



Bitcoin for Community Organizations

Governance security and service

A practical guide for Lions clubs, Knights of Columbus units, charitable foundations and other community organizations.

Use Bitcoin only where the organization has authority, trained people and a recoverable operating process. Begin with education. Accept or hold funds only after the precise activity has passed the organization's financial and legal review.

1

Organizational authority

Governing rules
Donor restrictions
Recorded approvals

2

Control and recovery

Independent keys
Verified transactions
Tested succession

3

Capacity to serve

Usable resources
Continuity of services
Honest risk limits

Assess each safeguard before committing charitable resources.

Three distinct safeguards. Sound technology supports responsible stewardship; it cannot supply legal authority or guarantee future purchasing power.

This Spark House publication brings the original Bitcoin model into a practical framework for gifts, custody, spending, reporting and officer succession. It applies the ethical questions of Magnifica Humanitas to community service without presenting the encyclical as a Bitcoin endorsement.

Research edition 1 • 9 October 2026. United States examples, with Minnesota law identified where relevant. Independent educational publication; no affiliation with or endorsement by Lions International or the Knights of Columbus is claimed.

The procedures and resolution are proposed templates. Publication does not adopt them for any organization, establish a receiving wallet or authorize movement of funds.



Choose a useful and permitted activity

The best starting point is a modest educational program that helps members recognize fraud, understand digital signatures and practice financial oversight without putting charitable resources at risk.

Activity	Potential benefit	Boundary before proceeding
Education using test funds	Digital literacy and volunteer training	Use a simulation or test network with no economic value; distinguish it visibly from mainnet.
Receiving a gift	More donor choice and direct transfer	Confirm the recipient, gift terms, allowed asset and custody or conversion route.
Paying an approved recipient	BTC settlement without a custodial balance	Recipient must consent and be able to use BTC; retain all spending approvals.
Holding a reserve	Direct control of a scarce digital asset	Separate investment authority, liquidity planning and loss capacity are required. No return is promised.
Displaying a copper wallet	History and community education	Treat the object and any associated BTC as separate assets and responsibilities.

A decision that protects the mission

1. Identify the need Bitcoin would meet and the people who benefit.
2. Check the actual entity's rules and obtain any required superior approval.
3. Demonstrate custody, recovery, accounting and a workable exit before a funded pilot.
4. Decline or defer the activity if a requirement remains unresolved.

Spark's Bitcoin project permits native BTC mainnet only. It excludes independent fork currencies, tokens, wrapped claims, stablecoins, lending, leverage, financial derivatives and fiat substitutes. This project mandate does not change another organization's rules or required reporting currency.

Reading map: authority and organization examples, pages 3-5; ethics and security, 6-9; operating procedures, 10-14; pilot and adoption records, 15-17; sources, 18-22.



Establish the organization and its authority

Start with the legal recipient, not the group's familiar name. A local club, foundation, council, assembly, donor-advised fund and international body can have different owners, powers and tax treatment. A donation link for one does not authorize another to accept or hold Bitcoin.

Build an authority record

1. Record the entity's full legal name, jurisdiction and tax status; keep identifiers in the private administrative record.
2. Collect the charter, current constitution and bylaws, superior policies, gift instruments, bank and investment rules, spending resolutions and insurance terms.
3. Cite each provision that permits the proposed receipt, custody, investment, conversion and expenditure. A broad permission to receive electronic payments may not permit a Bitcoin treasury.
4. Record who interprets conflicts and who can approve an exception. Preserve the actual decision and effective date before soliciting funds.

Decision	Evidence needed
Accept a gift	Eligible recipient, permitted asset, donor restrictions and acknowledgment procedure.
Hold BTC	Permitted custody and investment arrangement; written exposure and liquidity limits.
Spend or transfer	Required resolution, vouchers and officers, plus verified destination and purpose.
Change restrictions	Lawful donor consent or other applicable process; signers cannot rewrite a gift alone.

For a qualifying Minnesota institutional fund, section 309.74 ties management to charitable purpose, donor intent and prudent conduct. It includes a diversification duty unless special circumstances justify a different course. A Bitcoin-only preference is not an automatic exception. Determine first whether the statute applies to the particular fund. [R4]

Recommended control: keep the authority record with the financial policy and review it whenever officers, laws, governing documents or the proposed activity change. A vote cannot cure a conflict with a superior rule.



Lions clubs and LCIF

Use the club's adopted documents and applicable international and district rules. The current standard club constitution and bylaws, LA-2 for 2026-27, are revised July 2, 2026. [L1]

Preserve the purpose of public funds

Public fundraising proceeds and their gains remain for public benefit. Lions' guidelines expect spending in the year received unless funds are designated for a long-term project. Permanent specimen funding needs a compatible, properly designated purpose. [L2]

Keep administrative and public funds separately accounted for. One checking account is permitted when records preserve that distinction; separate accounts are a recommended control. Public fundraising funds cannot finance club administration. [L2]

Retain club financial controls

Standard rules require board expenditure oversight, annual audit, regular reports and approved deposits. Best-practices guidance recommends two signatories from different households. Bitcoin controls must preserve required approvals and be assessed against deposit rules. [L1, L3]

Understand the LCIF route

Verified LCIF route



Separate proposal



LCIF's verified processor route converts the gift. Direct organizational BTC custody is a separate proposal that requires its own authority and controls.

LCIF's official giving page links to Every.org, which states that it converts cryptocurrency donations to U.S. dollars. This route does not establish local-club custody authority or show that LCIF retains BTC. It does not meet Spark's unconverted-BTC project mandate. [L4, L5]

LCIF and a local club are distinct recipients. Check the donee, receipt, fees, irrevocability, grant terms and intended purpose before directing a donor to a processor.

Lions' standard purposes and meeting rules prohibit sectarian religious debate. Present Magnifica Humanitas as optional comparative ethical reading for interested people; do not use it as Lions governing authority or a condition of participation. [L1]



Knights councils and Fourth Degree assemblies

Council authority comes before custody

The 2026 Charter, Constitution and Laws preserve formal receipt, custody, payment and recordkeeping duties. Section 122 governs council funds and specified resolutions; sections 135, 139 and 140 assign financial duties; section 145 provides annual audit and financial supervision. Multisignature software cannot replace those requirements. [K1]

The Fraternal Excellence Guide effective May 1, 2026 permits electronic payment services as supplements to traditional accounts, but separately restricts holding and investment arrangements. Self-custodied BTC is not among its listed ordinary account choices. Obtain a written determination from the competent Knights authority for the exact proposal; a local council vote alone does not establish permission. [K2]

The guide requires council ownership of accounts, authorized officer access and separation from personal funds. It retains section 122(b) procedures for distributions. A distinct Knights of Columbus Charitable Fund donor-advised arrangement gives a council grant-recommendation rights under its rules, not control of a local Bitcoin wallet. [K2]

Apply assembly rules separately

The public Fourth Degree law copy reviewed is revised January 2018, incorporating amendments through June 2017. It assigns separate responsibilities to the Faithful Navigator, Comptroller, Purser and Trustees, including approved deposits, written payment orders and an annual audit. Verify later directives and the actual assembly bylaws before applying it. Council officer changes cannot simply be imported into assembly practice. [K3]

Resolve edition conflicts explicitly

The consolidated council laws adopted August 6, 2026 are later than the May guide and include changed officer provisions. Older manuals and forms may use different titles or audit schedules. Preserve the current law and obtain transition guidance instead of combining incompatible descriptions. Annual council audit, rather than the older semiannual formulation, is the current requirement in the reviewed law. [K1]

Recommended next step: submit a precise proposal through established Knights channels identifying gift acceptance, any processor conversion, custody, duration, spending, records and recovery. Until authority is resolved, limit activity to education and review. Do not treat an accounting form's "other assets" field as permission to acquire BTC.

A bond or insurance policy must be checked for the proposed digital-asset arrangement. No coverage of key theft, operational error or market loss is established by this guide.



Apply Magnifica Humanitas to stewardship

Pope Leo XIV's Magnifica Humanitas, dated May 15, 2026, addresses the human person in the age of artificial intelligence. Its principles of common good, subsidiarity, participation and accountability provide an ethical lens for technology decisions. It is not a Bitcoin instruction, investment authorization or endorsement of this project. [E1]

Ethical question	Recommended organizational application
Does the activity serve people?	State the charitable outcome and protect essential services from a BTC loss.
Can members participate meaningfully?	Explain choices plainly, record concerns and preserve a genuine approval process.
Who can exercise power?	Separate approvals, signing and review; provide independent checks and a complaint route.
Who is excluded or exposed?	Keep assistance accessible without requiring recipients to own BTC or reveal wallet history.
Who bears environmental costs?	Consider energy, equipment and wider community effects when selecting activities or providers.

These controls are Spark's practical applications of the ethical questions, not requirements quoted from the encyclical. Sections 59-76 and 83-89 are especially relevant to shared goods, digital power and institutional accountability. [E1]

The Catechism's treatment of stewardship, justice and promises supports honest handling of entrusted goods. Caritas in Veritate considers finance in relation to human development. Laudato Si calls for serious assessment of environmental effects. None establishes a BTC price floor or eliminates prudential judgment. [E2, E3, E4]

Catholic institutions should use their competent ecclesial and organizational guidance. Lions and other non-Catholic organizations may consider the principles voluntarily while retaining their own mission, inclusive membership and governing rules.

Oeconomicae et pecuniariae quaestiones recognizes legitimate risk-management functions while criticizing harmful financial practices. Spark's exclusion of derivatives and fiat substitutes is its chosen asset mandate; it is not a claim that Church teaching condemns every derivative or conventional currency. [E5]

Keep responsibility with people. Automated tools may assist record preparation; they should not hold organizational secrets, invent approvals or independently authorize spending.



Understand what Bitcoin can protect

Bitcoin combines signatures, transaction validation and proof of work to maintain a shared transaction history. A full node independently checks the rules it follows. Confirmations make reversal more costly under the security assumptions; they do not provide an absolute guarantee or make a mistaken payment reversible. [T1]

Feature	Practical benefit	Remaining risk
Direct key control	An authorized holder can sign without a custodian's permission.	Lost or stolen keys can cause permanent loss.
Public transaction history	An auditor can verify outputs and transfers.	The ledger does not prove donor intent, legal ownership or charitable delivery.
Divisibility	One BTC divides into 100 million satoshis.	Fees can make tiny gifts or payouts uneconomic.
Rule-based issuance	Supply rules can be checked by validating software.	Scarcity does not guarantee demand, price or purchasing power.
Global network	Direct transfers can cross borders.	Local law, recipient access, liquidity and reporting still matter.

The 2008 white paper is foundational, not the complete present-day specification. Bitcoin mainnet has adopted upgrades, including SegWit and Taproot. Independent chains such as Bitcoin Cash and Bitcoin SV remain distinct assets under Spark's mandate. [T1, T9]

Selected security research formalizes assumptions and studies incentive failures. The Bitcoin Backbone work, selfish-mining analysis and fee-only incentive analysis describe conditional results; none certifies a particular wallet or guarantees future network security. [T10]

Relative safety depends on the threat. Cold storage reduces exposure of signing keys to online attacks; multisignature can reduce dependence on one key. Neither prevents price declines, dishonest approvals, collusion or every software failure. [T2, T3]

A drop in purchasing power can impair service even when every satoshi is still present. Plan for that outcome before holding funds needed for rent, grants, food or other time-sensitive obligations.



Compare custody and payment choices

Arrangement	Useful capability	Principal tradeoff
Single hot wallet	Convenient small payments.	Online key exposure and dependence on one signer; unsuitable for a material reserve.
Single cold signing device	Less routine online key exposure.	One compromised or lost secret may defeat the arrangement.
Independent 2 of 3 keys	Two signers required; one unavailable signer can be tolerated.	More training and recovery complexity; two compromised keys can spend.
External custodian	Provider handles parts of operation and recovery.	Contract, access, insolvency and cybersecurity dependence; verify legal ownership and coverage.
Donation processor	Can simplify donor experience and receipts.	May convert or take custody; recipient, fees and gift terms differ.
Lightning payment setup	Can support small, frequent BTC payments.	Adds channel, liquidity, availability and backup duties; custodial versions add provider risk.

This is a comparison of mechanisms, not a statistical safety ranking or endorsement of a vendor. Only use an arrangement your organization is permitted and competent to operate. [T2, T6, T11]

Make custody conditions explicit

Document who can spend, freeze access, restore a wallet, rotate officers and obtain records. For providers, review withdrawal control, asset segregation, governing jurisdiction, fees, incident handling and termination. A proof-of-reserves snapshot alone does not establish ownership, liabilities or continuing solvency.

Bitcoin held directly is not an FDIC-insured bank deposit. A provider's relationship with a bank does not itself insure the customer's crypto. Ask for the actual insurance wording and exclusions, not a logo or marketing assertion. [R5]

Keep the project asset boundary

Wrapped BTC adds an issuer, bridge or custodian claim. Fund shares add product and custody dependencies. Futures and options may hedge price exposure but add margin, liquidity, basis and counterparty risks; leverage can force liquidation. Stablecoins add issuer, reserve and redemption risks. These products are excluded by Spark's project mandate. The comparison at sparkworks.org/crypto documents their differences.

Lightning moves BTC through a separate payment protocol; it is not an independent fork currency. Its technical relationship to Bitcoin does not make it suitable for a long-term organizational reserve. [T11]



Receive gifts with clear terms

Use this proposed process only after the authority review. The donor should know the exact recipient, purpose, asset, fees, any conversion, holding intention and handling of mistaken or restricted gifts before transferring value.

1. Approve the gift. Confirm that the organization can accept the asset and fulfill the restriction. Decline incompatible conditions or resolve them before receipt.
2. Issue a verified destination. Use an organizational wallet with tested recovery. Two authorized reviewers should verify the published address or invoice through a trusted process; a copied QR image is not sufficient evidence.
3. Protect donor privacy. Prefer fresh addresses for distinct gifts. Keep names, correspondence and gift restrictions in protected records rather than on-chain messages.
4. Verify receipt independently. Check the actual network, amount, transaction identifier and confirmations. Do not accept screenshots as proof. Use a documented confirmation threshold proportionate to value and reversal risk.
5. Acknowledge and classify the gift. Record BTC units, time, fees, valuation method, restriction and reconciliation reference. Identify the legal donee correctly, particularly when a charitable intermediary is involved.
6. Release it for use only under the approved policy. Resolve unexpected amounts, suspicious contacts and conflicting instructions. A refund is a new authorized payment to a verified recipient, not an automatic reversal.

A reusable public donation address exposes contribution history and may link donors. A fresh address improves separation but does not guarantee anonymity. Do not promise anonymous giving while collecting identifying records. [T1]

A donor's comment in a blockchain transaction does not automatically create an accepted gift agreement. Obtain and retain the agreed terms through the organization's normal process.

For cross-border transfers, check the applicable recipient, sanctions, registration and reporting obligations before launch. Direct settlement does not remove those requirements.

Do not publish a payment address until the recipient, authority, wallet and recovery process are verified. This guide supplies no receiving destination.



Authorize and verify every payment

A Bitcoin signature proves control of a key. It does not prove that the signer complied with the bylaws, donor restrictions or a spending resolution. Keep the authorization record separate and connect it to the transaction record. [T12]

1. Request. Record the purpose, payee, restricted fund, amount or valuation basis, fee limit and required delivery date.
2. Approve. Obtain the required resolution, voucher and officer approvals. Address conflicts of interest. Technical signers should see evidence of approval.
3. Verify the payee. Confirm the destination through a known independent channel. Do not rely solely on an email, chat account or urgent change request.
4. Prepare. Build the transaction using the approved wallet policy. A partially signed Bitcoin transaction can carry information between a coordinator and signing devices. [T5]
5. Inspect and sign. Each signer checks the destination, amount, change output and fee on the trusted device or independently verified transaction details. Unexplained outputs or mismatched policy are reasons to stop. [T6]
6. Broadcast and reconcile. Keep the transaction ID, approvals and confirmation record. A reviewer checks the resulting outputs, accounting entries, restrictions and delivery evidence. Record fees separately.

Keep recovery and spending distinct

An emergency restoration should re-establish secure control; it should not create an informal spending exception. Where a compromise requires urgent protective movement, use a preapproved emergency process and document the authority, destination and review.

Use timelocks cautiously

A Bitcoin timelock constrains spending only when the funded output actually encodes the relevant condition. A website promise, printed date or locked display case cannot add it later. Changing an existing coin's spending conditions generally requires an authorized transaction. [T8]

A timelock cannot check a donation's charitable purpose, make humans honest or guarantee that the organization will have functioning keys when the time arrives. Avoid custom scripts without qualified review and a tested recovery plan.



Handle copper wallets as two assets

A copper cold-wallet collectible can have metal and collector value, plus BTC associated with a key concealed inside it. Authenticate the exact model, edition, address relationship, provenance and condition before making a claim about a specimen.

Question	Evidence	Limit
What is the object worth?	Metal content, condition, provenance and comparable completed sales.	A retail asking price is not a realized value or appraisal.
Is BTC associated with it?	Independently verified unspent outputs for the correct address.	An engraved denomination or historic deposit is not a current balance.
Can only the organization spend?	Reliable knowledge of key generation and every access path.	An intact seal cannot prove the maker or an earlier holder kept no copy.
Will BTC retain purchasing power?	No conservation or custody test can establish this.	Market value can change while the object and BTC units remain intact.

For Blockchain Mint / Cold Storage Coins products with a manufacturer-created key under a tamper-evident seal, maker trust remains part of the system. Manufacturer instructions are product-specific; they are not an independent audit of a particular specimen. Physical stress tests also have limited scope and cannot certify every unit. [P1, P2]

Preserve the exhibit and protect entrusted funds

Handle by the edges, avoid cleaning, and use appropriate inert storage with stable conditions. Photograph public surfaces, condition and provenance without exposing a private key. Inspect the seal and reconcile the address periodically. [P3]

If the gift requires an undisturbed funded specimen, disclose the unresolved key-copy and recoverability risks and determine whether the organization can accept them. Monitoring can detect a spend; it cannot prevent one.

Where authority and gift terms permit stronger control, move the associated BTC to newly generated organizational keys and retain the object as a documented redeemed exhibit. Sweeping spends outputs to new keys; merely importing the old secret leaves its prior copies usable. Opening can reduce collector value. [T7]

Do not perform a sweep without authority to alter the specimen and move its funds. Do not solicit additional public deposits to a manufacturer-key address on the assumption that its intact seal makes those deposits safe.



Maintain records and meet reporting duties

Record both the BTC quantity and the valuation required by the applicable accounting framework. A Bitcoin-only asset mandate does not excuse reporting in a legally required currency. Valuing an asset in dollars for a report is not the same as holding a dollar substitute.

Record	What to retain privately
Authority	Applicable rules, approvals, gift agreement, restrictions and review dates.
Receipt	Recipient, date and time, BTC units, transaction ID, valuation source and acknowledgment.
Payment	Purpose, payee verification, approvals, outputs, fees and evidence of delivery.
Custody	Public policy identifiers, assigned roles, access changes and test results; secrets stored separately.
Reconciliation	Opening and closing units, receipts, payments, fees, exceptions and reviewer signoff.

United States charitable gifts

Verify the actual recipient's eligibility before promising tax deductibility. A club's or fraternal unit's exempt status does not by itself establish that every gift is deductible. Digital-asset gifts are noncash contributions. The IRS's current FAQ addresses valuation, acknowledgment, Form 8283 and reporting. [R1]

For a donor claiming a deduction of \$250 or more, provide a timely acknowledgment with the organization's name, description of the noncash gift and the required goods-or-services statement. The acknowledgment describes the donated asset rather than assigning the donor's deduction value. [R2]

A claimed digital-asset deduction above \$5,000 generally requires a qualified appraisal. Signing the donee portion of Form 8283 acknowledges receipt and reporting duties; it does not endorse the appraisal. Apply the current instructions and the donor's circumstances. [R1]

A disposition of covered charitable deduction property within three years can require Form 8282 and a copy to the donor. Its instructions generally require filing within 125 days of disposition, subject to exceptions. Calendar the duty when receiving the gift, including gifts a processor may sell. Confirm which entity is the donee. [R1, R3]

Use the current filing instructions and a qualified adviser for the entity's jurisdiction. This operational summary is not an appraisal, tax opinion or determination of any donor's deduction.



Prepare for incidents and officer succession

Recognize an incident early

A missing device, exposed backup, unrecognized transaction, mismatched receiving address, unexplained output or unavailable signer should trigger the documented incident process. Treat uncertainty about a key as a custody problem requiring assessment, even before a confirmed loss.

1. Pause new solicitations and routine payments through the affected arrangement. Remove compromised payment instructions from public channels.
2. Notify the designated officers through known channels. Preserve transaction IDs, logs and access records without copying secrets into reports.
3. Determine which keys, backups, accounts and people may be affected. Use an independent clean environment for assessment.
4. If authorized and necessary, move remaining funds to a newly verified policy with uncompromised keys. Do not reuse a suspected secret or trust a recovery service that requests it.
5. Meet applicable reporting, donor, insurer and law-enforcement obligations. Explain confirmed facts and unresolved points separately.
6. Reconcile the loss or protective transfer, investigate the cause, retrain and obtain permission to reopen the process.

Plan a normal handover

Officer succession should include governing documents, restricted-fund records, wallet policy, service contracts, open obligations and secure access arrangements. A departing signer may retain a seed copy; changing a job title or login does not revoke that secret.

Where keys must change, rehearse a new approved wallet policy and transfer funds under the established authorization process. Verify that the new team can restore, receive, sign, reconcile and report before closing the old arrangement.

Report accountability without exposing people

Publish purpose, aggregate receipts and expenditures, policy changes and appropriately scoped independent review. Keep donor identities, extended public keys, signer locations, recovery instructions and security weaknesses out of public reports.

A public balance is not a complete audit. Reviewers need records of ownership, restrictions, liabilities, approvals and actual charitable use. Give auditors the access they need without giving them spending secrets.



Run a limited pilot and review results

The following sequence is a proposed implementation pattern, not a commitment to receive gifts or an allocation recommendation. Advance when the evidence is sufficient, not merely when a date arrives.

Stage	Work	Decision evidence
Education	Train officers; use a simulation or test network; identify a service need.	Members can explain the asset, keys, fees, privacy and failure scenarios.
Authority review	Resolve entity, rules, restrictions, holding permission and reporting.	Dated written approvals for the precise activity.
Recovery rehearsal	Test wallet policy, receiving verification, all intended signing combinations and succession.	Independent reviewer observes successful recovery without collecting secrets.
Small authorized pilot	Use a written value cap, permitted purpose and named reviewers.	Receipts and payments reconcile; fees and staff time are understood.
Continue or stop	Assess service outcomes, exceptions and capacity.	A recorded decision with revised limits or a controlled closure.

Set limits the organization can defend

Choose an exposure limit based on the organization's obligations and capacity to absorb a complete loss without abandoning essential services. Record the rationale. Do not derive a universal "safe percentage" from this guide.

Plan what happens if purchasing power drops sharply, fees rise, two volunteers leave, software support ends or a provider blocks withdrawals. Where the project prohibits conversion, document a permitted way to use or transfer BTC and how other obligations will remain funded.

Measure useful outcomes

Review net support delivered, donor experience, volunteer hours, total costs, unresolved restrictions, custody incidents and recovery readiness. An increase in BTC price is not a substitute for demonstrated charitable benefit.

A proposed quarterly review and a review at every officer transition can supplement the organization's mandatory audit schedule. Keep or change that cadence through the organization's own adoption process.

An organization may reasonably conclude that education or referring a donor to a separately authorized recipient is its best use of Bitcoin knowledge.



Proposed resolution for organizational review

Complete and adapt this text only after competent review. It has no effect until adopted by the proper body and reconciled with superior rules. Knights units must resolve the account and custody authority described on page 5 before using it for a funded activity.

The governing body of [legal entity] authorizes [precise activity] for [charitable purpose], subject to [identified governing provisions and required written determinations]. This authorization applies only to the named entity and does not imply approval by an international body, foundation or Church authority.

The permitted asset is native BTC on Bitcoin mainnet. Independent forks, other tokens, wrapped or synthetic claims, stablecoins, lending, leverage, derivatives and fiat substitutes are outside this project mandate. Required accounting and legal obligations remain in force. Any change to the mandate requires the applicable approval process and review of donor restrictions.

The organization will not solicit or receive BTC until [designated reviewers] certify in writing that gift terms, receiving verification, custody, recovery, reporting and incident procedures are operational. The authorized custody arrangement is [policy identifier and approval reference]. No private key or seed phrase will appear in this resolution.

The maximum exposure is [cap and measurement method], justified by [service obligations and loss capacity]. Funds restricted to incompatible uses or holding conditions will not be accepted. The organization will not promise a return, stable purchasing power or insurance coverage that has not been confirmed in writing.

Receipt, recording, approval, signing and independent review will be assigned to [eligible roles] consistently with existing rules. Every payment will retain its required resolution or voucher, destination verification, transaction record and reconciliation. Technical signature thresholds do not replace spending authority.

The organization adopts [recovery and succession procedure] and [incident procedure]. Emergency protective transfers require [specified lawful authority]. Signer replacement, restriction changes and any closure will follow the same governing framework.

The organization will acknowledge gifts, protect personal data, keep records and meet reporting requirements under [jurisdiction and applicable policy]. Reports will distinguish BTC quantities, required valuations, restrictions and actual charitable outcomes.

The governing body will review the arrangement on [date or cadence], at officer transition and after a material incident or rule change. It may suspend new receipts when controls or authority are insufficient.

Adopted by [body] on [date], under resolution [identifier]. Required superior determination [reference]. Effective date [date]. Recorded by [authorized role].



Record the decision and readiness evidence

Use this as a blank review record. Checkboxes and signatures document a decision; they do not supply authority that the organization does not possess.

Legal entity _____

Jurisdiction and controlling documents _____

Proposed activity and charitable purpose _____

Policy and gift terms version _____

Evidence to attach

- Written authority for receipt, holding, conversion if any, and spending.
- Required superior determination and donor restrictions.
- Named eligible roles and independent review arrangements.
- Verified wallet policy and receiving process, with secrets excluded.
- Observed recovery and handover rehearsal results.
- Exposure limit, service continuity plan and incident procedure.
- Accounting, acknowledgment, reporting and insurance assessment.

Decision

☐ Education only ☐ Defer pending evidence ☐ Decline

☐ Authorize the specifically documented activity subject to its conditions

Unresolved conditions _____

Approval body and resolution _____

Effective date _____ Review date _____

Authorized recorder _____ Date _____

Independent reviewer _____ Date _____

Retain the completed record in the organization's protected financial files. Do not upload names, private contacts, seed words, extended public keys or recovery locations to the public project pages.

Further reading and current project policy: sparkworks.org/bitcoin and sparkworks.org/crypto. Sources follow. Recheck editions and binding local instructions before implementation.



Sources for organizational authority

[L1] Lions Clubs International. [Standard Club Constitution and By Laws LA 2](#). 2026-27; revised July 2, 2026. Selected Constitution II, V, VIII and XI; By-Laws III and IX. Standard rules, not proof of a particular club's adoption or BTC authority.

[L2] Lions Clubs International. [Use of Funds Guidelines](#). Effective July 12, 2025. Six-page FAQ, especially questions 27-30 on investment gains, long-term designation and separate accounting.

[L3] Lions Clubs International. [Best Practices for Financial Transparency](#). DA-BPFT.EN 6/2024. Four-page guidance on approval, signatories, reconciliation and audit. Recommendations are distinguished from governing rules.

[L4] LCIF. [More Ways to Give](#). Live page reviewed October 9, 2026. Cryptocurrency section identifies the Every.org route. Does not establish local-club custody authority.

[L5] Every.org. [Supported cryptocurrencies and donation process](#). Updated March 3, 2026. Provider description of automatic USD conversion after confirmation. Terms and operational performance can change.

[K1] Knights of Columbus. [2026 Charter Constitution and Laws](#). Adopted August 6, 2026. Selected sections 122-145 and adoption certificate; not the full 119-page text. URL retains "2025"; the inspected PDF is the 2026 edition.

[K2] Knights of Columbus. [Fraternal Excellence Guide](#). Effective May 1, 2026. Selected financial, electronic-payment and investment sections, printed pages 17-19, 33-36 and 78-80. Later consolidated law governs conflicts.

[K3] Knights of Columbus. [Laws and Rules Governing the Fourth Degree](#). Amendments through June 2017; Rev 1/18. Selected sections 21-24. Public copy found; verify later directives and actual assembly bylaws.



Sources for Catholic ethical reflection

[E1] Pope Leo XIV. [Magnifica Humanitas](#). May 15, 2026. Selected sections 59-76 and 83-99. Principles concerning digital power and accountability; the guide's Bitcoin applications are editorial judgments.

[E2] Holy See. [Catechism of the Catholic Church](#). Paragraphs 2407-2412. Justice, entrusted property, harmful speculation and promises. Not a technical or asset-specific policy.

[E3] Pope Benedict XVI. [Caritas in Veritate](#). June 29, 2009. Selected sections 45 and 65-66 on ethical economic and financial activity.

[E4] Pope Francis. [Laudato Si](#). May 24, 2015. Selected sections 182-186 on environmental assessment and precaution. Does not supply a Bitcoin energy estimate.

[E5] Congregation for the Doctrine of the Faith and Dicastery for Promoting Integral Human Development. [Oeconomicae et pecuniariae quaestiones](#). 2018. Selected financial ethics discussion, including section 26. Distinguishes legitimate functions from harmful practices.

This is a bounded selection of primary sources, not an exhaustive theological or scientific review. Sources were checked for this edition; organizational rules and live service terms require rechecking before use.

No Catholic source cited here establishes a Bitcoin investment endorsement, a condemnation of every conventional currency, or an exception to governing financial rules. Human dignity and responsible service guide the practical recommendations.

Further annotated technical, historical, environmental and ecclesiastical reading is available through the project's evidence library at sparkworks.org/bitcoin.



Sources for Bitcoin and wallet controls

- [T1] Satoshi Nakamoto. [Bitcoin A Peer to Peer Electronic Cash System](#). 2008. All nine pages reviewed; emphasis on sections 2-6, 8, 10-11. Foundational model with assumptions, not a complete current specification.
- [T2] Bitcoin.org. [Securing your wallet](#). Live guidance reviewed October 9, 2026. Backup, offline storage, multisignature and succession guidance. General security advice does not authorize organizational holdings.
- [T3] Bitcoin.org. [Some things you need to know](#). Live guidance reviewed October 9, 2026. Volatility, irreversible payments, confirmation and privacy considerations.
- [T4] Bitcoin Improvement Proposals. [BIP 380 Output Script Descriptors](#). 2021; current specification reviewed. Descriptor and key-expression format. Private keys can appear in descriptors; recovery requires the relevant wallet policy.
- [T5] Bitcoin Improvement Proposals. [BIP 174 Partially Signed Bitcoin Transaction Format](#). 2017; current specification reviewed. Roles and information exchange for transaction construction and signing. A PSBT is not an organizational approval.
- [T6] Sparrow Wallet. [Connected Hardware Wallet and Best Practices](#). Live documentation reviewed October 9, 2026. Device verification and signing guidance; companion best-practices page informs custody tradeoffs. No vendor endorsement. [Companion source](#).
- [T7] Electrum. [Frequently Asked Questions](#). Live documentation reviewed October 9, 2026. Importing versus sweeping private keys. A sweep moves outputs; importing retains the old key's authority.
- [T8] Bitcoin Improvement Proposals. [BIP 65 CHECKLOCKTIMEVERIFY](#). 2014. Script-enforced locktime conditions. A policy statement cannot alter an already funded output.



Sources for protocol development and research

[T9] Bitcoin Improvement Proposals. [Segregated Witness and Taproot](#). BIP 141 and BIP 341. Selected metadata and specification scope identify mainnet consensus upgrades. Separate chains are not interchangeable with BTC. [Companion source](#).

[T10a] Garay Kiayias and Leonardos. [The Bitcoin Backbone Protocol Analysis and Applications](#). EUROCRYPT 2015. Formal model and security assumptions. Selected abstract and model discussion; no claim of proof for every real-world deployment.

[T10b] Eyal and Sirer. [Majority Is Not Enough Bitcoin Mining Is Vulnerable](#). Financial Cryptography 2014. Selected selfish-mining result and assumptions; modeled incentives, not a current measurement of all mining behavior.

[T10c] Carlsten Kalodner Weinberg and Narayanan. [On the Instability of Bitcoin Without the Block Reward](#). ACM CCS 2016. Selected fee-only incentive analysis; conditional research, not a forecast date for network failure.

[T11] Lightning Network contributors. [BOLT 0 Introduction](#). Current protocol documentation reviewed. Payment-channel architecture and operational scope. Custodial products introduce separate provider dependencies.

[T12] Bitcoin Developer Guide. [Transactions](#). Selected technical sections reviewed. Unspent outputs, signatures, scripts and multisignature transaction structure.

Citations marked T10 refer collectively to T10a-T10c. Their publication identities and DOIs were checked against Crossref; metadata verification is not a full-text review.

Recommendations in this guide combine those technical mechanisms with organizational separation of duties, recordkeeping and recovery planning. They are proposed operating controls, not claims that the white paper prescribed a modern nonprofit treasury.

Scientific models, software documentation and ethical teachings answer different questions. None alone verifies a particular specimen, organization, wallet, balance or set of signers.



Sources for reporting and physical specimens

- [R1] Internal Revenue Service. [Frequently asked questions on digital asset transactions](#). Questions 78-81; added December 15, 2025. Noncash gifts, appraisals, donee acknowledgment and disposition reporting. Apply current instructions and eligibility rules.
- [R2] Internal Revenue Service. [Charitable contributions Written acknowledgments](#). Current official guidance reviewed. Description of noncash gifts and goods-or-services statements; the donor's claimed value is not assigned by the acknowledgment.
- [R3] Internal Revenue Service. [Form 8282 and instructions](#). Rev October 2021; current form reviewed. Covered dispositions within three years, filing deadline and exceptions.
- [R4] Minnesota Revisor of Statutes. [Prudent management and gift restrictions](#). Sections 309.74 and 309.755. Donor intent, prudence, diversification and restriction changes for covered institutional funds. Applicability requires entity and fund review. [Companion source](#).
- [R5] Federal Deposit Insurance Corporation. [Understanding Deposit Insurance](#). Current official guidance reviewed. Deposit-insurance boundaries; crypto assets are not insured deposits.
- [P1] Blockchain Mint. [Cold Storage Coins Frequently Asked Questions](#). Manufacturer page reviewed October 9, 2026. Product mechanism and manufacturer-key custody. Manufacturer statements do not authenticate or audit a specimen.
- [P2] Jameson Lopp. [Cold Storage Coins physical stress review](#). Independent test report. Tested-unit heat and physical resilience observations; destructive conditions and the review's scope limit generalization.
- [P3] United States Mint. [Caring for Your Coin Collection](#). Current official guidance reviewed. Handling, cleaning and storage guidance; numismatic conservation does not secure a Bitcoin private key.