crypto.com

Distributed Crypto Custody

April 2022

Research and Insights

Research Manager
Kevin Wang

Head of Research & Insights
Henry Hon PhD, CFA

Published on 6 May 2022

RESEARCH DISCLAIMER

The information in this report is provided as general commentary by Crypto.com and its affiliates, and does not constitute any financial, investment, legal, tax, or any other advice. This report is not intended to offer or recommend any access to products and/or services. The views expressed herein are based solely on information available publicly, internal data, or information from other reliable sources believed to be true.

While we endeavour to publish and maintain accurate information, we do not guarantee the accuracy, completeness, or usefulness of any information in this report nor do we adopt nor endorse, nor are we responsible for, the accuracy or reliability of any information submitted by other parties. This report includes projections, forecasts, and other predictive statements that represent Crypto.com's assumptions and expectations in light of currently available information. Such projections and forecasts are made based on industry trends, circumstances, and factors involving risks, variables, and uncertainties. Opinions expressed herein are our current opinions as of the date appearing in this report only.

No representations or warranties have been made to the recipients as to the accuracy or completeness of the information, statements, opinions, or matters (express or implied) arising out of, contained in, or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) that may arise from any person acting on any information and opinions contained in this report or any information made available in connection with any further enquiries, notwithstanding any negligence, default, or lack of care, is disclaimed.

This report is not meant for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of Crypto.com in any form is prohibited except with the written permission of Crypto.com. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of, or located in a jurisdiction, where such distribution or use would be contrary to applicable law or that would subject Crypto.com and/or its affiliates to any registration or licensing requirement.

The brands and the logos appearing in this report are registered trademarks of their respective owners.

Contents

Executive Summary

- We define distributed custodial solutions as the ways in which to distribute sole control of a transaction across multiple parties/devices in order to avoid a single point of failure. There are mainly two solutions that achieve this: multi-signature (multisig) and multi-party computation (MPC).
- A multisig wallet requires multiple private keys to sign a transaction in order for that transaction to be executed.
    - Multisig transactions in Bitcoin are implemented using pay-to-script-hash (P2SH) script. Data shows that Bitcoin's multisig usage is still at a low level in terms of the number of existing BTC held in P2SH addresses, as well as the number of UTXOs.
    - For Ethereum, multisig wallets are developed by using smart contracts. Gnosis Safe is a popular multisig wallet in Ethereum with over US$72B total value stored in its smart contract.
- Multi-Party Computation (MPC) involves parties that do not trust each other jointly computing a function over their inputs while keeping those inputs private. The usage of MPC in blockchain key management is more specific — via the Threshold Signature Scheme (TSS).
- Notably, the main difference between multisig and MPC is the formation of a 'private key'.
- Multisig and MPC are both powerful custodial solutions, but they are not necessarily suitable for every case. They require people to have some knowledge about crypto and are not suggested for beginners. But we believe that, as the crypto custody space develops and evolves, these distributed custodial solutions could be the future of crypto custody.

1. Introduction

One of the most important features of crypto is decentralisation. Although crypto itself is securely backed by blockchains, crypto assets suffer risks due to the improper methods of custody. **Crypto custody is not only responsible for storing private keys (e.g., in software or hardware), but also for deciding the scheme of signing transactions by using private keys.** The whole procedure should be secure enough to avoid disclosing private keys.

Generally, crypto custodians for institutional investors adopt multi-layer architecture to add limited-access control of assets based on the roles of the people who can touch the assets. Meanwhile, this separation of responsibility also requires that the control of private keys should be distributed in order to improve security.

For the self-custody scenario, the security issues of custody are also important, as it has a direct impact on crypto adoption. For instance, Chainalysis noted that an estimated US$3.7 million worth of Bitcoin (BTC) (today worth over US$140 billion) has been lost due to those who forgot their private key. Therefore, technically, it could be a significant improvement if distributed custody was adopted in self-custody. The term distributed means that the processing is shared across multiple nodes, but the decisions may still be centralised and use complete system knowledge.

In this article, **we define distributed custodial solutions as the ways to distribute the single control of a transaction to multiple parties in order to avoid a single point of failure. There are mainly two solutions to achieve this: Multi-signature (multisig) and multi-party computation (MPC).**

1.1 Traditional Crypto Wallets

Before we deep-dive into the methodology behind distributed custody, let's review and understand how the traditional non-custodial wallet (NCW) works. Non-custodial wallets allow users to retain full control of their funds because the private key is stored locally with the user. But how do non-custodial wallets actually work and store assets (private keys)?

The generation of private keys starts from the Secret Recovery Phrase (or mnemonic phrase/seed phrase). However, the mnemonic phrase doesn't equal the private key. Simply put, **individual private keys are "children" of a mnemonic phrase.** We discuss the generation of the mnemonic phrase below and why it should be kept safe.

Master Seed

Before further exploration, an understanding of the relationship between a Hierarchical Deterministic (HD) wallet and a master seed is required.

The traditional crypto wallet is a Hierarchical Deterministic (HD) wallet that generates virtually infinite numbers of private/public key pairs with a single master seed. With the single master seed stored in a central location, users can regenerate all the subkeys and restore the entire wallet without remembering all the individual private keys.

A master seed is generated from a hexadecimal entropy. (In computing, entropy is the randomness collected by an operating system or application for use in cryptography.) If entropy can generate a master seed to access users' keys, what is a mnemonic phrase used for?

Mnemonic Phrase

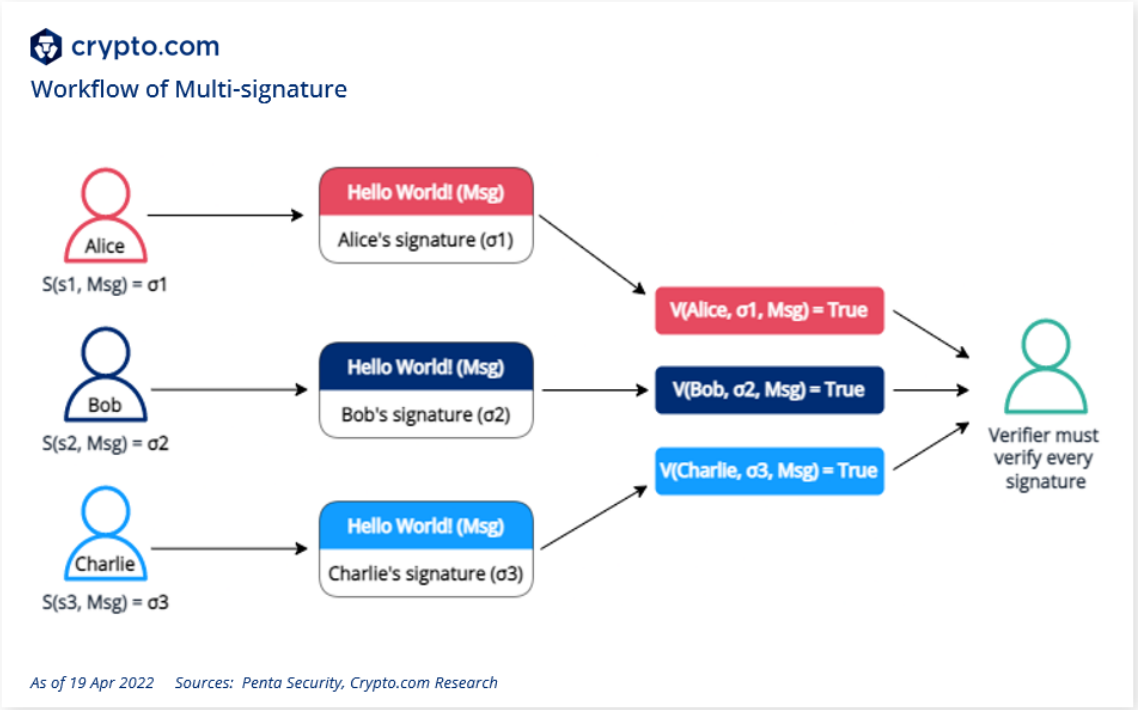
It's very difficult for humans to memorise many random letters to access a wallet. Therefore, Bitcoin developers first came up with a way to transform an entropy into a more readable and recognisable form. The transformation is documented in BIP-39; the below table explains how this procedure works.

From Entropy to Mnemonic Phrase (for 128 Bits Entropy)	
1	Generate entropy (usually 128 bits for 12 words or 256 bits for 24 words).
2	Hash the entropy with SHA-256 and take the first 4 bits as the checksum.
3	The 4-bit checksum is added to the entropy, which is then divided into 11-bit length segments.
4	Match these 11-bit segments with BIP-39 English word list (total 2,048 words).
5	The result is the 12 mnemonic words.

2. Multi-Signature (Multisig)

Multi-signature (multisig) is a wallet that requires multiple keys in order to sign a transaction before it can be executed. Multi-signature transactions in Bitcoin are performed using pay-to-script-hash (P2SH) transactions. For Ethereum, multisig wallets are developed by using smart contracts.

Multisig refers to requiring multiple private keys in order to authorise transactions instead of a single signature from one key used in a traditional crypto wallet, as discussed above. Generally, multisig transactions have an m-of-n form, where **m** stands for number of signatures required to spend funds and **n** stands for maximum number of public keys permitted to sign. The workflow of multisig is shown below:



Multisig has a number of applications:

- Dividing up responsibility for possession of assets amongst multiple people.
- Avoiding a single point of failure, making it substantially more difficult for the wallet to be compromised.
- Backing up m-of-n, where loss of a single seed doesn't lead to loss of the wallet.

The most standard combination of keys for multisig wallets is 2-of-3, where 2 private keys out of 3 are needed in order for a transaction to be executed. Thus, even if the safety of one of a user's private keys was compromised, the hacker still

couldn't steal their bitcoin, as gaining access to the second key is needed in order to sign off transactions out of users' wallets. This minimum number (2, in this 2-of-3 case) is referred to as the threshold.

Multisig is considered a potential solution for crypto custody because:

- It's more secure than the single-signature, as multisig wallets reduce the dependence on a single person and single point of failure.
- It can achieve escrow transactions, allowing third-party participation in escrow transactions between two parties (A and B).

However, multisig isn't perfect. The drawbacks of using multisig wallets include:

- The information of which public keys used to redeem the funds is disclosed.
- The transaction cost can be very high since multiple parties are required to sign it.
- The security policy is fixed and inflexible once the multisig address is created. (It cannot update from 2-of-3 to 3-of-5 multisig in Bitcoin, for example.)

2.1 Multi-Signature in Bitcoin

P2SH Address

Traditional Bitcoin wallets rely on a simple send-receive system, the **pay-to-pubkey-hash (P2PKH)** address (**an address starting with 1**), which is the standard transaction for Bitcoin. This means that for every Bitcoin wallet there's one wallet address, which is a hash of the public key, associated with a user's private key, which is required to redeem the coins.

Multisig transactions in Bitcoin are done using a pay-to-script-hash (P2SH) address (address starting with 3). P2SH allows Bitcoin to have the function of custom contracts, including multisignature logic (with the OP_CHECKMULTISIG operation). In a multisig transaction, one address can have **n** number of associated private keys, with a threshold of **m** number of these keys in order to spend the funds. This is referred to as an m-of-n multisig.

Bitcoin proposed the specification of multi-signature in BIP-11, which prompts the three-party escrow (buyer, seller, and trusted dispute agent), with transactions requiring 2-of-3 signatures:

1. The buyer, seller, and agent each provide a public key.
2. The buyer then sends coins into a 2-of-3 CHECKMULTISIG transaction, and the transaction ID goes to the seller and the agent.

3. The seller fulfils their obligation and asks the buyer to co-sign a transaction (already signed by seller), which sends the tied-up coins to the seller.

P2SH transactions were standardised in BIP-16, allowing them to be sent to a script hash instead of a public key hash (P2PKH). To spend bitcoins sent via P2SH, the recipient must provide a script matching the script hash and data, which makes the script evaluate to True.

Here, we take a savings account that parents created for their child as an example of the 2-of-3 scheme. The child can spend the money with the approval of either parent, and the money cannot be taken away from the child unless both parents agree. The steps of a Bitcoin multisig wallet works roughly as follows:

1. Generates a multisig address based on a set of public keys and a "threshold" parameter, which is the minimum number of signatures required to trigger a spend.
2. Funds the new multisig address, producing an unspent transaction output (UTXO) owned by the multisig address.
3. Creates a new, raw offline transaction to spend the multisig's UTXO.
4. Signs the raw transaction with one private key, which returns a hex string.
5. Signs the hex string with another private key, which returns a new hex string.
6. Continues step 5 until the threshold is met (e.g., 3 signatures out of 5). Sends the result in a script with the UTXO to spend. The bitcoins will transfer to the desired recipient.

Although the multisig transaction is achieved via P2SH script, the scripts increase the size of Bitcoin transactions. Moreover, the size of the script signature would grow linearly according to the number of participants in the multisig. To solve this problem, the Bitcoin community proposed to replace the currently used ECDSA signature with the Schnorr signature, which can reduce the transaction size by aggregating **m** number of signatures into one signature. This update was included in the Bitcoin Taproot upgrade in November 2021. Additionally, since the multiple signatures are cryptographically combined into one, privacy is also enhanced, as it becomes more difficult to identify each participant's transaction inputs where the private data is stored.

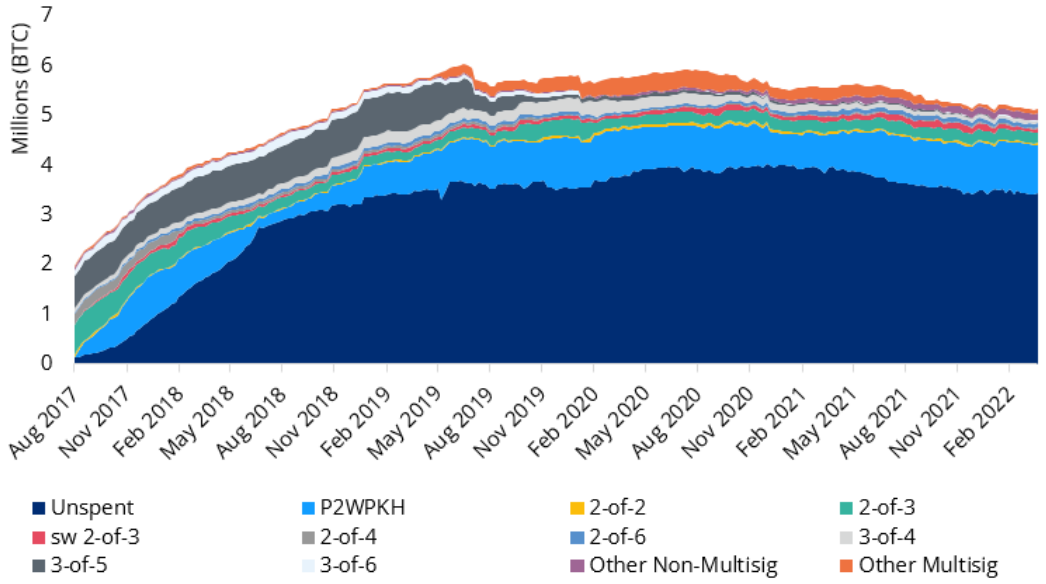
The first multisig wallet was launched in August 2013 by BitGo. As the methodology of creating multisig addresses is widely adopted, many wallets are enabling the creation of Bitcoin multisig, including Freewallet, Carbon Wallet, and Blockstream Green wallet. Additionally, this page can create and spend from multisig addresses.

However, data shows that Bitcoin's multisig usage is still at a low level in terms of the number of existing BTC held in P2SH addresses, as well as the number of UTXOs.

crypto.com

Breakdown of BTC Stored in P2SH Addresses by Type

BTC multisig addresses are the minorities

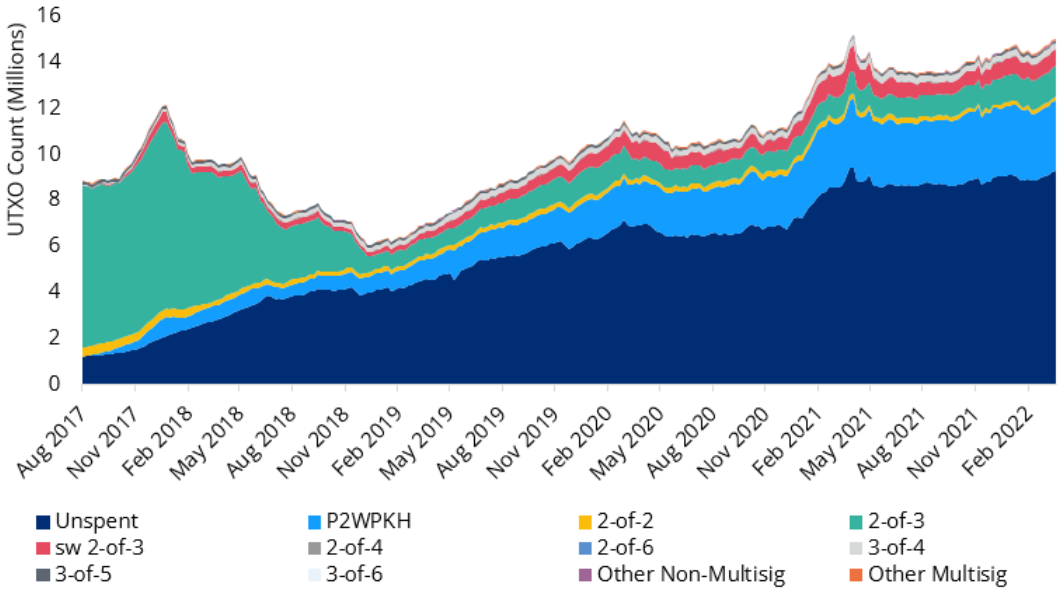


As of 19 Apr 2022 *Sources: txstats.com, Crypto.com Research*

crypto.com

Breakdown of BTC P2SH Outputs by Type

2-of-3 multisig was popular during 2017-2018, but plunged heavily since Q3 2018



As of 19 Apr 2022 *Sources: txstats.com, Crypto.com Research*

2.2 Multi-Signature in Ethereum

Unlike UTXO-based transactions in Bitcoin, Ethereum uses account-based transactions. Accounts are fundamental Ethereum components that can hold funds and execute transactions. In Ethereum, there are two types of accounts:

- Externally Owned Accounts: Also called wallets, these are the simplest accounts, having a balance and executing transactions. These accounts are controlled by private keys and have no associated code.
- Contracts Accounts: They are actually smart contracts. These also have a balance, but not private keys. These accounts are associated with code and can be executed by transactions or calls from other contracts.

In Ethereum, multisig wallets are developed by using smart contracts, in which complex logic is implemented. **Gnosis Safe is a popular multisig wallet in Ethereum with over US$72 billion total value stored in its smart contract.** Below are some notable representatives of Ethereum multisig wallets:

Multisig Wallet	Features	Total Value Stored
ConsenSys	- The smart contract is simple and cleanly written. - Not regularly maintained; passed to Gnosis Safe for further development.	N/A
Gnosis Safe	- Based on the ConsenSys multisig wallet, with many improvements and continued active development. - Users manage their own funds via multiple devices; no third parties.	US$72 billion
Argent	- Argent is a social recovery wallet supported by the concept of 'guardians' — accounts on Ethereum to which users give permission for help with limited security actions. A guardian can be hardware, a trusted person, or a third-party service. - Supports layer 2 transactions.	US$77 million
BitGo	- Adopts 2-of-3 multisig. - Its 'Safe Mode' can be set on a wallet contract, preventing ETH and ERC20 tokens from being sent anywhere other than to wallet signers.	N/A

As of 18 Apr 2022 *Sources: Dune Analytics, Crypto.com Research*

3. Multi-Party Computation (MPC)

In MPC, a set of parties that do not trust each other try to jointly compute a function over their inputs while keeping those inputs private. The usage of MPC in key management on blockchains is more specific — via the Threshold Signature Scheme (TSS). TSS is a (**t**,**n**)-threshold signature scheme that distributes signing power to **n** parties, with any group of at least **t** parties able to generate a signature. In many crypto materials, the two terms (TSS and MPC) are often used interchangeably, but strictly speaking, Threshold Signature Scheme is the subfield of MPC.

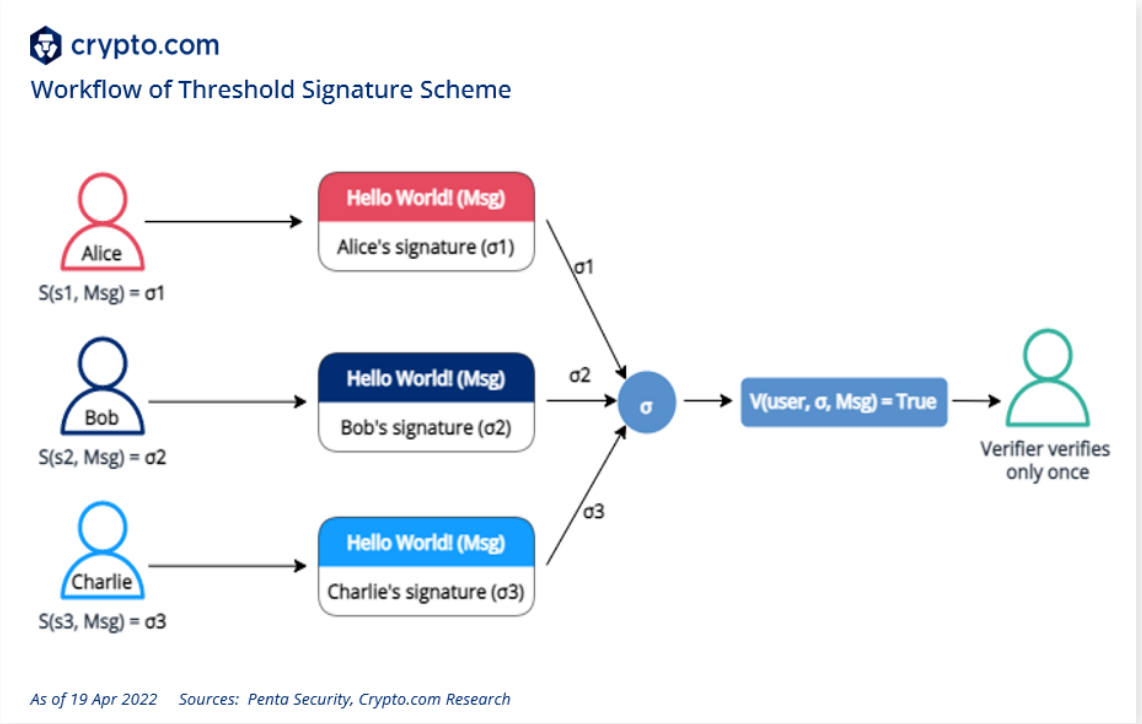
The two basic properties that an MPC protocol must ensure are:

- Privacy: The private information held by the parties cannot be inferred from the execution of the protocol.
- Accuracy: If a number of parties within the group decides to share information or deviate from the instructions during the protocol execution, the MPC will not allow them to force the honest parties to output an incorrect result or leak an honest party's secret information.

Before introducing TSS, here is a refresher on the generation of new addresses from a classic blockchain: 1) creating a new address by generating a private key, 2) computing the public key from the private key, and 3), deriving the blockchain address out of the public key.

With TSS, a set of parties jointly compute the public key, with each holding a secret share of the private key (the individual shares are not revealed to each other). From the public key, the address is derived in the same way as in the traditional system, making the blockchain agnostic to how the address is created. This is a huge advantage because the entire key can't be obtained by compromising a single party, and each party holds just one part of it. Therefore, TSS is considered to be a modern key to managing assets securely for custodians.

Similarly, when signing transactions, instead of a single party signing with their private key, a distributed signature between multiple parties is generated. So each party can produce a valid signature as long as enough of them are acting honestly.



It is important to mention that distributed key generation is designed to allow for different types of access structures: the general **"t** out of **n"** setting is enabled to extend to **m** arbitrary failures in private key-related operations, without compromising security. Additionally, TSS-based wallets have an impressive security feature that enables private key rotation without changing the corresponding public key and blockchain address. Private key rotation, also known as proactive secret sharing, is yet another MPC protocol that takes the secret shares as input, then outputs a new set of secret shares. The old secret shares then can be deleted, and the new ones can be used in the same way.

Multisig (m-of-n, at least **m** signatures are required out of **n**) has a similar scheme with TSS. In fact, multisig is an emulation of TSS. However, there are also many differences between TSS and multisig. **Notably, the main difference between multisig and TSS is the formation of a 'private key'.** For multisig, each participant contributes their private key in order to sign their approval on the multisig address and deliver the transaction. For MPC, there is only one private key, which is split into encrypted shares, where any predetermined number (**t**) of the total number of shares (**n**) are required to make a transaction. We summarise their similarities and differences in the table below:

Item	Multisig	TSS
Environment	On-chain	Off-chain
Number of verification	M	1
Number of public and private keys required	M public keys M private keys	1 public key 1 private key
Final private key can be reconstructed?	Yes	No
Private key rotation	No	Yes
Exposure of identity	All participants' public keys will be disclosed	No

As of 19 Apr 2022 *Source: Crypto.com Research*

Despite the advantages of TSS and the significant development in its implementations, there are still some limitations and concerns. For one, TSS requires participants (at least the threshold number of participants) to collaborate online at the same time. In comparison to classic public key cryptography, TSS protocols can also be very complex, and it is far from a tried-and-tested place.

One project in the exploration of TSS for crypto wallets is ZenGo, which is a 2-of-2 TSS that applies an ECDSA signature (the signature algorithm used by Bitcoin, Ethereum, and others); the two parties are the ZenGo server and the ZenGo user's mobile device. However, it's not a full non-custodial wallet, and users can't fully control their assets.

4. Conclusion

Both multisig and MPC can sign transactions in distributed ways, providing higher security than the traditional crypto wallet by avoiding a single point of failure. Although MPC is more efficient and more private than multisig, it doesn't mean that MPC will replace multisig. On the contrary, multisig has signature accountability, while MPC doesn't. In multisig, a specific number of parties need to sign transactions, which are recorded on the blockchain. Accountability may not be a big drawback, but it is vital in monetary systems, especially when considering the differences for people with different roles and storage. Meanwhile, MPC is not currently well-supported by hardware wallets.

Multisig and MPC are both powerful custodial solutions, but that doesn't mean they are suitable for every case. They require that people have some knowledge about crypto and are not suggested for beginners. But we believe that, as the crypto custody space develops and evolves, these distributed custodial solutions could be the future of crypto custody.

References

Adarme, Nicole, and Johann Bornman. “Crypto Custody Solutions for Organizations Entering the DeFi Space | MetaMask Institutional.” *ConsenSys*, 2 November 2021, https://consensys.net/blog/metamask/metamask-institutional/crypto-custody-solutions-for-organizations-entering-the-defi-space/.

Antonopoulos, Andreas. “BIP39 and mnemonic phrase.” *New day crypto*, 7 August 2021, https://newdaycrypto.com/bip39-and-mnemonic-phrase/.

Belshe, Mike. “Multi-Sig vs MPC: Which is more secure?” *Official BitGo Blog*, 11 September 2019, https://blog.bitgo.com/multi-sig-vs-mpc-which-is-more-secure-699ecefc8430.

“BIP 0039.” *Bitcoin Wiki*, 10 September 2013, https://en.bitcoin.it/wiki/BIP_0039.

Bronkema, Wietze. “Introduction to Multisig Contracts | by Wietze Bronkema | MyCrypto.” *Medium*, 15 January 2020, https://medium.com/mycrypto/introduction-to-multisig-contracts-33d5b25134b2.

Buterin, Vitalik. “Bitcoin Multisig Wallet: The Future of Bitcoin.” *Bitcoin Magazine*, 13 March 2014, https://bitcoinmagazine.com/technical/multisig-future-bitcoin-1394686504.

Cointelegraph. “A beginner’s guide to the Bitcoin Taproot upgrade.” *Cointelegraph*, https://cointelegraph.com/bitcoin-for-beginners/a-beginners-guide-to-the-bitcoin-taproot-upgrade.

Cryptopedia. “What Is a Multi-Signature Wallet?” 15 April 2022, https://www.gemini.com/cryptopedia/what-is-a-multi-sig-wallet-crypto-multi-signature-wallet.

Danise, Amy, and Fabian Friedrich. “Custodian And TSS: The Modern Keys To Managing Assets Securely.” *Forbes*, 28 February 2022, https://www.forbes.com/sites/forbescommunicationscouncil/2022/02/28/custodian-and-tss-the-modern-keys-to-managing-assets-securely/.

David. “The Magic Behind a Mnemonic Phrase and HD Wallets — Let Us Explain.” 26 April 2019, https://medium.com/cosmostation/the-magic-behind-a-mnemonic-phrase-and-hd-wallets-let-us-explain-43d9c97f6098.

Fireblocks. “MPC vs. Multi-sig.” 25 May 2021, https://www.fireblocks.com/blog/mpc-vs-multi-sig/.

Heart, Cassandra, and Arash Afshar. “Threshold Digital Signatures. By Cassandra Heart, Arash Afshar | by Coinbase.” *The Coinbase Blog*, 5 November 2021, https://blog.coinbase.com/threshold-digital-signatures-1d467054acd4.

MetaMask. “User Guide: Secret Recovery Phrase, password, and private keys.” *MetaMask Support*, 23 March 2022, https://metamask.zendesk.com/hc/en-us/articles/4404722782107#h_01FYVAXCSH95CQ08Q0P2VJA5HV.

“Multi-signature.” *Bitcoin Wiki*, 20 July 2021, https://en.bitcoin.it/wiki/Multi-signature.

Penta Security. “Why should we use MPC signatures in the blockchain?” *Penta Security Systems Inc.*, 27 July 2020, https://www.pentasecurity.com/blog/why-should-we-use-mpc-signatures-in-the-blockchain/.

“Protocol documentation.” *Bitcoin Wiki*, 30 July 2021, https://en.bitcoin.it/wiki/Protocol_documentation#tx.

Shlomovits, Omer. “Threshold Signatures Explained.” 21 July 2019, https://academy.binance.com/en/articles/threshold-signatures-explained.

ZenGo. “Security in-depth” *ZenGo*, https://zengo.com/security-in-depth/.

Zuidhoorn, Maarten. “The Journey from Mnemonic Phrase to Address | by Maarten Zuidhoorn | MyCrypto.” 3 June 2020, https://medium.com/mycrypto/the-journey-from-mnemonic-phrase-to-address-6c5e86e11e14.

e. contact@crypto.com

Published on 6 May 2022