Using Multi-Signature Accounts for Corporate Governance

By Pamela Morgan, Empowered Law

Bitcoin allows us to keep complete control over our money, without the need for banks or custodial accounts. Ownership and control of the keys is the only thing that determines control over the funds. With that great power comes a significant responsibility: if you lose control of your keys, lose your keys, forget your password or become incapacitated, you lose your funds and those that depend on you lose too. There's no recourse for you, your family, your heirs, your company employees, your shareholders. Whether you are managing your personal funds or managing funds for a company, your control and power come with a great deal responsibility. If you are managing company funds however, you have a fiduciary duty and your company's survival might depend on it. Fortunately, there's a better way to manage that fiduciary duty, with the use of bitcoin's multi-signature capability. This article will examine the use of multi-signature in bitcoin as a tool for responsible corporate governance and for managing the risk of theft, loss, embezzlement or incapacity.

Bitcoin's Multi-signature Feature for Corporate Accounts: Imagine you just invested 100BTC in a company, run by Alice and Bob, the CEO and CFO respectively. If the company uses a bitcoin wallet to store funds, who should control the keys? What happens if Alice or Bob die or are incapacitated by illness? Would you expect the company to have a contingency plan for continued operations? Would you expect the company to have a way to access your investment? What if you were an employee of the company? Would you expect to be paid for the work you've done? Should the company stop operations? Many business owners would want their business to continue operating, if for nothing more than the opportunity to help support their families and leave a legacy after they are gone. The continuity of properly staffed and managed organizations do not hinge on one or two people. However if all company funds are exclusively controlled by one person, and their private keys become unavailable to the organization, for any reason, the organization immediately becomes insolvent, as the funds are effectively frozen.

Beyond survivability of the funds in the case of incapacity or death, we must also consider the possibility of theft, embezzlement or loss of the keys. A single-owner bitcoin wallet is vulnerable to theft and must be diligently backed-up to avoid loss. Relying on a single-owner bitcoin wallet also means that the investors and managers of the company must trust the owner of the wallet and are vulnerable to that person embezzling funds or being coerced by thieves.

Single-owner accounts are a bad idea, in bitcoin as in traditional finance. In a business environment, single-owner bitcoin wallets concentrate risk and responsibility to one person, making the funds susceptible to theft, loss, embezzlement, and operational disruption due to temporary or permanent incapacity. There's a better way: bitcoin's multi-signature capability.

This article focuses on implementing multi-signature accounts as a solution to this problem, balancing security interests with good corporate governance. First we'll look at traditional corporate banking practices and governance as well as the benefits and shortcomings of these practices. Then we will consider multi-signature accounts as a solution and explore the benefits and shortcomings of those. Next we will discuss how to implement a multi-signature solution, including how to set up accounts, who should serve as signers, and what processes should be implemented. Finally, we will review an example implementing these processes.

Traditional Corporate Separation of Duties: Separation of duties is a best practice within established corporations. Simply put, separation of duties is the division of certain responsibilities between different persons in the organization to add a layer of protection for shareholders and an accountability structure within management. For example, it's common to require approval from both the CEO and the CFO for large expenditures, transfer or sale of capital and large assets.

The CEO maintains executive power, deciding what to spend; the CFO provides oversight and accountability for shareholders. This separation of duties provides protection against a broad range of scenarios both internal and external, intentional and accidental such as embezzlement from either executive, coercion of either executive, impersonation, and theft or loss of credentials. One party does not hold all of the spending authority and therefore cannot individually subject the company to significant loss by way of inappropriate spending.

Most traditional corporate bank accounts are set up to require multiple signatures to effectuate a transaction. Typically, a number of people are given signing authority on each account. These people are added to each account as "authorized signers". For example, on an operations account, the authorized signers might include a bookkeeper, an accounting manager, the CFO, and the CEO. Cheques drawn from this account would require two signatures, such as the bookkeeper and the accounting manager, in order to be valid. If the bookkeeper leaves the company, the CFO or CEO could step in to sign cheques until a suitable replacement is found, without impacting company operations. The company would not need to worry about the bookkeeper independently withdrawing all funds from the account because transactions require two signatures.

Bitcoin's Multi-Signature Addresses Achieve Separation of Duties: Multi-signature addresses allow us to access the benefits of a traditional multi-signer account without bank reliance or constraints. Multi-signature addresses provide similar corporate governance measures, as transactions require more than one signature to be valid, however organizations should use caution when implementing them. In a traditional setting, banks play a hidden role in the transaction. While bank approval is not generally required for activity, the bank provides a method of recovery in the case of incapacity or death of an authorized signer. This is an important and relevant service for all accounts, including bitcoin and other cryptocurrencies, and by excluding traditional banks from the process we must look to alternative solutions to this problem. Multi-signature accounts can provide an elegant, easy-to-implement solution.

If a signer approves the transaction but is unable to execute it, due to travel, illness, or a planned vacation (remember these transactions often require access to cold storage, secure internet connectivity, and PGP signed emails), the transaction can be executed by the third party. If a signer becomes incapacitated, through illness or death, the accounts are not effectively frozen because the third party can be asked to sign transactions.

Multi-signature addresses, by design, allow for an easy separation of duties. While traditional bitcoin addresses allow transfer of funds by presenting one "proof" consisting of a public key and private signature; multi-signature accounts require one proof for each required signature. Multi-signature accounts require M of N signatures, meaning you could set an account up to require 2 of 2 signatures, 2 of 3 signatures*, 2 of 4 signatures, 3 of 3, and so on. While the benefits of separation of duties could be achieved by implementing a 2 of 2, organizations should implement no less than 2 of 3 signatures, in order to provide for continuity in the event one of the signers or the signer's credentials become unavailable.

Bitcoin's Multi-Signature Addresses are Superior to Traditional Bank Accounts: Traditional banks can be compelled to hold, freeze, or confiscate customer funds because banks hold funds in custodial accounts and banks are profit-driven organizations subject to strict regulation. Because the bank holds the funds, the bank can be compelled to continue to hold them by an outside organization having influence over the bank, despite a request to release funds by the original depositor. Funds can also be frozen for administrative purposes, because of misunderstandings or clerical errors by the bank, because of bankruptcy or insolvency of the bank or for a myriad of other reasons, entirely unrelated to fault or behavior by the account holder. Simply put, your ability to repossess your funds is subject to bank approval.

Multi-signature bitcoin addresses are not subject to requests by third-parties, including governments, and therefore funds held in these accounts are not subject to holds, freezes, or confiscation. Control lies entirely with ownership and control over the signatory keys. If you can create the necessary signatures, nothing can stop you from processing a transaction. Conversely, without the necessary signatures, no one else holds power or control over the funds. They can neither spend them, nor stop the holders of the keys from spending them.

Using a Third Party to Protect Business Operations

As mentioned above, banks play a hidden role, providing accessibility to funds in the event of incapacity of an account holder or authorized signer. Bitcoin accounts need similar protection but instead of running to banks for protection, we can use multi-signature technology to provide protection without unnecessary risk.

Who Should Serve as the Third Party? Third party is used in this context to mean the emergency signer, not necessarily the third person on the account. What are the characteristics of someone who should serve as a third signer? Consider the "real world" model where the bank is a relatively neutral third party, who has a relationship with the company but is not involved with day-to-day operations and is constrained by their own internal practices and the legal environment in which they operate. This model can be replicated in the virtual world, without adding additional layers of complexity, by choosing a party who has similar characteristics.

The ideal third party will be professional, knowledgeable about the technology and security protocols, and independent of business operations. Why are these characteristics important? Professionalism is important because the third party will be your backup to access funds in the event a signer becomes unavailable. The third party should be reliable, available upon short notice, communicative, and responsive. The third party must be knowledgeable in the technology, have a thorough understanding of how to use multi-signature accounts, and best practices for security - such as offline key generation and storage. They should understand principles of conflict of interest and be able to maintain a distance from operations, so that they will not be subject to coercion or other undue influence. A disinterested third party also provides investors, employees, and the community with an increased level of protection thereby justifying an increased confidence in operations as evidence of good corporate governance.

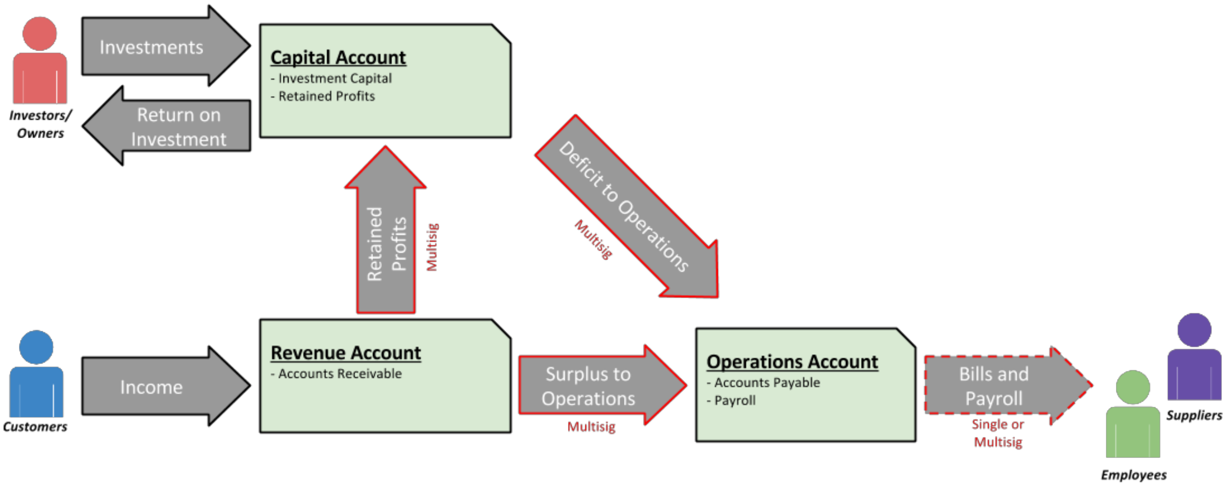
What the Third Party Should Not Do: The third signer should not also act as an entity for dispute resolution due to conflict of interest. Organizations can seek dispute resolution through traditional justice systems (though the level of justice, efficiency, and effectiveness varies by jurisdiction), alternative dispute resolution ("ADR") mechanisms, or ideally negotiation with the other party. As a matter of good governance, internal dispute resolution methods should be selected at organizational inception. There are many viable ADR mechanisms available including traditional or online arbitration, mediation with contractual settlement, and collaborative law with contractual settlement. When a dispute arises, the third party should not execute any transactions until the dispute has been appropriately resolved and proof of resolution is presented to the third party.

How would the third party know of a dispute? One way to ensure the third party does not execute any transaction without consent of all signers is to implement a process requiring verification of consent by all signers. This protective measure ensures that no one signer can bypass internal controls and seek approval of the external third party to consummate an unapproved expenditure. Verification also ensures that no internal party can claim they didn't consent to a transaction after execution. The verification requirement also encourages open communication among the signers, which should lead to early identification of misunderstandings and better overall management of the financial health of the company.

The Process

Setting Up Accounts / Multi-Signature Addresses: For many organizations a three account system will work well to provide internal controls and a reasonable level of security. The three accounts are the **capital account**, to hold investment and profits, the **operations account**, to pay operational expenses, and the **revenue account** where clients deposit payment for goods and/or services. The interplay between the accounts and stakeholders are depicted below.

Example of Funds Flow Using Three Multi-Signature Addresses / Accounts



In the illustration above, notice that deposits into each account can be executed with a single signature, withdrawals typically require more than one signature. The structure itself provides one layer of protection by separating funds, the multi-signature requirements provide another, the third party signer provides a third layer of protection.

The level of organizational control and oversight will vary for each organization, and for each account within each organization. However there are some simple best practices that should be considered when setting up organizational multi-signature accounts. Also remember that there are no limits on the number of bitcoin accounts an individual or organization can create, use, or abandon - without fees, without explanation, and without bureaucratic paperwork. Finally, note that in this section the word account is used in place of multi-signature address to parallel account structure in traditional corporate banking and for ease of reading. Each account listed could more accurately be described as a multi-signature address.

Capital Account: Every company should have an independent capital account. Deposits in this account should include initial funding by owners and investors, continued funding by owners and investors, and profit. Withdraws from this account could include bi-weekly or monthly transfers to the operating account if necessary, distribution of profits to owner’s personal accounts, or transfers to an owner or investor as a buy-out or return of equity.

Capital Account Set-Up: A multi-signature capital account should be set up to require no less than two of three signatures. Some companies invite investors to be signers on the capital account, some do not. There are benefits and drawbacks to each position. A well-funded profitable organization will typically have a large balance in the capital account, thereby justifying additional security measures and controls such as additional signature requirements. Regardless, remember not to inadvertently give control of the account to directors and/or investors by incorrectly setting up the account to allow them to authorize transactions independently. For example, if the authorized signers on a capital account are two investors, two directors, and one third party, the required signatures should be no fewer than three of five. Note that under this arrangement if the two investors convinced one director to withdraw funds, the three of them could execute the transaction without approval of the other director or the independent third party. This is why the account set up and strategy should be carefully considered prior to funding and the company should consult with a professional in this space. Set up correctly, this system provides superior internal checks and balances for directors, provides investors with the ability to monitor and possibly exert some control over large expenditures, and includes a contingency signature plan through an independent third party.

Operations Account: Every company should have an operations account which is used to fund the day-to-day operations of the company. All organizational expenses, except transfers directly from the capital account for the reasons stated above, should be paid from this account. For new companies, initial funding will likely come from the capital account. After the organization establishes positive cash flow (as explained below), this account should be funded from the revenue account. There will be a lot of activity on this account, as it is used to fund operations. Therefore this account is separated from the capital account in order to shield capital from mistakes and malfeasance.

Operations Account Set-Up: The set up of this account will depend largely on your organizational structure and the internal controls of your organization, however there are some best practices to consider. Be sure consider the balance between trust, accountability, and efficiency. While some companies use a traditional one signer account for the organizational account in order to expedite payments, for the reasons above, it’s not advised. At minimum, the account should be set up as a one of two, as a safety net in case the regular signer (eg. a bookkeeper or admin) becomes incapacitated or unavailable. A better practice would be to require two of three, with an outside third party as the third signer. Remember, the two internal signers on this account can be, but do not need to be, the same internal signers as the capital account. The third party can be the same because they should be independent. Typically investors are not signers on this account as they are not involved in day-to-day business operations. Some organizations implement additional internal controls, such as requiring email verification for expenditures exceeding 25BTC. Your multi-signature professional should be able to provide a number of set-up options, explain the benefits and drawbacks of each, to help you decide what is best for your organization.

Revenue Account: Every company should have a revenue account, to which clients make payments. Whether the organization sells goods or services, the incoming revenue account should be separate from the operational expense and capital accounts. Typically a revenue account should be swept into the operational account and/or the capital account, weekly or bi-weekly, depending on cash flow. If sales are good, this account should have a lot of incoming activity. Clients make payments to multi-signature accounts just as they would to a traditional bitcoin address, however instead of paying an address that begins with a “1” (traditional bitcoin address) they pay an address that begins with a “3” (multi-signature address). You could use this as an opportunity to inform clients about your corporate governance strategy and why you're using multi-signature accounts, which will likely set you apart from your competition.

Revenue Account Set Up: Set up of the revenue account or accounts will depend largely on the organizational needs and structure. Some organizations will have more than one revenue account. However, all revenue accounts should require a minimum of two of three signatures, again utilizing an outside third party as the third signer. Sometimes a three of five or a four of seven signature design is used. The signers can be, but do not have to be, the same signers on the operations account. The revenue account should be set up similarly to the operations account, in structure and policies. As always, be sure to discuss options with your multi-signature professional prior to implementation.

Transactions

Preliminary Testing Before Funding: After the accounts are set up, each address should be tested first by funding it with a very small amount of bitcoin. Why? To ensure access to the funds, the ability to transfer as expected, and to provide an opportunity for everyone to practice the transfer protocol. Every combination of signatures should be tested. For example, if the operations account is set up as a two of three the following tests must be conducted:

Test 1: Alice + Bob
Test 2: Alice + Ellen
Test 3: Bob + Ellen

Never move a large amount of bitcoin into a multi-signature address until you have thoroughly tested the technology, your implementation of it, and process with all participants and ensured everything works well with small amounts.

Transaction Protocol: Requests for signatures, whether they are sent for signing to another employee or an independent third party, should follow a protocol. Why? Simple standardized procedures serve to reduce errors and provide accountability.

The following protocol standards were adopted by one of my clients, who has agreed to allow me to share them in this article for illustration purposes. Protocols should be adjusted for your specific organizational needs. Though not discussed below, proper key storage and offline signing protocols should be included in all implementations.

Signature Request Protocol: Signature requests should be delivered via email, with all authorized signers cc'd. They should include a properly formed transaction, that the person simply needs to sign and return to the sender. The email should include enough information to allow the internal directors to make a business decision as to whether or not the transaction should be executed. Alternatively, the email could reference a prior conversation, meeting, or email without disclosing material business concerns. If a signer becomes incapacitated, proof of incapacity satisfactory to the third party signer, must be provided along with the signature request.

Verification Protocol: When a request is sent to the third party, they will independently verify consent of all signers prior to signing the transaction. If the third party cannot obtain consent from all of the other signers, then the third party will not execute the transaction without proof of incapacity. Proof of incapacity requirements, thresholds for transaction execution, and third party signer protocols should be defined specifically for each organization prior to implementation of the multi-signature corporate governance strategy.

Broadcast Protocol: Transaction originators should be the ones to broadcast the finalized (fully signed) transaction to the bitcoin network, giving them one more opportunity for review. Additionally, having the originator be responsible for transmitting the transaction properly aligns the authority with the responsibility, avoiding confusion or process errors.

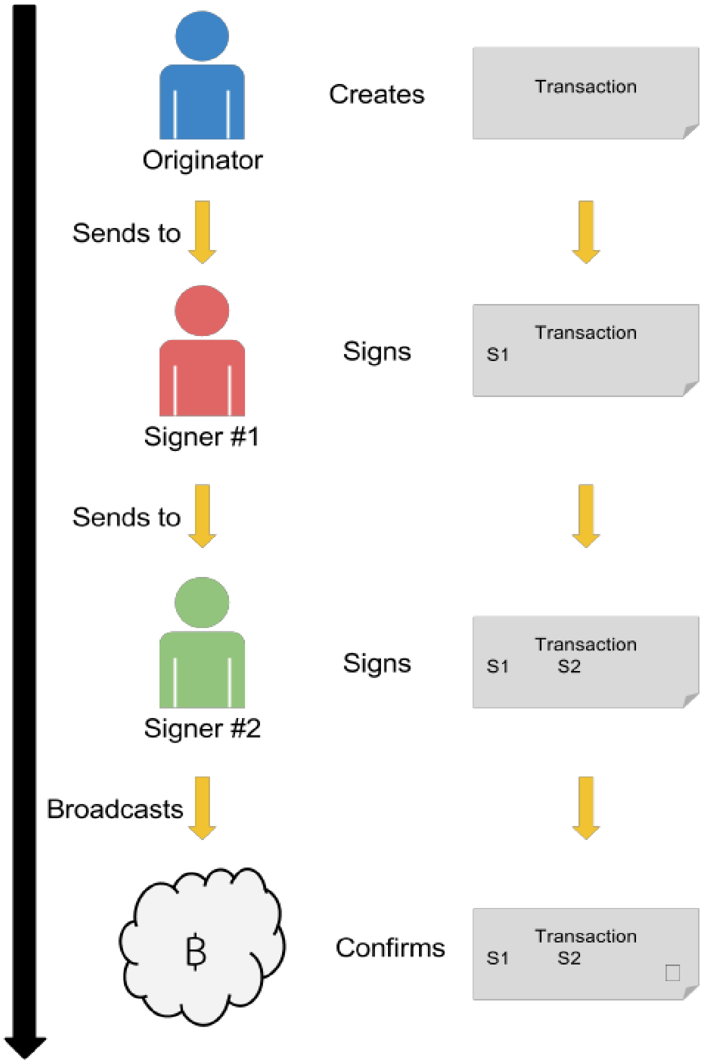
Transaction Examples

In the following examples, assume the authorized signers are Alice, CEO; Bob, CFO, and Ellen, the independent third-party signer and the account requires valid transactions be signed by two of the three authorized signers.

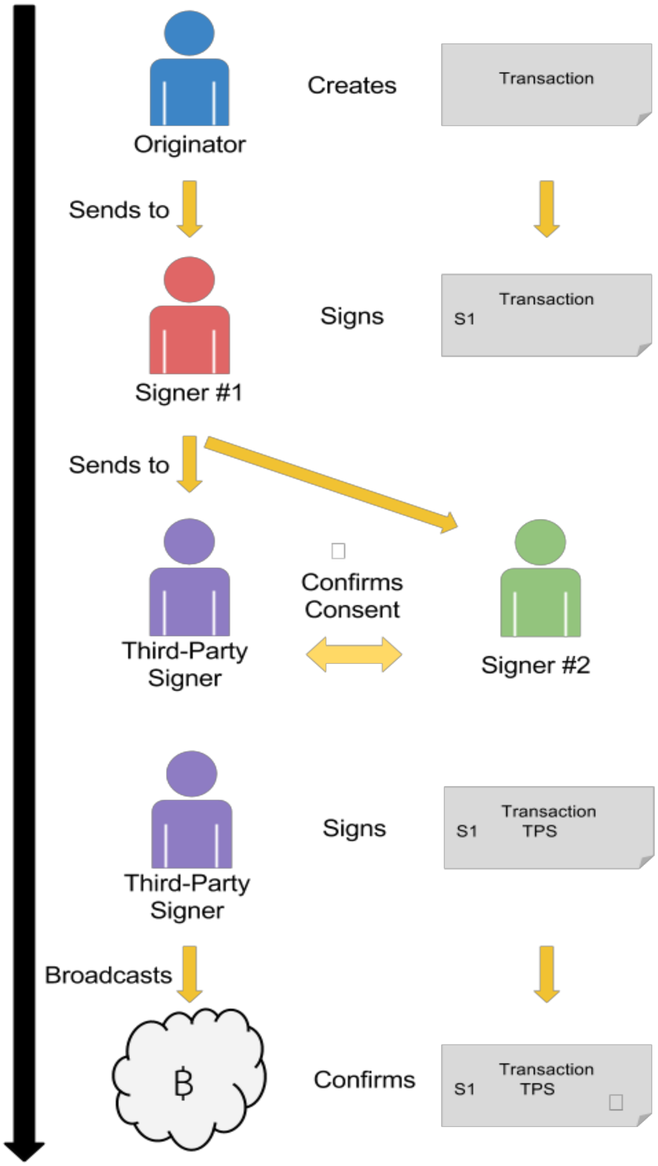
Most transactions will not require the involvement of the third party at all. If the two authorized signers agree on the transaction and both signers are available, the transaction is executed by the employees (in this case Alice and Bob). If however, one of the signers is traveling and cannot access cold storage, the organization can still access funds by requesting a signature from the third party (in our example, Ellen).

Alice and Bob would like to move 25BTC from the revenue account to the operations account in order to fund payroll. Either Alice or Bob could create the transaction, using a multi-signature service like www.coinb.in/multisig.

Normal transactions, both employees available to sign: For purposes of this example, assume Alice creates the transaction and signs it. She can then send an email to Bob, directly, requesting his signature on the transaction. Bob can then counter-sign the transaction. Now the transaction has the requisite two signatures. Bob returns the transaction by email to Alice and Alice transmits it to the bitcoin network, thereby executing it and transferring the funds.



Example of a transaction requiring the third party: Bob is on vacation and accidentally drops his laptop in the pool. Alice prepares and signs a transaction transferring funds from the revenue account to the operating account so that she can make payroll payments. She emails Bob, requesting the second signature and receives the bad news: Bob cannot sign because the key was stored on the laptop. There's a backup in Bob's safe back home but he won't be able to access it for another two weeks. Bob has been planning this vacation all year and really doesn't want to cut it short. Bob and Alice decide to send the transaction to Ellen for her signature, to ensure employees are paid on time. Alice then forwards the transaction to Ellen and after a brief, slightly embarrassing phone call between Bob and Ellen, Ellen counter-signs the transaction with Bob's verbal approval. Ellen sends it back to Alice and Alice transmits it to the bitcoin network. Bob can continue his vacation and the employees will be paid on time.



Multi-signature corporate bitcoin accounts are inexpensive to implement, an effective governance tool, improve security and resilience and can be implemented today with only minor process changes in every bitcoin startup company. There's really no excuse for poor financial governance.

Thanks to Andreas M. Antonopoulos for security process advice and review, Nikos Bentenitis of CoinSimple for corporate governance and implementation testing and many others for their review, feedback and comments.

Pamela Morgan is an attorney and business consultant focusing on using blockchain technology to improve business and legal processes. Her smart law practice, Empowered Law offers Third-Party Multi-Signature services, including complete documentation, software tools, process manuals and implementation advice for effective financial governance in bitcoin companies. Contact pamela@empoweredlaw.com for details.