Managing seized cryptoassets

Practical lessons from an international roundtable

In September 2026, asset management practitioners, prosecutors, police and private-sector specialists from 17 countries met in Luxembourg to discuss how to manage seized cryptoassets.

Co-organised by the Luxembourg Bureau de gestion des avoirs and Basel Institute on Governance, the roundtable was held under the Chatham House rule on the sidelines of the 10th Global Conference on Criminal Finances and Cryptoassets. This publication emerges from that roundtable.

The document is structured around eight questions, because the focus is on questions that asset management practitioners need to consider rather than one-size-fits-all answers that do not exist. Laws, institutions and resources differ, as the examples given by participants demonstrate. Technical terms are explained in the glossary at the end.

The discussions confirmed that managing cryptoassets should be framed within the lifecycle of a case, from pre-seizure planning to disposal. Decisions taken at one stage can have significant consequences at later stages.

The diagram below shows the main stages in managing a seized cryptoasset, indicating the most relevant questions for each.

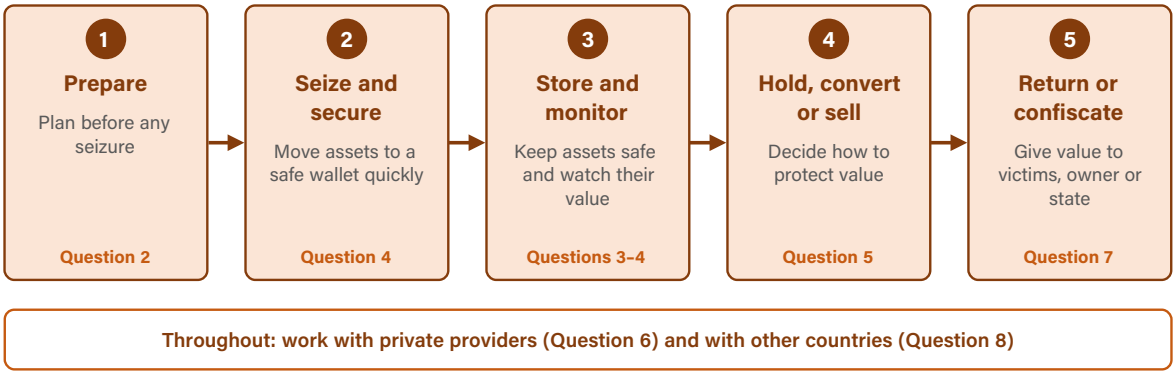


Figure 1. The lifecycle of a seized cryptoasset.

Key messages at a glance

The fundamental principles of asset management continue to apply

1 Cryptoassets should be managed lawfully, securely, transparently and with the objective of preserving value. The particular characteristics of cryptoassets require those principles to be adapted, especially in relation to custody, control, volatility, technical expertise and timing.

Preparation and early coordination are critical

2 Authorities should involve the relevant asset management expertise as early as possible and establish custody, decision-making and communication arrangements before a seizure occurs.

There is no one-size-fits-all model

3 The right arrangements depend on national legislation, institutional structures, available expertise and the assets involved. They also need to evolve: a model that works immediately after seizure may not suit months or years later, so authorities should be able to adapt.

Security is a governance issue as much as a technical one

4 Multi-person approval, role-based access, key protection, audit trails, business continuity, data protection and clear liability arrangements are essential safeguards.

Preserving value requires active decision-making

5 Authorities need clear criteria and responsibilities for deciding whether assets should be held, converted or sold. Where interim-sale powers exist, they should be matched by the institutional capacity to monitor markets and act within the relevant timeframes.

Public authorities should retain responsibility for decisions concerning seized assets

6 Private-sector providers can provide valuable technical and operational support, but outsourcing should not result in a loss of public control or accountability.

Choose the right route to sell and return

7 There is no single way to sell or return a cryptoasset. The sale method should suit the asset, its liquidity and the amount at stake, and the process should be auditable. Authorities must also decide whether owners and victims receive the asset itself or its value, bearing in mind that many victims have no wallet.

Cooperation is a practical capability

8 Networks of asset management offices, asset recovery offices and other practitioners can provide contacts, expertise, training and support for difficult cases. Building these networks can reduce duplication and help authorities develop solutions that are proportionate to their needs.

1 Why are cryptoassets different from other seized assets?

Cryptoassets are property that can be seized and confiscated. The usual principles of asset management still apply: preserve the value of the asset, comply with applicable laws, keep good records and be accountable and transparent.

During the roundtable it became clear that all categories of seized assets have their own specific characteristics. Cryptoassets are no different – they need to be handled according to their specificities.

Some features of cryptoassets need special attention:

- **Speed**. Cryptoassets can be moved anywhere in the world in seconds. Transfers usually cannot be reversed.
- **Control through keys**. Whoever has the private key or recovery phrase can move the asset. If the key is lost, the asset cannot be recovered. If the key is compromised, the asset can be transferred.
- **Changing value**. Prices can rise or fall sharply in a few days. Some tokens lose all their value or are removed from exchanges or blockchains.
- **Variety**. There are thousands of types, with different technical characteristics and degrees of volatility. One European asset management office (AMO) holds around 300 different types.
- **Technical complexity**. Different networks and wallets work in different ways, so mistakes are easy to make.

The most important operational issue is control. The asset is recorded on the blockchain. The private key is what allows someone to move it. Asset management arrangements must address the asset itself and the procedures, systems and people through which it is controlled.

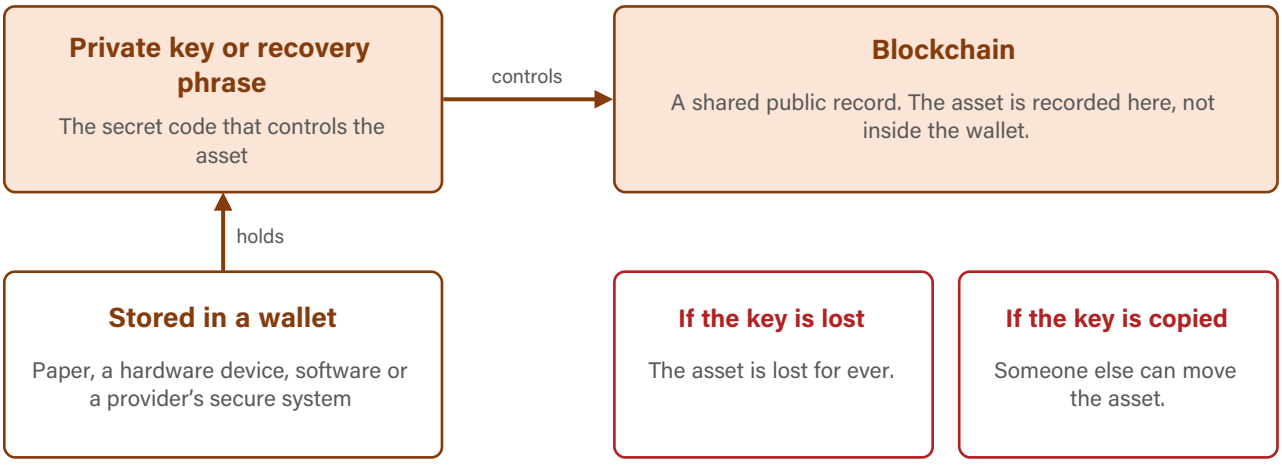


Figure 2. How control of a cryptoasset works.

2 What should we prepare before cryptoassets are seized?

"Cryptoassets should not be treated as an afterthought to a seizure." This was a key message from the start of the roundtable. Authorities should plan for the whole life of the asset: identification, transfer, storage, management, sale and return.

Coordination is crucial. The asset management authority should be involved as early as possible. This allows authorities to identify legal, technical and operational issues before the seizure takes place. That minimises the risk of mistakes or decisions taken under pressure.

Before a seizure, authorities should consider:

- **The legal powers available**. Does the seizure order provide for the transfer of the asset? Can the asset be transferred, converted or sold before the final judgment? If it does not, is an additional court decision required?
- **Roles and responsibilities**. Decide who makes decisions, who carries out transfers, and who can be contacted at short notice.
- **A custody solution**. A clear system needs to be in place beforehand: a wallet or account should be ready before the seizure. Send a small test transaction first, then the rest.
- **Basic information about the asset**. Record the type of asset, the network, its approximate value, where it is held (an exchange or a private wallet) and any possible third-party interests.
- **An estimate of costs**. Consider transfer fees, bank charges, provider fees and potential costs associated with liquidation.

Pre-seizure planning becomes even more relevant in complex or cross-border investigations, where suspects, assets and service providers may be located in different jurisdictions. Authorities should establish the necessary channels of cooperation before the seizure, if possible.

Example: In 2019, one agency received a foreign request for legal assistance and had 72 hours to seize cryptoassets. There were no laws or procedures for cryptoassets at the time. The team used its network of contacts, found a secure solution and completed the transfer at 6am. The former head of the agency advised others to prepare now: "the call will come eventually."

Example: A prosecutor wanted to seize a new token that could not yet be traded. Before acting, they asked the asset management agency for advice. The agency explained the risks and requested one more week to find a solution. That week allowed them to find a safe technical solution.

3 What are the options for managing seized cryptoassets?

There is no single correct model when establishing a seizure, management and realisation capability. The main options discussed were:

- **Hold the assets in government-controlled wallets**. These can provide direct control over the assets and private keys. They may use cold, hot or split-key (where the key is divided into parts held separately) arrangements. This approach can also include 24/7 availability, but requires technical expertise, security measures, key management, staff and backups. Internal custody can support the development of institutional capacity, rather than relying entirely on external providers. While recruiting and retaining experts within the public sector can be challenging, law enforcement agencies may have significant expertise and knowledge that can be leveraged.
- **Use a specialist private provider** for storage, a management platform or liquidation services. This provides access to expertise and can also include 24/7 availability and support for many types of asset. However it can create dependency and costs and a risk of loss of control.
- **Combine these approaches (a hybrid model)**. The authority keeps control of decisions, and a provider supplies technology or services.

The key point is that outsourcing a technical function does not mean outsourcing public responsibility. Authorities should retain control over decisions affecting the asset.

The choice depends on legal framework, the number and value of cases, their duration, technical expertise, budgets, the types of assets, and how sensitive the cases are. The management strategy should also influence the choice of model.

- If the strategy is to systematically use interlocutory sales and store the assets for a very short period of time, it may be of interest to involve an external partner.
- If one expects to hold the assets for longer periods of time, it might be of interest to create internal solutions for the various management models at the authority's disposal (placing some assets overnight to generate interest, interlocutory sales, storing for longer periods, etc). Some very sensitive cases, such as terrorism investigations, should not be shared with private companies and may need a fully internal solution.

The table below compares the three options.

Option	Control by the authority	Technical work for the authority	Cost	Main dependencies
Government-controlled wallets	High	High	Set-up and staff costs	Low
Private provider	Depends on the contract and approval rules	Low	Ongoing fees	High (provider)
Hybrid model	High if decisions remain with the authority	Medium	Medium	Medium

Table 1. Comparing the main options for managing seized cryptoassets.

Example: Institutional models evolve. One AMO first used its own hardware wallet but felt uncomfortable. Its concerns were limited support for different coins, security, who holds the codes and personal risk for staff. It moved to a specialist provider. Later the provider added a digital platform where police can get a deposit address instantly, even by scanning a QR code. The AMO called this "a game changer."

Example: One police unit started with paper wallets. It is now moving to encrypted, split storage on government-controlled infrastructure so that keys and case data stay in the country. It will completely manage and maintain its own solution and can adapt as soon as it needs to. All the data remains on national servers.

Can't one just leave assets at the exchange?

Best practice is clear: a cryptoasset enforcement programme should not just implement track and trace capabilities, but also seizure, management and realisation from the start. As such, most enforcement programmes will never need to leave assets at an exchange.

Leaving assets at an exchange is not recommended, due to risks including the exchange going bankrupt, no longer trading in a particular token or failing to cooperate with law enforcement.

If a seizure, management, and realisation capability is not yet in place, then assets can be left within exchanges which comply with freezing orders until the capability is in place.

4 How do we keep seized cryptoassets safe and under our control?

Many losses stem from risks linked to people and weak procedures or access controls, not from technology.

- **Never rely on one person**. Use the "four-eyes principle" (at least two people check each action) and multi-person approval for every transfer.
- **"Fast in, slow out."** Secure assets immediately at the moment of seizure. Subsequent transfer or sale should require careful, documented approval by several people.
- **Separate custody from decision-making**. A provider may store the keys but should never be able to move assets without the authority's approval.
- **Limit access**. Apply role-based access controls and ensure that access is removed promptly when staff change roles.
- **Keep full and immutable records**. Record every address, transfer, transaction ID, approval and incident for audit purposes.
- **Clarify liability and insurance**. Establish who bears responsibility if keys are lost, assets are stolen or the value of the asset declines. Contingency plans should also be considered. Insurance should not be treated as a substitute for sound custody arrangements.
- **Check how secure a "secure" solution really is**. As one participant said, "cold is no longer simply cold." Storage methods offer very different levels of protection.
- **Consider data sovereignty and confidentiality**. Sensitive case information should not be automatically placed on an external platform. External providers should receive only the information necessary for the service they are providing.

Example: In one country, police put USD 19 million of cryptoassets in a paper wallet inside a sealed envelope. A temporary court clerk opened the envelope, copied the keys and resealed it. A couple of months later, the funds had gone.

5 Should we hold the cryptoassets or sell them before the case ends?

Participants did not identify one single solution, as it depends greatly on laws, institutional capacity, expected duration of the case and the type of asset that has been seized.

5.1 Reasons to sell early

- It fixes the value at a defined point and avoids price crashing and delisting.
- It reduces storage costs and security risks.
- An asset management authority should seek to preserve value, not to speculate on future value movements. One participant said speculating on volatile cryptoassets such as meme coins rising or falling in value is "not compatible with our mandate."
- A clear legal framework for interim sales protects officials by establishing objective criteria, from claims that they sold at the wrong time.

Volatility should not be treated as a reason to fear cryptoassets and sell everything early as a result. Other financial and physical assets can also fluctuate in value. The relevant question is whether authorities have an appropriate legal and operational framework to manage the risk.

5.2 Reasons to hold

- The law may require the same asset to be returned.
- Some assets, such as stablecoins pegged to a stable fiat currency like the dollar, are less volatile and can earn a return while they are held. Generating interest on these assets might be a viable option, provided that the legal framework allows for this. This may lead to better victim compensation. The opportunities and risks strongly depend on the asset in question, since some stablecoins – particularly algorithmic ones – can also crash in value.
- An appeal against the sale decision may affect the timing of the sale.

Preserve value or increase it?

Cryptoassets such as Ether and Solana can be "staked" to earn a reward ("yield"). An innovative solution for stablecoins pegged to a fiat currency like the dollar is to place these in a tokenised money market fund that is fully backed, low risk and easy to convert back. This is similar to placing seized cash in a money market fund. Before using either option, check that the law allows it, that the risks are acceptable for public funds, and who is responsible for any loss.

5.3 Who decides when or whether to sell

The effectiveness of interim sales depends on who is responsible for monitoring the market and taking the decision to sell. Magistrates may have the legal authority to approve the sale but may not be institutionally equipped to monitor cryptoasset markets.

Some countries are giving AMOs the power to decide on sales, since this decision is purely administrative and is not connected to the criminal case. It emerged from the roundtable discussions that there is no single approach to choosing when to sell the asset, especially before confiscation.

Example: One AMO reported that their approach to the timing of sales of seized or confiscated cryptoassets differs:

- In the case of an interim sale (before a final decision), the AMO will sell the cryptoassets immediately after receiving the decision to sell by the competent magistrate.
- In the case of the sale of confiscated assets, the AMO could hold onto them to identify favourable market conditions.

However, it can be difficult to know when market conditions will change. In the case of the confiscated cryptoassets, the market conditions were not favourable at the time of receiving the confiscation decision. The AMO waited and saw the market conditions slowly go up and down and they kept on fluctuating. Finally, after a few months, the AMO sold the cryptoassets when the market had risen slightly again.

When deciding whether to hold or sell, authorities should consider:

- expected duration of the proceedings;
- volatility and liquidity;
- custody costs;
- whether the asset may be returned to the suspect or the victim;
- the likelihood of delisting or depreciation;
- the type of asset;
- procedural safeguards of affected persons.

Some participants raised an ethical and regulatory question about selling privacy coins, which are designed to be difficult to trace.

However, realising the value of privacy coins does not necessarily mean placing that asset back into retail circulation. Some specialist providers exist who have received the necessary regulatory permissions to lawfully hold and realise them on behalf of authorities.

Applicable law may mean affected persons have rights to be informed, to be heard and to appeal. The European Court of Human Rights requires a fair balance between the public interest and property rights.

The diagram below sets out the questions to ask. It does not give one answer, because each case is different.

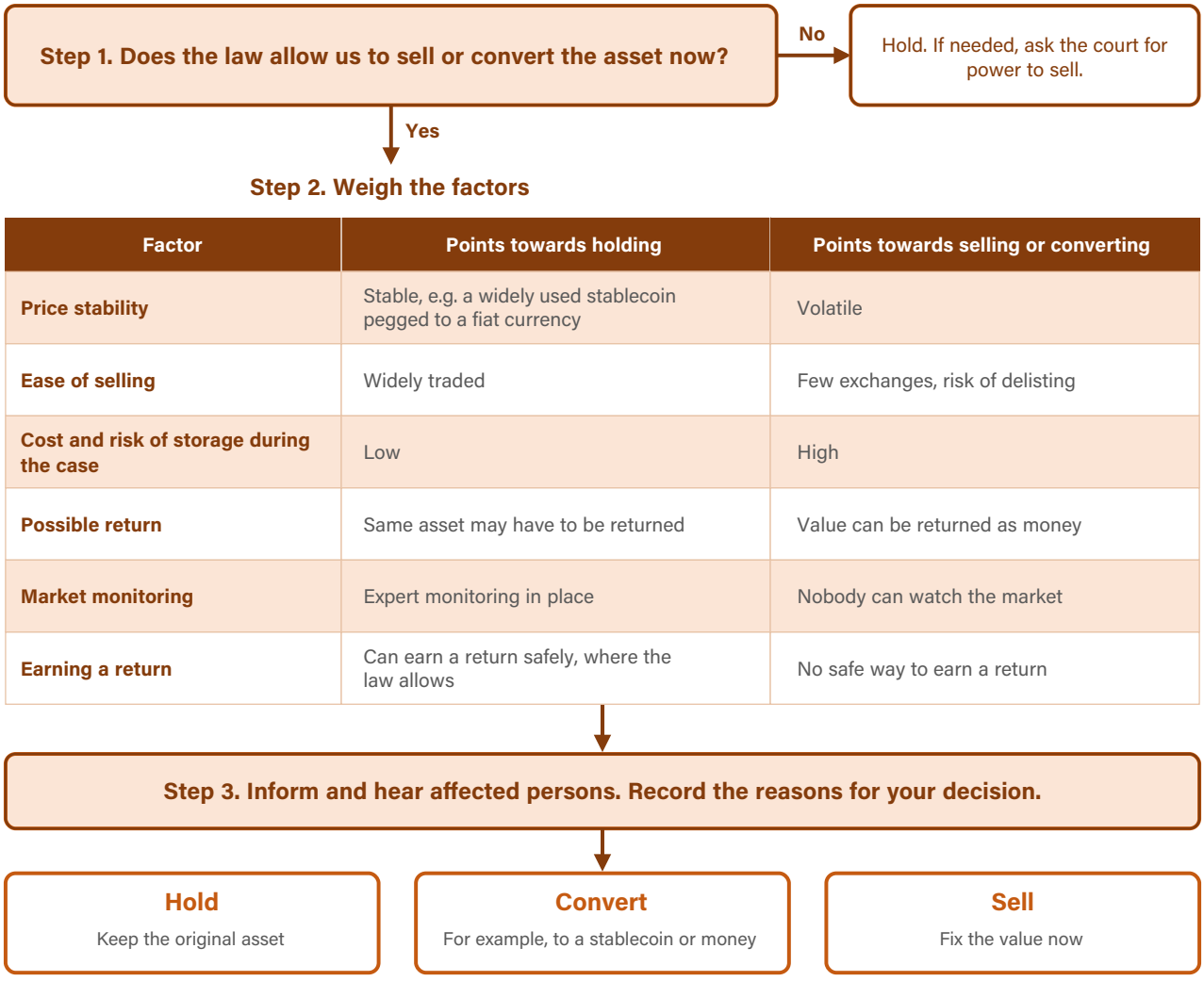


Figure 3. Hold, convert or sell: questions to ask. Graphic created using Claude.

Example: One agency converted volatile cryptoassets into stablecoins and later into fiat money, with the agreement of the defendant, the defence lawyer and the prosecutor. The conversion had a deadline of 3 to 6 weeks and a price limit.

Example: An agency received USD 8.3 million in a stablecoin. The court order allowed management but not sale, so the agency asked prosecutors to seek a change to the order.

6 What are considerations when contracting specialist expertise or platforms from the private sector?

Private-sector providers can support every stage of the process: storing and managing assets, liquidating them and supporting technical reporting.

Pragmatic cooperation between the public and private sectors is recommended, but external expertise should fill capacity gaps rather than replace public-sector responsibility. A provider said it clearly: "There is no delegation of public control. Never, ever."

Authorities should identify which functions they need to perform themselves and which can be outsourced. A participant advised: "You shouldn't fully trust any private company. You should build infrastructure that allows companies to take over some areas… but also retain control."

Private companies rely on business-focused rules and laws, and there might be risks associated with a company that the government does not face. Examples include bankruptcy, a change of law in the country in which they were established or a change in obligations under a law to which they are subject.

6.1 Before procurement

Authorities should:

- **Decide what type of assistance is required** across the whole process, including storage, management, sale, conversion and payments to victims. Be aware of the information shared with external partners.
- **Engage with the market**, for example with a request for information. Ask what providers can really do, what support they can provide, how fast they can respond and under which laws they operate.
- **Consider jurisdictional aspects**. Provider location, corporate structure, regulation and jurisdiction can affect access to information and business continuity.

Security and leveraging public-sector expertise

Participants raised that before turning to a private-sector solution, it is important to leverage the expertise that exists within national law enforcement agencies. This is also vital for security reasons. One law enforcement participant said:

> "To ensure the highest standards of security, consult with law enforcement agencies and leverage their internal knowledge and expertise. Importance must be placed on strict adherence to judicial procedures to mitigate the

risk of information leakage. All operational information must be treated as sensitive data and shall not be disclosed to third parties."

6.2 Selecting a provider

Technical capacity should be tested rather than assumed. For example, one exercise during a tender included a practical technical demonstration. This can help authorities assess whether the provider can perform the required tasks under realistic conditions.

Authorities should also:

- **Understand the legal and regulatory framework**. Ensure that the tender criteria are consistent with applicable legal and regulatory requirements. Verify the provider's regulatory status and any history of fines. Check which supervisor oversees the provider in the relevant jurisdictions and which activities (anti-money laundering registration, custody, trading or exchange) are covered. "Registered" in a country is not the same as "regulated" there.
- **Do not rely on certifications alone**. Certifications should not be treated as a substitute for due diligence and ongoing oversight. In one widely reported case, a contractor with a recognised security certification suffered an insider theft of about USD 46 million.
- **Verify authorisation requirements**. If the provider will sell or return assets, confirm that it is authorised to trade cryptoassets and convert them into fiat currency in the countries involved.
- **Understand fee structures**. Agree whether the provider charges a percentage of the sale, a fixed fee or both, and whether it earns anything from the price itself. This needs to be allowed by the legal framework. In the case of victim compensation, for example, can the government hold back a certain amount in order to pay the external provider?

Ensuring tender criteria align with regulations: EU examples

The EU regulatory framework has direct implications for what authorities should expect from providers. Authorities should verify that providers are legally permitted and operationally equipped to custody, transfer and realise the specific assets concerned. For example, a MiCA authorisation does not guarantee that a provider can offer services in relation to every cryptoasset. Restrictions may apply to particular tokens, including USDT. For this reason, authorities should not assume that a provider can handle all seized assets.

Similar considerations apply to privacy coins. From 10 July 2027, Article 79 of Regulation (EU) 2024/1624 prohibits credit institutions, financial institutions and cryptoasset service providers from maintaining anonymous accounts, including through anonymity-enhancing (privacy) coins.

6.3 Contract terms

Contracts should address:

- service levels, response times and reporting, with penalties if they are not met;
- liability and insurance based on real risks (one tender that asked for broad insurance made costs "ridiculous");
- arrangements if the provider becomes insolvent;
- rules on data ownership and access;
- how to move assets to a new provider, and who pays the fees;
- include all other external providers that might be involved in the process;
- flexibility for new types of assets and technology;
- offboarding costs and responsibilities;
- data portability and exit strategy.

Flexible fee structures may be appropriate where the number and value of seizures are unpredictable. Authorities should understand the complete cost of service, including case-management fees, fixed or recurring charges, and transaction or network costs.

6.4 Managing the contract

Manage the contract actively. Several participants noted that a strong tender can fail if the contract is not actively monitored. Authorities should review service levels, security incidents, costs and the provider's ability to meet contractual requirements.

Authorities should also avoid excessive operational dependency. If a provider changes its supported assets, technology or business model, a realistic transition plan should be in place.

Example: One country's provider decided to stop supporting some types of cryptoassets. The AMO ended up with two systems, which was more complicated than one. It now has to move over USD 100 million to a new provider and decide who pays the transfer costs.

Example: One provider offers a single standard contract to many regional authorities. It has no minimum fees, so offices with no cryptoassets yet are ready if a seizure happens and don't have to pay out any ongoing costs.

7 How do we sell cryptoassets and return their value to victims or the state?

7.1 Selling

Possible sale mechanisms include:

- Regulated exchanges or brokers
- Specialist liquidation providers
- Online auctions
- Staged sales

Authorities should avoid designing a framework around a single sale mechanism. The appropriate method depends on the asset, liquidity, market conditions, transaction size and legal requirements. Physical auctions, for example, do not work for cryptoassets.

Authorities should also:

- **Seek the best available price**. Whoever carries out the sale should be able to find liquidity in several markets, not only one exchange, similar to strategies taken in traditional financial markets. This minimises risks of market manipulation and prices dropping in the case of large crypto sales.
- **Use an auditable process**. The authority should be able to demonstrate how the sale price was established and retain a complete record of the transaction.
- **Consider the status of the assets**. Tracing tools often mark seized cryptoassets as linked to criminal activity. Some exchanges will then refuse to accept or transact them.
- **Plan for whitelisting and other compliance requirements**. Official addresses may need to be approved in advance to avoid transactions being blocked.
- **Keep proceeds separate and accounted for**. The treatment of proceeds should be determined in advance, including what happens if confiscation succeeds or fails.

7.2 Returning assets or value

Authorities should:

- **Decide in advance** whether the cryptoasset or its monetary value will be returned. In one country, if the asset is still held, the owner gets the same cryptoasset back. If it was sold, the owner gets the money from the sale, valued at the time of sale.

- **Consider that the asset may be returned to the suspect**. If a court orders a return but the asset has been sold, authorities may have to buy it back or give the suspect the countervalue achieved in the sale.
- **Consider the options for returning assets to victims**. Victims may not have a wallet and may need the asset to be sold for them. In some cases, assets may be tainted or flagged as criminal assets.
- **In fraud cases**, decide whether victims receive what they invested or also any "profits". This procedure needs to be in line with procedures regarding other assets such as traditional financial products, cash seized or money in bank accounts.
- **Consider how debts, compensation claims or legally required deductions are treated** and inform the affected persons.

Example: One AMO received a decision to return cryptoassets to a victim of a scam. It was an elderly victim who didn't have a wallet. In such a case, the AMO proposed to the victim to sell the crypto for them and return the value.

Example: An offshore exchange froze assets for a country but refused to sell them or send them to that country due to the country having high risk scores for corruption and money laundering on international indices. A private provider stepped in and received the assets, sold them and sent the money back, with support from a foreign law enforcement agency.

Example: One country first uses the money to pay the person's public debts – criminal, tax, social – and warns recipients about this in writing.

8 How can we learn from and work with other countries?

International cooperation was identified as one of the most practical ways of building capability. Authorities do not need to develop every solution independently, considering technical and operational practices evolve rapidly.

- **Use practitioner networks**. They allow quick, informal contact alongside formal legal cooperation. They help both with cases, for example when one country manages assets for another, and with learning and training.
- **Share experiences, including mistakes**. Lessons from unsuccessful approaches can help other authorities avoid repeating the same mistakes. One agency head said: "bad results are called experience."
- **Cooperate within the country too**. Police, prosecutors, AMOs, judges and regulators should establish channels for regular cooperation. Some countries use multidisciplinary task forces. Experts are available quickly and meet regularly in order to discuss potential issues at hand and find solutions before problems emerge.
- **Build and retain institutional knowledge**. No country can have a crypto expert in every unit, and trained staff are often recruited elsewhere. Nevertheless, the aim should be for governments to build competences in these areas. Private companies could support AMOs in building these competences in order to keep them in house, in addition to providing software and expertise.

Networks can provide value beyond training: they can offer trusted contacts and access to experience that would otherwise require costly external consultancy.

Example: The Balkan Asset Management Interagency Network (BAMIN) has grown to 24 members. Each member names two contact people. The network meets once a year, has written a guide with 25 indicators for effective AMOs, and uses peer reviews. Members ask each other about everything, from cryptoassets to cash and real estate. Its main challenge now is finding funding to keep meeting.

Example: One agency prepared for its first major cryptoasset case by holding weekly calls with network colleagues and attending training. When it received USD 8.3 million in a stablecoin, it was ready.

Emerging cooperation mechanisms among AMOs and asset recovery practitioners at the European and regional level provide further opportunities for this type of exchange. New international instruments and guidance, including the EU Directive on asset recovery and confiscation, the Additional Protocol to the Council of Europe's Warsaw Convention and the FATF Asset Recovery Guidance and Best Practices, give authorities a stronger shared basis for this work.

As one participant said,

"the network is about the people."

About and acknowledgements

This publication is part of the Basel Institute on Governance Policy Brief series, ISSN 2624-9669. You may share this publication under a Creative Commons BY-NC-ND 4.0 International licence.

Suggested citation: Basel Institute on Governance. 2026. 'Managing seized cryptoassets'. Policy Brief 18, Basel Institute on Governance. Available at: baselgovernance.org/resources/publications/pb-18-cryptoasset-management.

The roundtable on which the publication is based was co-organised by the Basel Institute on Governance and Luxembourg's Bureau de gestion des avoirs (BGA) as a side event to the 10th Global Conference on Criminal Finances and Cryptoassets. Around 50 participants from the public and private sectors, representing 17 jurisdictions, took part. The organisers thank all participants for sharing their experience so openly during the roundtable and in consultations on the draft. Thank you also to Laura Mossong, Rita Simões and Monica Guy for their role in preparing the draft and integrating feedback.

The document does not necessarily represent the views of the moderators, the organisers or participants' institutions, or the official position of the Basel Institute on Governance, its donors and partners, or the University of Basel. AI tools were used in preparing this publication in line with the Basel Institute's standards for responsible AI use.

We welcome feedback and contributions to this ongoing debate and invite you to contact us at info@baselgovernance.org.

Key terms

Address (deposit address)	A code of letters and numbers that shows where cryptoassets can be sent. It works like a bank account number and can be shared safely.
Asset management office (AMO)	A public body that looks after seized and confiscated assets, protects their value and often sells them.
Blockchain	A shared public record of all transactions on a cryptoasset network. Anyone can view it, but past entries cannot be changed.
Blockchain analytics	Software that follows the movement of cryptoassets on a blockchain to trace where they came from and where they went.
Cold wallet (cold storage)	A wallet kept offline, such as a hardware device or paper. It is harder to hack but slower to use.
Confiscation	A final court decision that permanently removes an asset from its owner, usually giving it to the state.
Conversion	Exchanging one cryptoasset for another (for example, a stablecoin) or for ordinary money.
Cryptoasset	A digital asset recorded on a blockchain, such as Bitcoin. Also called crypto, a virtual asset or a digital asset.
Custody / custodian	Custody means holding and protecting assets for someone else. A custodian is the organisation that does this.
Delisting	When an exchange stops trading a cryptoasset. This can make the asset difficult or impossible to sell.
Exchange	A company where people buy, sell and hold cryptoassets. Exchanges can often freeze accounts when authorities ask them to.
Fiat currency	Ordinary government money, such as euros or US dollars.
Four-eyes principle	A rule that at least two people must check and approve an action before it happens.
Hardware wallet	A small physical device, similar to a USB stick, that stores private keys offline.
Hot wallet	A wallet connected to the internet. It is quick and easy to use but more exposed to hacking.
Interim (interlocutory) sale	Selling a seized asset before the final court decision, usually to protect its value.
Liquidity	How easily an asset can be sold quickly without its price falling.
Multi-person approval (multisignature)	An arrangement where a transfer can only happen if several people or several keys approve it.
Network fee	A small fee paid to process a transaction on a blockchain, also called a “gas fee.” It usually has to be paid in the network’s own cryptoasset.
Paper wallet	Private keys or a recovery phrase printed or written on paper.

Privacy coin	A cryptoasset designed to hide who sends and receives it, which makes tracing very difficult.
Private key	A secret code that gives control of cryptoassets. Anyone who has it can move the assets.
Recovery phrase (seed phrase)	A list of usually 12 or 24 words that can recreate a wallet and all its keys. It must be protected as carefully as the private key.
Registered vs regulated	A company registered in a country may only have a legal address there. A regulated company is supervised by an authority in that country.
Request for information (RFI)	An early step in public procurement. The authority asks companies what they can offer before designing a tender.
Seizure (or freezing)	A temporary measure that stops the owner from using or moving an asset while a case continues. Terms differ between countries.
Service level agreement (SLA)	Part of a contract that sets measurable standards, such as how fast a provider must respond.
Split-key storage	A method where a private key is divided into parts held in different places or by different people, so no one person has full control.
Staking	Locking up certain cryptoassets, such as Ether or Solana, to help run a blockchain network, in return for a reward.
Stablecoin	A cryptoasset designed to keep a stable value, usually linked to a currency such as the US dollar.
Test transaction	A small transfer sent first to check that the address and process are correct, before moving the full amount.
Token	A cryptoasset created on an existing blockchain rather than having its own. Many stablecoins are tokens.
Tokenised money market fund	A share in an ordinary money market fund, recorded as a token on a blockchain. It can be held and transferred like other cryptoassets and converted back into stablecoins or cash.
Transaction ID (transaction hash)	A unique code that identifies one transfer on a blockchain. It should be recorded as evidence.
Virtual asset service provider (VASP)	A business that provides cryptoasset services, such as exchanges and custodians. This term is common in laws and international standards.
Volatility	How much and how quickly an asset's price goes up and down.
Wallet	A tool, either software or a device, that stores the keys needed to access and move cryptoassets.
Yield	The income earned from an asset over time, for example from staking cryptoassets. Usually shown as a percentage per year. Also called a return.

Basel Institute on Governance
Steinenring 60
4051 Basel, Switzerland

+41 61 205 55 11
info@baselgovernance.org
baselgovernance.org

The Basel Institute on Governance is an Associated Institute of the University of Basel.