but does not automatically move funds into separate wallets. Segregation must be set up via rules. In addition to its wallet-integrated checks, BitHide also offers a standalone AML bot, which lets users manually check addresses directly in Telegram.



4. Integrations and Developer Experience

Even the most secure and compliant crypto wallet is of little use if it doesn’t integrate well with your existing systems and provide a good developer experience. B2B users need a solution that can plug into websites, apps, and back-end processes with minimal friction. Let’s break down the most critical integration factors to look at.

Application Programming Interface



API Availability and Ease of Use

A robust API is non-negotiable for crypto payment gateways targeting businesses. The wallet should expose RESTful endpoints or SDKs that allow your backend to perform key actions:

- generate deposit addresses
- check balances
- initiate withdrawals
- get notifications of incoming payments

Without API support, you would be stuck doing things manually, which is infeasible at scale.

When comparing solutions, it’s important to look not only at the availability of endpoints for all operations, multi-sig, and fee controls, but also at how callbacks are handled. Imagine this: a user tops up their balance on a trading platform, the wallet sends a callback, but due to a connection failure the platform «misses» it. In BitHide, that callback can be resent manually right from the transaction history — no developers or support staff required.

It’s also critical to evaluate security. If callbacks are not encrypted, an attacker could intercept them and alter the deposit amount. In BitHide, all callbacks are encrypted, eliminating such risks and making the integration truly secure.

Integration Methods (Widgets, Payment Pages, iFrame)

In addition to raw APIs, many crypto gateways offer pre-built integration options like hosted payment pages or embeddable widgets. These can shorten time-to-market if you want a quick way to accept crypto on your site.

Documentation and Developer Support

Good documentation can save days of developer time. Need to check:

Clear guides, code examples, and reference docs for all API endpoints.

Support channels

Do they have a dedicated technical support team or community forum?

SDKs and sandbox environments

Some services offer a testnet/sandbox mode, allowing you to test integration without using real funds.

Speed of Integration and Deployment

From a project management perspective, you want to gauge how quickly you can go live with the solution. Self-hosted solutions might require deploying software on your servers. Check if the process is well-automated or if it’s complex.

5. Transparency and Control

This last category ties together many of the previous points: transparency (being able to see and audit what's happening) and control (having ultimate authority over assets and operations). In evaluating solutions, consider how much control you retain versus the provider, and how much visibility you get into the system's functioning and your transaction data.

Control of Assets and Data

Custodial service

they control your crypto (legally and technically)

Non-custodial service

the control remains with you

From a control standpoint, non-custodial will always give you more authority. In addition, non-custodial solutions can be deployed on the client's own server, providing even greater control over data and assets.

Real-Time Transaction Tracking

A transparent solution lets you monitor transactions in real time:

- seeing incoming payment confirmations
- tracking outgoing transaction statuses
- having overall insight into blockchain activity

Many providers offer a dashboard that shows transaction history, but if you have high volume, a generic dashboard may lag or present only aggregated info.

Trust and Verification

If you opt for a custodial provider, it is important to check:

- Does the provider conduct regular audits
- Publish Proof-of-Reserves
- Do they disclose where they store data or how they secure keys (HSMs, multi-sig, MPC)

Public companies or well-regulated ones might have independent audits to look at.

6. Industries and Providers

Industries and Providers

Industry	Solutions
iGaming & High-Risk Business	• **BitHide** — no KYC restrictions, privacy (Proxy Payments, Dark Wing), flexible payout automation (bulk payments, auto-withdrawals, crypto payroll module), API + payment widget. • N**OWPayments** — plug-and-play solution for small gaming operators, ready-made plugins for Shopify/WordPress. • Pl**isio —** basic integration option for small gaming platforms.
Forex, CFD & Trading Platforms	• **BitHide** — suitable for brokers who need crypto payments + automated AML (Telegram bot, AML Data Warehouse). • F**ireblocks** — for regulated Forex and CFD platforms requiring enterprise compliance and custodial infrastructure. • B2**BinPay —** regulated solution with PSP and exchange integrations.
E-Commerce & Online Retail	• **NOWPayments** — quick plugins for Shopify, WooCommerce, Magento. • C**oinGate** — fiat settlement option. • Pl**isio —** convenient for small online shops with simple requirements. • Bit**Hide —** for larger merchants needing automation, bulk payouts, and privacy.
Corporations & Institutional Clients	• **Fireblocks** — enterprise-grade, full custodial control + SDK, built-in AML, secure multi-user access. • **Coinbase Commerce** — best fit for companies already in the Coinbase ecosystem. • **B2BinPay** — regulated PSP/exchange solution. • B**itHide** — for enterprises requiring full control and flexibility in high-risk segments (self-hosted model, advanced automation).

Every business has unique needs, so it’s important to match the solution type to your context.
Here is a brief guide on which kind of crypto payment solution is best suited for whom:

Custodial Cloud Wallets

Custodial Cloud Wallets / Payment Gateways

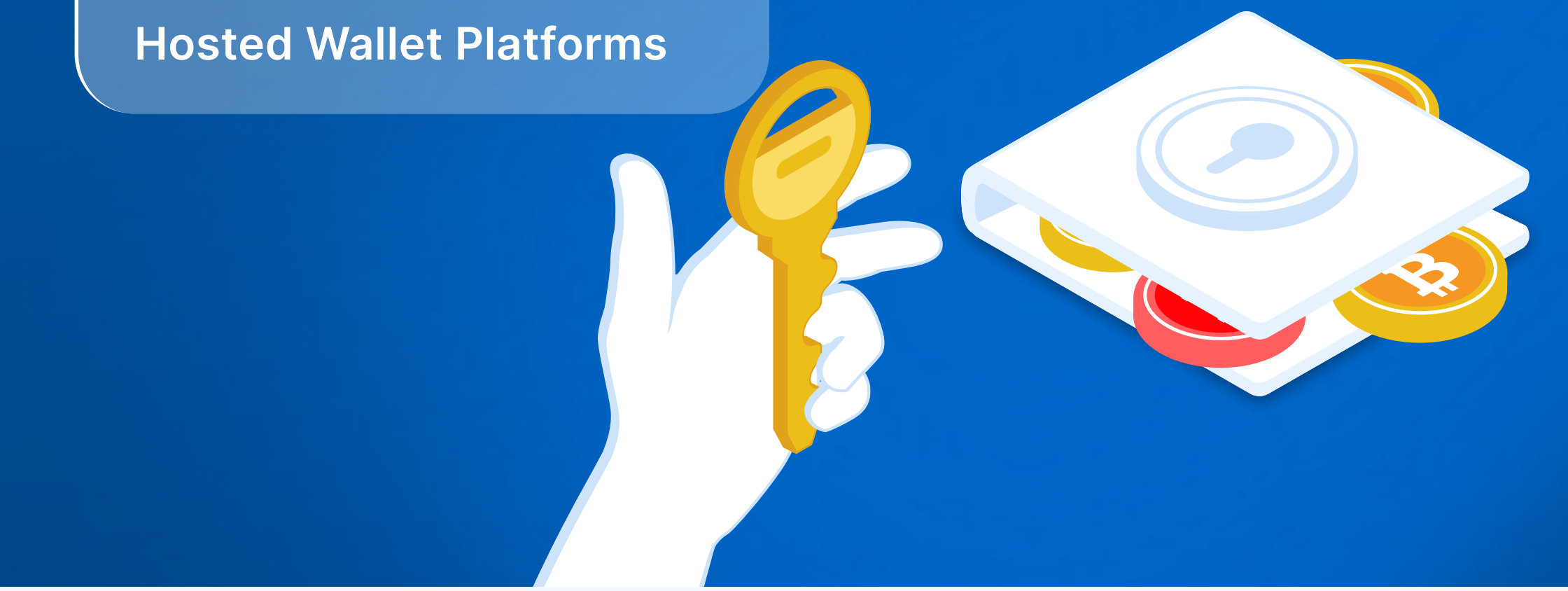
It is suitable for companies that prioritize simplicity and do not need full anonymity or control. Small-to-medium businesses new to crypto, or those who prefer an outsourced compliance and security model, can benefit from custodial services. These solutions handle key management and regulatory compliance (KYC/AML) on your behalf, reducing your operational burden. They're also quick to get started with — often just an account signup.

Custodial gateways are also appropriate in heavily regulated contexts where you want a third party in charge. Keep in mind, you trade away control for ease-of-use: as one source put it, custodial wallets undermine the decentralized ideal and can expose you to hacks, freezes, or service changes outside your control. Thus, they are best for low-risk, low-volume applications or early-stage adoption where convenience outweighs the absolute need for self-sovereignty.

Examples: **CoinGate** or **B2BinPay** — convenient for businesses that value ease of use and are willing to accept counterparty and censorship risks, as already demonstrated by frozen funds and hacks of custodial platforms.

coingate B2BINPAY

Non-Custodial Self-Hosted Wallet Platforms



Non-Custodial Self-Hosted Wallet Platforms

It is suitable for businesses that demand full control, privacy, and scalability, especially in high-risk or high-volume sectors. If your business cannot afford to have funds frozen or data leaked, and if you operate in industries like online gambling, forex trading, adult services, etc., a self-custodial solution is likely the best fit.

Additionally, large enterprises handling millions in crypto (e.g., crypto exchanges, large investment firms, or tech companies with significant crypto treasury operations) benefit from the advanced features and control of self-hosted solutions. They can integrate the wallet deeply into their infrastructure, customize it, and ensure compliance policies are tailored to their needs. The trade-off is that you require the technical capability to manage the system. Still, the result is that your business has ultimate ownership of the wallet, with no intermediary that could impede transactions.

For many B2B use cases today, given the increasing clarity in regulations and the availability of mature self-hosted solutions, the pendulum is swinging toward self-custody for B2B crypto payments – empowering businesses to be “THEIR OWN BANK”. The growth of companies like BitHide and others, the doubling of on-chain B2B crypto usage in just one year, underscores that more firms see value in controlling their crypto destiny.

Examples: BitHide — for companies in high-risk segments where control and privacy are critical. **BTCPay Server** — for technically skilled teams aiming for full sovereignty with open-source, primarily within the Bitcoin ecosystem.

Today, the market is increasingly moving toward non-custodial crypto payment solutions, as businesses become “their own bank.” The growth of solutions like BitHide and the doubling of B2B crypto volumes over the past year confirm this trend.

Hybrid / institutional solutions

Hybrid / institutional solutions

These are suitable for companies that need a balance between security, convenience, and regulatory compliance.

Example: Fireblocks — a platform for regulated organizations and large enterprises that require not only asset protection but also built-in, auditable compliance tools.

Fireblocks

MASTER COMPARISON TABLE

Crypto Payment & Wallet Solutions for B2B

Provider	Custody Model	Best For	Compliance / AML Features	Privacy Features	Developer Experience
Fireblocks	Hybrid (Custody + SDK)	Enterprises, Institutions	Built-in AML via Chainalysis/ Elliptic; Regulated	None (Audit-focused)	Full API + SDKs + Sandbox; Enterprise docs
Coinbase Commerce	Hybrid (Default non-custodial, opt-in custodial)	Businesses already in the Coinbase Ecosystem	Native compliance, regulatory coverage	None	REST API + plugins; Easy integration
BitHide	Non-Custodial	Enterprises, High-Risk businesses, PSPs, E-Commerce	Integrated AML (incl. Telegram bot)	Proxy Payments, Dark Wing (Tor+VPN)	REST API + Webhooks; Detailed permission system
B2BinPay	Custodial	Regulated exchanges, PSPs	Integrated AML (3rd-party)	None	API + Merchant tools; Moderate Docs
NOW Payments	Non-custodial (Temp custody optional)	SMEs, merchants seeking simplicity	Basic AML checks	None	Easy REST API, plugins for Shopify
CoinGate	Custodial	Merchants wanting fiat settlement	Basic AML/KYC for withdrawals	None	API + Plugins; Easy but limited
Plisio	Non-custodial (short-term custody)	Small online businesses	Basic AML checks	None	API + Plugins; Entry-level dev experience
BTCPay Server	Non-custodial, self-hosted	Tech-savvy teams, maximal control, for BTC only	None (user must integrate manually)	Optional Tor; Full source flexibility	Full open-source code, max flexibility, but DIY
Wasabi Wallet	Non-custodial (end-user focus)	Privacy-first treasuries, smaller ops	None	Tor + CoinJoin mixing	Minimal API; Designed for individual use

Reference List

1. Barbaravičius, Vilius. “Crypto Scams Guide for Business | How to Avoid With CoinGate.” Best Bitcoin & Crypto Payment Processor, May 16, 2025. https://coingate.com/blog/post/crypto-scam-threats.

2. “BTCPay Server Documentation | BTCPay Server,” n.d. https://docs.btcpayserver.org/Guide/.

3. BTCPay Server Foundation. «BTCPay Server Foundation, ” n.d. https://foundation.btcpayserver.org/.

4. Chainalysis. “The Blockchain Data Platform - Chainalysis,” August 7, 2025. https://www.chainalysis.com/.

5. CoinGate. “The Best Crypto Payment Gateway & Processor | Accept Crypto Payments.” Best Bitcoin & Crypto Payment Processor, August 13, 2025. https://coingate.com/.

6. “Coinbase Security,” n.d. https://www.coinbase.com/security.

7. Elad, Barry. “Stablecoin Statistics 2025: Growth, Adoption, and Regulation.” CoinLaw, September 6, 2025. https://coinlaw.io/stablecoin-statistics/.

8. “A New Standard in Global Crypto Payments | Coinbase Commerce,” n.d. https://www.coinbase.com/commerce.

9. Fireblocks. “Crypto Enterprise-Grade Security Platform | Fireblocks,” June 6, 2025. https://www.fireblocks.com/platforms/security.

10. Fireblocks. “Embedded Wallets | Fireblocks,” July 28, 2025. https://www.fireblocks.com/platforms/embedded-wallets/.

11. Fireblocks. “Fireblocks | Leading Digital Asset Infrastructure,” August 25, 2025. https://www.fireblocks.com/.

12. London. “Blockchain Analytics & Crypto Compliance Solutions | Elliptic,” n.d. https://www.elliptic.co/.

13. “Network-Level Privacy | Wasabi Docs,” n.d. https://docs.wasabiwallet.io/why-wasabi/NetworkLevelPrivacy.html.

14. NOWPayments. “Crypto Payment Gateway — the Best Solution for Accepting Cryptocurrency for Your Business,” April 4, 2025. https://nowpayments.io/.

15. NOWPayments. “Where Are My Funds Stored?” NOWPayments, April 22, 2021. https://nowpayments.io/help/about-nowpayments/about/where-are-my-funds-stored.

16. Plisio. “Cryptocurrency Payment Gateway,” n.d. https://plisio.net/.

17. Plisio. “WHMCS Cryptocurrency Payment Plugin - Plisio,” n.d. https://plisio.net/whmcs-accept-crypto.

18. “Regulation - 2023/1114 - EN - EUR-Lex,” n.d. https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng.

Reference List

19. Research, Cointelegraph. “Samourai Wallet Shutdown: Implications for Other Privacy and Self-custody Tools.” Cointelegraph, June 14, 2024. https://cointelegraph.com/news/samourai-wallet-shutdown-implications-for-other-privacy-self-custody-tools.

20. Team, BitHide. “Added Proxy Payment Capability | Release 2.35.” BitHide Blog, July 31, 2024. https://bithide.io/blog/release-2-35/.

21. Team, BitHide. “Coinbase Hack: How Attackers Stole Data From 70,000 Customers.” BitHide Blog, August 21, 2025. https://bithide.io/blog/crypto-exchange-hack-coinbase-2025/.

22. Team, BitHide. “Dark Wing Technology: Absolute Anonymity and Data Protection in Blockchain.” BitHide Blog, August 22, 2025. https://bithide.io/blog/dark-wing-blockchain-anonymity/.

23. Team, Chainalysis. “2025 Crypto Crime Mid-year Update: Stolen Funds Surge as DPRK Sets New Records.” Chainalysis, August 18, 2025. https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/.

24. Team, Chainalysis. “2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized.” Chainalysis, June 5, 2025. https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

25. “Tether Acknowledged by U.S. Authorities for Freezing $1.6M Connected to Terrorism Financing - Tether.io,” n.d. https://tether.io/news/tether-acknowledged-by-u-s-authorities-for-freezing-1-6m-connected-to-terrorism-financing/.

26. “The FATF Recommendations,” n.d. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

27. “The State of Crypto: the Future of Money Is Here,” n.d. https://www.coinbase.com/ru/blog/the-state-of-crypto-the-future-of-money-is-here.

28. “Wallet FAQ | BTCPay Server,” n.d. https://docs.btcpayserver.org/FAQ/Wallet/.

29. “Wasabi Wallet: The Privacy Focused Bitcoin Wallet,” n.d. https://wasabiwallet.io/.

30. “Crypto Payment Gateway & Processing | B2BINPAY,” n.d. https://b2binpay.com/en.

31. “Crypto Wallet for Business,” n.d. https://bithide.io/.