

Sovereign Individual Guide

A Handbook for Building
True Sovereignty



INTRODUCTION

The New Framework for True Sovereignty

The world is changing faster than legacy systems can adapt. Wealth is becoming increasingly digital, borders are becoming more fluid, and governments are becoming more interventionist. For high-net-worth individuals, the old assumptions about safety, mobility, and financial access no longer hold.

In this environment, true sovereignty is not a luxury. It is a strategic necessity.

Sovereignty has two equally important dimensions:

Financial Sovereignty

Control over your wealth without intermediaries, single points of failure, or permissioned systems.

Jurisdictional Sovereignty

Control over your life, mobility, and identity documents through diversified residencies, citizenships, and legal ties.

Both pillars work together. Financial sovereignty protects your wealth. Jurisdictional sovereignty protects your future. Combined, they create resilience against political instability, banking fragility, and sudden changes in domestic policy that can disrupt your life or restrict your freedom.

This guide brings these two worlds together.

How to navigate this guide

PART 1:

Created by Casa, Part 1 lays out the principles of securing your digital wealth through multi-key self-custody. It explains why controlling your own keys is foundational to long-term financial safety, privacy, and independence.

PAGE 4 - 14

PART 2:

Created by CitizenX, Part 2 expands your sovereignty beyond your assets and into your identity, mobility, and global positioning. It introduces the frameworks and tools that allow you to strategically diversify your citizenships, establish alternative residencies, and choose the jurisdictional environment that aligns with your goals and values.

PAGE 15 - 21

Together, these two perspectives form a modern sovereignty model built for individuals who want control, optionality, and peace of mind in an uncertain world.

This is your blueprint for taking ownership of both your wealth and your life.

Sovereignty always begins with the layer you can control most directly: your wealth. Before exploring how to build jurisdictional optionality across borders, you must first ensure that your assets are protected from institutional, operational, and political risks. That foundation is built through self-custody.

The next section outlines the case for self-custody and why holding your own keys is the essential first step toward financial sovereignty.

The Case for Self-Custody

Financial sovereignty begins with a simple principle: true ownership requires control.

For most of history, this meant physical possession: gold in a vault, cash under the mattress, property with a deed. But as finance digitized, control and ownership diverged. Your bank balance is a database entry, not an asset you hold. Your brokerage account represents shares held in “street name” by a custodian, not certificates in your possession.

Bitcoin changed this equation. For the first time, digital bearer assets became possible: money you can truly own and control without intermediaries. But ownership alone isn’t enough. Self-custody is the practice of holding your own keys, making you the only party capable of moving your bitcoin. Without self-custody, you’re trusting someone else to honor your claim to your wealth.

That trust, as history repeatedly demonstrates, can be misplaced.



The Custody Risk Trade-off

The institutions holding your wealth operate within systems you don't control. Whether traditional banks or cryptocurrency custodians, the fundamental compromise remains the same: you've outsourced ownership in exchange for convenience and perceived security.

COUNTERPARTY RISK

When you use institutional custody, you're trusting the custodian's solvency, operational security, and fiduciary responsibility. Major crypto custodians like Coinbase hold billions in client assets, making them attractive targets for sophisticated attacks. A security breach at a centralized custodian could put massive amounts of client funds at risk simultaneously.

Custodial insurance exists, but it's never large enough to cover catastrophic events. In a scenario where the custodian lost keys to client funds, you would receive pennies on the dollar. The insurance provides psychological comfort, not comprehensive protection.

LOSS OF CONTROL

Institutional custodians must comply with government mandates, court orders, and internal compliance decisions, even when those decisions harm depositors. Your funds can be frozen, withdrawal limits can be imposed, or access can be restricted without your input or consent. The custodian stands between you and your wealth, making decisions based on their regulatory obligations and risk management, not your interests.

When a crisis arrives, whether economic, political, or operational, these intermediaries become instruments of control rather than protectors of your wealth.

The 2019 Lebanese banking crisis continues today, with depositors still unable to access their savings after five years. These weren't rogue actors, these were established financial systems that subordinated individual property rights to systemic preservation.

Self-Custody as Sovereignty

Understanding these risks transforms self-custody from a technical best practice into a strategic imperative. When you control your keys, you hold sovereignty over your wealth:

No counterparty risk:

Your bitcoin exists independently of any institution's solvency or goodwill

No permission required:

You can transact at any time, with anyone, anywhere, without authorization

No geographic vulnerability:

Your wealth isn't trapped in a specific jurisdiction's banking system

No debasement:

Your share of the 21 million bitcoin supply remains constant regardless of monetary policy

Self-custody doesn't eliminate all risks. Physical security, operational security, and inheritance planning create their own challenges. But it fundamentally shifts the nature of risk from institutional and political to personal and manageable. You're no longer hoping your custodian remains solvent or your access remains unrestricted. You're taking responsibility for your own financial sovereignty.

For the internationally-minded individual pursuing jurisdictional diversification, this alignment is natural. Just as you wouldn't concentrate all your legal and residential ties in one country, you shouldn't concentrate control of your wealth in one key, one device, or one location. But sovereignty brings responsibility. Moving from institutional custody to self-custody isn't enough if you're simply replacing one single point of failure (the institution) with another (yourself). True financial sovereignty requires upgrading your security model to match the level of control you're taking on, not just for your protection today, but to ensure your family can access your wealth if something happens

to you. Financial sovereignty and jurisdictional sovereignty aren't separate strategies, they're complementary expressions of the same principle: distributed control, resilient systems, and long-term security.

True sovereignty means your security is future-proof, resilient against evolving threats while giving you peace of mind to live your life without constant worry about your wealth.

This guide distills some of the core principles behind Casa's Wealth Security Protocol, a comprehensive framework designed to ensure you have the best security model possible for the long-term. We'll show you the most common threats bitcoiners face today, how to layer protections, prepare for worst-case scenarios, and strengthen defenses against both external threats and internal mistakes. With the right security foundation, self-custody becomes not just possible, but sustainable.

Understanding the Threat Landscape

Digital asset security involves far more than the obvious threats of hackers or device failures.

Risks can emerge from unexpected places: coercion, natural disasters, or gaps in inheritance planning, yet these often go unnoticed.

Recognizing the full spectrum of risks isn't about alarmism, it's about clarity. When threats are understood in context, it becomes easier to see how they might play out in real life and where the most important vulnerabilities lie. That clarity turns a scattered set of concerns into a coherent picture of what's at stake.

Threat	How It Can Happen	Primary Risk to Your Setup
Data & Credential Loss	Lost seed phrase, device failure, misplacing backups, forgotten passwords, discarded hard drives	You simply lose access forever
Phishing / Social Engineering	Fake support representatives sending emails claiming to be from Coinbase/exchanges, Fake wallet UI, credential replays, UI spoofing, malicious websites, false upgrade notices, tampered software downloads, false	You give away secret material, credentials, seed phrases to attackers posing as legitimate support
SIM / Telecom Hijack	Ported phone number, SIM swap (attacker convinces phone company or pays off insider)	You receive 2FA or recovery push codes that attackers intercept
Network / Infrastructure Attacks	MITM on your device, malicious WiFi, compromised DNS, man-in-the-middle attacks intercepting communications	You're tricked into signing malicious transactions or revealing credentials
Malware / Supply Chain	Malicious firmware, keyloggers, compromised libraries, fake hardware wallets, tampered devices during shipping, backdoored updates	Your private key is exfiltrated during use or stolen before you even receive the device
Physical / Coercion Attacks	Forced disclosure at gunpoint, kidnapping, tampering with physical devices, wrench attacks (violence or threats)	You surrender keys or seeds under duress; portable and irreversible nature of crypto makes this especially dangerous
"Animal / Child / Pet" Risks	Accidental deletion, curious user error, children or pets interfering with devices or backups	You delete or corrupt backups accidentally
Insider / Service Provider Risk	Host compromise, colluding employees, secret key theft from service provider, malicious insiders at custody services	Third party gains unauthorized access to your keys or account
Platform / Hosting Attack	Cloud provider compromise, database leaks, backup storage breaches	Data or backups leak or get manipulated by compromised infrastructure
Code Dependency / Update Attack	Backdoored library, malicious update pushed to wallet software, compromised open-source dependencies	Software you rely on is compromised, enabling key theft or transaction manipulation
Official Seizure / Regulatory Risk	Government demands, legal intervention, civil asset forfeiture, border confiscation	Devices or keys forcibly seized by authorities
Inheritance & Succession Failures	Poor transmission, ambiguous instructions, lack of documented recovery process	Wealth becomes inaccessible after your passing; heirs can't recover funds
Address Spoofing / Transaction Misdirection	Rogue address in UI, DNS hijack, clipboard hack that replaces addresses	You send funds to the wrong destination
Extreme Disaster Scenarios	Natural disaster, nuclear event, loss of jurisdiction, all backup locations destroyed simultaneously	All redundant backups are destroyed or unreachable
Extortion / Blackmail	Coercing disclosure via threats (not physical violence), leveraging personal information	You give up secrets from pressure or fear

In practice, data/credential loss, phishing, supply chain, and coercion cause the majority of failures. Early setups should focus there, and then layer up.

Building a Robust Base

Self-custody security begins with building a foundation that can withstand the most common and most devastating risks. Rather than thinking in terms of features or devices, imagine your setup as a layered defense system. Each layer addresses different categories of threats, ensuring that no single mistake, accident, or attack leaves your wealth vulnerable.

LAYER 1:

Awareness of Multi-Key Security

Threats: Credential loss, device failure, single point of failure, network attacks, malware, SIM hijacking, phishing, supply chain attack

Tactic: Use a multi-key scheme (3-key vault or 5-key vault) distributed across diverse device types (Trezor hardware wallet, Coldcard hardware wallet, Yubikey, mobile key and recovery key from Casa) to eliminate single points of failure. This ensures that no single compromise, malfunction or phishing attempt can lead to total loss of funds.

The biggest vulnerability in self-custody is a single point of failure. A wallet that depends on only one device or one backup can be lost, stolen, or compromised in an instant. Once that happens, funds may be gone forever.

This is why multi-key security is foundational. By spreading control across multiple keys, no single device or mistake can jeopardize the whole system. Diversity of devices, storage environments, and manufacturers further reduces the chance that one exploit could compromise everything.

LAYER 2:

Geographic & Logical Redundancy

Threats: Disaster scenarios, theft, jurisdictional seizure, site-level compromise, physical coercion, network attacks, internal service provider attack

Tactic: Geographically distribute and isolate keys using a multi-key vault to minimize both physical and operational risks. Even if one key is lost, stolen, or destroyed, your assets remain safe because an attacker or disaster would need to compromise multiple keys across different places at the same time to gain control.

Self-custody doesn't just face digital risks, it's also exposed to physical and environmental threats. If all keys or backups are concentrated in one location, a single event such as a fire, flood, theft, or legal seizure could make them inaccessible all at once.

This is why strong security frameworks emphasize distribution and separation. Resilient systems spread keys and backups across different locations and safeguards, reducing the chance that a single disruption can't endanger the entire system. **Security depends on diversity and distance.**

LAYER 3:

Privacy & Security

Threats: Data breaches, doxxing, targeted phishing/SIM-swap, regulatory exposure, third-party leakage.

Tactic: Share minimum required information, use pseudonymous contact and shipping details, ensure data is used only for its intended purpose and deleted when no longer needed, compartmentalize information, limit who has access to your full custody setup, avoid linking real identity to Bitcoin holdings publicly, don't discuss your bitcoin holdings or wealth publicly, avoid posting pictures or information that could reveal your location on

Security isn't just keys and hardware. It's keeping your identity out of an attacker's crosshairs. A customer database that ties real-world details to custody setups becomes a targeting map. Treat privacy as a control that reduces blast radius: share the minimum required, prefer pseudonymous contact and shipping details, ensure any data is used only for its task and erased when done, and expect your provider to compartmentalize and tightly gate access.



The less personal data attached to your setup, the fewer paths an adversary has to reach you. Shrink the data, shrink the attack surface.

Advanced Hardening, Inheritance & Audit

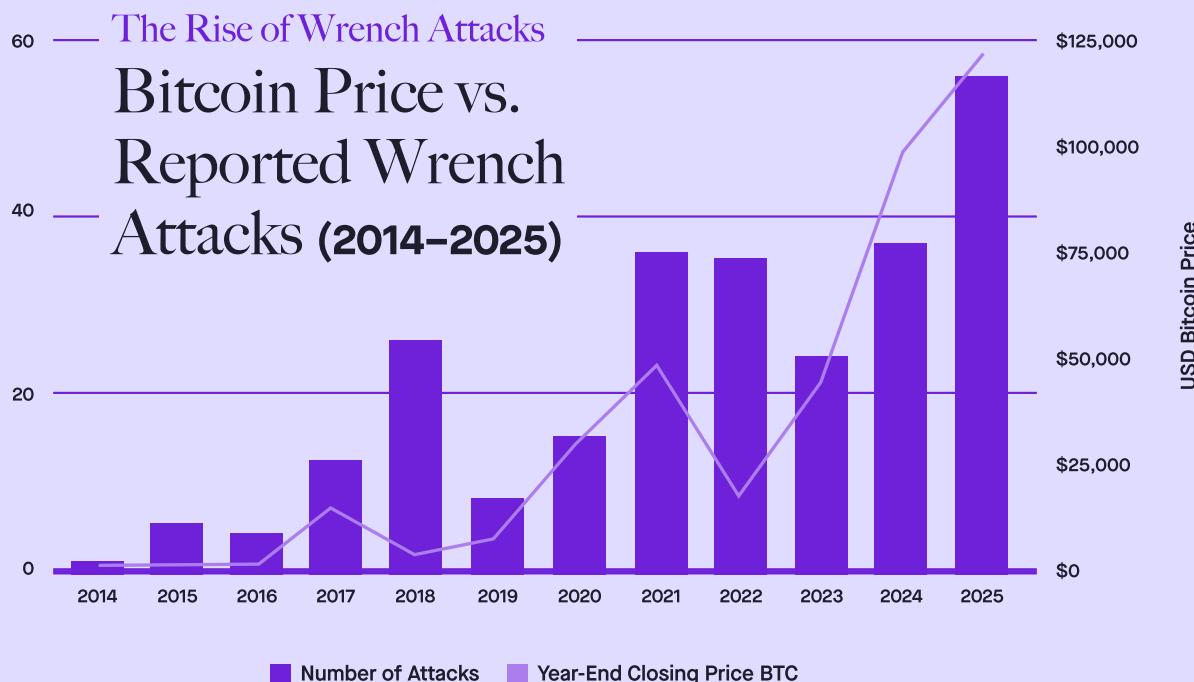
Once the base is secure, the next layers address the more complex, but equally critical, risks: coercion, inheritance, and evolving threats.

LAYER 4: Defense Against Coercion

Threats: Coercion / Physical Attack Mitigations, Fail-Safe Layers, Child/Pet attack

Tactic: Build defense-in-depth with deniability and concealment: use decoy paths, layered secrets, tamper-evident devices, dead man's switches, and avoid exposing your full key setup.

Not all attacks happen online. In some cases, the greatest risk is physical coercion: being pressured or threatened into surrendering access. Preparing for this means introducing safeguards such as decoy accounts with small balances, tamper-evident hardware that wipes itself under attack, or systems where no one key can unlock full control.



Treat security as a living system: audit, rotate/retire, monitor, and record. Defenses remain legitimate only when they adapt to the world as it is, not as it was.

LAYER 5: Inheritance and Succession

Threats: Poor transmission, ambiguous instructions

Tactic: Have an Inheritance plan. Don't assume your heirs will be able to recover funds without guidance. Use Casa's built-in inheritance functionality to securely share recovery details with your chosen executor or beneficiary. This approach combines clear instructions, multi-key based access controls, and tested recovery workflows to ensure your assets remain protected yet passable to the right people.]

The ultimate measure of any custody plan is whether it can outlast you. Without a clear strategy for inheritance, digital assets can easily become inaccessible, leaving loved ones locked out permanently.

This is why awareness of succession planning is critical. Strong custody frameworks account for the transfer of access, balancing clarity for heirs with safeguards that prevent misuse. Legal instruments, encrypted instructions, and gradual access models are all tools that can be used to ensure assets don't disappear into limbo.

Security isn't complete unless it protects both your wealth and the people meant to inherit it.

LAYER 6: Hardware Diversity

Threats: Software vulnerabilities, supply-chain attacks, single-vendor flaws, new attack vectors.

Tactic: Conduct regular audits to verify backups, diversify hardware and software (never rely on one brand), verify device authenticity and tamper-evident seals, prefer wallets with smaller and well-audited codebases, retire aging tech, monitor disclosures, and document all operational changes.

Self-custody is never static. Devices age, firmware updates introduce unknowns, and attackers evolve. A plan that feels secure today won't hold tomorrow if it relies on one vendor or isn't re-examined with fresh assumptions. Diversifying platforms reduces correlated risk, authenticity checks catch supply-chain compromises early, and choosing minimal, well-audited firmware shrinks the attack surface.

These measures aren't about paranoia. They're about ensuring that even under duress, your system doesn't collapse in a single moment of pressure.

The Result: Self-Custody Resilience

A strong self-custody approach isn't achieved all at once.

It grows by addressing different categories of risk over time. Reducing single points of failure, building in redundancy, confirming recovery methods, guarding against coercion, planning for succession, and revisiting safeguards regularly are all essential pieces of the bigger picture.

Each layer ties directly to real-world threats. Long-term protection comes from seeing the full spectrum of risks clearly, understanding the principles that counter them, and recognizing when those principles aren't being applied.

Casa's Wealth Security Protocol is grounded in these principles and extends beyond them. With this framework, you create a system designed to protect not only your wealth today, but also for every tomorrow that matters.

**Layer 1:
Awareness of
Multi-Key Security**

**Layer 2:
Geographic & Logical
Redundancy**

**Layer 3:
Privacy as Security**

**Layer 4:
Defense Against
Coercion**

**Layer 5:
Inheritance and
Succession**

**Layer 6:
Hardware Diversity**



Understanding Multi-Key Architecture

Throughout this guide, we've referenced multi-key security as the foundation of robust self-custody. But how does it actually work, and why is it so fundamentally different from traditional single-key wallets?

HOW MULTI-KEY VAULTS WORK

A multi-key vault (also called multisignature or multisig) fundamentally changes how bitcoin custody works. Instead of one private key controlling your bitcoin, multiple keys are required to authorize any transaction. You set a threshold: perhaps 2 keys out of 3 total keys, or 3 keys out of 5. Any transaction requires signatures from the threshold number of keys to be valid.

Think of it like a bank vault that requires multiple keyholders to open. One person with one key can't access the contents. You need the threshold number of keys present and cooperating to unlock the vault. The difference is that with Bitcoin, these "keys" can be distributed across different devices, different locations, and even different jurisdictions, all while you maintain complete control without any third party involved.

When you create a multi-key vault, you generate multiple private keys and define the threshold required for spending. A common setup is 3-of-5: you generate five private keys, and any three of those five keys can authorize a transaction.

Each key typically lives on a separate device in a separate location. One might be on your mobile phone, another on a hardware wallet in your home safe, a third on a different hardware wallet in a bank deposit box, a fourth with a trusted family member, and a fifth held by a professional custody service as a recovery backup.

With a single-key wallet, security and access are binary. Either you have the key and complete

control, or you don't have the key and you have nothing. One compromised key means stolen funds. One lost key means permanently lost funds.

Multi-key vaults introduce resilience:

- **Partial compromise doesn't mean total loss:** If one key gets stolen, your bitcoin remains secure because the attacker can't meet the threshold. You have time to create a new vault and move your funds.
- **Partial loss doesn't mean permanent loss:** If one key is destroyed or lost, you still have access through your remaining keys. You can recover and create a new configuration without losing anything.
- **Distribution creates optionality:** You can keep one key accessible for quick transactions, another in secure long-term storage, and a third geographically distant.
- **Sovereignty remains intact:** Despite having multiple keys, you maintain complete control. There's no custodian, no third party with unilateral access, and no institution that can freeze your funds.

GEOGRAPHIC DISTRIBUTION FOR INTERNATIONAL INDIVIDUALS

For individuals living across multiple countries or maintaining ties to several jurisdictions, multi-key vaults turn geographic distribution into a security advantage.

The critical principle: your keys should be distributed across locations that are geographically distant from each other, not just in different buildings within the same city.

This distance creates friction that protects you against coercion, targeted attacks, and localized disasters that could compromise multiple keys simultaneously.

- **Keys in current locations:** Keep one or more keys where you currently spend time, providing easy access for regular transactions. This might be a mobile key on your phone or a hardware wallet in your primary residence.
- **Keys in stable, distant jurisdictions:** Place keys in countries known for rule of law and property rights that are geographically separated from each other. A safe deposit box in Singapore and another in Switzerland creates more friction than two boxes in the same city. The distance means an attacker would need to operate across multiple countries and time zones to compromise your setup.

- **Keys with trusted parties in different regions:** Family members, attorneys, or advisors in different countries (ideally on different continents) can hold keys. During your lifetime, they cannot access your funds without your cooperation and additional keys. After your death, they provide recovery mechanisms that work across borders. Geographic separation protects against scenarios where you're coerced or physically threatened, as you don't have immediate access to enough keys in any single location.
- **Professional custody backup:** A recovery key held by a specialized custody service serves as backup if you lose access to multiple keys through unexpected circumstances, while the service cannot access your funds unilaterally. This provides a fail-safe without creating a single point of control.

The result is a security model where distance works in your favor. Keys separated by thousands of miles means a localized disaster, whether natural (earthquake, flood, fire) or human-made (civil unrest, targeted attack, jurisdictional seizure), can only affect one key. An attacker who discovers one key location faces a massively more complex operation to compromise keys in other countries.

Even under duress, you can truthfully say you don't have physical access to enough keys in your current location to move funds. Your keys exist in multiple jurisdictions, creating redundancy against problems in any single location while maintaining your complete control. Geographic distribution transforms potential vulnerabilities into defensive advantages.



From Financial Sovereignty to Jurisdictional Sovereignty

Achieving financial sovereignty through self-custody is the first major step toward true independence. When you hold your own keys and remove single points of failure, you protect your wealth from institutional risk, political pressure, and operational fragility. You shift from hoping a system will protect you to knowing you control your future.

But for many internationally minded individuals, especially those with meaningful wealth, financial sovereignty on its own is not enough. Your assets may be secure, but your mobility, your taxes, your privacy, and your family's long-term safety still depend on the jurisdiction that governs you. Where you live, where you bank, where you spend most of your time, and which governments can claim authority over you is as consequential as how you store your bitcoin.

Just as a multi-key vault distributes control across devices and locations to eliminate single points of failure, jurisdictional sovereignty applies the same principle to your life. By

diversifying your citizenships, residencies, and legal ties, you reduce dependence on any single state and create optionality for whatever the future holds.

The same principles that strengthen a resilient custody setup, such as distribution, redundancy, privacy, and optionality, also strengthen your personal sovereignty. If self-custody gives you control over your wealth, jurisdictional diversification gives you control over your mobility, your identity documents, and your family's long-term security.

CITIZEN X

This next section explores how citizenship, residency, tax residency, and legal structures serve as strategic tools to build that optionality. With CitizenX's expertise, you will learn how to apply the same security mindset that protects your bitcoin to protecting your freedom, your family, and your future across borders.



Jurisdictional Sovereignty

Jurisdictional sovereignty is how you gain optionality to choose which governments have authority over your identity, your income, your assets, and your heirs. By placing parts of your life in multiple jurisdictions, you reduce dependency on any single state and build resilience against political, economic, or legal instability.

This concept is rooted in a simple idea: the more optionality you have, the harder it becomes for any one government to restrict your movement, freeze your assets, or limit your opportunities. Sovereignty is not only about freedom from financial intermediaries. It is also about freedom from jurisdictional concentration.

Below are the main instruments available to build jurisdictional optionality.

The Flag Theory Toolbox

1. Citizenship

(Passports)

Citizenship provides full legal membership in a nation-state, along with rights such as a passport, voting, and consular protection.

Strategic value:

- An ultimate hedge against your home-country government
- A global mobility asset
- Consular and diplomatic protection abroad
- The right to live and work indefinitely in that country
- In many cases, an inheritable asset for your family

2. Residency

(Temporary or Permanent)

Residency provides the right to legally live in a country, even without citizenship.

Strategic value:

- Live in a country without visa runs
- Access to local banking, healthcare, and education
- Ability to eventually pursue citizenship through naturalization

3. Tax Residency

Tax residency determines where you report and pay taxes. Creating optionality here allows you to optimize your tax strategy or separate your personal life from an unfavorable jurisdictional tax regime.

4. Legal Entities and Trusts

Legal structures can separate personal liability from business assets and unlock opportunities for better tax treatment, asset protection, or cross-border operations.

Pathways to Citizenship

There are several ways to acquire a second citizenship, each with benefits, trade-offs, and timelines.

1

Citizenship by Investment (CBI)

A direct path to citizenship in exchange for investment or donation. Countries that offer this route provide fast, predictable access to a second passport.

2

Residency by Investment (RBI) / Golden Visas

Just like CBI, these programs grant residency in exchange for a qualifying investment. They typically require minimal or zero physical presence and, in many cases, open a clear path to permanent residency and eventual citizenship through naturalization.

Currently available routes:

3

Citizenship by Descent

With this route, you don't get to pick the country—your ancestors determined this for you decades or centuries ago. But if you qualify for citizenship by descent, this is the lowest-hanging fruit in the entire Flag Theory toolbox: a legitimate second passport at low cost. Even if the country's politics or tax regime isn't perfect today, it's almost always worth claiming and keeping this nationality running in the family as a legacy play.

4

Residency to Naturalization

The classic route: obtain legal residency, live in the country for the required number of years (typically 2-10), then apply for citizenship through naturalization. This path exists in almost every country on earth, provided you can secure an initial residency permit that fits your profile and you're genuinely willing to spend the necessary time on the ground.

Important: A handful of countries offer permanent residency but explicitly block any route to citizenship, no matter how many decades you live there.

Strategic Considerations When Choosing a Plan B Country

In Flag Theory, your “Plan B country” serves as a hedge—a second citizenship or residency that acts as an insurance policy against potential crisis in your primary jurisdiction or specifically in your life. To select the optimal one, begin with a structured security model thought process, similar to threat modeling in custody solution or cybersecurity. This ensures your Plan B is tailored to your needs, resilient, and cost-effective. You can utilize this as your worksheet to help you map out the strategy:

1 Identify Your Assets: Begin by mapping what you are actually trying to protect.

- **Personal freedom** (global mobility, physical safety, medical autonomy)
- **Family** (lifestyle, education options, healthcare access, future opportunities)
- **Wealth** (liquid assets, income streams, crypto, real estate, businesses)
- **Legacy** (generational wealth transfer, inheritance planning, dynasty protection)

2 Define Your Plausible Threats

Next, identify the scenarios that could impact your life or your wealth. Threats vary depending on your location, your profile, and your worldview.

- High-net-worth individual in a politically volatile region
- Bitcoiner facing imminent capital controls or confiscation risk
- Business owner hit with aggressive tax hikes or retroactive wealth taxes
- Parent in a country sliding toward conscription, mobilization, or war

3 Identify Attack Vectors

Each threat can manifest in a specific way. Understanding these “points of failure” helps you design an effective Plan B.

- Sudden travel/exit bans (passport revocation)
- Currency controls or forced repatriation (your bank account gets frozen or confiscated)
- Asset freezes, wealth taxes, or forced “solidarity contributions”
- Targeted extradition or politically motivated prosecution
- Drafting orders for you or your kids
- Medical/travel restrictions in a new pandemic or war

4 Evaluate Your Time Window

Not all threats operate on the same timeline. Your Plan B strategy should match your urgency.

- **0-3 months** → geopolitical flare-up, capital controls incoming, or red flags everywhere
- **3-24 months** → elections that could go very wrong, new tax laws proposed, civil unrest warming up
- **2-5 years** → proactive, building the escape pod while things are still calm

5 Assess Expense vs. Security Reward

This is your personal cost-benefit analysis. The question is not “What is the cheapest option?” but “What gives me the right level of security, mobility, and peace of mind for the price?”

For high-net-worth individuals, speed, stability, and long-term certainty often outweigh cost.

Additional Factors to Consider When Choosing a Jurisdiction

Geopolitics

Depending on your home country and your political views you will optimize for the country that is on the right trajectory according to your values and principles.

Family Composition

Are you able to include your children? How much will this affect the cost of execution? Can you include your elderly parents? Can you include your civil spouse without a government issued marriage certificate?

Taxes

Understand how obtaining a second passport or residency affects your tax obligations.

Key questions include:

- What is your current tax residency?
- How do you properly exit it?
- Can you transfer assets without triggering exit tax?

Mandatory Military or Civic Obligations

Some countries have mandatory service that applies to citizens and sometimes residents. Evaluate the implications for you and your children.

Extradition and Enforcement Risk

Does the jurisdiction have treaties, political will, or economic pressure to enforce foreign judgments? Is enforcement selective (only violent crime) or broad (includes tax, speech, political cases)?

Options Available on the Market

El Salvador

Time to passport: 6 weeks

Price: \$1,000,000

Strong passport, Bitcoin-native program, Bitcoin-friendly jurisdiction, fast and straightforward due diligence.

Sao Tome and Principe

Time to passport: 3-4 months

Price: ~\$110,000

Serbia

Time to passport: 4-6 months

Price: ~\$440,000

Saint Kitts and Nevis

Time to passport: 8 months

Price: ~ \$290,000

Grenada

Time to passport: 8-10 months

Price: ~\$280,000

Bringing Financial and Jurisdictional Sovereignty Together

True sovereignty is not achieved through a single decision. It is the cumulative result of many deliberate choices that reduce your reliance on fragile systems and increase your control over your future.

Financial sovereignty begins with holding your own keys.

When you remove intermediaries and eliminate single points of failure, you protect your wealth from the institutional, political, and operational risks that have trapped generations before you. You create a resilient foundation for long-term security and peace of mind.

Jurisdictional sovereignty extends that foundation beyond your bitcoin.

It gives you the ability to choose where you live, where you pay taxes, which governments can claim authority over you, and what opportunities are available to you and your family. By securing citizenships, residencies, and legal ties in multiple jurisdictions, you diversify the “attack surface” of your life, not just your assets.

Together, these two pillars form a holistic sovereignty model:

- Your wealth is protected by multi-key security and distributed control.
- Your life is protected by jurisdictional diversification and global mobility.
- Your family is protected by inheritance planning, future-proof structures, and parallel access to opportunity.

This is the modern sovereign strategy: distributed keys, distributed jurisdictions, and distributed dependencies. The purpose is not to live in fear. The purpose is to live with clarity, intention, and freedom.



Casa and **CitizenX** share a commitment to helping you build this independence thoughtfully and securely. Whether you are protecting meaningful bitcoin wealth, planning for your family's future, or establishing a geopolitical Plan B, the path forward is the same: reduce single points of failure, increase optionality, and strengthen the systems that safeguard what matters most.

You deserve a future that is not dictated by a single institution or a single jurisdiction. With the right structures in place, you gain the confidence to navigate an uncertain world with stability, mobility, and complete control over your financial and personal destiny.

This is what true sovereignty looks like.



SOVEREIGN INDIVIDUAL GUIDE

[Click to book a call today.](#)

