Multi-Signature Key Trusts:
A Cryptocurrency Inheritance System

Michael Rosenblum, Esq.[i]
Attorney at Law (New York, Florida, Colorado)
Solicitor of the Senior Courts of England and Wales
m@usatax.law

Shawn C. Snyder, MA., JD, LL.M.
Attorney at Law (Florida)
Board Certified in Wills Trust and Estate (Florida)
Shawn@snyderlawpa.com

Abstract. By default, decentralized cryptocurrencies are not objectively subject to a traditional estate plan. Entrusting one or more third parties with M-1 signature authority over an M-of-N multi-signature cryptocurrency wallet at divestment by the owner (i.e., at death or as a lifetime gift) maximizes the likelihood of beneficial ownership of the wallet's contents being transferred pursuant to the transferor's wishes. Selection of properly incentivized/disincentivized third parties is critical. The ideal candidate is currently a fiduciary (such as an attorney or trust company) who understands not just applicable trust and estate (and related tax) law, but the technological underpinnings of cryptocurrencies.

1. Introduction

Cryptocurrencies predominantly eschew the use of trusted parties to process transfers of value. While the system is appealing for commercial transactions, it suffers from the inherent weaknesses of a trustless model. Complex donative transfers (i.e., gifts with "strings") are not currently possible without trust, since transactions are computationally impractical to reverse and the transferee is vested with absolute control of the cryptocurrency on receipt. If the transferee(s) can be absolutely trusted by the transferor, no third party is required. Otherwise, a third party's involvement appears unfortunately necessary at present to ensure compliance with the transferor's estate plans.

Smart contracts (i.e., automated programs developed within a cryptocurrency protocol) may reduce or remove the need for a third party in the future. The cost, however, is increased risk of diversion via code exploitation. Unless smart contracts can be made virtually hack-proof, third party involvement should remain the most attractive solution to the cryptocurrency inheritance problem.

In this paper, I propose a cryptocurrency inheritance system based around the entrustment of multi-signature ("multi-sig") cryptocurrency wallet keys ("Keys"). This arrangement minimizes the trust required of heirs and third parties by exposing the entrusted Key holder to legal recourse under fiduciary liability causes of action.

2. Multi-Signature Wallets

Multi-sig cryptocurrency wallets require more than one authorization ("signatures") to send funds, thereby allowing asset control to be decentralized among multiple entities. Standard transactions on a cryptocurrency network are single-signature ("single-sig") transactions. Multi-sig functionality was added to the Bitcoin protocol in 2012 and has since been introduced to various alternative protocols. Multi-sig functionality can also be implemented by third party custodians, such as cryptocurrency exchanges, in their second layer systems. Because these second layer schemes inherently subject the underlying funds to the custodian's control, I do not consider them further in this paper.

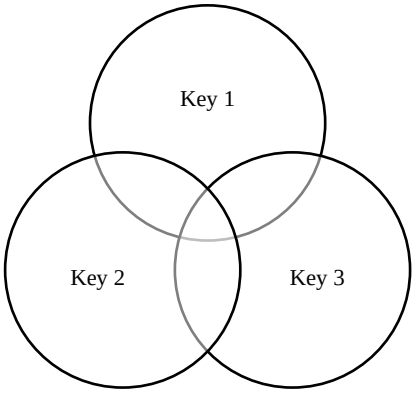


Figure 1: 2-of-3 Multi-Sig

Multi-sig wallets are sometimes referred to as M-of-N ("minimum" of "number") wallets. N number of private keys (with asymmetrically encrypted public key corollaries) exist for a given M-of-N wallet, but each key contains a public key script which conditions the expenditure of wallet funds on the co-signatures of M-1 other private keys. A party (or group of parties) with access to less than M private keys can only transact with the wallet by decrypting the public-key-encrypted blob for enough inaccessible private keys necessary to reach M – a task currently believed to be computationally infeasible. The most common M-of-N wallet for escrow is a 2-of-3 wallet, although other common arrangements include 2-of-2, 2-of-4, 3-of-5, and 4-of-7.

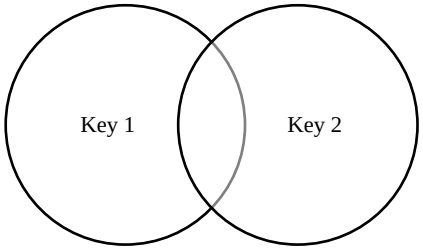


Figure 2: 2-of-2 Multi-Sig

Confident use of a multi-sig wallet requires virtual certainty by the cryptocurrency owner that no untrusted party or coalition can obtain the threshold number of private keys without the cooperation of such key's owners. To achieve this level of assurance, the wallet must be generated securely and, thereafter, each key holder must secure their private keys. At the outset, it should be confirmed, to the greatest possible degree, that the hardware and software used to generate the M-of-N wallet has not compromised.

3. Single-Signature Wallet Inheritance Structures Generally Contraindicated

In most scenarios, sharing the private key to a single-sig wallet as a method of wealth transfer unnecessarily increases the risk of fund diversion or loss. This is because access to a single-sig wallet key is tantamount of absolute control over the underlying funds and, as such, there can be no guarantee the additional or successor controller will abide by the initial controller's wishes. A limited exception may exist for bequests of an entire wallet balance to a single heir, which could be accomplished by securing the single-sig wallet key in a location accessible only by said heir following the owner's death. Arguably, even this use is suboptimal because it creates an avoidable risk vector (compromise of the secure location by anyone other than the intended heir).

4. 2-Party Versus 3-Party Multi-Signature Structuring

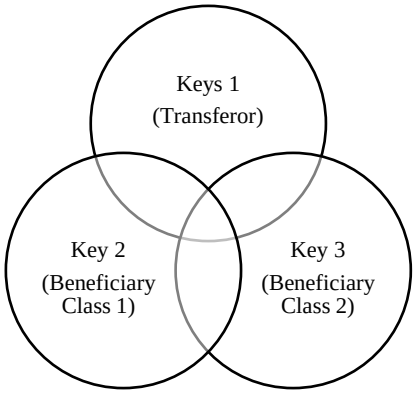


Figure 3: 2-Party 2-of-3 Multi-Sig With Transferor Involvement

Broadly, the universe of multi-sig wallet wealth transfer structures can be divided into two classifications: those involving third parties and those not involving third parties.

In the former group, multi-sig keys are ultimately distributed among the ultimate beneficiaries. The transferor may also be involved during his or her life. The primary advantages of 2-party structures are increased privacy (knowledge of the existence of the wallet may be kept entirely "in the family") and decreased cost (unrelated third parties will usually require compensation).

The leading disadvantage of 2-party structures relates to conflict of interest. Without the transferor or a disinterested key holder to arbitrate, decisions as to how to use wallet funds may be deadlocked due to acrimony amongst the beneficiaries. Without requiring the involvement of the transferor or a disinterested key holder, coalitions of beneficiaries might be able to disinherit other beneficiaries, notwithstanding that doing so is contrary to the transferor's intent.

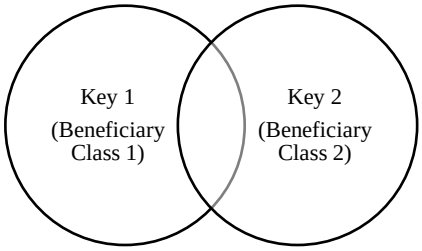


Figure 4: 2-Party 2-of-2 Multi-Sig Without Transferor Involvement

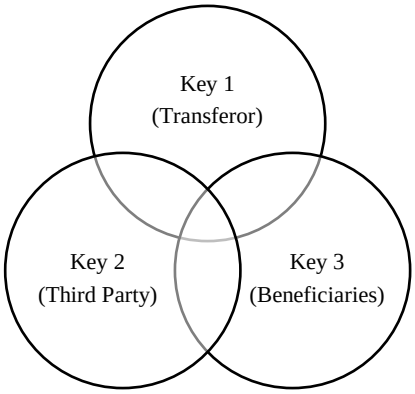


Figure 5: 3-Party 2-of-3 Multi-Sig With Transferor Involvement

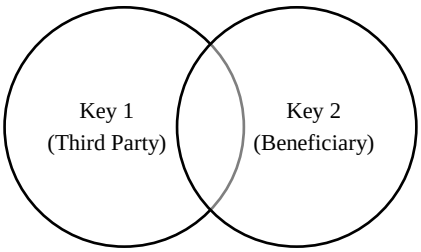


Figure 6: 3-Party 2-of-2 Multi-Sig Without Transferor Involvement

To involve a third party, multi-sig keys not held by the transferor are distributed among said third party and the beneficiaries. Under a 3-party system, the risks of deadlock and diversion inherent to 2-party structures are minimized as long as the third party is properly incentivized to follow the transferor's wishes and disincentivized to contravene them.

5. Indication for Unrelated Professional Fiduciary in 3-Party Multi-Signature Cryptocurrency Transfer Structures

Generally, a third party multi-sig key holder will be properly motivated (and therefore more trustworthy) if they are compensated for their involvement and exposed to liability for misuse of their key. This combination of "carrot" and "stick" will be more likely to align the third party's self-interest with that of the transferor if the third party is unrelated to any of the beneficiaries. Put differently, there will always

be some degree of risk that a related third party could be politically motivated to further the interests of a specific beneficiary.

Confidence in the allegiances of a rational independent third party, however, depend entirely on economics. Formulaically, the economic gain from compensation less the economic loss from liability must be greater than the economic gain from disobedience. The critical variable under this paradigm is the economic loss from liability exposure, since compensation will ultimately be dictated by market conditions and it should be assumed the financial incentive to collude with a beneficiary will be great. Liability exposure is greater for professional fiduciaries than it is for amateur unrelated third parties, since the professional fiduciary may suffer economic loss due to reputational damage in the event of a publicized breach of fiduciary duty. In other words, a professional fiduciary maintains a risk mitigation advantage over an unrelated amateur fiduciary so long as it is more lucrative for the professional fiduciary to service multiple clients loyally than to betray one client.

6. Using Trusts to Structure Multi-Signature Cryptocurrency Transfers

A trust is a 3-party fiduciary relationship used predominantly in common law legal systems in which the first party (the "settlor" or "trustor") transfers ("settles") property upon the second party (the "trustee") for the benefit of the third party (the "beneficiary"). The trustee is the legal owner of the entrusted property, as fiduciary for the beneficiary who is the equitable owner of said property. Trustees thus have a fiduciary duty to manage the trust to the benefit of the equitable owners. The existence of this duty is what exposes the trustee to liability in the event of mismanagement.

A trustee's management discretion is governed by the law under which the trust is settled and, assuming the arrangement is memorialized in writing, the trust instrument. In most jurisdictions, the terms in the trust instrument are allowed to take precedence over default rules expressed by such jurisdiction's trust law, with notable exceptions beyond the scope of this paper. As a general matter, however, it is fair to say that the settlor of a trust has a great deal of flexibility in determining how the trust will be administered, provided that the arrangement is agreeable to the trustee.

Any type of property may be held in trust, which, although there is no definitive precedent on the subject, presumably includes both cryptocurrencies and multi-sig wallet keys. If cryptocurrencies are settled directly, the trustees must have exclusive access to the keys of the trust's wallet to avoid legal disrespect of the arrangement as a sham, precluding any meaningful use of multi-sig wallets. Settlement of a multi-sig key, however, allows for the marriage of technology (the multi-sig wallet) and legality (the trust).

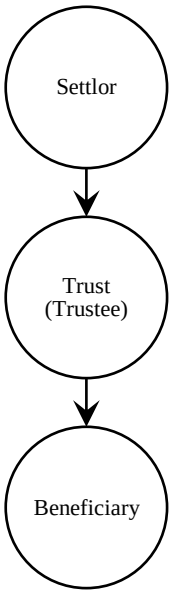


Figure 7:
General Trust Structure

7. Summary Examples of Multi-Signature Key Trust Plans

The following examples briefly illustrate how a multi-sig wallet key trust might work in common wealth transfer planning scenarios. In practice, the cryptocurrency owner's unique situation will inform both the specific implementation of both the multi-sig wallet and the associated trust instrument.

Example 1 (Blended Family)

The cryptocurrency owner ("Client") is a married individual with 1 adult child born out of a prior marriage ("Child 1") and 1 predeceased child ("Child 2") with his or her current spouse ("Spouse"). Child 1 has 2 minor children ("Grandchild 1" and "Grandchild 2"), as does Child 2 ("Grandchild 3" and "Grandchild 4") (Children and Grandchildren are collectively referred to as "Descendants"). Client's typical inheritance desires involve collective provision for Spouse and Descendants while Spouse lives and, after Spouse dies, fair distribution of any remainder amongst the 2 bloodlines. Client is survived by Spouse, who is survived by Child 1 and Grandchildren 1-4.

Client perceives a conflict of interest within the family and, as such, wishes to involve one or more third party fiduciaries to avoid infighting and ensure compliance with Client's intent. Due to the inherent nature of cryptocurrencies, however, Client cannot trust any single third party, notwithstanding that it may be a fiduciary, with absolute control of the cryptocurrency funds.

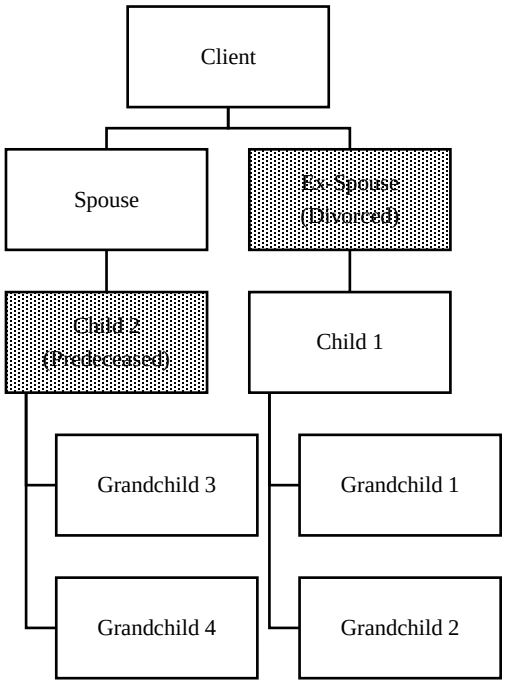
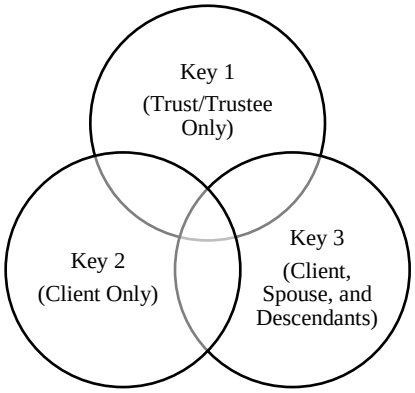


Figure 8: Blended Family Tree

Scenario 1A (Planning for Transfers at Death to a Blended Family)

The fiduciary arrangement is memorialized as a revocable trust, allowing Client, as settlor, to unilaterally unwind the planning. A professional third party fiduciary ("Trustee") serves as trustee. The type of multi-sig scheme used turns on whether Client wishes to unilaterally control the wallet and the extent to which Client seeks to mitigate risks associated with coercion or accidental Key loss.



To give Client unilateral wallet control, a 2-of-3 multi-sig wallet is created in the presence of Client and Trustee. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known only to Client and is irrecoverable in the event of Client's death or incapacity. Key 3 is initially known by Client but is later shared with Spouse and Descendants. For privacy, Key 3 may be shared with Spouse and/or Descendants after Client's death or incapacity. Client's ability to transact unilaterally allows for a duress attack on Client to divert wallet funds. If a Key is lost, the wallet can be emptied into a new wallet with the remaining Keys and loss of funds is avoided.

Figure 9: 2-of-3 Multi-Sig
With Client Unilateral Control

To preclude unilateral wallet control and maximally mitigate coercion risk, a 2-of-2 multi-sig wallet is created in the presence of Client and Trustee. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known by Client but is also shared with Spouse and Descendants. For privacy, Key 2 may be shared with Spouse and/or Descendants after Client's death or incapacity. Trustee's required cooperation maximally mitigates duress attacks on Client. Accidental Key loss results in an absolute loss of funds.

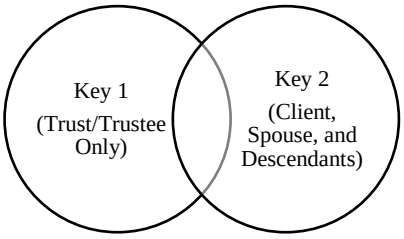


Figure 10: 2-of-2 Multi-Sig
Without Client Unilateral Control

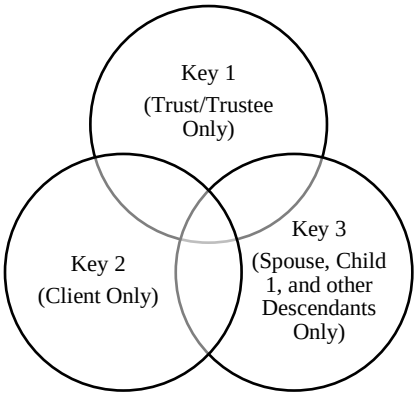


Figure 11: 2-of-3 Multi-Sig
Without Client Unilateral Control

To prohibit unilateral wallet control, moderately mitigate coercion risk, and mitigate Key loss risk, a 2-of-3 multi-sig wallet is created in the presence of Client, Trustee, Spouse, and Child 1. Grandchildren need not be present as long as it can be reasonably ensured that they will receive their Keys from Spouse or Child 1. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known only to Client and is irrecoverable in the event of Client's death or incapacity. Key 3 is initially known only to Spouse and Child 1 but is later shared with the other Descendants. For privacy, Key 3 may be shared with Grandchildren after Client's death or incapacity. Client does not know Key 3, so Client and at least 1 of Spouse or Descendants must be coerced to divert wallet funds. If a Key is lost, the wallet can be emptied with the remaining Keys and loss of funds is avoided.

In all cases, the trust instrument provides that during Client's life, Trustee must sign transactions at Client's direction (in the absence of Client's duress). Client may also remove and replace the trustees; if removed, Trustee becomes legally obligated to transfer custody of Key 1 to a successor trustee of Client's choosing. The combination of these trust terms ensures that Client maintains indirect control over Trustee and the entrusted Key during his or her life.

In all cases, on Client's death, multi-sig wallet cannot be spent without the cooperation of Trustee and any one of Spouse or Descendants. The instrument directs Trustee to hold Key 1 in further trust and sign transactions within a predetermined discretionary standard for Spouse and/or any Descendants. Optionally, when considering whether to engage in a transaction, Trustee may be directed to give preference to Spouse's needs. Because the continuing trust is a "sprinkle" or "pot" trust, no new wallets need be created at this time. Because Spouse and Descendants all have duplicate copies of Key 3, Trustee can make distributions to any of them without the consent the other beneficiaries. The trust instrument allows Trustee to withhold distributions to all beneficiaries if Trustee has reason to believe Key 3 has been withheld from any beneficiary.

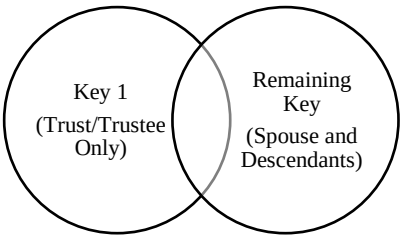


Figure 12: Remaining Multi-Sig
Following Client's Death

The trust instrument provides that while Spouse survives Client, Spouse and all Descendants, acting unanimously, may remove or replace Trustee with another unrelated professional fiduciary. Trustee has no incentive to veto a transaction resulting in a distribution to Spouse or Descendants unless such distribution exceeds Trustee's discretion. If Spouse and Descendants agree that Trustee is incorrectly withholding distribution consent, Spouse and Descendants may replace Trustee with another mutually agreeable unrelated professional fiduciary or, in the alternative, attempt to litigate the matter. Because Client's intentionally lost Key exposes the wallet to increased risk of inaccessibility, the trust instrument also provides that Trustee, Spouse, and Descendants may agree to transfer the existing wallet balance to an alternative multi-sig scheme to mitigate Key loss risk, provided, however, that any such scheme does not allow for transactions without the trustee's cooperation.

On Spouse's death, the trust instrument provides that Trustee is to distribute the remaining wallet balance *per stirpes* in further trusts for Descendants. As Child 2 has predeceased Spouse, 3 trusts with corresponding multi-sig wallets are created: a trust for Child 1 and Child 1's descendants (Grandchildren 1 and 2) ("Child 1's Trust"), a trust for Grandchild 3 and Grandchild 3's descendants ("Grandchild 3's Trust"), and a trust for Grandchild 4 and Grandchild 4's descendants ("Grandchild 4's Trust") (generically, a "Descendant Trust"). Under the *per stirpes* distribution rules, Child 1's Trust is funded with 50% of the wallet balance and each of Grandchild 3's Trust and Grandchild 4's Trust are funded with 25% of the wallet balance.

The trust instrument provides that upon reaching a certain age, the primary beneficiary of each Descendant Trust may act as trustee and remove or replace Trustee. If Child 1 is old enough to act as trustee of Child 1's Trust and chooses to do so immediately, the corresponding wallet may be created by Child 1 without Trustee's involvement; it will be Child 1's responsibility as Trustee to ensure the Child 1 Trust wallet is properly secured and protected against improper diversion. Because Grandchild 3 and 4 are minors, Trustee continues to serve as Trustee of Grandchild 3's Trust and Grandchild 4's Trust and participates in the new wallet creation ceremony with such Grandchild's legal representative.

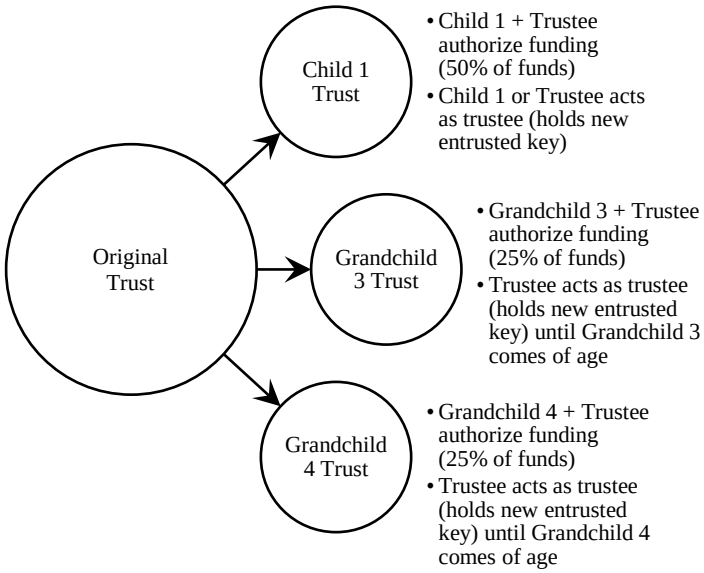


Figure 13: New Wallet Creation Following Spouse's Death

Each newly created wallet must have multi-sig authentication to ensure that wallet funds are accessible on the death of any given Descendant. The initial multi-sig scheme used will likely be 2-of-2, with the initial trustee receiving Key 1 and every trust beneficiary receiving Key 2. The trust instrument provides that the initial trustee and all currently living trust beneficiaries may agree to an alternative multi-sig scheme to mitigate Key loss risk, provided, however, that any such scheme does not allow for transactions without the trustee's cooperation. Once the new wallets have been created, each of Child 1, Grandchild 2, and Grandchild 3 initiate (via their shared original wallet key) a funding transaction for their respective trust, which Trustee subsequently authorizes after confirming the funding amounts are correct.

Scenario 1B (Planning for Lifetime Transfers to a Blended Family)

The number of trusts, initial trustees, and type of multi-sig scheme used turns on the extent to which Client seeks to mitigate collusion and Key loss risks. Generally, Client cannot have unilateral wallet control and qualify the transfer as a legally respected gift.

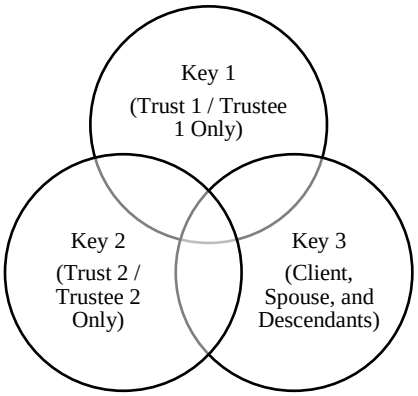


Figure 14: 2-of-3 Multi-Sig
Dual Trust / Higher Key Availability

To mitigate Key loss risks, 2 substantially identical irrevocable trusts are created ("Trust 1" and "Trust 2"). An unrelated professional fiduciary ("Trustee 1") serves as initial trustee of Trust 1 and another unrelated professional fiduciary ("Trustee 2") serves as initial trustee of Trust 2. A 2-of-3 multi-sig wallet is created in the presence of Client, Trustee 1, and Trustee 2. Key 1 is known only to Trustee 1 and Key 2 is known only to Trustee 2; each Key is immediately secured in 2 geographically distant safe deposit boxes in the names of the respective trusts. Key 3 is initially known by Client but is later shared with Spouse and Descendants. For privacy, Key 3 may be shared with Spouse and/or Descendants after Client's death or incapacity. Loss of any 1 Key will not result in wallet inaccessibility. Administration costs are increased under this dual trust plan. Transactions may not be vetoed by Client, Spouse or Descendants and, hypothetically, Trustee 1 and Trustee 2 could collude to divert funds. As Trustee 1 and Trustee 2 are unrelated professional fiduciaries, the risk of collusion is minimized.

To avoid the increased cost and collusion risk associated with dual professional fiduciary involvement, 1 irrevocable trust is created. Trustee serves as initial trustee. A 2-of-2 multi-sig wallet is created in the presence of Client and Trustee. Key 1 is known only to Trustee 1 and is immediately secured on behalf of the trust. Key 2 is initially known by Client but is later shared with Spouse and Descendants. Client may opt to share Key 2 with Spouse and/or Descendants after Client's death or incapacity. If either Key is lost, the wallet becomes inaccessible.

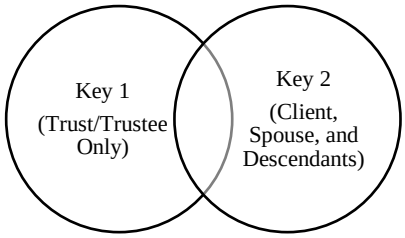


Figure 15: 2-of-2 Multi-Sig
Single Trust / Lower Key Availability

In either case, because Client is not a beneficiary of the trust(s), Trustee(s) are prohibited in the trust instrument from signing transactions resulting in distributions to or for the benefit of anyone other than Spouse and Descendants. Unlike the revocable trust described above, Client is precluded from mandating trustee distributions. Client (and, optionally, Spouse) may remove and replace the trustees (with anyone other than Client); any removed Trustee becomes legally obligated to transfer custody of their respective Key to a successor trustee of Client's choosing.

Client's death is a non-event from a trust administration perspective. If a single trust is used, trust administration follows the revocable trust scenario (Scenario 1A). If a dual trust plan is used, the only notable difference is that Trustee 1 and Trustee 2, acting together, do not require the cooperation of any Descendants to fund new wallets.

Example 2 (Unified Family)

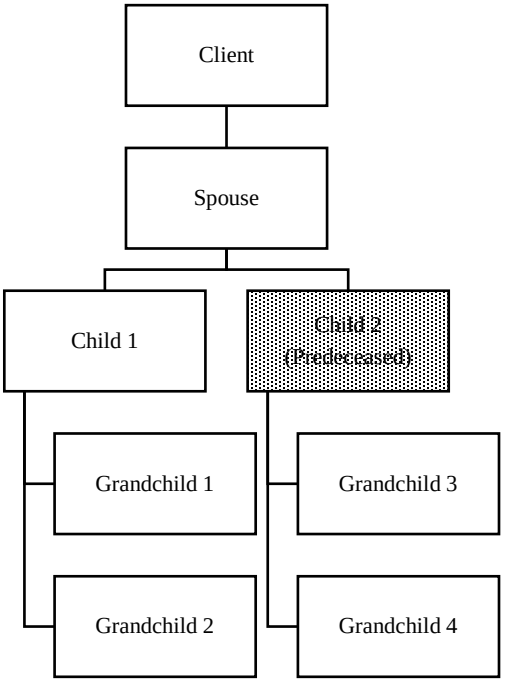


Figure 16: Unified Family Tree

Client is a married individual with 2 children ("Child 1" and "Child 2") born from his or her only spouse ("Spouse"). Child 1 has 2 children ("Grandchild 1" and "Grandchild 2"), as does Child 2 ("Grandchild 3" and "Grandchild 4") (Children 1-2 and Grandchildren 1-4 are collectively referred to as "Descendants"). Client has typical inheritance desires that include providing for Spouse and Descendants collectively while Spouse lives and, after Spouse dies, equally distributing any remainder *per stirpes* amongst the Descendants in further trust. Client is survived by Spouse, who is in turn survived by Child 1 (an adult) and Grandchildren 1-4 (minors).

Client anticipates no conflicts of interest within the family and implicitly trusts Spouse. Client wishes for a third party to be meaningfully involved only if Client and Spouse are unable to act. Due to the inherent nature of cryptocurrencies, however, Client cannot trust any single third party, notwithstanding that it may be a fiduciary, with absolute control of the cryptocurrency funds.

Scenario 2A (Planning for Transfers at Death to a Unified Family)

The fiduciary arrangement is memorialized as a revocable trust, allowing Client, as settlor, to unilaterally unwind the planning while he or she is alive and has legal capacity. A professional third party fiduciary ("Trustee") is named as initial trustee. The type of multi-sig scheme used turns on whether Client wishes to allow unilateral transactions, bilateral marital transactions, and the extent to which Client seeks to mitigate risks associated with coercion or accidental key loss.

To give each of Client and Spouse unilateral control, a 2-of-3 multi-sig wallet is created in the presence of Client, Spouse, and Trustee. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known only to Client and Spouse and is irrecoverable after Client and Spouse are dead and/or incapacitated. Key 3 is initially known by Client and Spouse but is later shared with Spouse and Descendants. To keep the wallet balance unknown to Descendants, Client and Spouse may opt to share Key 3 with Descendants after Client and Spouse have both died. Client's and Spouse's ability to transact unilaterally allows for a duress attack on either Client or Spouse to divert wallet funds. If a Key is lost, the wallet can be emptied into a new wallet with the remaining Keys and loss of funds is avoided.

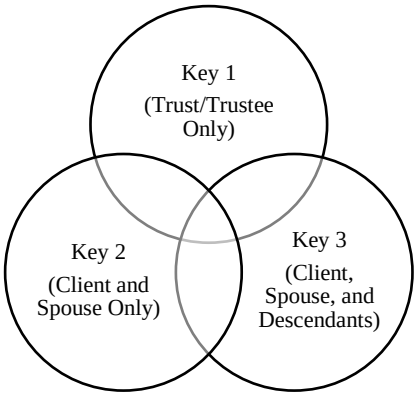


Figure 17: 2-of-3 Multi-Sig
With Unilateral Client/Spouse Control

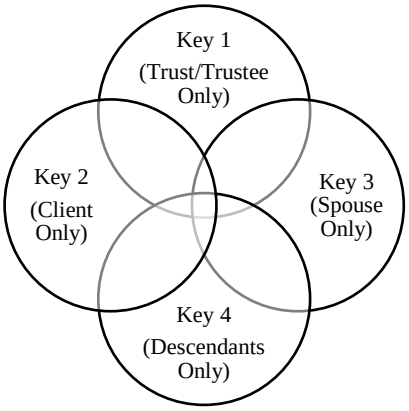


Figure 18: 2-of-4 Multi-Sig With Bilateral Marital Control

To prohibit unilateral control, moderately mitigate coercion risks, and mitigate Key loss risks, a 2-of-4 multi-sig wallet is created in the presence of Client, Trustee, Spouse, and a representative for Descendants. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known only to Client and is irrecoverable in the event of Client's death or incapacity. Key 3 is known only to Spouse and is irrecoverable in the event of Spouse's death or incapacity. Key 4 is known only to Descendants' representative and is later shared with Descendants (but not Client or Spouse). Because neither Client nor Spouse does not know Key 3, coercion of Client is ineffective in and of itself. If a Key is lost, the wallet can be emptied into a new wallet with the remaining Keys and loss of funds is avoided.

To preclude unilateral or bilateral marital control and maximally mitigate coercion risk, a 2-of-2 multi-sig wallet is created in the presence of Client and Trustee. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known by Client but is also shared with Spouse and Descendants. For privacy, Key 2 may be shared with Descendants after Client's death or incapacity. Trustee's required cooperation maximally mitigates duress attacks on Client. Accidental Key loss results in an absolute loss of funds.

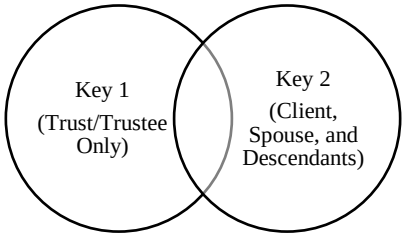
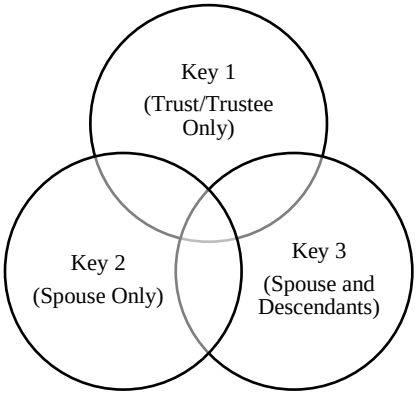
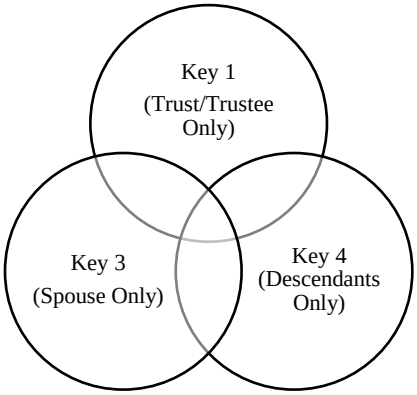


Figure 19: 2-of-2 Multi-Sig Without Unilateral or Bilateral Marital Control

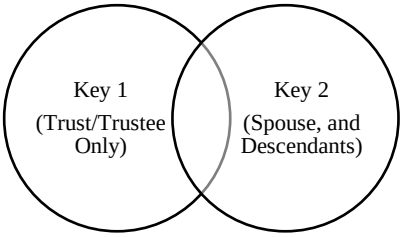
With the exception of the following differences, trust administration follows the analog blended family scenario (Scenario 1A). While Spouse survives Client, the trust instrument allows Spouse to not only remove or replace Trustee with another unrelated professional fiduciary, but to act as trustee himself or herself; this is allowed because, unlike in the blended family scenario, Spouse has no obvious bias toward certain Descendants. Further, in all of the multi-sig wallet implementations other than the 2-of-2 scheme, Spouse has the ability to transact with the wallet after Client's death in her individual capacity without Trustee's cooperation.



(Figure 17 Implementation)



(Figure 18 Implementation)



(Figure 19 Implementation)

Figure 20: Remaining Multi-Sig Keys Following Client's Death

Scenario 2B (Planning for Lifetime Transfers to a Unified Family)

Lifetime cryptocurrency transfer planning for a unified family is substantially similar to its blended family counterpart, except that Spouse's lack of obvious bias toward any certain Descendants allows Client to trust Spouse with unilateral wallet control. The number of trusts, initial trustees, and type of multi-sig scheme used turns on whether Client wishes to grant Spouse unilateral wallet control and the extent to which Client seeks to mitigate coercion, collusion, and Key loss risks.

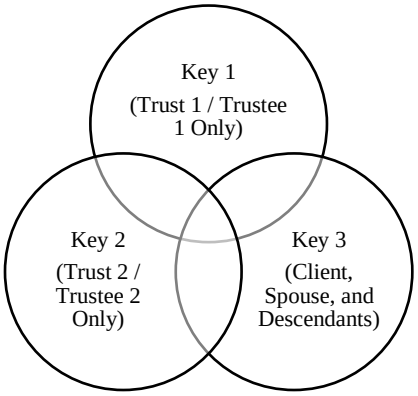


Figure 21: 2-of-3 Multi-Sig Dual Trust / High Key Availability Without Unilateral Spousal Control

To preclude Spouse's unilateral wallet control and mitigate Key loss and coercion risks, 2 substantially identical irrevocable trusts are created ("Trust 1" and "Trust 2"). An unrelated professional fiduciary ("Trustee 1") serves as initial trustee of Trust 1 and another unrelated professional fiduciary ("Trustee 2") serves as initial trustee of Trust 2. A 2-of-3 multi-sig wallet is created in the presence of Client, Spouse, Trustee 1, and Trustee 2. Key 1 is known only to Trustee 1 and Key 2 is known only to Trustee 2; each Key is immediately secured in 2 geographically distant safe deposit boxes in the names of the respective trusts. Key 3 is initially known by Client and Spouse but is later shared Descendants. For privacy, Client and Spouse may opt to share Key 3 with Descendants after Client and Spouse are dead and/or incapacitated. Loss of any 1 Key will not result in wallet inaccessibility. Administration costs are increased under this dual trust plan. Transactions may not be vetoed by Client, Spouse or Descendants and, hypothetically, Trustee 1 and Trustee 2 could collude to divert funds. As Trustee 1 and Trustee 2 are unrelated professional fiduciaries, the risk of collusion is minimized.

To avoid the increased cost and collusion risk associated with dual professional fiduciary involvement**,** prohibit Spouse unilateral wallet control, mitigate Key loss risks, and moderately mitigate coercion risk, 1 irrevocable trust is created. Trustee serves as initial trustee. A 2-of-3 multi-sig wallet is created in the presence of Client, Spouse, and Trustee. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known only to Spouse and is irrecoverable in the event of Spouse's death or incapacity. Key 3 is initially known only to Client but is later shared with the other Descendants. For privacy, Key 3 may be shared with Descendants after Client and Spouse are dead and/or incapacitated. Client does not know Key 2 and Spouse does not know Key 3, so either Client and Spouse or Spouse and at least 1 Descendant must be coerced to divert wallet funds. If a Key is lost, the wallet can be emptied with the remaining Keys and loss of funds is avoided.

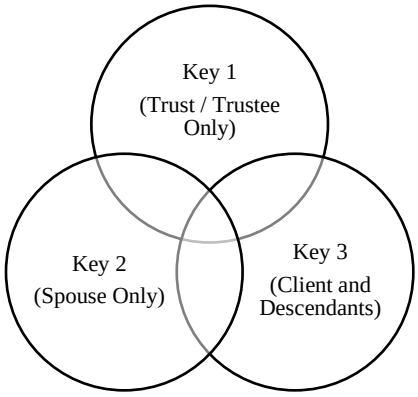


Figure 22: 2-of-3 Multi-Sig Single Trust / High Key Availability Without Unilateral Spousal Control

To avoid the increased cost and collusion risk associated with dual professional fiduciary involvement**,** grant Spouse unilateral wallet control, and mitigate Key loss risk, 1 irrevocable trust is created. Trustee serves as initial trustee. A 2-of-3 multi-sig wallet is created in the presence of Client, Spouse, and Trustee. Key 1 is known only to Trustee and is immediately secured on behalf of the trust. Key 2 is known only to Spouse and is irrecoverable in the event of Spouse's death or incapacity. Key 3 is initially known only to Client and Spouse but is later shared with the other Descendants. For privacy, Key 3 may be shared with Descendants after Client and Spouse are dead and/or incapacitated. Spouse's ability to transact unilaterally allows for a duress attack on Spouse to divert wallet funds. If a Key is lost, the wallet can be emptied into a new wallet with the remaining Keys and loss of funds is avoided.

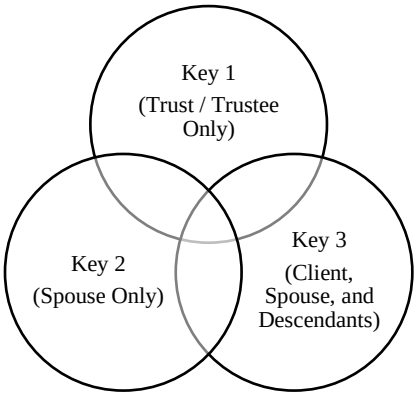


Figure 23: 2-of-3 Multi-Sig
Single Trust / High Key Availability
With Unilateral Spousal Control

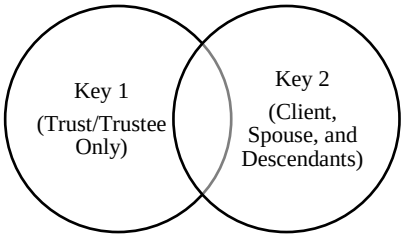
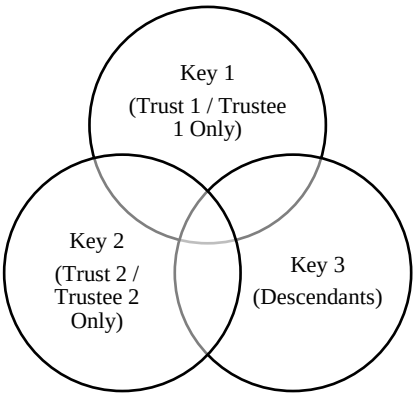


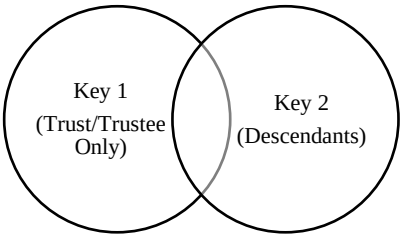
Figure 24: 2-of-2 Multi-Sig
Single Trust / Low Key Availability
Without Unilateral Spousal Control

To maximally mitigate coercion risk, 1 irrevocable trust is created. Trustee serves as initial trustee. A 2-of-2 multi-sig wallet is created in the presence of Client, Spouse, and Trustee. Key 1 is known only to Trustee 1 and is immediately secured on behalf of the trust. Key 2 is initially known by Client and Spouse but is later shared with Descendants. For privacy, Key 2 may be shared with Descendants after Client and Spouse are dead and/or incapacitated. If either Key is lost, the wallet becomes inaccessible.

With the exception of the following difference, trust administration follows the analog blended family scenario (Scenario 1B). Because Spouse has no obvious bias toward certain Descendants, while Spouse survives Client, the trust instrument allows Spouse to act as trustee himself or herself. While Spouse could technically serve as initial trustee, thereby avoiding the associated cost of professional fiduciary involvement, doing so will make the trust unattractive to successor professional fiduciaries because it will be impossible for said successor fiduciary to independently confirm that Key 1 (the entrusted key) was not compromised while Spouse was serving as trustee.



(Figure 21 Implementation)



(Figures 22-24 Implementation)

Figure 25: Remaining Multi-Sig Keys Following Spouse's Death

8. Transfer and Inheritance Tax Considerations

Generally, at the time of this writing, the laws and jurisprudence surrounding taxation of cryptocurrencies are in their infancy. For example, the only current guidance by the United States Internal Revenue Service on the taxation of cryptocurrencies is Notice 2014-21, which states that for United States federal tax purposes, cryptocurrencies are treated as property rather than currency. In the absence of clear defined rules or guidance, cryptocurrency owners are forced to guess as to how the relevant tax systems apply to their planned transfers. This guess can be educated by existing foundational wealth transfer law concepts to the above described scenarios. Before any planning is implemented, cryptocurrency owners should obtain current advice from tax practitioners in any jurisdiction with nexus to the plan (i.e., the jurisdictions of the settlor, trustee, trust, and beneficiaries).

Broadly, transfer taxes apply when beneficial ownership of property is irrevocably divested from the transferor. As such, it stands to reason that transfers of multi-sig keys to revocable trusts should not attract transfer tax liability; instead, any applicable transfer tax exposure should trigger on Client's death. Transfers of unfunded wallet multi-sig keys to irrevocable trusts are unlikely to be taxable. However, funding of such a wallet may attract immediate transfer tax liability depending on the rights and/or interests reserved by Client in the trust instrument and whether Client has unilateral access to a threshold number of keys. If the cryptocurrency market continues to grow explosively, trust planning that removes future cryptocurrency appreciation from the transferor's estate may be extremely attractive to transferors subject to the United States wealth transfer tax system.

9. Privacy Considerations

At present, it is unclear precisely how authorities will apply the 2 international automatic exchange of information ("AEOI") regimes, the Foreign Account Tax Compliance Act ("FATCA") and the Common Reporting Standard ("CRS"), to cryptocurrency transfer structures such as those described in this paper. AEOI regimes generally attempt to create global tax transparency by imposing information reporting obligations on certain financial institutions ("reporting FIs") in participating nations who custody or control assets for or on behalf of individuals from other participating nations. Unlike traditional financial assets, cryptocurrencies do not require the involvement of an FI; rather, funds are cryptographically custodied across the network in a decentralized manner. However, both trusts and their trustees are, in some cases, treated as reporting FIs under both AEOI regimes.

The FATCA and CRS rules are complex and a full treatment is beyond the scope of this paper. In brief, the relevant questions used to determine whether an AEOI reporting obligation exists in the structures contemplated by this paper are:

1. Is the custodian of the multi-sig key (i.e., the safety deposit box operator) in a jurisdiction that participated in FATCA or CRS?
2. Is the trust settled in a jurisdiction that participates in FATCA or CRS?
3. Is the trustee located in a jurisdiction that participates in FATCA or CRS?
4. If the answer to any of questions 1, 2, or 3 is yes, does the entrusted multi-sig key constitute a "reportable account" under the relevant AEOI regime?
5. If the answer to question 3 is yes, is the custodian, trust, or trustee a reporting FI under the relevant AEOI regime?

10. Conclusion

I have proposed a system for inheritance of cryptocurrencies with the minimal amount of reliance on trust. I started with the framework of multi-sig wallets, which removes the need for absolute trust of a single party, but is incomplete without a way to ensure the transferor's wishes are effectuated. To solve this, I propose contributing enough multi-sig keys to one or more trust entities to prevent spending without the cooperation of the professional trustee(s). Each professional trustee need only be relied on to not collude with a threshold number of other key holders to divert funds (a scenario that exposes the professional trustee to significant legal liability and reputational damage risk).

---

[i] As an homage to Satoshi Nakamoto, this whitepaper has been intentionally written in the style of his or her whitepaper. Background information on multi-signature and single-signature wallets has been paraphrased from publicly available sources and should not be construed as the author's original thoughts.