Blockchain, Crypto, and Financial Abuse: Pathways from Survival to Sovereignty

by Karin Kusano
Founder of FAFA Foundation

The Problem: Economic Coercion is Systemic

U.S. federal definitions now explicitly recognize economic abuse as behavior that "coercively deceptively, or unreasonably controls or restrains a person's ability to acquire, use, or maintain economic resources," including not only restricting but also exploiting the victim's financial resources—for example, draining accounts, forcing loans, or manipulating credit to the abuser's advantage.

Empirically, financial abuse is nearly universal among survivors. Studies by the National Coalition Against Domestic Violence (NCADV) show that 99% of domestic violence cases involve some form of financial abuse . *Those who experience physical or sexual violence, stalking, or psychological aggression, 99% also experience financial coercion.* Moreover, the number one reason survivors stay or return to abusers is financial insecurity—they cannot afford to leave or remain safe.

The scope extends globally. Research finds that economic coercion cuts across regions, cultures, and income levels; studies in the U.S., UK, Australia, and low- and middle-income countries consistently show financial abuse as one of the most pervasive but underreported forms of intimate partner violence . In many cases, survivors report that financial abuse was the *first and ongoing tactic* of control—one that made leaving practically impossible.

Traditional finance amplifies these harms through centralized chokepoints:

- Joint accounts can be drained or frozen at will.

- Identity verification processes can be manipulated by abusers with access to documents.

- Signatures can be falsified on loans, credit applications, or transfers.

- Opaque records and jurisdictional barriers prevent survivors from quickly tracking or reclaiming their own re

Sector data further indicate that victim-survivors are more likely to disclose financial abuse to banks and financial institutions than to police or shelters, making financial systems the *frontline of detection and response*. Yet those very institutions can inadvertently reinforce dependency, especially when their policies fail to account for coercive control.

Blockchain as a Pathway to Financial Autonomy

Financial abuse remains one of the most pervasive yet underreported forms of domestic violence. Survivors are often systematically stripped of the resources they need to secure independence and safety. Traditional banking and financial systems—anchored in centralized institutions—can inadvertently reinforce this vulnerability. When abusers control joint bank accounts, forge signatures, or exploit access to personal financial information, survivors may find themselves cut off from even the most basic resources.

As the global financial system undergoes rapid digitization, blockchain and digital assets present an alternative framework that challenges these vulnerabilities. At its core, blockchain technology is a decentralized ledger, enabling secure peer-to-peer transfers without reliance on banks or other intermediaries. Digital assets—ranging from cryptocurrencies to tokenized real-world assets—allow individuals to store and transfer value with varying degrees of anonymity and privacy. These innovations have been praised for democratizing finance, but they also raise valid concerns about security, regulation, and misuse.

Nonetheless, if implemented responsibly, blockchain-based financial tools can provide survivors with mechanisms to reclaim autonomy over their assets and reduce susceptibility to economic exploitation. Its core features—decentralization, pseudonymity, and irreversibility—align closely with the needs of individuals facing financial abuse:

1. Unhindered Access
   Traditional accounts can be frozen, closed, or manipulated under false pretenses—sometimes at the abuser's request. In contrast, blockchain wallets remain under the sole control of the keyholder, ensuring access cannot be revoked by a partner, bank, or third party.

2. Pseudonymity
   Blockchain addresses do not require legal names or identifying information. This pseudonymity helps survivors shield financial activity from abuser surveillance. However, if a wallet address is linked to a real identity, transaction details may become visible, requiring careful use of privacy practices.

3. Portability of Funds
   Blockchain-based assets can be accessed from virtually anywhere with an internet connection. This mobility is critical for survivors who may need to relocate quickly; funds can be preserved and retrieved in a new location without relying on physical banks or local institutions.

Taken together, these properties position blockchain as more than a technological innovation—it is a potential lifeline for financial resilience, allowing survivors to safeguard resources, maintain independence, and pursue safety without total dependence on centralized institutions.

The features outlined above demonstrate how blockchain technology reshapes what is possible for survivors of financial abuse. Yet the significance becomes even clearer when these capabilities are contrasted directly with the limitations of traditional finance. Traditional banking systems—designed around centralized authority, identity verification, and gatekeeping—often reinforce the very vulnerabilities abusers exploit. Blockchain and DeFi, by contrast, offer permissionless access, custody independence, and global portability.

To illustrate this contrast, the following table compares the key barriers survivors face within traditional finance against the alternative pathways made possible through blockchain systems.

Barrier / Issue	Traditional Finance	Blockchain & DeFi
Account Access	Bank accounts can be frozen, closed, or drained—sometimes at the abuser's request. Survivors may be locked out entirely.	Wallets are self-custodied; access is controlled only by the keyholder. No one can unilaterally revoke access.
Identity Requirements	Requires government ID, credit checks, or co-signers. Abusers often exploit or withhold documents.	Permissionless wallets require no ID to create; survivors can transact pseudonymously.
Privacy	Transactions, account details, and KYC records may be exposed to abusers or leaked in data breaches.	On-chain addresses are pseudonymous; privacy tools (zk-proofs, mixers, address rotation) add further protection.
Asset	Funds are tied to local banks;	Assets are borderless and

Barrier / Issue	Traditional Finance	Blockchain & DeFi
Portability	cross-border transfers are slow, expensive, and sometimes blocked.	accessible anywhere with internet. Survivors can flee and still retain funds.
Proof & Transparency	Paper trails can be altered, hidden, or destroyed; subpoenas required for discovery.	Transactions are immutable and auditable on-chain, providing instant evidentiary proof of flows.
Custody Security	Survivors often forced into joint accounts or shared cards, vulnerable to exploitation.	Options like cold storage and multi-signature wallets distribute control, preventing unilateral abuse.
Investment Barriers	Survivors often excluded from wealth-building due to accredited-investor rules, high minimums, or lack of margin access.	DeFi and tokenization lower entry barriers; anyone can participate with small amounts, building assets gradually.
Aid & Disbursement	Relief funds may be intercepted, delayed, or conditioned on abuser cooperation.	Smart contracts enable automated, direct, and conditional transfers (e.g., rent paid directly to landlord).
Global Reach	Survivors abroad may lack local bank access or face discriminatory policies.	Permissionless protocols operate globally; anyone with a wallet can join, regardless of geography.

Why Blockchain Changes the Feasibility Frontier

Peer-to-Peer Networks and Censorship Resistance

Bitcoin's original design eliminated the need for a central intermediary to authorize transfers, proving that censorship-resistant value transfer at a global scale is possible. This ensures that no government, bank, or abusive partner can unilaterally block, reverse, or freeze a transaction. For survivors, this creates a vital safety net: their funds remain accessible as long as they control their private keys.

Transparency and Safety Trade-Offs

All wallet transfers on public blockchains are on-chain, permanent, and auditable. This transparency empowers survivors and their advocates to uncover hidden assets,

document patterns of coercion, or provide evidence of financial exploitation. Yet transparency is a double-edged sword: if an abuser links a wallet address to a survivor's identity, their entire transaction history may be exposed.

To mitigate this, survivors can use privacy-enhancing technologies such as mixers, zero-knowledge proofs (zk-proofs), or privacy-preserving blockchains. These tools allow them to protect identity while still proving ownership or value. Survivors must strike a balance: transparency is powerful in legal disputes, while pseudonymity remains essential for safety.

Smart Contracts as Automated Protection

Smart contracts enable funds to move according to pre-programmed rules, reducing opportunities for coercion. Survivors can receive aid through contracts that:

- Release funds only for specific purposes (e.g., rent, groceries).
- Enforce time locks, preventing impulsive or coerced withdrawals.
- Provide escrow protections, ensuring money reaches its intended recipient without interception.

By embedding rules directly in code, smart contracts replace human discretion—often manipulated in abusive contexts—with trustless, rule-based systems.

Cold Storage and Custody Safety

Cold storage—keeping private keys offline on hardware devices or paper backups—adds critical protection. Even if an abuser compromises a connected device, they cannot remotely drain funds held in cold storage.

The challenge lies in key management: if a key is lost or destroyed, funds may become permanently inaccessible. Survivors can mitigate this by using multi-signature arrangements (e.g., survivor + trusted nonprofit + legal advocate). This distributes responsibility and ensures no single party, including an abuser, can unilaterally control funds.

Portable Identity: DIDs and Verifiable Credentials

Emerging standards such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs 2.0) allow survivors to prove facts—such as age or participation in a relief program—without exposing full personal data. Selective disclosure protects sensitive information while granting access to essential services. For survivors, this technology enables safer participation in aid programs and financial platforms without fear of exposure.

Know Your Customer (KYC) requirements create particular risks for survivors:

- Data sharing risks: Abusers may gain access to stored identification documents.

- Privacy breaches: Centralized exchanges, if hacked, can expose survivors' sensitive personal data.

- Exclusion: Survivors who lack documents—because passports or IDs are withheld—may be barred from using centralized platforms.

A dual approach is needed. Regulated on-ramps must adopt survivor-sensitive safeguards, such as confidential handling of documents and emergency protections. At the same time, permissionless systems must remain open to ensure survivors retain at least one pathway into financial participation.

DeFi and On-Chain Participation

Decentralized Finance (DeFi) represents the next frontier of empowerment. Through onchain protocols, survivors can:

- Earn yield through lending pools or staking, without needing a traditional brokerage account.

- Swap tokens on decentralized exchanges (DEXs) without identity verification or gatekeeping.

- Access liquidity instantly through automated market makers (AMMs), bypassing intermediaries or biased institutions.

DeFi participation is inherently permissionless—anyone with a wallet can engage. For survivors, this drastically lowers barriers to saving, investing, and rebuilding. In this way, blockchain evolves from a defensive tool (protecting assets from abuse) into an offensive opportunity: a system that enables survivors to grow wealth, build literacy, and re-enter the financial system on their own terms

Mapping Abuse Patterns to On-Chain Controls

The power of blockchain is not only in moving assets freely but in programming how those assets behave. Patterns of financial abuse—unauthorized withdrawals, intercepted benefits, hidden assets—can be met with on-chain controls that re-engineer financial systems for protection rather than exploitation.

- Unauthorized withdrawals & joint-account lockouts → Multi-Signature Vaults. Survivors can set up wallets that require two of three signatures to release funds

(e.g., survivor + trusted advocate + nonprofit). This prevents unilateral draining of accounts, while small hot wallets remain available for everyday use.

- Interception or coercion of benefits → Smart-Contract Escrow.
  Aid funds or wages can be routed directly to landlords, utility providers, or secure accounts through programmable contracts. Time-locks and "circuit-breaker" duress mechanisms allow survivors to pause or delay suspicious transfers.

- Hidden joint assets → On-Chain Auditability.
  Public ledgers record every transfer, creating a tamper-evident trail. Forensic blockchain tools can uncover concealed wallets and asset dissipation, aiding both survivors and courts in ensuring fair settlements.

- Identity exposure risks → Selective Disclosure via DIDs/VCs.
  Survivors can prove eligibility for relief (e.g., age, program participation) without exposing full identity. Rotating wallet addresses further reduces traceability.

- Barriers to rebuilding wealth → Tokenization & Permissionless Markets.
  Survivors can begin rebuilding with small amounts by accessing fractional ownership in real-world assets, staking opportunities, or low-cost investments through decentralized exchanges.

- Coerced debt → Survivor-Friendly Protocols.
  Blockchain-based credit systems could integrate tags for coerced debt, freezing or invalidating abusive liabilities while supporting survivor credit-repair initiatives.

Real World Applications
Evidence, Discovery, and Due Process in Family Law

Financial disputes in court often collapse into "he said, she said" battles over bank statements, missing records, or conveniently timed withdrawals. Blockchain changes that landscape by offering a shared source of truth. Because transactions on public ledgers are immutable and time-stamped, they can serve as a verifiable record of financial activity that neither party can alter retroactively.

This creates several advantages for survivors navigating custody battles, divorce, or property division:

- Accelerated discovery. Instead of waiting for subpoenas or dealing with stonewalling by opposing parties, counsel can often inspect relevant wallet activity directly on-chain. This reduces delays and legal costs while preserving evidence that might otherwise be hidden or destroyed.

- Reduced factual disputes. Immutable records establish exactly when and how funds moved. Survivors can demonstrate patterns of coercion—such as repeated

withdrawals after late-night text exchanges—or show attempts to dissipate assets in anticipation of divorce. The ledger speaks where memory or testimony may falter.

- Privacy management. Transparency must be balanced against safety. Linking a survivor's identity too closely to a wallet address could expose an entire financial history to an abuser. Courts and counsel should therefore adopt protective orders, pseudonymous filings, or selective-disclosure tools to ensure that only relevant portions of on-chain activity are entered into evidence.

In this way, blockchain is not simply a financial refuge—it also reshapes the evidentiary framework of family law. Survivors gain a tool to corroborate their claims with digital certainty, while judges and lawyers gain access to a higher standard of proof. At the same time, safeguards are essential to prevent transparency from becoming another avenue of surveillance or harm.

Economic coercion is not a side issue of domestic violence—it is its financial backbone. It is the reason so many survivors cannot leave, return when they wish they could stay away, and remain trapped even after separation. For decades, our financial systems—designed around centralized control, identity verification, and opaque recordkeeping—have been weaponized against survivors rather than shielding them.

Blockchain technology, if implemented responsibly, shifts this feasibility frontier. What once required trust in institutions that too often failed survivors can now be achieved through decentralized custody, programmable safeguards, pseudonymous participation, and immutable records. These tools are not abstractions; they are lifelines. They allow a mother to preserve her children's rent money from an abuser's reach, a survivor to carry her savings across borders, or a family court to resolve financial disputes with clarity rather than conjecture.

But technology alone will not end financial abuse. Policymakers must act to ensure that the next generation of financial infrastructure is built with survivor safety at its core. That means:

- Supporting pilot programs that integrate survivor-sensitive blockchain wallets and smart contract protections.

- Funding education and literacy initiatives so survivors understand both the power and the risks of digital tools.

- Enacting protective legal frameworks that allow blockchain evidence in family court while safeguarding survivor privacy.

- Encouraging financial institutions and fintech innovators to adopt survivor-informed design as a standard, not an afterthought.

Survivors do not need charity; they need access, autonomy, and dignity. They need systems that cannot be hijacked by those who would control them. The question before us is whether we will allow financial abuse to remain invisible—or whether we will lead in harnessing technology to finally dismantle it.

This is not only a matter of innovation. It is a matter of justice. A society that enables survivors to protect their resources is a society that enables them to reclaim their futures. Blockchain is not a cure-all, but it represents an inflection point. We stand at a crossroads: continue with systems that perpetuate dependency, or reimagine finance as a tool of liberation.

The human right of financial sovereignty can be a reality

REFERENCES

(NCADV). Financial Abuse Factsheet.

Postmus, J.L. et al. (2020). Measuring Economic Abuse in the Lives of Survivors: Scale Development and Implications for Policy.

Adams, A.E., Sullivan, C.M., Bybee, D., & Greeson, M.R. (2008). Development of the Scale of Economic Abuse.

Sharp-Jeffs, N. (2015). Money Matters: Research into the Extent and Nature of Financial Abuse.

UN Women (2020). Financial and Economic Abuse in the Context of Domestic Violence.

Surviving Economic Abuse (SEA). (2021). Financial Abuse and Coercive Control Reports.