Request

WWW.REQUEST.FINANCE

@REQUESTFINANCE

The ultimate **Web3 CFO guide**

2025 EDITION

A PRACTICAL GUIDE

Actionable insights from finance and operations professionals at hybrid companies, Web3 Foundations, and DAOs.

Key Insights

We spoke to 300 finance and operations leaders at Web3 companies. We wanted to find out their biggest challenges when they started their new role and what they learned.

1. **Education is needed to help finance professionals understand Web3.** Most CFOs at Web3 organizations have prior experience in financial operations, accounting, or similar roles but struggle to learn about Web3.

    - 46% of Web3 CFOs indicated they had more than 3 years of experience in a finance or accounting role before joining a Web3 organization.
    - Over 48% of CFOs at Web3 organizations said they did not have formal onboarding processes when they started.
    - 55% said that knowledge of Web3 was one of the biggest gaps in their professional knowledge when they started as Web3 CFOs.

2. **Financial Operations (FinOps) tooling in Web3 represents a tremendously underserved SaaS category.** Existing payments, accounting, or enterprise resource planning (ERP) tools are ill-suited to the needs of Web3 CFOs.

    - When asked about the availability of FinOps tooling in Web3, over 41% of CFOs polled said it was "insufficient" compared to Web2.

3. **Web3 CFOs are re-emphasizing self-custody of their organization's digital assets**.

    - About 91% of Web3 CFOs indicated that over half of their organization's digital assets and crypto treasury are held in self-custody today.
    - Interestingly, most Web3 CFOs polled were already actively practicing self-custody. 59% of Web3 CFOs indicated that the risks of centralized crypto platforms led to a shift towards more self-custody.

4. **Despite the challenges, Web3 CFOs are optimistic about the growing need for more finance professionals in the blockchain space.**

    - 64% of Web3 CFOs polled estimate that the demand for finance, accounting, tax, and audit professionals will grow over the next 12-24 months.

About Us

Request Finance is an enterprise app founded by CFOs and YCombinator alumni who aim to increase digital currency adoption for the first 100,000+ businesses. The thesis is that blockchain technology will help build a more transparent, borderless, and innovative financial system.

Finance persons use the all-in-one finance solution for crypto and fiat Accounts Payable, Accounts Receivable, and Accounting, plus payments to 190+ countries.

Since launching to the public in 2021, the software has helped simplify and automate around $1 billion in crypto and fiat invoices, payroll, expenses, prizes, and grant disbursements.

Trusted by over 3,000 teams like The Sandbox, OpenZeppelin, and Arbitrum. Self-custodial and compatible with hundreds of crypto wallets and accounting software.

MORE ON WWW.REQUEST.FINANCE

Our Contributors

AND +300 FINANCE AND OPERATIONS LEADERS

Special Thanks

About this Guide

WHO IS THIS FOR?

If you manage financial operations (FinOps) at a company, foundation, or decentralized autonomous organization (DAO) dealing with crypto somehow, this Guide is for you.

Titles don’t matter. For simplicity, we use the title “chief financial officer” or “CFO” to refer to the person responsible for a team's financial health and operations. Your actual title may vary. But no matter the title, the responsibility for the team’s financial health, daily functions, and compliance falls on you.

Knowledge of economics, finance, or accounting is helpful but not necessary for you to understand or use this Guide.

HOW WILL IT HELP ME?

This Field Guide is not a textbook laden with theoretical nuance. It is a practical, everyday resource drawn from the experiences and insights of over 300 finance and operations leaders at crypto companies.

It is filled with actionable insights, illustrative case studies, and best practices that are easily accessible for busy professionals like yourself. Whether you are new to the role or the industry, this Guide contains practical resources to help you excel in key areas of FinOps in crypto.

WHERE SHOULD I START?

The Guide is organized from the basics of setting up a crypto wallet, to more advanced topics like treasury management. But you need not read it from cover-to-cover in one sitting. You can refer to the relevant sections as needed during the course of your work.

What's inside the Guide

Foreword from **our CEO**

Our world is dramatically different from the one I knew when I first began my journey as a CFO.

Finance is changing. Money has become programmable. Decentralized Finance (DeFi) platforms enabled by new crypto-economic primitives like smart contracts and blockchain payment rails are opening new possibilities at an unprecedented scale.

Organizations, too, are changing. The normalization of remote work and the mushrooming of decentralized cooperatives like DAOs have enabled new and global ways of creating value collaboratively.

The Web3 CFO Guide is aimed at helping you manage these exciting new frontiers as a CFO. The insights are based on our interviews with over 300 finance and operations leaders at hybrid companies like The Sandbox, Decentraland, and more. Many of them are active members of the web3financeclub, with team sizes varying between dozens to thousands of employees and contributors.

We want to thank all who contributed to this Guide. Your insights and experiences will be invaluable to helping Web3 CFOs maximize their role's value and their teams' effectiveness.

For more detailed insights or questions, we encourage you to contact us or any authors listed at the back of this document.

CHRISTOPHE LASSUYT,
CO-FOUNDER, REQUEST FINANCE

CHAPTER 1.0

Challenges facing Web3 CFOs today

What are some of the biggest hurdles that Web3 CFOs face? These represent areas of opportunity for best practices, and new tooling to emerge.

Challenges facing Web3 CFOs today

Despite the tremendous opportunities in Web3, CFOs in the space face a number of challenges today.

1. HIGH ENTRY BARRIER

Many Web3 CFOs came in with prior experience in a finance role, with 55% citing gaps in their knowledge of crypto, DeFi, or other blockchain technologies as one of the biggest handicaps when they started.

"I would describe it as a learning cliff - just an endless wall," said one CFO.
"It feels like infinite learning."

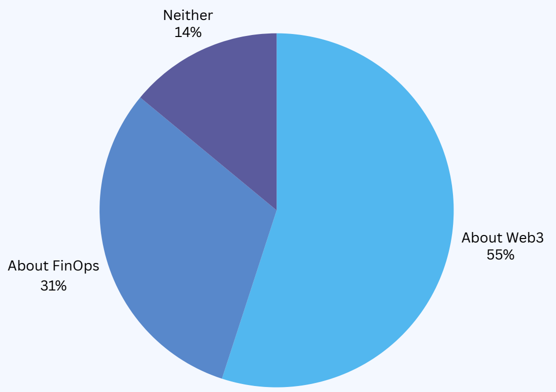


Fig 1. - How would you rate the most significant knowledge gaps when you started as a Web3 CFO?

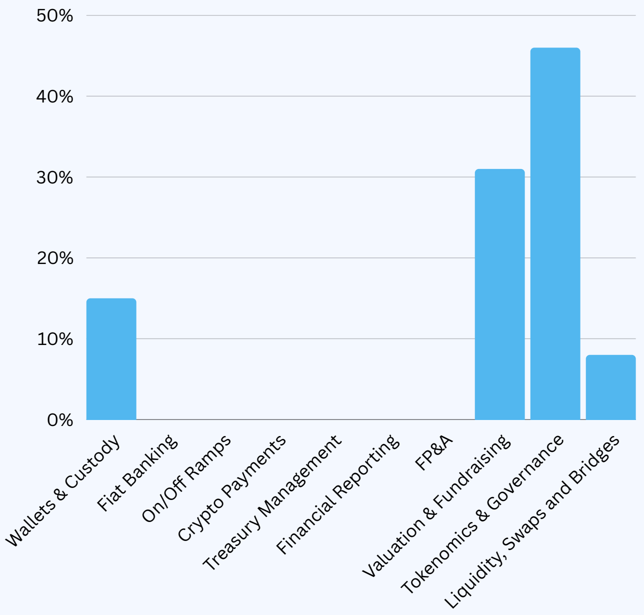


Fig 2. - What are some topics that you feel are under-addressed in the community for Web3 CFOs?

A common refrain we heard was the difficulty in **keeping up with the rapid pace of new technologies and applications,** from Layer 1s and 2s to the alphabet soup of ZKPs, NFTs, EIPs, and more.

Many CFOs face challenges such as sifting through vast amounts of new information and trying to understand and incorporate new decentralized applications (dApps) into their workflows.

“Nothing worth achieving comes easy. In crypto, the challenges make the rewards extraordinary", shared Delphine Genin-Gross, Founder of Digital Assets & Web3 CFO. Her words highlight the fast pace and complexity of the Web3 industry.

In addition to the challenges of having to get up to speed about crypto, DeFi and other blockchain technologies, over 48% of CFOs at Web3 organizations said they did not have formal on-boarding processes when they started in their roles (Fig. 3)

"It was all self-taught" said one CFO. "Years of nail-biting trial and error", said another in an interview.

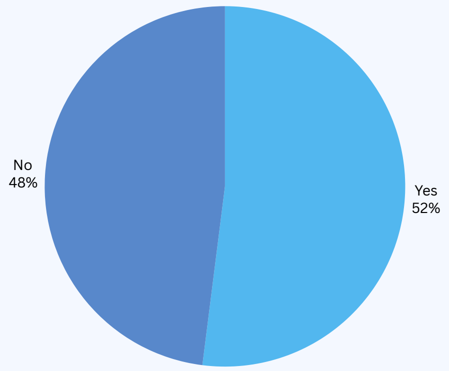


Fig 3. - Did you have any formal on-boarding process, or orientation as a Web3 CFO when you started your role?

"Taking a crypto accounting course is a solid start, but it's not some magic shortcut. You've got to put in the hours, get comfortable with block explorers, and make friends with sub-ledgers."

- Umar, CEO and founder, The Accountant Quits

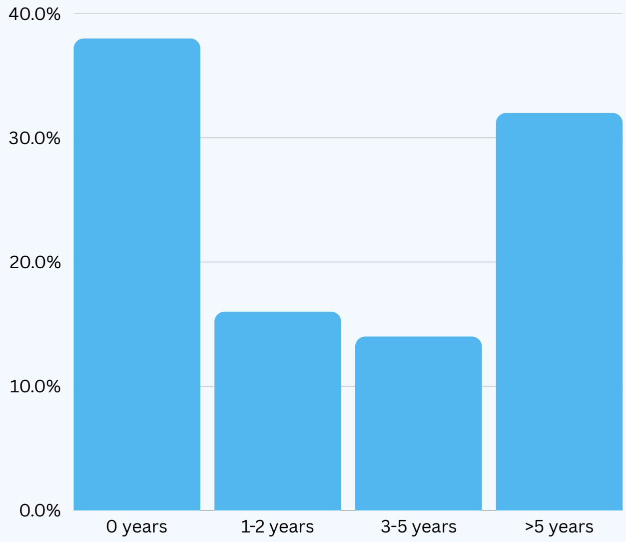


Fig 4. - How many years of experience did you have in a finance, accounting, or audit role prior to working in Web3?

Most Web3 CFOs are hired based on their experience in traditional finance or accounting roles (Fig. 4).

Nearly 54% indicated that they had some prior experience, while 46% had more than 3 years of experience in a finance role before joining a Web3 organization.

The gulf between the norms, concepts, and practices in traditional finance and blockchain is also a source of friction when working with external partners like accountants and auditors.

"People who know Web3 ... hardly know finance, and vice versa", explained Modesta Masoit, ex-finance director at DappRadar.

There may be considerable demand for **greater education around Web3 among traditional accounting, tax, and audit professionals**.

Those who understand the technology will be better positioned to serve a growing segment of crypto-native clients.

2. LACK OF TOOLING

FinOps tooling in Web3 represents a tremendously underserved SaaS category, and many CFOs were familiar with it in previous roles outside of crypto.

When asked about the availability of FinOps tooling, over 41% of Web3 CFOs polled said it was "insufficient" compared to Web2 (Fig. 5).

In the survey comments, one CFO wrote, "Software is not perfect yet, but it has huge potential. "

"Together with AI, Blockchain will make accounting so smooth we will forget it ever existed"

"Crypto is changing the rules of accounting and ERPs don’t seem to see it coming."

"Onchain data retrieval still sucks sometimes."

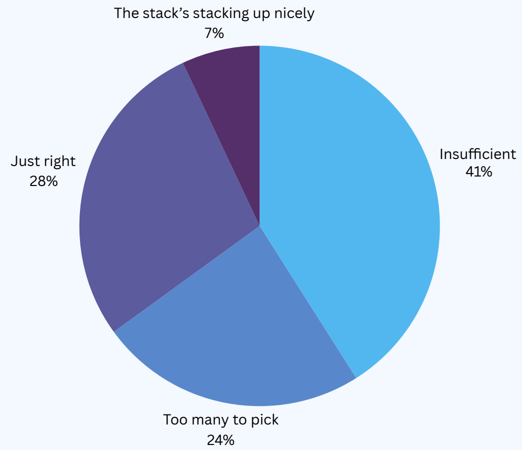


Fig 5. - How would you rate the availability of tools in the Web3 CFO's FinOps stack compared to Web2?

Yet, traditional accounting software cannot meet the needs of the Web3 CFO.

There is **an urgent need for more crypto-native accounting tools** to pull and label data from various blockchain networks for financial reporting purposes.

The demand for no-code blockchain analytics tools was also a key issue highlighted.

Despite the existence of platforms like Dune Analytics, writing specific queries to meet the crypto accounting needs of CFOs still requires programming languages like SQL.

Few CFOs have the technical know-how or the time to create customized reporting tools in-house.

The lack of appropriate tooling has led many Web3 CFOs to fall back on familiar but painstaking manual reconciliations on spreadsheets and using macros and pivot tables for financial reporting in crypto.

CHAPTER 2.0

Roles & Responsibilities

Defining your role is an exercise in thinking about what the most important activities are, and how you can add value in those domains.

Roles & Responsibilities of a Web3 CFO

As a CFO at an innovative hybrid company, DAO, or Foundation, you are at a time of tremendous opportunity. **Defining your role is an ongoing exercise** in thinking about the most important activities and how you can add value in those domains.

Your role spans three domains: operations, compliance, and strategy.

1. OPERATIONS

In the operational domain, the finance function ensures that ongoing operations run effectively; **in support of other business functions** such as paying talent, or processing (and limiting) expenses incurred by the sales & marketing team.

2. COMPLIANCE

There is also a renewed focus on the role that CFOs can play to provide visibility into an organization's financial health, and assurance to stakeholders by ensuring **compliance with tax, accounting, and other regulatory requirements**.

FinOps tools in Web3 like Request Finance can help CFOs to shape the way businesses manage their money by automating, and optimizing existing workflows while giving the entire organization a real-time view of their financial health.

3. STRATEGY

Yet, your role can also be strategic: **exploring pathways to profitability, generating measurable value, and establishing or improving critical processes**. While the operational role is an important one, CFOs are no longer relegated to merely supporting the company's operations, or controlling costs. Indeed, over the last few years, the CFO role has become increasingly strategic, thanks to the introduction of novel financial technologies.

There has been considerable excitement around how companies can offer "embedded finance" services within their own platform. The range of novel financial services and instruments is endless.

Empowered with new Web3 primitives, CFOs can also drive significant revenues with various yield-bearing treasury management instruments, open up new revenue streams and customer engagement touchpoints with NFTs, or help increase customer retention with novel payment tools.

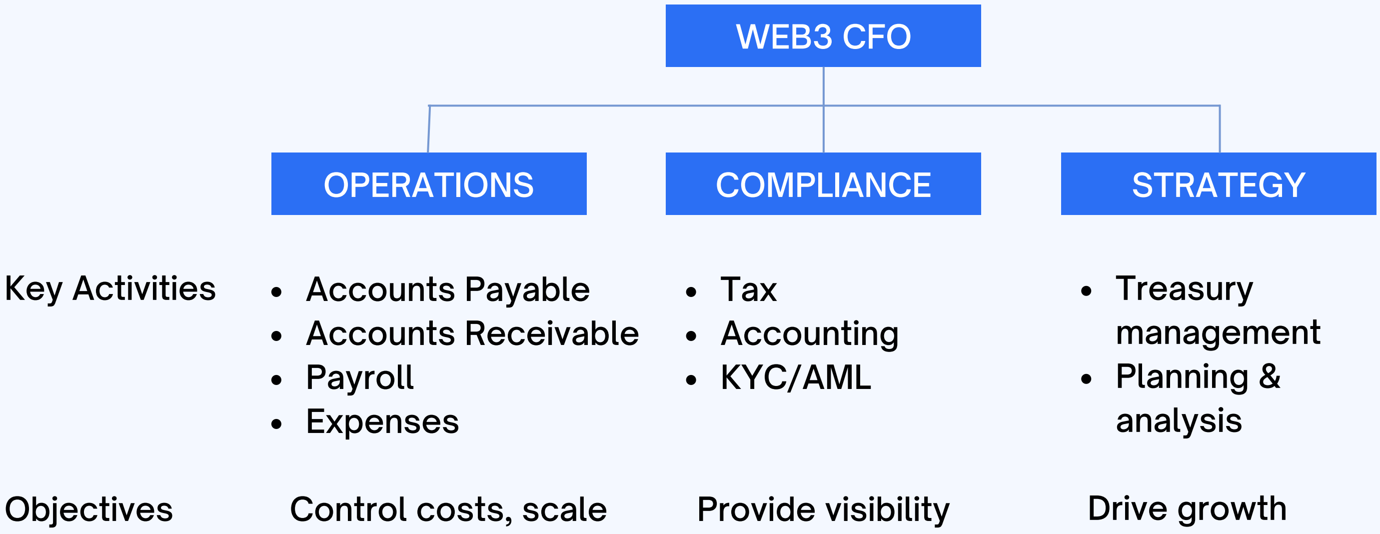


Fig. 6. - Overview of a Web3 CFO's Roles & Responsibilities

Web3 organizations deserve and need better software tools to help finance and operations teams manage their day-to-day finance workflows. **Automating repetitive processes like payments and integrating with other applications** is key to simplifying FinOps for Web3 teams.

These tools can also empower CFOs to add strategic value through better visualization and reporting of the organization's crypto asset values, and cash flows across different chains, token types, and platforms.

Blockchain technologies can allow every Web3 organization to have the transparency of a publicly listed company—in some ways even more so—with the ability to monitor finances or mark assets to market values in real-time rather than quarterly.

As better tools and processes emerge, Web3 organizations can distinguish themselves not only based on other business fundamentals but also on how well their financial operations are run.

Despite the challenges facing Web3 CFOs, many remained optimistic about the **growing need for more finance professionals in the blockchain space**.

64% of Web3 CFOs estimate that the demand for finance, accounting, tax, and audit professionals will grow over the next 12-24 months (Fig. 7).

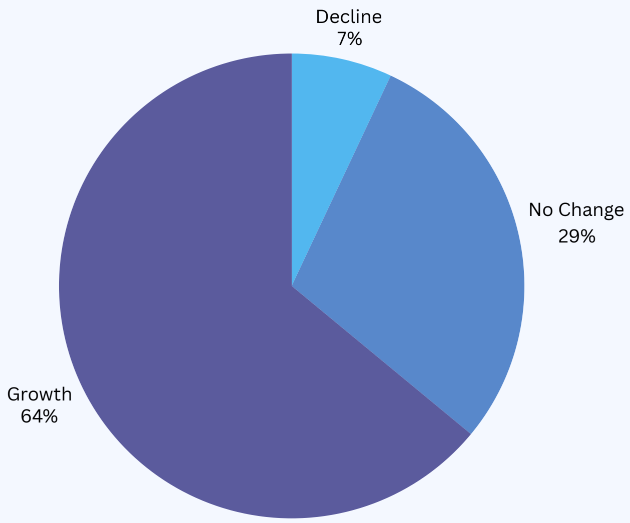


Fig 7. - How do you foresee the demand for finance, accounting, tax and audit professionals in Web3 over the next 12-24 months?

Bullish. 📈🐂

CHAPTER 3.0

Crypto Wallets & Custody

Understanding wallets, their different strengths and limitations, is key to managing your team's crypto assets.

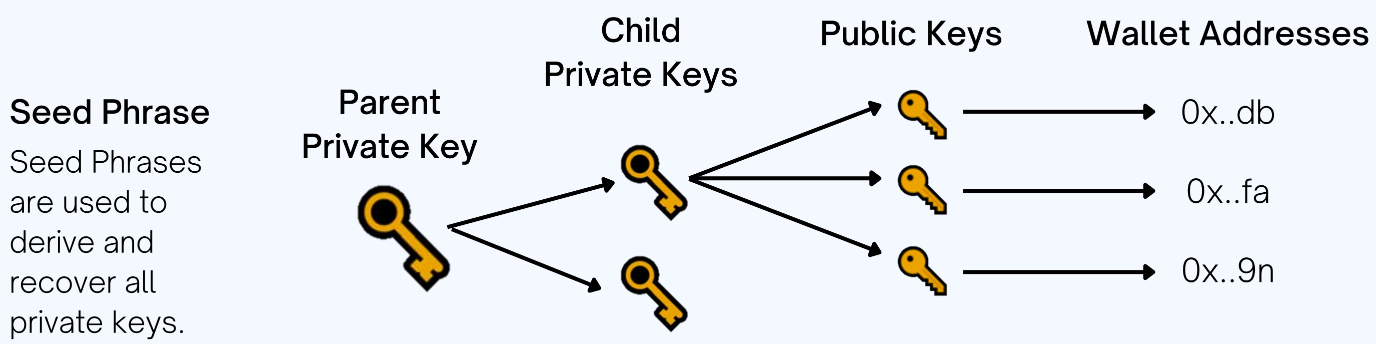
Crypto Wallets & Custody

CRYPTO WALLETS, KEYS, & ADDRESSES

Wallets and keys are **the crypto equivalent of bank vaults** - where your funds cannot be moved without your consent. Understanding them is key to managing your team's crypto assets.

- **Crypto wallets** are software programs that store private and public keys, which are used to send and receive cryptocurrency respectively. Unlike regular wallets, your crypto always lives on the blockchain, which is a digital ledger that records transactions, and account balances.
- **Public keys and wallet addresses** are like bank account numbers, or wire transfer instructions you can share publicly to receive deposits.
- **Private keys** are like authorized signatures that allow you to send and withdraw money. They are used to "sign", or authenticate blockchain transactions. Crypto wallets use a seed/recovery/backup phrase to algorithmically create private keys. They must be safeguarded at all costs. Each seed phrase can also be used to generate multiple wallet addresses linked to it.

HIERARCHICAL DETERMINISTIC (HD) WALLETS



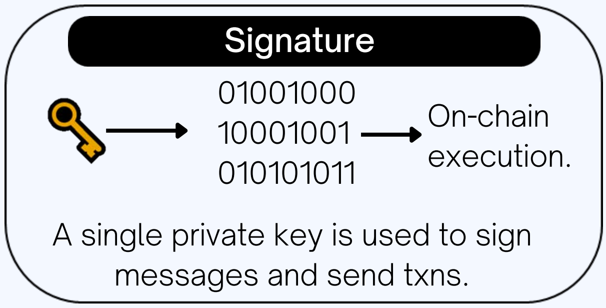


Fig 8. - Visualizing the relationship between seed phrases, private keys, public keys and wallet addresses

TYPES OF CRYPTO WALLETS

There are different types of crypto wallets. Each has its own advantages and disadvantages, allowing them to **play different roles, and meet different needs** in your crypto FinOps.

While most CFOs already likely have existing wallets in use at their organization, this section can still be relevant.

Understanding different wallets can help you **evaluate whether your organization's current crypto wallets are being used in a way that is fit-for-purpose**. For instance, if your company's entire annual payroll is being held on an centralized exchange's hot wallet, you may want to rethink that practice. "We've always done it this way" is a poor reason to maintain an existing process.

Here, we map out what we consider to be the most crucial distinctions between wallet types that you should consider when choosing to adopt wallets for your Web3 organization's needs.

IS IT CONNECTED TO THE INTERNET?

YES	NO

HOT WALLET 🔥

Hot wallets are convenient because they allow you to quickly and easily access your coins. Rabby and Metamask are often used as hot wallets.

They are the most common type of wallet and are ideal for storing "petty cash" in crypto, trading on exchanges, and interacting with dApps.

However, they are also more vulnerable to hacking because they are connected to the internet.

COLD WALLET 🧊

Cold wallets are more secure, but they are not as convenient because you cannot access your coins as quickly.

The most common type of cold wallet is a hardware wallet, a physical device that stores your crypto keys. Hardware wallets are best treated as safe deposit vaults, used to secure undeployed assets.

Hardware wallets are very secure because they are not connected to the internet and are difficult to physically tamper with.

HYBRID WALLET 🔥 🧊

Several crypto wallet providers aim to give organizations the security of a hardware wallet, with the convenience of hot wallets connected to the internet.

For example, Ledger Enterprise stores your sensitive data, including your private key and governance rules, in Hardware Security Modules (HSM), enabling a hot/cold setup.

An HSM is a physical computing device purpose-built for secure key storage and cryptoprocessing.

Signing transactions can be made with keys while the keys reside within the secure hardware environment.

The transactions are verified using Personal Security Devices (PSD) like a bank account token and signed by the Hardware Security Module (HSM) before being broadcast to the blockchain.

HSM-based wallets like Ledger or Trezor can be connected to a network or used in offline mode to protect wallets that are completely disconnected from the internet.

As we will explore later in the Guide, the risk of signing a smart contract is that it could interact maliciously with the content of your wallet.

Hybrid wallets can allow CFOs to determine whether a specific wallet address will be cold by deciding whether you will use it to sign transactions.

Organizational-grade solutions like the Ledger Enterprise also typically provide a SaaS-like platform.

This allows globally distributed teams to operate from anywhere in the world and to automate operations using APIs that connect to a variety of third-party dApps and DeFi platforms.

"Working in finance within Web3 is both rewarding and challenging—crafting new frameworks, managing complex crypto ecosystems, and implementing best-in-class practices to bring structure to a rapidly evolving industry."

- Daniel Adler, Founder, Cryptocurrency Jobs

WHO CONTROLS THE PRIVATE KEYS?

JUST ME

SELF-CUSTODIAL 👑

You have complete control over your assets when you own and manage your private keys.

This is like keeping cash in a safe deposit box in your home.

However, that is not to say that there are no risks! You rely on your home's security systems or the design of the safe deposit box. The Request Finance blog has a detailed comparison of self-custodial wallets.

NOT ME

CUSTODIAL ⛓️

You are depositing funds into a crypto wallet whose private keys do not belong to you.

In effect, the institution that controls the private keys to the wallet is either acting as a trustee or a borrower. The former cannot do anything with your assets except as instructed; the latter can.

In many cases, a custodian may claim to be a trustee but, in fact, is fraudulently using your assets in violation of that trust.

ME & OTHERS

MULTI-SIG, OR MPC 🤝

Multi-signature (multi-sig) wallets use different signatures generated by several private keys to sign transactions, like nuclear submarine missile launches in the movies, which require different keys held by different officers. Safe and Squads are the multisigs people are used to. 🔑 🔑 🔑

Multi-party computation (MPC) 🔑 -> 🧩🧩🧩 wallets split a single private key into multiple shards or shares—like a jigsaw puzzle, split among authorized signatories. Fireblocks provides an MPC wallet.

Note: Multi-sig or MPC wallets are not always self-custodial. Custody is shared because the keys or key shards are not always owned by you alone.

Crypto custody is not a binary choice between self-custody or completely relegating control to a third-party custodian.

Rather, custody of your crypto assets should be seen as **a spectrum consisting of both (i) who and (ii) how many people control access** to a wallet.

MPC vs Multi-sig

A multi-sig or MPC wallet will likely represent **most organizations' best tradeoff between security and usability**.

How can CFOs decide between a multi-sig or MPC wallet? A blog article by Nichanan Kesonpat for the 1kxnetwork provides a more detailed discussion of the technically adroit CFO.

But for those who want the TL;DR - here is a practical summary of some key differences between the two types of wallets:

PROS 👍

MPC

👍 **No single point of failure.** A whole private key is never concentrated on one device at any time. There is also no seed phrase.

👍 **Adjustable signing schemes**. Organizations can dynamically adjust approval signing schemes while maintaining the same wallet address. Just like changing the authorized signatories on a corporate bank account without changing the account number.

👍 **Granular Access Controls**. Organizations can assign an unlimited number of transaction approvers to a policy and delegate permissions that reflect organizational roles and security measures (timelocks, multi-factor authentication, fraud monitoring).

👍 **Lower Transaction Costs.** MPC wallets are represented on the blockchain as a single address, for which gas costs are the same as regular private key addresses. This can be important for users who have hundreds of transactions per day.

MULTI-SIG

👍 **No single point of failure**. Multiple signatures are needed to execute a transaction.

👍 **Upgradable signing schemes.** Can change their signature scheme to more gas efficient, or quantum-resistant ones. They can also use secure enclaves on iOS and Android devices, turning phones into hardware wallets.

👍 **Programmable Access Controls**. Users can define policies, set timelocks, spending limits, and automation (harvest farming rewards, limit orders).

👍 **Extensible.** Thanks to the composability of smart contracts, wallet developers can create an app store for new features like NFT lending frameworks, DAO voting modules, and DeFi asset management services.

👍 **Programmable Recovery.** Wallets can offer several options to recover funds into the smart contract itself, such as account abstraction, social recovery, or deadman switches.

PROS 👍

MPC

👍 **Blockchain Agnostic.** Key generation and signing relies on off-chain cryptography. Extending compatibility to new blockchains is straightforward as the wallet needs to be able to generate signatures using the algorithm recognized by that chain.

MULTI-SIG

👍 **On-Chain Accountability.** On-chain signature authorization policies explicitly state which keys were used to sign a transaction, making operations more transparent and straightforward to audit if something goes wrong. MPC signing happens off-chain. Safe (multi-chain) and Squads (Solana) have been helpful so far.

CONS 👎

MPC

👎 **Off-Chain Accountability.** Signing authorization policies and approvals are managed off-chain, so these custom rules are still subject to centralized failures. Off-chain rules and signing hinder transparency and call for more rigorous operational audits.

👎 **Incompatible with most conventional wallets** like Ledger and Trezor as there is no seed phrase or whole private keys stored on a single device, but MPC hardware wallet options like Cypherock are available.

👎 **Mostly siloed, bespoke products**. Many MPC libraries and solutions are not open-source, so there is no easy way for the ecosystem to independently audit and integrate them or conduct post-mortems if something goes wrong.

MULTI-SIG

👎 **Higher transaction fees.** Smart contract wallets charge higher fees than regular, single-address transactions because multiple signatures need to be verified. Actions such as adding/removing owners and changing the threshold also require an on-chain transaction.

👎 **Not universally supported.** While smart wallets can deploy on any EVM chain at the same address, they need bespoke implementation on non-EVM chains.

👎 **Incompatible with non-upgradeable contracts.** While EIP-1271 allows applications to sign on behalf of contract wallets, it is still not universally supported and cannot be added to non-upgradeable contracts.

Evaluating crypto wallets

With hundreds of options available, it can be challenging to know which crypto wallet is right for you. As a CFO, the stakes are even higher. You need to be sure that you're choosing a wallet setup that will protect your company's crypto assets and give you the peace of mind you need to focus on your job.

To help you cut through the noise, you must first understand what's important to you before looking at how the different wallet types map to those needs. It's important to remember that you can **use different wallets to meet different needs**.

When choosing a crypto wallet, consider the following factors:

1. SECURITY 🔒

Security is paramount when choosing wallets. This includes who controls your private keys and how transactions are approved, which affects your ability as a CFO to implement **access control management, spending policies, limits, and permissions**.

Other security measures in a crypto wallet include fraud detection and prevention features, two-factor authentication (2FA), or seed phrase recovery.

A wallet's track record, including time in the market or previous security breaches or hacks, should also be noted.

2. CHAINS ⛓️ & TOKENS 💰 SUPPORTED

The wallets you choose should **support a wide range of blockchain networks and token types,** such as non-fungible tokens (NFTs). The more extensive the support for different chains and currencies, the simpler your organization's wallet management will be.

3. ADDITIONAL FEATURES 💪

Wallets increasingly offer additional features to increase usability, including converting or "swapping" token types within the wallet, offering native staking, or other features like making batch payments.

These features should help to **simplify and automate your FinOps processes** in crypto.

4. COST & FEES 💸

Depending on which wallets you use, users are charged **one-time upfront costs or ongoing fees**. Hardware wallets typically only have upfront costs. Custodial or multi-sig wallets may charge ongoing fees for custody, on/off ramp fees, transaction fees, conversion fees, and staking fees.

5. PRIVACY 🤫

Privacy is slightly contentious, especially after the US Treasury's sanctions on the popular cryptocurrency mixer Tornado Cash. However, there are legitimate reasons why CFOs may want to have optional privacy-preserving transactions, like when making payroll.

Web3 CFOs need to **balance privacy with compliance with accounting and financial reporting requirements.** This can be challenging, as privacy-preserving crypto payments may make it more difficult to track and report on financial transactions.

This may involve **using specialized privacy-preserving apps while implementing strict internal controls and processes** to ensure that their organizations can support privacy-preserving crypto payments while meeting their financial reporting obligations.

Here's a handy checklist for CFOs to use when evaluating crypto wallets:

CUSTODY

- Where are my private keys / key shares / key shards? Who will own them?
- What percentage of my private keys or key shards do I control?
- Can I have instant access to my assets and execute transactions anytime, anywhere?
- Do I have a robust recovery protocol?
- Is the governance engine secure? How?
- What happens if the service provider stops operating?
- What happens if servers are down?
- Have industry security experts audited the technology provider?

Managing crypto wallets

Tools are only as good as their users. The most sophisticated kitchen stocked with top-of-the-line equipment and the finest ingredients is unlikely to produce the same food quality when staffed with part-time, fast-food fry cooks.

Crypto CFOs would know more than just what types of crypto wallets there are; they would also know how to **use them in a fit-for-purpose manner**.

Regardless of which crypto wallets you choose to use, here are six universal best practices that you can consider implementing at your organization:

BEST PRACTICES

1. ALWAYS HOLD MOST ASSETS IN SELF-CUSTODY 👑

Self-custody means survival. When you deposit assets into wallets like a centralized exchange, they have complete access to and control your private keys and funds.

Remember: **deposits are liabilities owed to depositors**. The balance shown on your deposit account with any institution or platform is merely a reflection of the outstanding debts owed to you, not monies you actually have control over or assets held in reserve. Debts are promises to repay, and promises are easily broken.

Third-party custody exposes your organization to **serious counterparty risks**. Such risks include, but are not limited to:

- Halting or limiting withdrawals due to solvency or liquidity issues,
- Freezing of funds pursuant to law enforcement actions or court injunctions,
- Hacks by external actors or malicious insiders.

Such events may negatively impact your organization's cash flows or, worse still - hit the balance sheet if the **funds are unrecoverable or uneconomical to recover via litigation**. In a memo circulated to the British War Cabinet in 1945, economist John Maynard Keynes wrote: "Owe your banker £1,000 and you are at his mercy; owe him £1 million and the position is reversed". To this, we might add, "But if your bank owes someone else £10 billion - you are all kaput".

OPERATIONS

- Does the solution support the blockchains and tokens I want to use?
- Are there transfers/transaction limits or minimums?
- Are there fees involved?
- Does my setup scale across teams and projects?
- How can I connect my accounts to my backend systems?
- How can I automate my workflow to be more efficient?
- Do I have access to Web3 use cases (NFTs, DeFi, staking)?
- Can I implement privacy-preserving solutions?

GOVERNANCE

- What are the different user roles, and how do they interact?
- What are my teams and my back office allowed to do?
- Who has access to what?
- How can I prevent internal collusion?
- Can I create and manage whitelists?
- Can I implement governance policies and user access rules when I want? How long does it take?
- Can I choose who will be involved in the approval process for all transactions?

FINANCIAL REPORTING & COMPLIANCE

- How can I track my administrator and operator activities?
- How can I meet financial reporting and other audit requirements?
- Is the technology recognized and approved by regulators?
- Can I collect data from various chains and token types easily and with clarity?

“Safe is securing more of the crypto ecosystem than ever with $100B in assets stored across millions of smart accounts.”

Lukas Schor, Co-founder at Safe

Each time a centralized exchange (CEX) or centralized finance (CeFi) lending platform runs into financial trouble; it brings down all the fund managers, companies, and employees whose crypto assets are stored in their custodial wallets.

In contrast, despite the string of collapsed CeFi platforms in 2022, including Celsius, Hodlnaut, FTX, and DCG, virtually none of the over 2,300 teams using Request Finance at the time were materially impacted.

This is thanks to the fact that **using decentralized apps (dApps) like Request Finance requires you to use your own self-custodial wallet**. That means there can never be paused withdrawals, or frozen funds - ever.

Money is to organizations what blood is to our bodies. Its circulation maintains the essential functions that keep us alive and healthy. Deprived of it, irreparable damage and death follow quickly.

2. USE DIFFERENT CRYPTO WALLETS FOR DIFFERENT PURPOSES 👛

It is possible to generate multiple wallet addresses linked to the same seed phrase and private key. That would be like having several bank accounts with the exact same login details. But this is not always ideal, particularly when it comes to resilience to hacks or implementing access controls.

Dividing up the company's assets into **multiple crypto wallets with different seed phrases** is ideal for three reasons:

1. CLARITY

Your company's monies serve different functions: the revenue you bring in, the money that goes out to pay the bills, and the retained earnings you set aside to be invested externally or to grow the business.

Lumping it all together in one wallet can make it difficult to monitor your organization's crypto finances.

Consider maintaining **at least three crypto wallets**: one for receiving payments, another for paying expenses, and a third wallet that acts like a savings account (Fig. 9 below).

2. CONTROLS

Having different crypto wallets with different private keys helps you implement proper financial controls in your organization.

There are numerous case studies of criminal breaches of trust by rogue employees absconding with funds.

Financial controls are crucial for crypto companies. In the words of the American rapper, Kanye West, "**no one man should have all that power**".

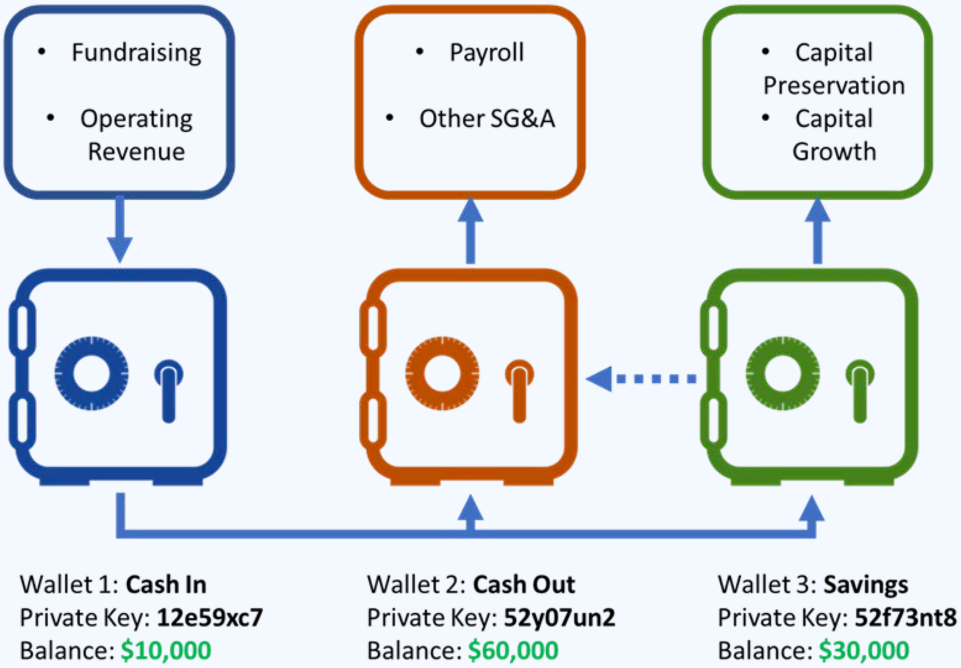


Fig 9. - Example illustrating $100,000 in crypto, held across different wallets,. Arrows show flows of funds between, and in and out of wallets.

This makes it easier to track cash flows, which is useful data when preparing financial statements or planning for the future.

To report your crypto holdings to tax agencies, it is critical to **have separate crypto wallets for each taxable entity**.

It is common for organizations to have more than one operating entity. For instance, Protocol Labs is a research, development, and deployment laboratory that spins off independent projects, including IPFS, Filecoin, libp2p, and many more.

Avoid commingling funds and transaction flows between different entities to simplify your financial reporting in crypto.

3. SECURITY

Over the years, billions of dollars in crypto have been lost to hacks due to insecure crypto wallet management.

In 2024, stolen crypto funds spiked by approximately 21% year-over-year (YoY) to reach a volume of $2.2 billion. Many victims had their hot wallet funds stolen.

Someone may be hacking your device, communication software, or crypto exchange to obtain your wallet's private keys.

A person with your private keys can drain your company's funds. If your seed phrase becomes somehow compromised, **all the wallet addresses generated using that seed phrase are compromised**. (Fig 10 below)

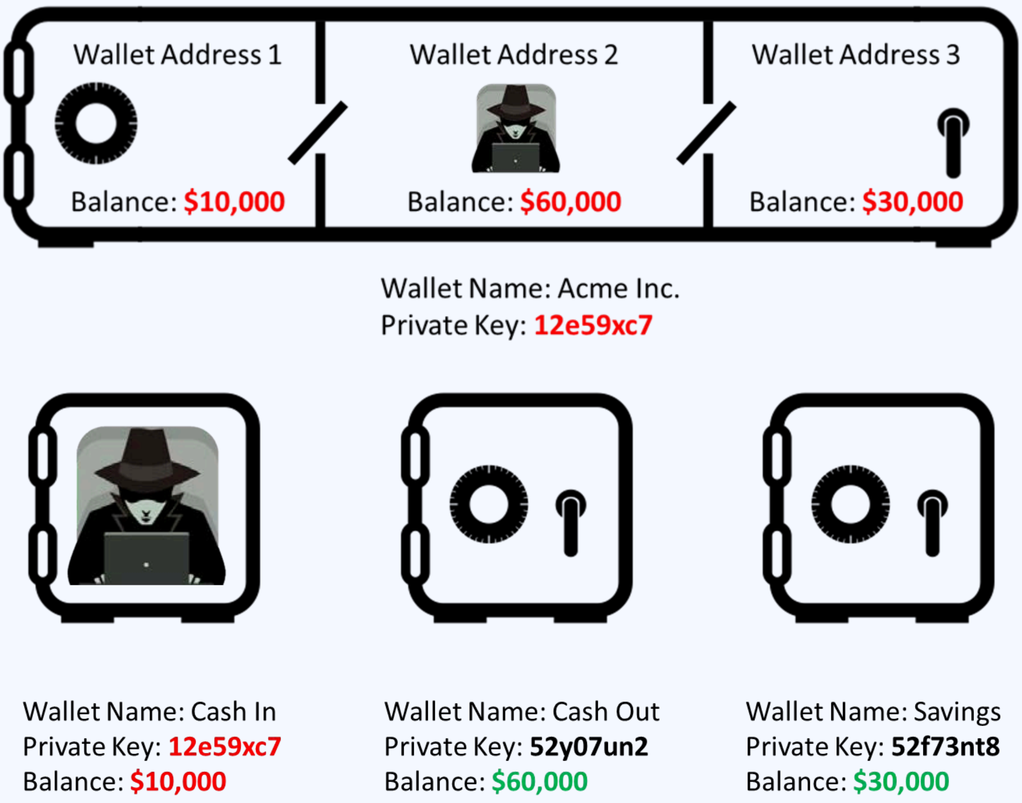


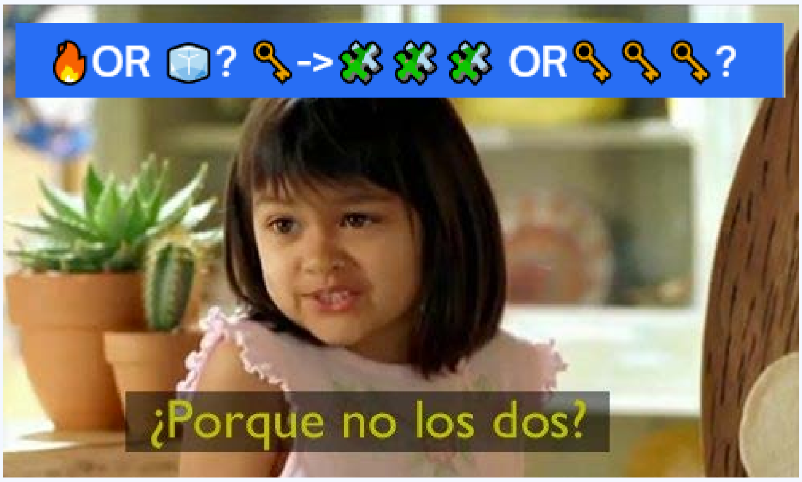
Fig 10. - Assets secured by more private keys means greater security.

Diversification is critical in managing your organization's investment portfolio and storing your company's crypto inventory. Never put all your eggs in one basket.

Limiting the amount of funds stored in any wallet **limits the damage any hack can have on your company's overall crypto inventory**.

3. USE A MIX OF WALLET TYPES 👨‍🍳

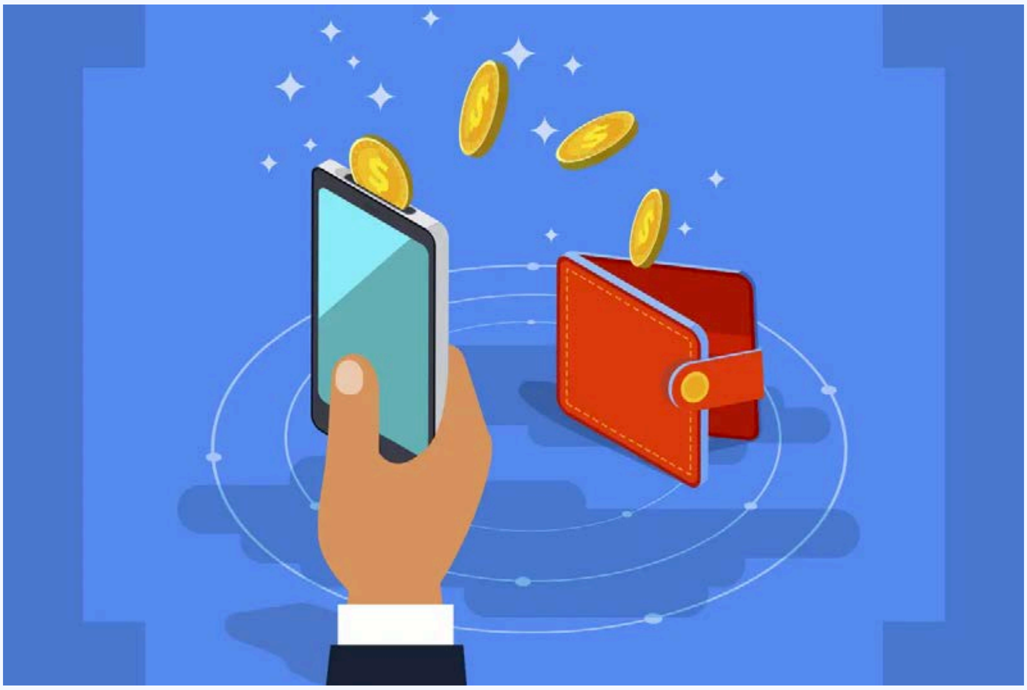
CFOs may understandably find themselves struggling to pick between the different wallet types. To borrow the famous Spanish quip from a 2005 TV taco commercial: "Porque no los dos?" (Why not both?).



Both hot and cold wallets have strengths and weaknesses that can complement each other. So why not use both hot and cold wallets in your organizational setup? Cold wallets are the equivalent of a safe vault at the bank or the company's office. Hot wallets are the equivalents of petty cash in your wallet. You likely already have both. The same could well apply to the wallets you choose to manage your organization's crypto treasury.

Given the trade-offs when using either type of crypto wallet, **a combination of cold and hot wallets is usually ideal**. This allows you to have the accessibility of a hot wallet for processing accounts payable and the peace of mind and security of a cold wallet to safeguard the dormant portion of your crypto treasury. Each crypto wallet can be designated for a specific purpose, optimizing for either ease of use or security depending on the specific use case for a wallet.

Similarly, when choosing between a multi-sig or MPC wallet, if costs permit and there are compelling operational reasons to justify the use of both, CFOs can consider **experimenting with different wallet technologies**.



The cryptocurrency management trilemma can be characterized as the challenge of solving for **Security, Usability, and Accountability.** An organization's treasury must be stored and managed to achieve all three key attributes, often in conflict.

There is no such thing as a perfect wallet, even though some may appear to come close. What CFOs could do is maintain a combination of wallet types that, as a system, optimizes for all three attributes as much as possible. More important than just the crypto wallets you pick are **the processes and controls that you put in place** at your organization.

4: HAVE A CLEAR SYSTEM FOR MANAGING YOUR ORGANIZATION'S CRYPTO WALLETS 🧑‍💻

1. DOCUMENTATION

Have clear oversight of your organization's wallets. Setting up multiple crypto wallets is easy. It can simplify your financial reporting and safeguard your crypto assets.

The problem is that even some of the largest crypto companies often neglect to maintain:

- a record of all their organization's wallets,
- the designation and purpose behind each wallet,
- each wallet's authorized signatories, and
- a clear process for approving the adoption of new wallets

You can also consider maintaining a living document on your organization's knowledge management system (KMS) like a Notion page.

It should clearly define the existence and reason for each wallet, with its accompanying wallet address.

Especially for larger organizations which are subject to audit requirements, this is crucial for simplifying the financial reporting process.

2. APPROVALS

Have a clear process for approving new wallets. When reviewing requests for new wallets, ensure they meet your organization's custody, security, and workflow requirements.

Ask questions like:

- Why does this wallet need to exist?
- Who should have access to this wallet?
- What is the expected flow of funds into and out of this wallet?
- How should crypto transactions from this wallet be labeled in the organization's chart of accounts?

"Managing crypto wallets properly is key to keeping assets safe and simplifying reporting. At Powerhouse, we focus on tracking wallet use and access to keep things secure"

- Dracaena Magenta, CFO, Powerhouse

3. RELATED PARTIES

Map out risks among your authorized signatories and their wallets. Web3 organizations must strive to develop or employ solutions to mitigate conflicts of interest and key person risks and safeguard their community's assets.

A multi-sig or MPC wallet eliminates the risk of overreliance on any one individual. If one key holder tried to funnel the multi-sig wallet's assets to a personal account, other holders would presumably refuse to sign the transaction, thus nullifying the transaction and preserving the funds.

However, they remain **vulnerable to collusion among interested or related parties**.

The more independent private key signatures required, the more protected the multi-sig wallet is. MakerDAO (now "Sky"), for example, required a two-of-three multi-sig, which requires "a quorum of 2 to authorize any transaction like engaging in DAO swaps." MakerDAO identified the public key of each signatory for additional transparency.

The treasury is the beating heart of any organization. Left in the hands of bad actors, all its funds could be drained with a few clicks - leaving it with serious going concern issues.

You can never be too safe regarding safeguarding your crypto treasury and having controls for on-chain payment authorizations.

4. PORTFOLIOS

Using a portfolio tracker can help to keep track of your different crypto wallets, their balances and transaction flows across different blockchain networks.

Nothing is more frustrating for a crypto accountant than preparing financial reports only to find out they didn't see every wallet they needed.

With multiple wallets to manage, it is critical to **keep an eye on all the different account balances** and know where your crypto is coming from and going.

Portfolio trackers monitor the balances across different wallets that you own.

5. SECURELY MANAGE YOUR WALLETS' SEED PHRASES 🌱

With multiple wallets, comes the need to secure multiple seed recovery phrases. If those twelve words represent total control over your funds, how do you keep them safe and accessible at the same time?

There will always be **a tradeoff between security vs. convenience**. That balance is something that you must judge to be appropriate for your organization's size, and operational workflows.

1. ACCURACY

Record your seed phrase accurately. Ensure that you preserve their exact spelling, and the sequential order in which they were given.

Never change the order of the words, or their spelling (e.g. "color" =/= "colour").

2. SECURE STORAGE

Store your seed phrase somewhere safe. One very powerful way to secure a recovery phrase would be to split it between safe deposit boxes in multiple locations (making sure there's redundancy in case something were to happen to any of the locations). Obviously this is not very convenient.

Some people use specialized services like Cryptosteel to engrave recovery phrases into durable materials like stainless steel.

For many people, simply writing your recovery phrase down and keeping copies in more than one safe location is a solid approach.

Some services offer to store an encrypted version of your recovery phrase in the cloud like Google Drive or iCloud. You may also consider keeping a copy of your recovery phrase somewhere safely offline.

3. BROWSERS

Use different browsers. This option is as straightforward as it sounds: if you've only got two or three seed phrases to manage, then you can simply install your web wallets in several different browsers, and use a different browser for each one.

Given the open-source nature of the modern web, there's not a definitive listing of browsers that any given browser wallet will or won't work in.

4. BROWSER PROFILES

Use different browser profiles. The easiest way to manage multiple wallets is to use browser profiles. Common web browsers like Chrome have instructions available here, and the steps are fairly simple.

Now all that's left is to open a browser window in that new profile, install the browser wallet as you normally would, and follow their instructions to restore your wallet using your seed phrase–or create a new one.

This will allow you to juggle between wallets with ease, as you can have multiple browser windows open, each one in a different profile, at the same time.

5. DISK ENCRYPTION

Enable full-disk encryption. To keep your computer and its contents as safe as possible from someone with physical access to your machine (e.g. for technical support), we recommend you enable full disk encryption on your computer.

On a Mac this is the FileVault feature. On Windows, you can enable BitLocker.

With full disk encryption, an attacker with physical access to your computer should not be able to extract any of its contents, including any cryptocurrency keys you have stored throughout your disk, but also site passwords, banking info, and other sensitive information.

As long as you have your recovery phrase, you have your crypto. If you lose a hardware wallet on a bus or break a phone containing a software wallet, you haven't lost your crypto — you can simply enter your recovery phrase into another wallet.

"In the world of crypto, speed and adaptability are critical. Navigating challenges like regulatory uncertainty and evolving business models requires CFOs to think several steps ahead and always have plan A to Z."

- Ping Lai Tan, CFO - CAKE Group

6. OBSERVE CYBER HYGIENE 😷

Remember, no matter how robust the security systems designed by crypto wallet companies may be, your systems are only as safe as your people are.

1. SMART CONTRACTS

Avoid interacting with malware, or risky smart contracts. Smart contracts that have not been audited, or tested by time and use are vulnerable to hacks.

Any interaction with a blockchain via a smart contract requires the use of software clients, which are vulnerable to bugs, exploits, and malware.

Your development team must thoroughly understand the client-side architecture of the smart contract, so that any client-side risk can be minimized.

Not doing so can run the risk of not only a lapse in data security, but "mistakes" in the execution of the contract that can result in lost funds.

Implement **reasonable and necessary data security practices**. This should include basic practices like software updates, security vulnerability patch protocols, password and security access managers.

Additionally, you could also consider **ongoing operational intelligence** on the actual blockchain to avoid potential vulnerabilities.

2. PHISHING & FRAUD

Screen for scammers. That does not mean being paralyzed by paranoia, but treating every interaction with a healthy dose of skepticism - especially when payments, or disclosing sensitive information is required.

"Social engineering" attacks are often used to bypass sophisticated technical controls put in place. Instead of trying to pick a well-designed lock, hackers can simply **trick one of your organization's members into handing over the keys**.

While it sounds like a tired cliche from every movie jailbreak scene, hundreds of millions of dollars have been stolen from tech giants like Facebook and Google, large global banks like the Oversea-Chinese Banking Corporation (OCBC), and even United States' Government Agencies.

One of the most damaging forms of social engineering attacks is Business Email Compromise (BEC). According to the FBI's Internet Crime Complaint Center (IC3), more than $26 Billion was lost to BEC scams in the last four years despite making up only 7% of spear-phishing attacks.

BEC is a specific type of phishing that relies on social engineering to trick people by **impersonating an authoritative figure within a company, or a trusted external partner**.

A common tactic is **fraudulent invoices**. Scammers pretend to be a vendor requesting payment for services performed for the company.

Often, this type of attack will masquerade as one of an organization's actual suppliers and use a realistic-looking invoice, but with the bank account details or crypto wallet address of the scammer.

The challenge with billing is that the team members who incur the bill, are typically not involved when the company's finance team reviews and pays invoices.

That makes it difficult for finance teams to verify if an invoice is legitimate or fraudulent, which ends up in legitimate bills not being paid on time, or worse - paying fraudulent invoices.

Shark Tank angel investor, Barbara Corcoran, once lost over $388,000 from invoice fraud. The fraudster used a spoofed email address to deceive Barbara's bookkeeper into wiring the money. The scam was discovered only when the bookkeeper copied Barbara's assistant in the reply email.

Scammers are also eager to target crypto payment apps without fraud detection tools.

To protect enterprise users from invoice fraud, Request Finance's crypto invoicing app allows you to require vendors to cc multiple people on invoices that you receive.

That way, your finance team can check with other team members on cc to ensure a legitimate bill. This should protect you from billing fraud while ensuring your company's bills are paid on time.

If you've been receiving unsolicited invoices that appear fraudulent, you can also block the issuer of those invoices.

Doing so will prevent them from sending you fraudulent invoices in the future. It also helps us identify suspicious issuers.

TIPS: If you are a CFO who cares about the safety of the company's funds, explore on-chain insurances like Opencover.
As for the whole company, train your colleagues using software like Riot.

"Offering financial guarantees to businesses that transact onchain is key to drive wider adoption. In the last few months, onchain insurance helped cover more than $100,000,000 in transactions for Request Finance clients"

- Jeremiah Smith, CEO at Opencover

CHAPTER 4.0

Fiat Banking

Going completely bankless is not always possible. Choosing a bank that can support your fiat payment needs is tough, but crucial.

Going bankless is hard

Someday, blockchain payment rails will dominate payments, stablecoins will have replaced fiat currencies, tradable assets will be tokenized, and decentralized finance platforms will stand where banks and other financial institutions once used to.

That day is not today.

The reality is that decentralized finance will continue to exist alongside its traditional counterparts for some time to come. Remember that the gold standard dominated global finance from around 1873 until the Nixon shock in 1971. That's nearly a century! Its predecessor, the silver standard, lasted even longer, starting with the Sumerians around 3000 BCE until 1873—nearly 4 872 years.

Today, traditional institutional investors who participate in your equity round may want to wire money in fiat. Your employees may prefer to receive a portion of their salaries directly in fiat currencies to meet daily expenses. You must purchase with merchants or vendors (normies) that only accept fiat.

If you are not powering your payments with a spend management app like Request Finance, choosing a bank that can support your fiat payment needs may be necessary.

BEST PRACTICES

The term “crypto-friendly” bank is somewhat of a misnomer. Few global banks today are truly friendly to crypto. This includes banks that may offer crypto custody or trading services in their private banking departments. And whenever a bank is known for being crypto-friendly, virality takes place until the bank’s compliance department limits the number of crypto clients.

Much of this has little to do with leadership attitudes and more with the risks or costs it imposes on banks’ ability to meet the regulatory requirements to keep their licenses.

This introduces serious challenges, and operational risks for your Web3 organization. However you choose to manage your organization’s fiat payment needs, here are three best practices to consider:

1. BANK USING SPECIAL PURPOSE ENTITIES 🏛️

Typically, when opening a corporate bank account, you must declare whether or not the business deals in cryptocurrencies. A declaration in the affirmative is highly likely to create problems, as Marc Andreessen explained on the Joe Rogan podcast and Qiao Wang at AllianceDao confirmed.

And, of course, making untruthful representations to your bank is inadvisable either. So, how do you navigate this conundrum if you cannot go completely bankless?

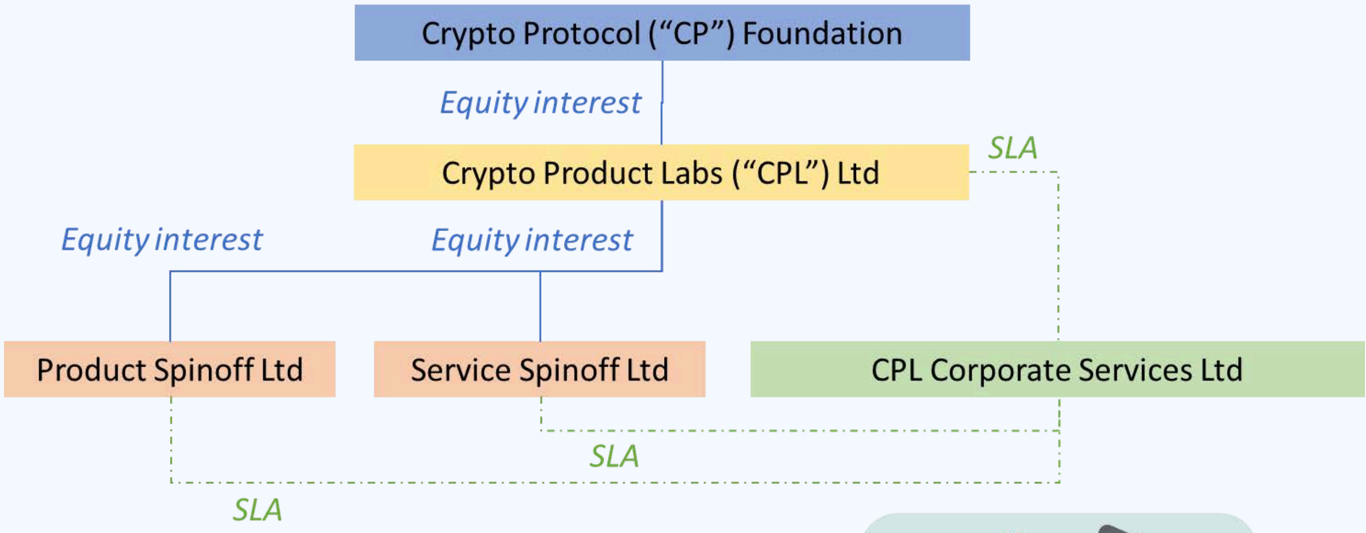
When speaking to CFOs of hybrid entities, we found that most had to **set up a bank account under a Special Purpose Entity (SPE) registered as a consulting or technology company**. This bank account serves their organization's fiat banking needs.

Consider the following hypothetical Web3 organizational chart, reminiscent of many others in the space (Fig. 11 below).

At the top is a non-profit foundation that manages the protocol layer. Below that is an affiliated or wholly-owned subsidiary that develops dApps or other spinoff technologies on top of the protocol.

CPL Corporate Services Ltd. could be a distinct SPE. It is not a subsidiary of any crypto-dealing companies. Instead, it can have **service-level agreements (SLAs) and covenants** with all the other entities in the chart.

Contracts with employees, service providers, or investors that wish to deal with the main organization in fiat can be either novated to or signed with this SPE instead.



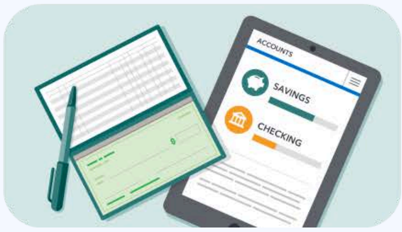


Fig 11. - Organizational chart of a typical Web3 group of companies

For example, employees wishing to work for CPL Ltd could be hired under the SPE, which has **an agreement to be an employer of record (EOR)** and manage payroll services for CPL Ltd.

This SPE could also have debt covenants extending interest-free credit lines to other entities, effectively allowing it to pay operating expenses in fiat, like cloud-hosting fees.

Note: seek advice from relevant Qualified Persons concerning your organizational structure and related matters like banking, trusts, subsidiaries, etc.

2. USE NEOBANKS & FINTECH BANKS

Smaller, regional, or local banks may be more open to onboarding companies that deal in crypto. However, these banks may have a more limited range of services that may hamper your banking needs. For instance, a smaller bank may not have convenient online banking services or may not support international payments.

Alternatively, you can consider **Non-Bank Financial Institutions (NBFIs) like fintech banks or neobanks** like Revolut. These companies tend to be more open to taking on risks that their banking partners or other traditional banks would ordinarily refuse to.

For instance, Aspire is a fintech platform based in Singapore. They help with the operating expenses of APAC web3 organizations, specifically their operating arm.

It is also worth noting that Siam Commercial Bank and DBS are well-established banks for crypto-related businesses.

However, fintechs and neobanks run on traditional banking rails, and are **subject to many of the same service limitations and failure points**. These include:

1. CENSORSHIP

Nobody cares about censorship - until they become its victims. In 2023, the CFPB (Consumer Financial Protection Bureau) received 2,941 complaints regarding bank account closures, marking a 50% increase from 2022 and nearly double that from 2020. Revolut withheld tens of thousands of dollars without explanation. Paypal and Venmo are also known for freezing accounts.

Many Non-Banking Financial Institutions (NBFIs) also consider crypto-related businesses high-risk. This is typically stated in their terms of service agreements, which are subject to change without prior notice.

For instance, in September 2023, Chase Bank announced that it would block all crypto-related payments for its UK customers, citing concerns over fraud and security.

Similarly, in 2024, HSBC Australia and Capitec Bank (South Africa) informed customers that they would block real-time payments to cryptocurrency exchanges to protect consumers from scams, citing anti-fraud measures.

These actions reflect a broader trend among banks to restrict or monitor cryptocurrency transactions due to fraud, security, and regulatory compliance concerns.

2. COST & SPEED

Fintech platforms ultimately rely on legacy banking rails and payment networks.

While they are quick to advertise low or no fees, what is hidden in the fine print is that:

- there are low holding and transfer limits on non-enterprise accounts
- currency conversion rates are poor, or
- same-day settlements for cross-border payments will typically be far more expensive than relying on crypto rails and other off-ramp methods (see the following section for more).

"The challenge of aligning a crypto startup's operations with a Belgian bank's stringent AML requirements often leads to delays and missed opportunities. Creating a dedicated framework for compliant crypto companies could alleviate these difficulties and promote growth in the Web3 sector."

- Koen Masschelein, Makofisc BV

3. SERVICE COVERAGE

Blockchain ledgers are born global; banking services are not. While many fintech platforms may serve most major currencies and markets, their coverage and penetration can vary considerably.

In contrast, when you use blockchain rails for payment, you will never need to ask: “Is it available in your country?”.

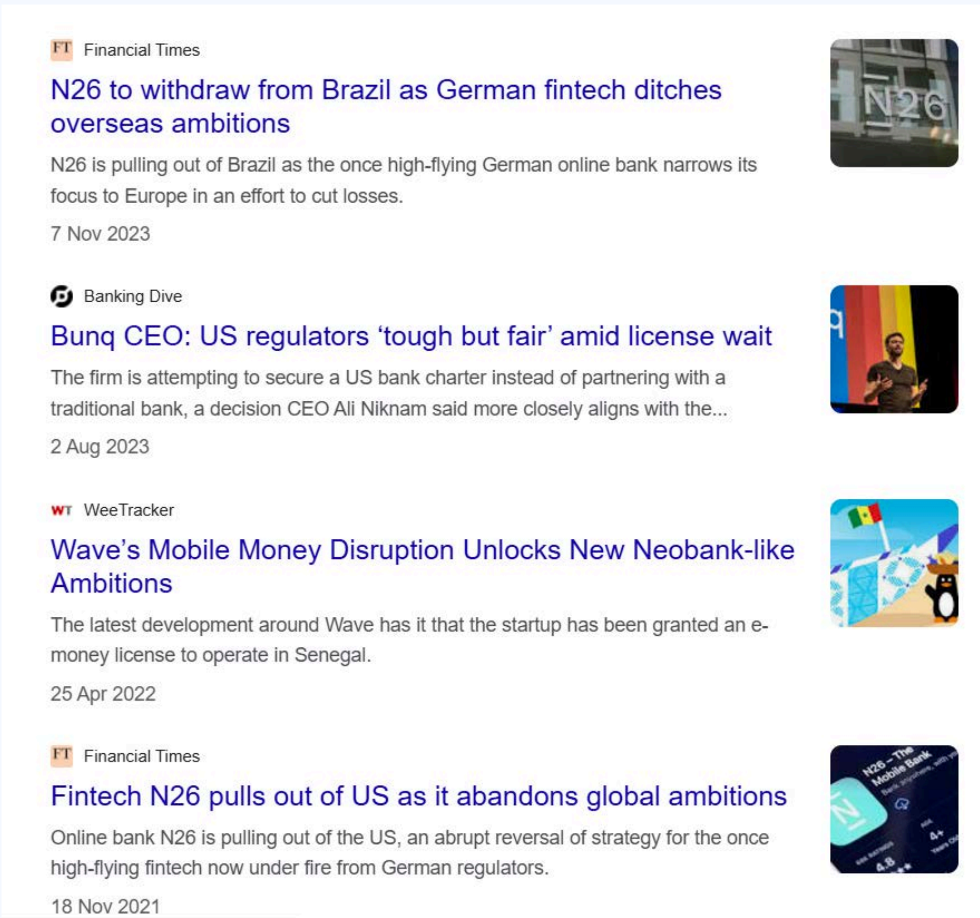
Fintech banks and payment processors have also **withdrawn service coverage from entire populations** after deciding that servicing a particular region or country is not economically viable (Fig. 12). These can be incredibly disruptive for businesses.

It is difficult to overstate the potential of having a borderless, programmable, internet-native financial system based on blockchain payment networks and DeFi versions of traditional financial institutions.

While the advent of mass adoption is still some time away, it is worth remembering that the internet transformed industries in ways people could not initially comprehend.

Famously, in 1995, Clifford Stoll, an American astrophysicist and tech pundit, scoffed at online courses, digital newspapers, and e-commerce.

As blockchain technologies mature and industry players focus on building useable platforms, we may someday look back on the skeptics in the same light as Clifford Stoll's greatest career *faux pas*.


Financial Times
N26 to withdraw from Brazil as German fintech ditches overseas ambitions
N26 is pulling out of Brazil as the once high-flying German online bank narrows its focus to Europe in an effort to cut losses.
7 Nov 2023

Banking Dive
Bunq CEO: US regulators ‘tough but fair’ amid license wait
The firm is attempting to secure a US bank charter instead of partnering with a traditional bank, a decision CEO Ali Niknam said more closely aligns with the...
2 Aug 2023

WeeTracker
Wave’s Mobile Money Disruption Unlocks New Neobank-like Ambitions
The latest development around Wave has it that the startup has been granted an e-money license to operate in Senegal.
25 Apr 2022

Financial Times
Fintech N26 pulls out of US as it abandons global ambitions
Online bank N26 is pulling out of the US, an abrupt reversal of strategy for the once high-flying fintech now under fire from German regulators.
18 Nov 2021

Fig 12. - Fintechs and neobanks can withdraw services abruptly

3. USE UNRELATED BANKING PROVIDERS 🧱

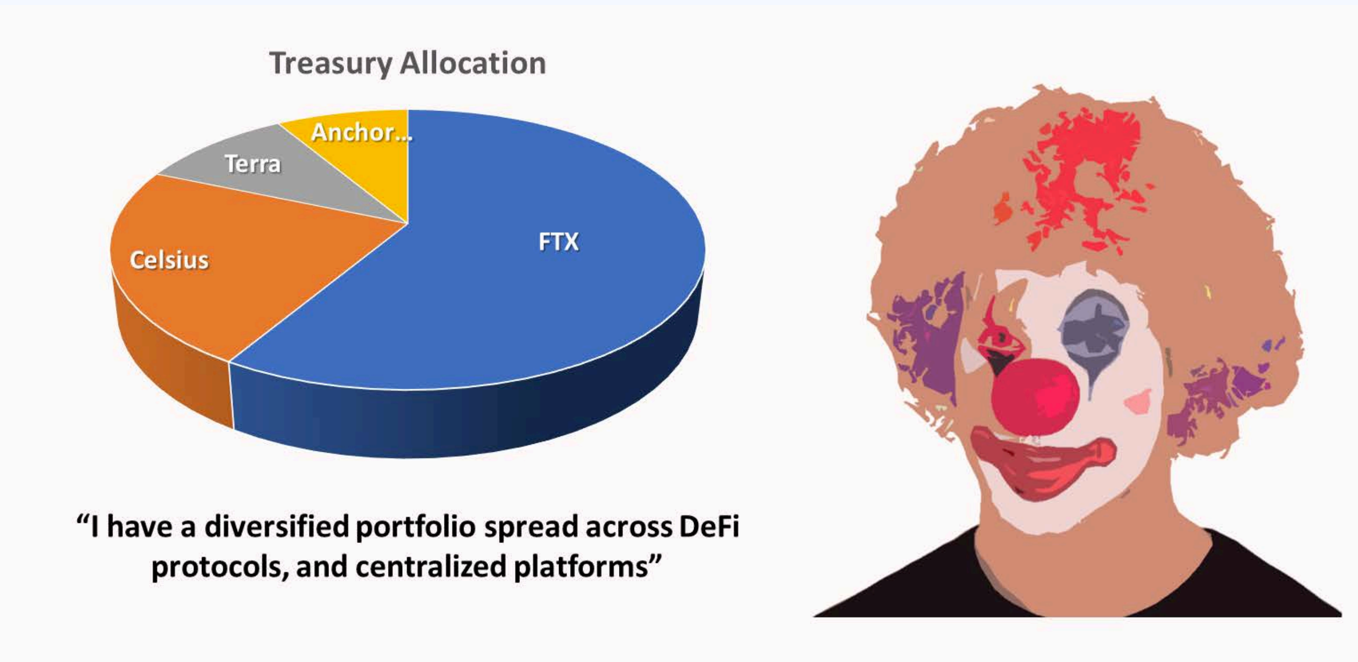
Just as it is prudent to diversify your company's crypto inventory across multiple crypto wallets, it would be similarly **wise to hold your company's fiat balances across multiple uncorrelated banking providers**.

It is important to ensure that your bank provider and NBFI are uncorrelated. What does that mean? <u>NBFIs, like neobanks, usually do not have their own banking licenses</u>. Rather, they act as user acquisition channel partners, akin to wholesale retailers to traditional banks.

So, for instance, if you already use Revolut in the United States, it would not diversify away your counterparty risk to use either Metropolitan Commercial Bank or Cross River Bank - both of whom are Revolut's local partners.

Diversification is about not having exposure to correlated risks. In practical terms, you should **ensure that your counterparties have little to no substantial dealings or linkages with one another**. The string of collapsing centralized crypto platforms exposed to contagion from the Terra/Luna implosion illustrates this well.

The insolvent, Singapore-based crypto lender Hodlnaut was placed under judicial management after reportedly losing $189.7 million in the collapse of the Terra ecosystem. When FTX collapsed, it resurfaced that Hodlnaut had consolidated over 71% of its assets on centralized exchanges, with $13.3 million being held on FTX, including bitcoin (BTC), ether (ETH), and stablecoins. **Once bitten, twice rekt**.



Check for linkages between your fiat banking services providers to diversify your risk of being de-banked in fiat. Should any of these NBFI banking services providers - or their core banking partners cut you off or go out of business, it must not dramatically impair your company's ability to conduct business operations involving fiat payments.

The fintech and banking landscape can change rapidly. Professional communities on Slack and Discord can help you access actionable intelligence from the experience of fellow web3 finance and operations professionals.

The web3 finance club is an exclusive, vetted community by crypto-friendly CFOs for crypto-friendly CFOs at a broad range of companies like The Sandbox, Decentraland, and Consensys in Web3, and also at Amazon and Adyen, for example.

"The challenge of aligning a crypto startup's operations with a Belgian bank's stringent AML requirements often leads to delays and missed opportunities. Creating a dedicated framework for compliant crypto companies could alleviate these difficulties and promote growth in the Web3 sector."

- Koen Masschelein, Makofisc BV

CHAPTER 5.0

On & Off Ramps

To move value between a crypto wallet and a bank account, or vice versa, you will have to rely on on and off ramps.

On & Off Ramps

In the first chapter, we discussed how and where to manage your company's crypto inventory via crypto wallets. In the second chapter, we addressed those same issues in fiat via banking services.

In this chapter, we address how exactly we can move value between decentralized finance and traditional finance.

How do you move money between crypto wallets and bank accounts? Notably, fiat on banking rails and crypto on blockchain networks live on entirely separate technology stacks. For now. Thus, fiat cannot easily be transferred into a blockchain wallet, and crypto cannot be stored in a bank account per se.

To move value between a crypto wallet and a bank account or vice versa, you will have to rely on on- and off-ramps.

On and off ramps, as their name suggests, are two sides of the same coin. On-ramps mean the exchange of fiat currencies for crypto. Off-ramps refer to the reverse: the exchange of crypto for fiat.

There are presently four primary means of doing so:

- **Centralized stablecoins.**
- **Decentralized stablecoins.**
- **Centralized exchanges.**
- **On/off ramp service providers.**

Let's examine each of these and what they are best suited for.

1. CENTRALIZED STABLECOINS

Stablecoins are cryptocurrencies with an exchange rate pegged to a fiat currency. USD-denominated stablecoins are a popular choice for enterprise crypto payments, making up about 71% of the crypto payments on Request Finance (Fig. 13).

The popularity of stablecoins can be explained by the obvious fact that most people do business in fiat rather than settling payments in shares of tech companies listed on the NASDAQ. Their stable prices make them ideal as a medium of exchange and unit of account—two of the three defining features of money.

Some of the most popular stablecoins, such as USDC, USDT, USDS, and even some non-USD stablecoins like XSGD, are issued by centralized entities in exchange for fiat currencies.

They are some of the most popular crypto payment options enterprises choose using Request Finance. USDC alone accounts for about 37% of all enterprise crypto payments in the app, followed by USDT (29%).

In effect, centralized stablecoins are tokenized deposits. Stablecoins are legally identical to the account balances on your bank statements or a centralized exchange. All deposits are debts owed to you by deposit-taking institutions.

Centralized stablecoin issuers promise 1:1 exchanges between fiat currencies and stablecoins.

However, it is important to note that stablecoin issuers' ability to meet redemptions depends on the composition and value of their assets held in reserve. There has been criticism towards USDT about the transparency of their reserves, for example.

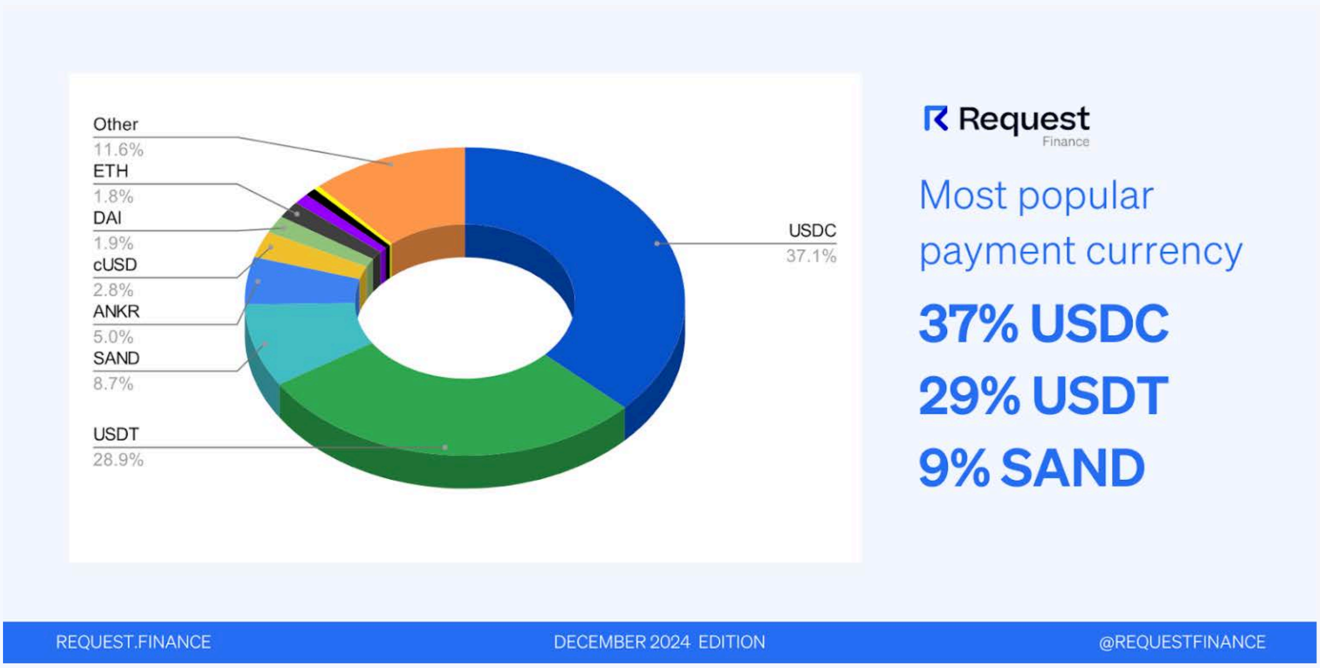


Fig 13. - Most popular tokens, crypto and stablecoins on Request Finance

Fig 14. - On & off ramping using centralized stablecoins

This composition can vary considerably depending on the issuer. For instance, as of December 2024, about 86% of Circle's reserves were held in weekly liquid assets, and 14% were held in cash at regulated financial institutions. Around the same time, cash and cash equivalent accounted for 84% of Tether's reserves.

To exchange for stablecoins, you deposit your fiat into their bank account, and they mint or issue an equivalent amount of stablecoins into your crypto wallet of choice (Fig. 14).

From there, you can either pay stablecoins to another crypto wallet address or swap your stablecoins on a cryptocurrency exchange for other crypto types. The reverse applies to redeeming stablecoins for fiat.

You must apply for a business account with one of these centralized entities. Sometimes, these are directly integrated into and thus accessible from within crypto wallets and payment apps.

For instance, in Request Finance's enterprise crypto payments app, users can easily pay or get paid with the EURe stablecoin issued by Monerium and directly cash out to any Single Euro Payments Area (SEPA) bank account in the Eurozone. The same applies to USDC by Circle.

This is one of the simplest ways to move value from a bank account to a crypto wallet and vice versa.

"Euro is more powerful on-chain. Now, there's no need for an on-ramp as users can directly send euros to their Web3 wallet"

- Arni Gudjonsson, CPO at Monerium

2. DECENTRALIZED STABLECOINS

Not all stablecoins are issued via a centralized entity. Decentralized stablecoins **mint synthetic stablecoins when users deposit other crypto assets into a smart contract** rather than wiring fiat into a bank account of a deposit-taking institution.

These smart contracts attempt to programmatically maintain a pegged exchange rate to a reference fiat currency. As part of their exchange rate policies, they mimic the decision rules and operations of central banks or currency boards worldwide. For example, Curve, one of the largest decentralized exchanges on Ethereum, has released a whitepaper detailing an example of one such implementation of a price stabilization mechanism.

Off-ramping using decentralized stablecoins is a misnomer, as it is not technically possible to deposit fiat currencies from bank accounts into these smart contracts. However, they exist in a middle ground between centralized stablecoins and using CEXes. It is possible to directly off-ramp some decentralized stablecoins in a roundabout manner that still appears nearly instantaneous.

Off-ramping using **decentralized stablecoins is useful for enterprises that wish to conduct their financial operations using non-USD stablecoins**.

The dominance of USD stablecoins largely owes to the USD's role as the reserve currency of many central banks worldwide and its utility in international business. USD stablecoins also provide easy access to many DeFi yield-bearing products and platforms.

However, non-USD stablecoins can enable Web3 companies to penetrate specific local markets deeper. After all, local spending on blockchain payment networks is already challenging, much more so using a USD-denominated currency.

Whether stablecoins are centralized or decentralized, they make sense.

“Stablecoins as a medium of exchange simplify the process.
Over time, stablecoins will likely just be referred to as "dollars”."

- Stani Kulechov, co-founder at Aave & Lens

3. CENTRALISED EXCHANGES

Centralized exchanges (CEXes) offer **more versatile on/off ramps**. Centralized stablecoin issuers enable on/off ramps only in single currencies. For instance, Circle only accepts USD deposits for USDC, and StraitsX accepts SGD deposits in exchange for XSGD.

Centralized exchanges typically accept fiat bank deposits via bank wires or credit cards, in many currencies, in exchange for most cryptocurrencies and stablecoins (Fig. 15)

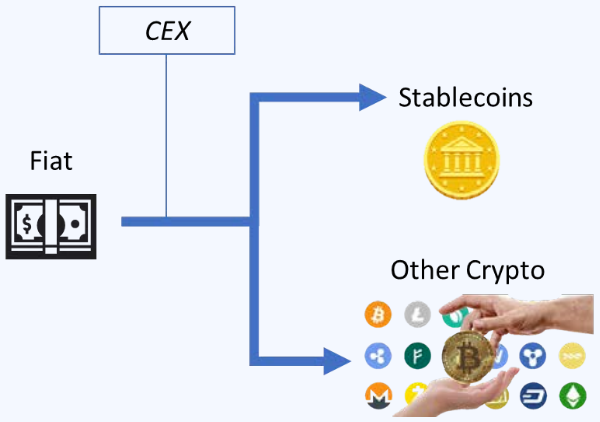


Fig 15. - On & off ramping using centralized exchanges

While using a CEX for on-off ramps certainly seems more elegant on paper, there are four other considerations to note. **Firstly, it can be costly and time-consuming**. Credit and debit cards are a popular way for retail users to purchase cryptocurrency via an exchange, but they come with high fees of up to 10% per transaction. This is generally unacceptable for enterprise use. Card payments are also used only for on-ramps but not off-ramps, as it is usually impossible to "withdraw" money onto a credit or debit card.

Secondly, you run the risk of being de-banked. Many banks and credit card issuers still consider such transactions suspicious, locking or even closing accounts after learning the nature of the transactions. For exchanges, the credit cards of certain countries — including Russia and Ukraine — are automatically rejected.

Thirdly, banks that tolerate transfers to cryptocurrency exchanges may still involve their compliance teams in asking detailed questions regarding the exact destination of funds and the reasoning behind crypto purchases. If and when transfers do go through, they can take several days. By then, prices might have fluctuated dramatically.

Lastly, the counterparty risks of dealing with a CEX are often higher. While CEXes and centralized stablecoins are deposit-taking institutions, it is typically easier to audit the reserves and liquidity of a centralized stablecoin issuer than a centralized exchange. It is generally easier to assess whether a centralized stablecoin issuer has the liquidity and solvency to honor its debt obligations than a CEX.

4. ON/OFF RAMP SERVICE PROVIDERS

An increasing number of players offer direct payouts, both from crypto wallets to bank accounts and vice versa.

These include NBFIs such as online brokerages like Robinhood, fintech payment processors like Stripe, and digital banks like Revolut, now offering crypto. In effect, these on/off-ramp providers are acting as their own exchanges and market makers.

Within this category are also **over-the-counter (OTC) desks**, often operated by CEXes. They are ideal for making outsized transactions, typically in the millions of dollars, more cost-effectively than making spot purchases on exchanges.

OTC desks are valuable because they can conduct large trades without moving the market against them. This effect is known as “slippage”. It occurs when large-scale buying causes prices to rise immediately before the targeted amount of cryptocurrency has been purchased, while selling causes it to fall before it’s all sold.

This is **ideal for cases where large amounts have to be off-ramped**. Examples include converting part of the capital raised in fiat from a venture funding round into stablecoins for global payroll.

Conversely, you could convert a portion of your organization’s crypto treasury to pay landlord bills, which may require a large upfront cash downpayment.

However, most on/off ramp service providers offer only self-on and self-off ramps. This is cumbersome because of the increasingly demanded need to transact stablecoins with third parties’ bank accounts.

Request Finance allows businesses to send stablecoins like USDC to hundreds of recipients on their bank accounts worldwide. Such third-party offramp solution saves hundreds of hours and divides the cost by five for enterprises.

Other businesses choose this solution to receive clients’ fiat payments directly in stablecoins on their wallet.

On & Off Ramps

BEST PRACTICES

On/off ramping is not as easy for businesses as it is for individuals. The nature and size of corporate banking introduce significantly greater fraud and AML risks. Traditional banks may de-bank corporate accounts that receive funds from bank accounts linked to centralized exchanges.

As local banks' risk tolerances can vary widely between countries, it is recommended that you consult with fellow professionals like those in the web3finance club.

Regardless of which off-ramp methods or specific service providers you use to convert your fiat to crypto or vice versa, there are four best practices to consider:

- **Map out your on/off ramp needs by payment corridors**
- **Avoid using on/off ramps to hold your treasury**
- **Implement a monitoring regime to screen for de-peg and liquidity risks**
- **There is safety in diversity**

1. MAP OUT YOUR ON/OFF RAMP NEEDS BY PAYMENT CORRIDORS 🗺️

Today, there are a myriad of on/off ramp methods compared to just a few years prior, in 2017.

At the enterprise level, many solutions providers are increasingly eager to peddle their latest and greatest universal on/off ramp solutions.

What most won't tell you during the pitch is that there is no such thing as a free lunch. **CFOs we interviewed quickly discovered one or more of these limitations** - in order of increasing egregiousness:

- Geographical coverage, or supported tokens/blockchains, is highly limited.
- There are serious daily transfer limits far below your organizational needs.
- Settlement times are the same as bank transfers.
- Fees are exorbitant if they rely on credit card payment networks.
- You must open a corporate bank account with their banking partner.
- Payment services licensing must be obtained as part of the onboarding process.

Remember that on and off-ramps ultimately mean dealing with geographically-bound banking networks.

Like the previous generation of fintech payment processors, they rely on a tech-enabled system to scale the ancient practice of Hawala banking to create the illusion of fast, global payouts.

To save yourself the time and frustration of being drip-fed limitations by various on/off ramp providers, you can map out your on/off ramp needs by payment corridors.

Review your company's employee, freelancer, contractor, and service provider database. **Map out the various country pairs and the fiat payments volumes between them**.

Armed with that knowledge, you will know which regions to prioritize on/off ramps for. This will give you more productive discovery calls with on/off ramp providers.

> "A key 2025 narrative will be optimizing off-ramps for cost, speed, and compliance. Providers with flexibility and broad coverage will thrive in this increasingly competitive niche."
>
> - Bayar Ali, CFO, Coinpayments

2. AVOID USING ON/OFF RAMPS TO HOLD YOUR TREASURY ⛔

On/off ramp wallets, especially third-party custodial ones should never be abused as treasury wallets to minimize exposure to counterparty risk from custodians.

While we already highlighted the importance of self-custody in the third chapter on crypto wallets, it is worth repeating here.

Too often, crypto companies are lulled into complacency and misusing centralized exchanges ("CEX") wallets to hold significant amounts of their treasury. Web3 CFOs should strongly **avoid abusing on/off ramps - especially CEXes in this manner**.

Consider the following example: You are the CFO of a wildly successful Web3 game developer. The date is 5 November 2024.

To settle your accounts payable in fiat at the end of the month, you need to off-ramp $500,000 in USDC from one of your treasury wallets. $400,000 is slated for the fiat portion of your payroll, and the remaining $100,000 is to pay your company's AWS cloud hosting fees in fiat.

You have been using FTX.com for the last two years to do this with zero hiccups. The process is seamless, the fees have been reasonable, and the settlement times are predictable.

If you had decided to move 500,000 USDC from your self-custodial treasury wallet to an FTX wallet now and leave it there until the end of the month, you would have quickly found yourself out of a job. This is exactly what numerous startups and venture funds did for their employees - including FTX's.

"We used the closely-associated exchange, FTX, as a custodian to store a significant proportion of the stablecoin investment we raised, i.e., our day-to-day operational budget."

- Yele Bademosi, CEO of African web3 startup, Nestcoin

3. IMPLEMENT MONITORING REGIMES TO SCREEN FOR DE-PEG AND LIQUIDITY RISKS ⚠️

Whichever stablecoins you choose to on/off ramp, it is recommended that you set notifications and alerts for social media activity and price action to screen for de-peg risks regularly.

Apart from screening for warning signs of stablecoin de-peg risks on your personal accounts, **consider recruiting the help of your marketing team**. They likely already have tools that monitor social media regularly as part of their workflows.

What de-peg risk criteria should Web3 CFOs screen for? **De-peg risks vary depending on the type of stablecoin.**

If your organization relies heavily on centralized stablecoin issuers to manage your organization's on/off-ramps, CFOs can **regularly review the attestation or audit reports provided by these issuers** as part of their disclosure regimes. Balance sheet issues could cause fatal bank runs. This also applies to screening liquidity risks when using other centralized entities like CEXes for on and off-ramps.

On the other hand, synthetic stablecoins are also subject to similar risks, **largely related to the design of their price stabilization mechanisms**. CFOs should review the design of these mechanisms closely, before deciding to rely on them as on/off ramp channels.

There is no such thing as an unassailable stablecoin model or, indeed, an infallible exchange rate policy. Catastrophic currency devaluations have happened in traditional foreign exchange markets and have happened with on-chain stablecoins.

Different stablecoin designs are subject to different risks, and Web3 CFOs must implement robust due diligence in evaluating stablecoins for enterprise use and adopt ongoing screening for specific de-peg risks.

Regular screening can enable CFOs to react promptly to protect their crypto treasury from such risks. Numerous examples show how vigilant monitoring of fear, uncertainty, and doubt ("FUD") on social media platforms has allowed individuals and companies to save hundreds of millions of dollars from exposure to collapsing stablecoins and centralized off-ramps.

Doom scrolling might save your organization from actual doom.

4. THERE IS SAFETY IN DIVERSITY

Use **a mix of on, and off-ramp channels that are as uncorrelated as possible**. In the example above, if you already use a CEX to meet over half of your monthly on and off-ramp volume, examine its shareholding structure and avoid using other entities linked to it.

Instead, you can use a different CEX that is not a subsidiary or partner to the one you currently use.

Better still, use a mix of other stablecoin issuers to meet the other half of your on/off ramp volume each month.

For example, if you already use a Circle Business Account for USDC, consider using a Paxos off-ramp for USDP.

Ideally, you can use **different on/off-ramp channels for different purposes**. For instance, you can consider using Request Finance or a CEX to off-ramp crypto for payroll and a centralized stablecoin issuer to off-ramp when paying expenses in fiat.

Diversification is a running theme throughout nearly all the best practices sections in each guide's chapters. Today, Web3 CFOs diversify their on/off ramp channels (Fig. 16).

The crypto industry's technical, regulatory, and market risks are rapidly evolving. In this environment, CFOs at crypto companies must never allow their organization to become reliant on a single provider - for anything that could jeopardize the company's finances.

That said, **more is not always better**. When modern body armor became available, American soldiers were given bulletproof armor to cover nearly every square inch of their bodies from head to toe. But lumbering around wrapped in armor like the Michelin man is counter-productive and exhausting. Today, soldiers typically wear just enough to cover their vital organs. Getting hit elsewhere might be devastating but not instantly fatal.

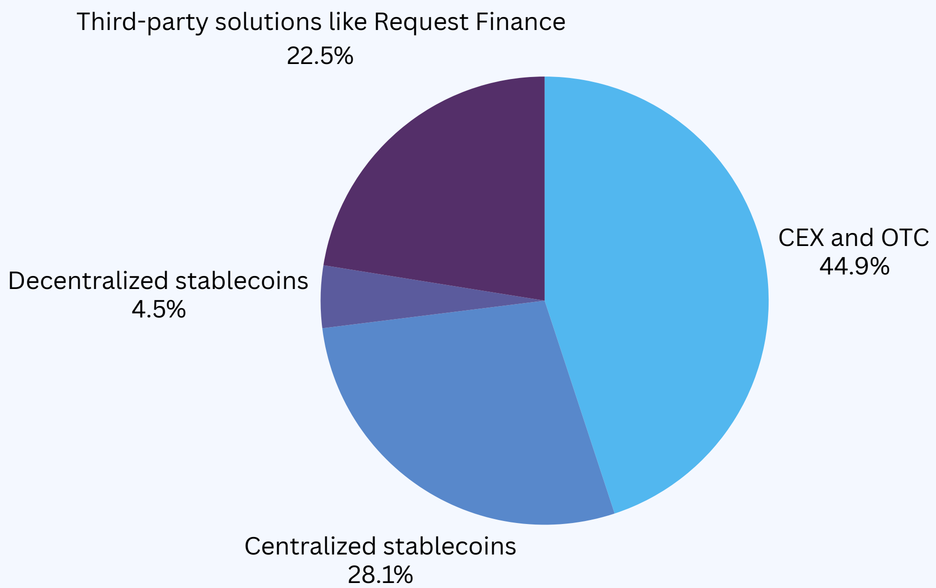


Fig 16. - What on/off ramp methods do Web3 CFOs use?

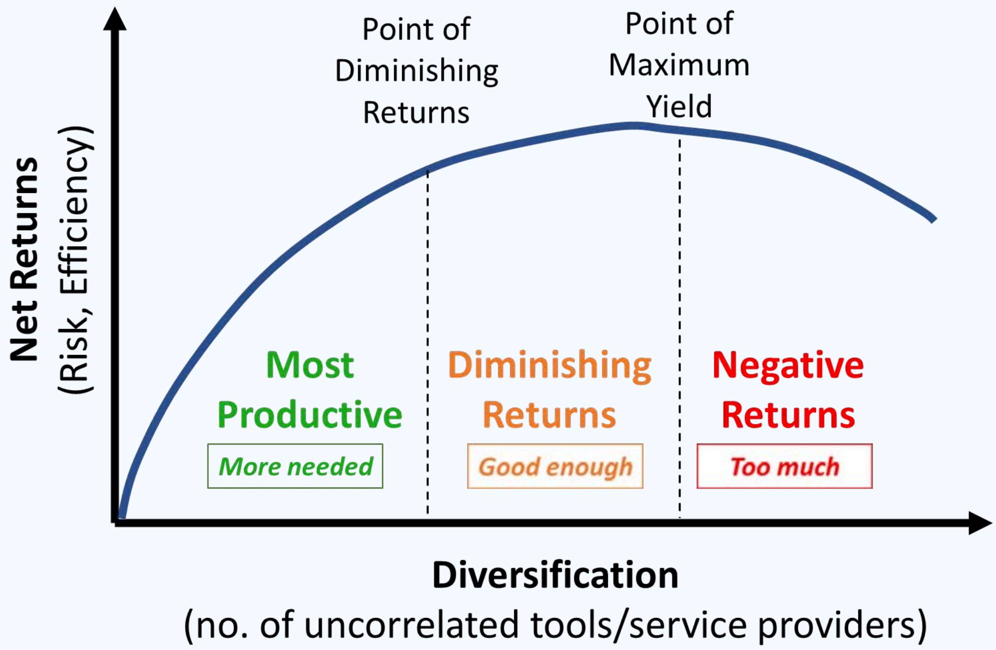


Fig 17. - Diminishing returns on diversification

Similarly, there are always diminishing *marginal net returns* to diversification (Fig. 17). At some point, these increased costs can outweigh whatever benefits you gain from diversification.

The more tools and channels you use, the less exposed you are to anyone failing.

However, this also means that you must expend more energy and time on systems and processes to manage these different tools.

Juggling too many tools or managing different systems poorly can introduce risks, too!

For example, if your organization had a hundred crypto wallets, ten different signatures would be needed to move funds between treasury wallets.

It is likely that either your Receivables/Payables processes will slow to a grinding halt or that even some wallets' private keys will be compromised or lost.

What, then, is an appropriate level of diversification?

A simple rule of thumb is this - **use at least two uncorrelated, extensively researched tools for each core activity area in your crypto finance stack:** (i) crypto wallets, (ii) banking services providers, and (iii) on/off-ramps.

Like our appropriately armored soldiers, Web3 CFOs can focus on using multiple tools to de-risk these three core areas. **They are the vital organs of your organization,** and tooling failures here will immediately impact your balance sheet and liquidity.

The breakdown of tooling in all other domains is not a direct and urgent threat to your organization's financial survival.

CHAPTER 6.0

Crypto Payments

In this chapter, we will cover the topic of managing payments in crypto. This includes getting paid, or paying out in crypto.

Crypto payments

At this point in the guide, we have covered how to store and manage your organization's crypto assets in wallets and meet your fiat banking needs.

We have also examined how to move money between fiat and crypto using various on/off ramp methods.

In this chapter, we will cover the topic of managing payments in crypto. This includes getting paid or paying out in crypto.

WHY CRYPTO PAYMENTS?

There are good reasons for organizations to consider accepting payments in crypto or making payments for their operating expenses in crypto.

1. SPEED & COST ⚡

Faster transaction speeds: Crypto payment rails often have faster settlement speeds than some neobanks and fintech payment processors, allowing quicker and more efficient transactions.

Blockchain networks, especially Layer 2s, typically have lower transaction fees than neo banks and fintech payment processors, leading to cost savings on high transaction volumes.

2. GLOBAL REACH 🗺️

Crypto payment rails are not limited by geographical boundaries, allowing businesses to transact with customers and partners in other countries easily.

Using a global, internet-native payments system enables your organization to hire talent and operate without borders. This allows your organization to grow faster and enter markets faster.

3. EMBEDDED DEFI 💵

Crypto also enables your organization to offer far more innovative **embedded DeFi services at a scale and cost unmatched by traditional** fintechs.

These services range from staking and lending to escrow smart contracts, programmatic loyalty rewards, and even Buy Now Pay Later ("BNPL") smart contract platforms such as Teller Finance and BNPL Pay.

4. NO CENSORSHIP 🗽

Last but certainly not least, **crypto payments are censorship-resistant**. As highlighted in the earlier chapter on fiat banking, having your funds frozen or confiscated is a real risk many businesses have discovered.

Traditional payment processors can also charge merchants higher fees, impose stricter transaction limits, or even deny service if they deem merchants high risk or objectionable.

Understanding blockchain transactions

Ideally, Web3 CFOs dealing with crypto understand the basics of blockchain technology. As a finance leader at your organization, you could dedicate regular blocks of time each week to learning and development.

Crypto-native CFOs can work better within their organizations and can better add value to Web3 teams than those who are not.

However, for this guide, **simple mental models of how blockchains work are sufficient**—even at the risk of oversimplification. It is neither necessary nor productive for most CFOs to grapple with the cryptographic primitives and distributed computing technologies that power blockchains.

Note: Some exceptions to this might be if you are a CFO working at an investment fund that engages in Maximal Extractable Value ("MEV") operations or a crypto mining company where block rewards form a significant part of your revenue streams.

Distributed Ledgers

For most CFOs, it is sufficient to think of **blockchains as distributed ledgers, much like Google Sheets.** It is accessible anywhere, anytime, by anyone with an internet connection.

Each person on the sheet can see the entire edit history of the ledger and has a full copy. Blockchains' global-first, internet-native design makes them attractive candidates for becoming the new scaffolding of a truly global economy.

Whenever someone wants to transfer between accounts in the ledger, they subtract from one account balance and add the same amount to another account. As the chapter on crypto wallets explains, all transactions require approval by signing with the payer's private keys.

Smart Contracts

Just like small programs like macros in Google Sheets can be written, the assets that live on blockchain ledgers can also be programmed using smart contracts. Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.

Smart contracts are typically used to **automate the execution of an agreement** so that all participants can be immediately certain of the outcome without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met. This makes smart contracts useful for payment services like escrow.

But more broadly, smart contracts can be used to build DeFi platforms like exchanges or lending platforms. Much like ride-hailing platforms automate the matching of riders and drivers, smart contracts can automate the functions of traditional financial intermediaries.

Examples of smart contract applications include matching buyers and sellers of commodities and securities by broker-dealers, matching asset owners to asset managers by fund houses, or even matching lenders to commercial banks.

Transaction Costs & Speed

Unlike Google Sheets, which are hosted on a cloud server owned or rented by Google, the distributed ledger is hosted by a network of peers or nodes. Each time a transaction is made, the payer must **pay the network's nodes** a “gas” fee for maintaining and authenticating copies of the ledger.

Gas is charged as a flat fee, payable in the network’s native token. It does not change regardless of the transaction amount but is subject to surge pricing. The more congested a network is, the higher the gas fee. Before you sign a transaction using your wallet, gas fee estimates will typically be shown to you.

In some cases, surging gas fees could make everyday payments even more costly than traditional payment rails. However, for large transactions ranging from hundreds to millions of dollars, the flat fee paid in gas is almost always cheaper and faster than traditional payments.

The method by which a blockchain protocol maintains harmonized records of the ledger is known as the “consensus mechanism.” Different **consensus mechanisms affect the speed at which payments are processed** on a blockchain network.

As a Web3 CFO, I know that these two issues in blockchain design impact the cost and speed of transactions when you make crypto payments. Various scaling solutions are being developed to allow you to achieve faster and cheaper blockchain transactions. These include:

- Layer 1 Scaling Solutions
- Layer 2 Scaling Solutions

Cryptocurrency price tracker CoinMarketCap has a fairly comprehensive guide on the different types of scaling solutions.

“As cryptocurrency adoption grows, more governments and businesses are embracing it as a key value transfer method. Up to 30% of the global population could adopt crypto for payments, driven by its speed and cost-efficiency.”

- Andrew Belonogov, Founder, TechAccountingPro

Token Swaps & Cross-Chain Interoperability

Different Layer 1 blockchains are like separate Google Sheets. They are not always interoperable! That poses challenges similar to not being able to transact across different banks. Thankfully, the extent of their fragmentation is far less than that of traditional banking systems.

Just as different scaling solutions have been developed to address the speed and cost of blockchain transactions, various solutions are being developed to enable interoperability between chains. These include:

- Bridges & Wrapped Tokens
- Sidechains & Parachains
- Cross-chain messaging protocols

A challenge for web3 CFOs to manage tokens - which can exist on different blockchain payment networks. For instance, the stablecoin USDC can be represented on both Ethereum mainnet and Polygon. Making a payment on any blockchain network **will require that you have a sufficient amount of its native token to pay for the network's gas fees.**

For Web3 CFOs, cross-chain interoperability issues and solutions are relevant when dealing with counterparties who may wish to either pay or be paid using different blockchain networks. It is both parsimonious - but not always possible for you to impose restrictions on your counterparties regarding the payment networks you prefer, especially if you are on the poorer end of the bargaining power spectrum in the relationship.

For instance, a boutique smart contract audit firm getting paid by a large DAO may not be able to demand that their invoice be settled in USDC on Polygon.

The simplest way to manage cross-chain payments is to acquire a floating balance of native tokens of the blockchain payment networks you wish to make payments on and choose wallets that support payments on those chains.

That being said, there are good reasons why you may not wish to maintain a balance of USDC on different chains. For example, it might result in an unnecessary expansion in the variety of crypto wallets you must maintain to store your treasury.

Web3 CFOs should familiarize themselves with using popular decentralized exchanges ("DEXes") like Uniswap, Jupiter, or Pancakeswap. They allow you to swap one token for another on the same chain and swap the same token between different chains. For example, if you have USDC on the BNB Chain, which you want to swap to USDC on the Ethereum Mainnet, you can use Uniswap.

DEXes are also ideal for rebalancing your crypto treasury's intertemporal exposure to specific tokens. Finance professionals with experience at large multinational corporations would be familiar with using traditional foreign exchange markets.

With DEXes, even the smallest business enterprise can diversify its treasury's currency exposures to various stablecoins and crypto tokens. For instance, a US company in Singapore can use a DEX like Uniswap to rebalance its exposure to the Singapore Dollar regularly and swap between XSGD and USDC stablecoins.

As discussed in the earlier chapter about on/off ramps, Web3 CFOs may need to diversify their stablecoin holdings based on their ongoing assessment of de-peg and redemption risks.

For instance, if your screening regime identifies elevated risks around the redemption of USDT for fiat, you may wish to reallocate more of your treasury towards USDC instead. A DEX like Uniswap would be ideal for this purpose.

"Cross-chain interoperability presents several challenges. The costs associated with swaps can significantly impact the bottom line, particularly for smaller businesses. Additionally, there are inherent risks involved. It is essential for CFOs to continuously seek out better solutions that are both cost-effective and secure."

\- Modesta Masoit, Founder of Fractional CFO Hub

Evaluating Blockchains

By now, you would have an actionable framework to understand the basics of blockchain transactions. You also have some understanding of the differences between various blockchains, cross-chain interoperability issues, and solutions to make transactions faster and cheaper.

But **which blockchain networks should CFOs use** for their organization? To answer this, it is helpful to think about what your goals are.

Let's examine some of these possible objectives and how they can inform your choice of blockchain network.

1. TRANSACTION COSTS & SPEED

The cost and speed of payments on blockchain networks impact your organization's operating costs and financial operations efficiency.

For instance, if gas fees on the Ethereum mainnet surge to uneconomical levels during the week you process your accounts payable, you may need to **consider alternative networks like Polygon, Avalanche, or Arbitrum**.

For instance, if the BNB Chain network goes down (as it has repeatedly), you cannot send or receive transactions on that particular blockchain.

To prevent your finance team from being caught off guard by reliability issues or high transaction costs on any one chain, CFOs can learn to use different blockchain payment networks and scaling solutions.

Using **crypto payment apps and wallets that support transactions across multiple blockchain networks** can also make it easier for Web3 CFOs to develop redundancies and ensure that their crypto financial operations are not overly dependent on one single chain.

For example, Request Finance's enterprise crypto payments app supports invoicing, bill payments, and payroll in over 20 blockchain networks, including Layer 2's like Optimism and Polygon.

2. DECENTRALIZATION

As a Web3 CFO, you should care about the decentralization of a blockchain network, not as a matter of ideology **but of practical security.** One vulnerability of blockchain networks is known as a "51 percent attack", where a hackers or malicious actors in collusion gain control of a majority of the nodes on the blockchain network. This allows them to create a "fork" of the blockchain with alternate blocks that allow them to "double-spend" the cryptocurrency.

While incredibly challenging to do on larger, decentralized blockchain networks, **it has happened in the past on networks whose nodes are largely dominated by related parties** acting in collusion.

3. ENERGY INTENSITY

Leaving aside the political or moral dimensions of energy consumption, Web3 CFOs have sometimes found it practical or expedient to consider the energy intensity of their blockchain networks.

For instance, a Web3 CFO may be in the process of raising venture capital funding from a fund manager whose mandate includes environmental, social, and governance (ESG) metrics.

The consensus mechanism design employed to manage a blockchain network can depend on the energy intensity and, by extension, your organization's carbon footprint.

For instance, proof-of-work blockchains may be more secure and decentralized in some ways, but there is more or less justified criticism of their energy consumption.

But **carbon accounting can be an inexact science,** especially given that many miners rely on renewable energy sources or natural cooling systems to reduce their operating costs.

There are **always tradeoffs between these objectives**, and few chains can satisfy them all equally — at least for now. While the Ethereum network is used for about 68% of crypto payments processed through Request Finance, transaction volumes on other chains are growing steadily due to its lower gas fees (Fig. 18).

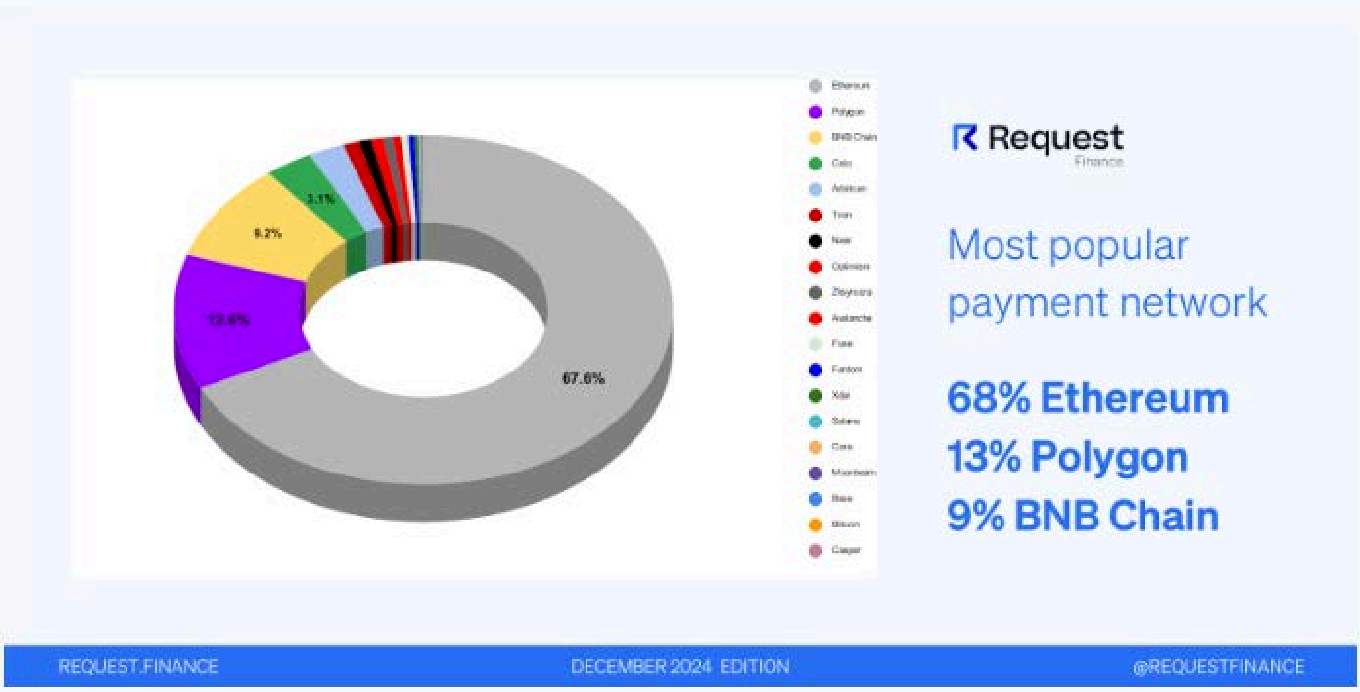


Fig 18. - Popular enterprise payment chains

Managing crypto payments

In the first chapter, we already covered the basics of signing transactions using public-private keys. So why, you might wonder, is there a need to discuss crypto payments in a separate chapter?

Many crypto wallets are not tailored to meet the needs of organizations. While many exist, their features and user experiences are often tailored almost exclusively for the usage needs of individual retail consumers, not enterprises.

The individual retail consumer needs a mobile-first crypto wallet to pay merchants online and at in-store POS terminals, split bills, and make ad-hoc peer-to-peer transfers. In contrast, enterprises have very different crypto payment needs.

What organizations need

Enterprises, foundations, and DAOs have **very different crypto payments needs**, including:

- Billing or invoicing clients for goods and services rendered
- Processing a large number of bills for goods and services consumed as operating expenses
- Managing payroll, equity, and token allocations
- Submitting, approving, and reimbursing travel & expense ("T&E") Claims
- Issuing and managing corporate expense cards
- Disbursing grants and bounties, airdrops and prizes, or investment capital

And perhaps most importantly of all, keeping accurate transaction records is a matter of personal finance for the individual retail consumer. In contrast, Web3 CFOs need tools to **manage their crypto payments to facilitate easy financial reporting** for internal stakeholders like management and investors and external parties like tax, audit, and AML authorities.

Thankfully, some applications like Request Finance are specifically designed to address the crypto payment needs of enterprises.

Billing in crypto

How can organizations get paid in crypto? **An organization's crypto/stablecoin billing needs may vary based on the nature of the goods or services provided**. For instance, a smart contract audit firm likely has a very different billing cycle than a blockchain analytics platform or a crypto transaction monitoring service.

There are two primary means by which Web3 CFOs can manage billing operations in crypto: invoicing and subscriptions.

1. DIGITAL CURRENCY INVOICES

Invoicing clients in digital currencies is especially relevant for companies that provide services to crypto-friendly organizations.

Examples include smart contract audit firms, software development houses, media and marketing agencies, and corporate services providers.

Request Finance is designed to simplify the invoicing process and meet enterprises accepting crypto payments' operational and compliance needs.

You can **automate recurring invoices** to bill your clients monthly or weekly. You can also schedule email reminders to chase upcoming bills or even past-due late payments.

It also lets you know when you have been paid. You can also **enable email notifications to let your clients know when your invoices have been sent**, rejected, accepted, or paid on-chain. Reconciliation is automated.

It also serves as deterministic proof of income. For example, if you receive a call from law enforcement agencies suspecting you of money laundering for an international scam ring or from tax authorities accusing you of unlawful tax evasion, you would have clear documentation.

Sending them your Etherscan wallet history does little good. Crypto wallet addresses' pseudonymous nature and transaction hashes' long alphanumeric strings are ill-suited for financial reporting or calculating tax liabilities.

With Request Finance, all this is **documented easily and in a human-readable format**.

All wallet addresses are also linked to real-world identities in a deterministic manner. Almost no chance of a wallet or payment being mislabeled by accident.

On the other hand, you may also be a CFO of a crypto-friendly enterprise that pays vendors, contractors, contributors, freelancers, and other service providers in crypto/stablecoins.

Many organizations have substantial proportions of their treasury in crypto and stablecoins from fundraising or investment events and prefer to pay for their operating expenses in crypto. Your organization needs a solution that allows you to pay bills and invoices easily in crypto.

Most organizations send and receive PDF invoices in different layouts and formats across different communication channels, such as email and messaging apps.

This is problematic for several reasons:

Firstly, operational efficiency is an issue when making crypto payments. Most companies manually copy the payment information from PDF invoices or a spreadsheet when paying the invoices. This is time-consuming and incredibly prone to human error.

In Request Finance, all wallet addresses are linked to names and emails. There is no chance of paying the wrong amount or to the wrong person. With our batch payments feature, you can review, approve, and pay hundreds of different wallets in tokens with just three clicks.

Secondly, there is also the issue of finance operations. With Request Finance, you can spare yourself the endless back-and-forth of unnecessary communications between freelancers and your company's finance department.

A common nuisance companies experience with invoices is that mistakes sometimes occur with the wrong billing information, such as the company's name, Tax ID, or address. This can cause needless delays in processing payments.

Request Finance allows you to send a payment link to your vendors or contractors. This will automatically create an already pre-filled invoice with your business information. They will need to fill out the rest of the invoice. Now, anyone can invoice you correctly in just a few clicks.

Thirdly, there is the issue of bookkeeping. PDF invoices typically have different layouts, which must be manually downloaded, properly named, and stored as files.

Their data must be extracted, compiled, and uploaded into bookkeeping or accounting software like Xero or Netsuite.

But how do you account for the historical exchange rates of invoices denominated in volatile cryptocurrencies or even fiat exchange rates? What about gas fees?

Request Finance automates all of this. You have a single, clean dashboard where you can see all your invoices in chronological order and filter by names, addresses, or payment status.

All this data, including historical exchange rates and gas fees, can be easily exported to tax or accounting software in a few clicks.

2. SUBSCRIPTIONS IN CRYPTO

Subscriptions in crypto/stablecoins are another topic that may be relevant if your organization accepts crypto payments.

Invoices are good enough for most B2B billing workflows - especially if there are lags between service delivery and payment.

Even for companies that wish to offer subscriptions in crypto, invoices can also be used to offer subscribers discounted lump sum payments for packages or bundles.

However, companies such as blockchain analytics tools, news, media, and other content platforms may prefer a crypto billing method that **supports direct debits at regular intervals from customers' crypto wallets.**

There are currently very few elegant blockchain-based solutions for merchants to regularly withdraw funds from their subscribers' crypto wallets.

True subscription on the blockchain is technically challenging. The blockchain was built with decentralization and security in mind.

Every transaction has to be signed and approved by the wallet owner — a "push" payment. This does not lend itself well to "pull" payments like subscriptions.

Three approaches currently exist to support subscriptions in crypto:

- streaming payments,
- token allowances, and
- NFT subscriptions

STREAMING PAYMENTS 🌊

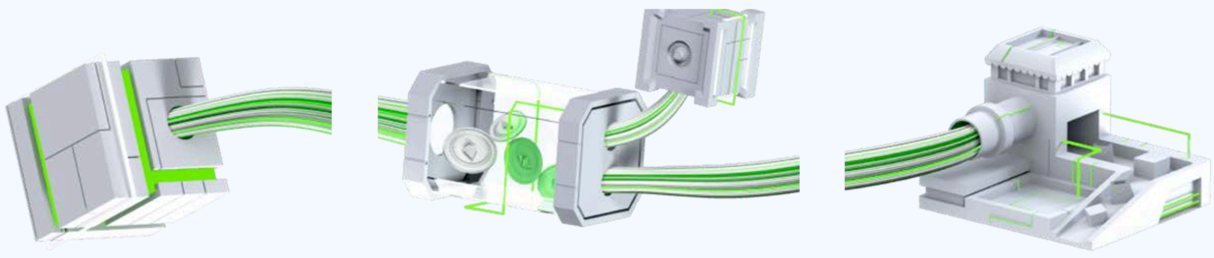
Payment streaming protocols like Superfluid allow your organization to bill subscribers or users every second. This would be ideal for on-demand, economy-sharing platforms like cars or bike-sharing apps.

In a single transaction, a subscriber could agree to transfer a fixed amount in a constant stream over a pre-defined duration. Every second, a tiny amount of the total bill will flow out of the subscriber's crypto wallet without additional gas fees. Similarly, cancellation is also only one transaction.

To use Superfluid's payments streaming, subscribers must wrap their ERC20 tokens into a Super Token, which is then used for payments. For instance, our hypothetical bike-sharing dApp could accept payments in a USD-pegged stablecoin like USDT or USDC.

But users would have to first wrap the USDC (ERC20 token) into Ux (Super Token) on the Polygon chain. Once under the Super Token standard, the subscriber can start paying for using the bike in a continuous stream.

Streaming Payments



Pay for subscriptions in ERC-20 tokens

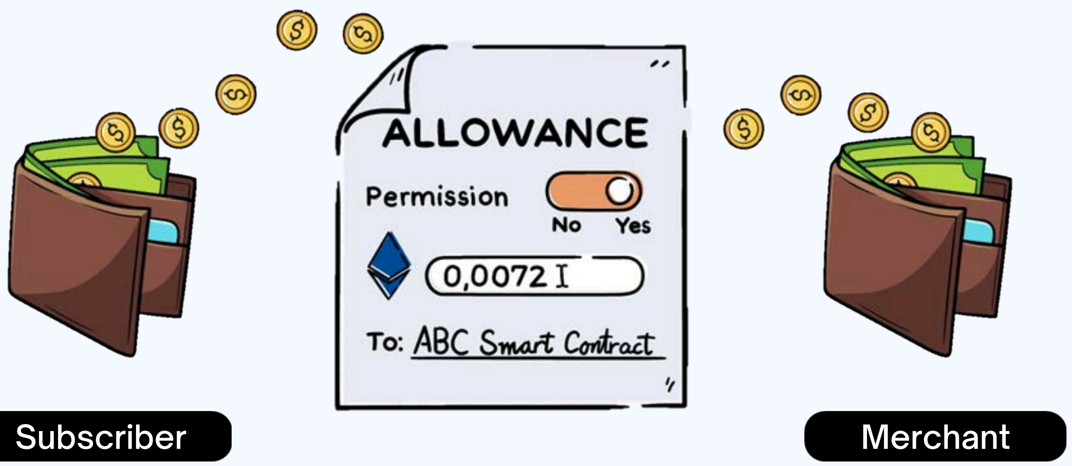
Wrap ERC-20 tokens into Super Token

Get paid every second until the stream ends

TOKEN ALLOWANCES ✅

Token allowances are the equivalent of **direct debit authorizations** in traditional finance.

It allows your subscribers to provide a **one-time approval for recurring payments**, enabling businesses to provide subscription-based services in a hassle-free manner.



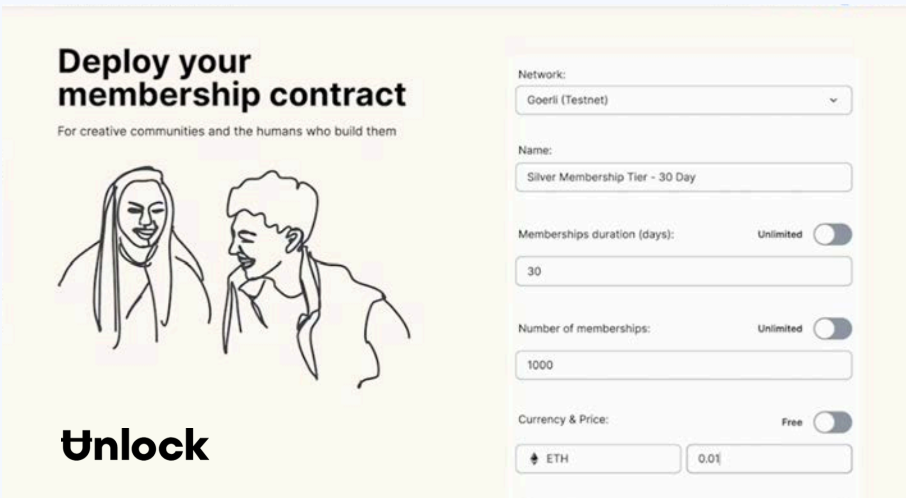
Merchants can automatically deduct subscription fees directly from subscribers' wallets at regular intervals over the subscription duration (e.g., 30 USDC per month).

Once the smart contract uses up the allowance for the given period, it cannot pull any tokens from the user's wallet until the periodic allowance is reset at the next time interval.

For instance, Suberra is developing a subscription payment standard through periodic allowances and time-gated smart contracts with pre-defined transaction values.

NFT MEMBERSHIPS 🃏

Another approach would be **recurring billing using NFTs that serve as digital membership cards**. For instance, Unlock Protocol enables NFT-based recurring subscriptions and memberships that are not manually renewed.



Compared to the payment streaming method above, Unlock can allow your product to **automatically enable or disable a user's access to your services depending on the NFT's validity**, which is tied to whether a member has paid their bills.

Additionally, billing subscribers via membership NFTs can allow you to easily develop commercial **partnerships with other merchants** to offer incentives, discounts, and other loyalty rewards that enhance the value of your membership plan.

For instance, our hypothetical bike-sharing dapp that uses Unlock Protocol's NFT membership to bill its users for using its bikes could also partner with coffee chains like Starbucks to offer a 10% discount on in-store purchases to members who have the bike-sharing membership NFT in their crypto wallet.

Comparing crypto billing methods

To help you evaluate which billing methods best suit your various use cases, here is a handy summary of the pros and cons of the four billing methods in crypto explored in this chapter.

PROS 👍

CRYPTO INVOICES

E.g. Request Finance

- 👍 It is ideal when there are long lags between delivery of the service and payment.
- 👍 One-time payment for packages or bundle deals.

STREAMING

E.g. Superfluid

- 👍 Stable cashflow for merchants.
- 👍 Ideal for time-based, on-demand, or pay-as-you-go services.

TOKEN ALLOWANCES

E.g.Suberra

- 👍 Direct debit authorizations simplify and automate collections with one-time approvals.
- 👍 Best for simple subscriptions.

NFT MEMBERSHIPS

E.g. Unlock Protocol

- 👍 NFTs can be used to enable/deny access to services based on payment history.
- 👍 Ideal for multi-merchant, membership and loyalty rewards programs.

CONS 👎

CRYPTO INVOICES

E.g. Request Finance

- 👎 No direct debits from subscribers' wallets.

STREAMING

E.g. Superfluid

- 👎 Requires additional steps to wrap tokens before they can be used to pay.

TOKEN ALLOWANCES

E.g.Suberra

- 👎 Not ideal for membership programs.

NFT MEMBERSHIPS

E.g. Unlock Protocol

- 👎 Requires the use of NFTs as a token-gating tool for all membership program merchants.

Compensation in Crypto

Compensation in crypto is also typically processed in stablecoins - at least in part, if not entirely. There are good reasons for this. This chapter will cover how to manage three different aspects of compensation in crypto:

- **Payroll**
- **Expenses, and**
- **Token Allocations**

CRYPTO PAYROLL

The Benefits of Using Crypto for Payroll

As mentioned at the start of this chapter, stablecoins offer a fast, cheap, universally accessible internet-native means of payment. Being able to pay anyone, anywhere, anytime greatly **expands your organization's ability to hire the best talent and enter new markets worldwide**.

How to Set Up a Crypto Payroll System

- **Employer of Record (EOR)**

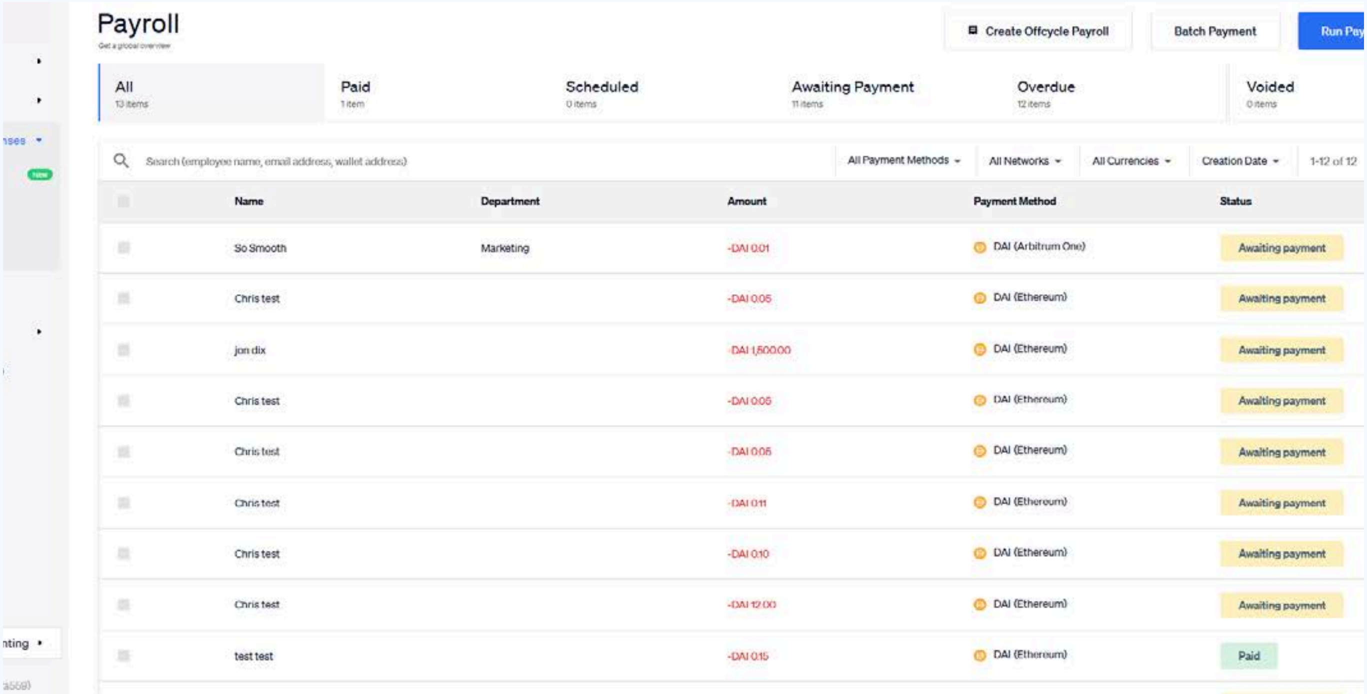
One of the complexities of global payroll for remote teams is having localized entities or subsidiaries that act as employers of record (EOR). In addition to incorporating **local entities wherever you wish to hire**, you will likely also need to deal with local labor laws that cover things like pension schemes.

Global payroll services providers like Deel or Remote.com do all these for you for a monthly fee per employee. They also allow payouts in crypto—albeit only to US residents, and employees have complained a bit because they must open an account with Coinbase.

- **Contractor Payouts**

Using an EOR to manage global payroll can be costly, and there are typically serious limitations when paying salaries in crypto or stablecoins. To address this, Request Finance introduced a crypto payroll module. You can choose from over 300 crypto and stablecoins to pay your team in and from 20 different payment networks.

You can also schedule recurring salary payments according to the frequency of how often they get paid in a month. Best of all, you can pay hundreds of salaries with just a few clicks. You can also view the history of your salary payouts or which team members have yet to be paid.



The limitations of Web3 solutions like Request Finance are that the people you hire will have to be legally considered contractors. Complying with all the complexities of local labor laws and easily paying in crypto is still challenging. However, this has been less of an issue for a growing legion of digital nomads working for DAOs and remote-first companies.

EXPENSES IN CRYPTO

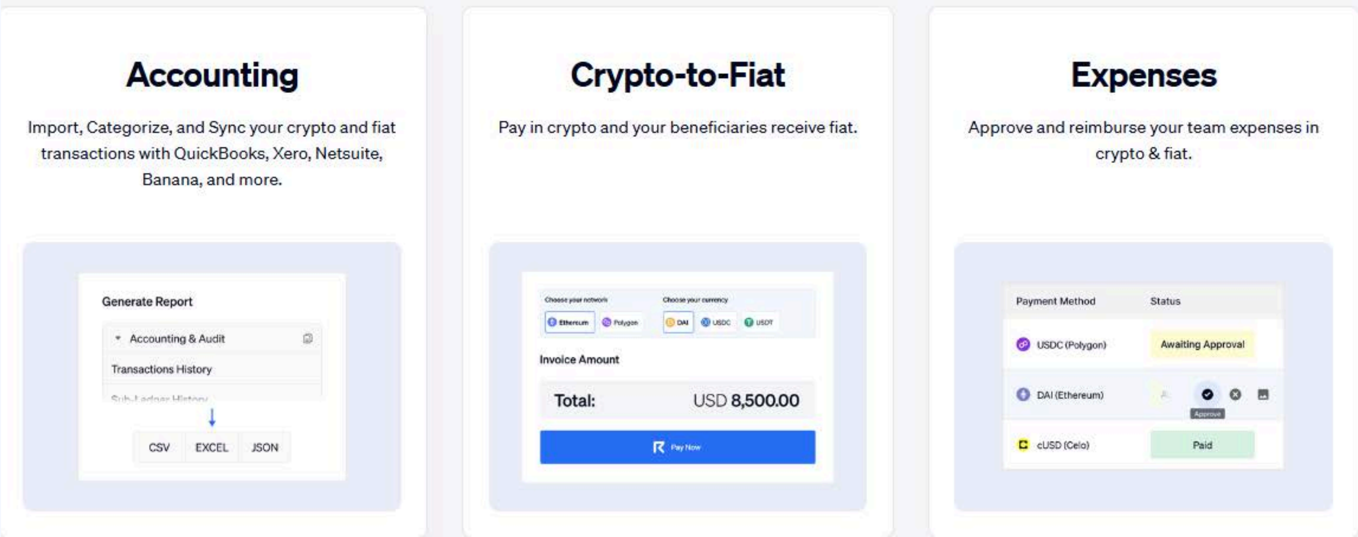
Expense management is a big deal for crypto-friendly companies. For one, it is closely tied to how an organization manages its burn rate—especially given that most crypto organizations' operating expenses are financed with investors' capital. After payroll, **travel and expenses (T&E) are typically the second-largest spending category** for companies. When these expenses aren't properly tracked and processed, that can interfere with a CFO's ability to budget and forecast for the future accurately.

T&E can also be used to reduce corporate tax liabilities. Under most tax regimes, T&E is also tax-deductible—insofar as proper records are kept to demonstrate that it is business-related. By maintaining the right documentation for the right period and ensuring that all deductions are valid, companies can be confident that they can maximize their allowable tax deductions.

Automating your organization's expense management can simplify the claims submission process, simplify documentation when claiming tax deductions, and enable employees to be reimbursed faster. No one wants to pay $1,000 in travel costs out-of-pocket for a business trip and then wait for months while those expenses are reviewed, approved, and reimbursed.

Additionally, the sales and business development teams frequently attend conferences and events and must **claim expenses like conference tickets or sponsorships paid in crypto**.

Many corporate expense management solutions are available, but few allow expense reimbursements in crypto. For instance, one of the most popular corporate expense management apps is Expensify, but the only cryptocurrency it supports for reimbursements is Bitcoin. Request Finance has an expenses module that allows CFOs to easily track, review, and reimburse expense claims in crypto, stablecoins, or fiat.



TOKEN ALLOCATIONS

In addition to ordinary wages paid in stablecoins to meet the team’s fiat expenses, many companies include governance or utility tokens in their compensation packages. These tokens are distinct from equity. Unlike equity, most tokens do not represent a claim on the future cash flows of an operating entity.

Token allocations—typically done as part of an initial coin offering (“ICO”)—align the team's incentives with the platform's long-term success. This inspires confidence in external stakeholders like users and early investors.

Token allocations have **significant differences when compared to traditional equity**. These include:

PROS 👍 VS. CONS 👎

CRYPTO TOKENS

- 👍 Valuation of tokens is marked to market in real-time.
- 👍 Instant liquidity and faster time-to-market.
- 👍 Zero exercise cost or windows like with share options.
- 👍 May not be subject to local regulations on capital gains taxes.
- 👍 Staking, lending, and yield incentives for earning extra tokens, and to access underlying liquidity without triggering a taxable event.
- 👍 No dilution, or at a minimum, dilution that’s transparent.

EQUITY

- 👎 Equity valuations are pegged to enterprise value assigned at the last fundraising round.
- 👎 Need to wait for an exit by way of acquisition or IPO).
- 👎 Share options have an exercise price, and windows.
- 👎 May be subject to capital gains taxes on equities .
- 👎 Limited upside on secondary markets without selling. Equity lines of credit are complex financing mechanisms.
- 👎 Subject to severe, and often opaque dilution.

It is worth noting that the specific tax treatment of token-based compensation may vary depending on the specific circumstances and details of the grant and any applicable tax treaties or other agreements between your local tax regime and the country where the company is based.

It is always a good idea to **consult with a qualified tax professional familiar with the laws and regulations in your local market** to ensure that you are properly accounting for and reporting any stock-based compensation.

Vesting refers to the process by which an employee becomes entitled to receive the shares of company stock or crypto tokens that have been granted to them as part of their compensation plan.

In general, vesting occurs over a certain period, known as the vesting period. It may be subject to certain conditions, such as the employee remaining with the company for several years or achieving certain performance goals.

The vesting of equity or token grants does not typically impact stock-based compensation's accounting and tax treatment.

The asset's value is **generally recorded as an expense** on the company's financial statements at the time of the grant, regardless of whether they have vested. This is especially true of token allocations.

The employee is also generally required to **pay taxes on the value of the tokens or equity at the time of the grant, even if they have not yet vested**. However, the vesting schedule may impact when the expense is recognized and when the employee must pay taxes.

For example, if the vesting period is three years, the company may choose to recognize the expense on its financial statements over the three-year vesting period rather than all at once. Similarly, the employee may be required to pay taxes on the value of the equity or tokens as they vest rather than all at once at the time of the grant.

Again, it is important to note that the specific vesting treatment may vary depending on the details of the grant and the applicable laws and regulations in your local market.

Similarly, **token and equity management platforms can help Web3 CFOs simplify allocations & vesting schedules**.

For example, Magna and TokenOps let organizations tag and trace smart contracts, token vesting, and distribution in crypto across blockchains.

"Projects on Arbitrum, Ethereum and Solana need proper token allocation systems to handle tokens with care"

- Bruno Faviero, CEO of Magna.so

The decision to offer tokens as compensation will depend largely on how the organization generates value and where the value accrues. It is also possible to offer a combination of tokens and equity as part of the compensation package.

In addition, you'll also need to consider:

- Payroll taxes and tax withholding
- Accounting and tracking token-based awards
- Legal documents and processes to ensure compliance with tax and securities laws

Note: Seek advice from qualified persons, such as a local tax advisor or accountant with experience with token compensation plans. You can find them in the web3finance club.

ACCOUNTING AND TAX TREATMENT

INCOME TAX

The expense is calculated by determining the value of the stock at the time it is granted to the employee.

This value is then multiplied by the number of shares granted to the employee.

For example, if a company grants an employee 100 stock shares worth $10 per share at the time of the grant, the expense would be $1,000 (100 x $10).

In terms of taxes, the employee will generally be required to pay taxes on the value of the stock when it is granted, even if they do not sell the stock.

The employee will be required to pay taxes on the value of the stock at their ordinary income tax rate.

For example, if the employee in the above example is in the 25% tax bracket, they would be required to pay $250 in taxes on the value of the stock (25% x $1,000 = $250).

CAPITAL GAINS TAX

If the employee later sells the stock for more than its value at the time of the grant, they may be required to pay additional taxes on the difference between the sale price and the value at the time of the grant, depending on whether local regulations levy "capital gains" taxes on tokens.

Much of this will vary depending on how crypto assets are treated in accounting. A later chapter in this Guide explores this topic in greater detail.

Managing crypto payments

BEST PRACTICES

Managing your crypto payments well involves operational efficiency, strategic insights, implementing proper processes and controls, and compliance with tax and AML regulations.

These four dimensions can help you **evaluate the tools that you choose to automate and simplify paying and getting paid in crypto**.

1. OPERATIONAL EFFICIENCY ⚡

Your payments tool could have features that give your team the ability to:

- Support various **crypto wallets, blockchain networks, and token types**.
- Support **programmable payment options** like smart contract escrow, streaming payments, or NFT subscriptions.
- Pay contacts **without needing to manually input** crypto wallet addresses
- Easily pay hundreds of different wallet addresses in a single **batch transaction**
- Automate **push notifications for on-chain payment** confirmations
- Integrations with **contract management software** to pull variables from signed contracts automatically create payment requests.
- Easily **send payment requests** to counterparties, with payment details included.
- Schedule **recurring payment** requests **or direct debits** from crypto wallets
- Send **automated payment reminders** for upcoming or delinquent payments
- Easily submit and reimburse **travel & expense (T&E) claims,** typically processed separately from payroll and sometimes claimable under contract terms with professional services providers.
- View, retrieve, and **export payment data** to accounting/tax software.

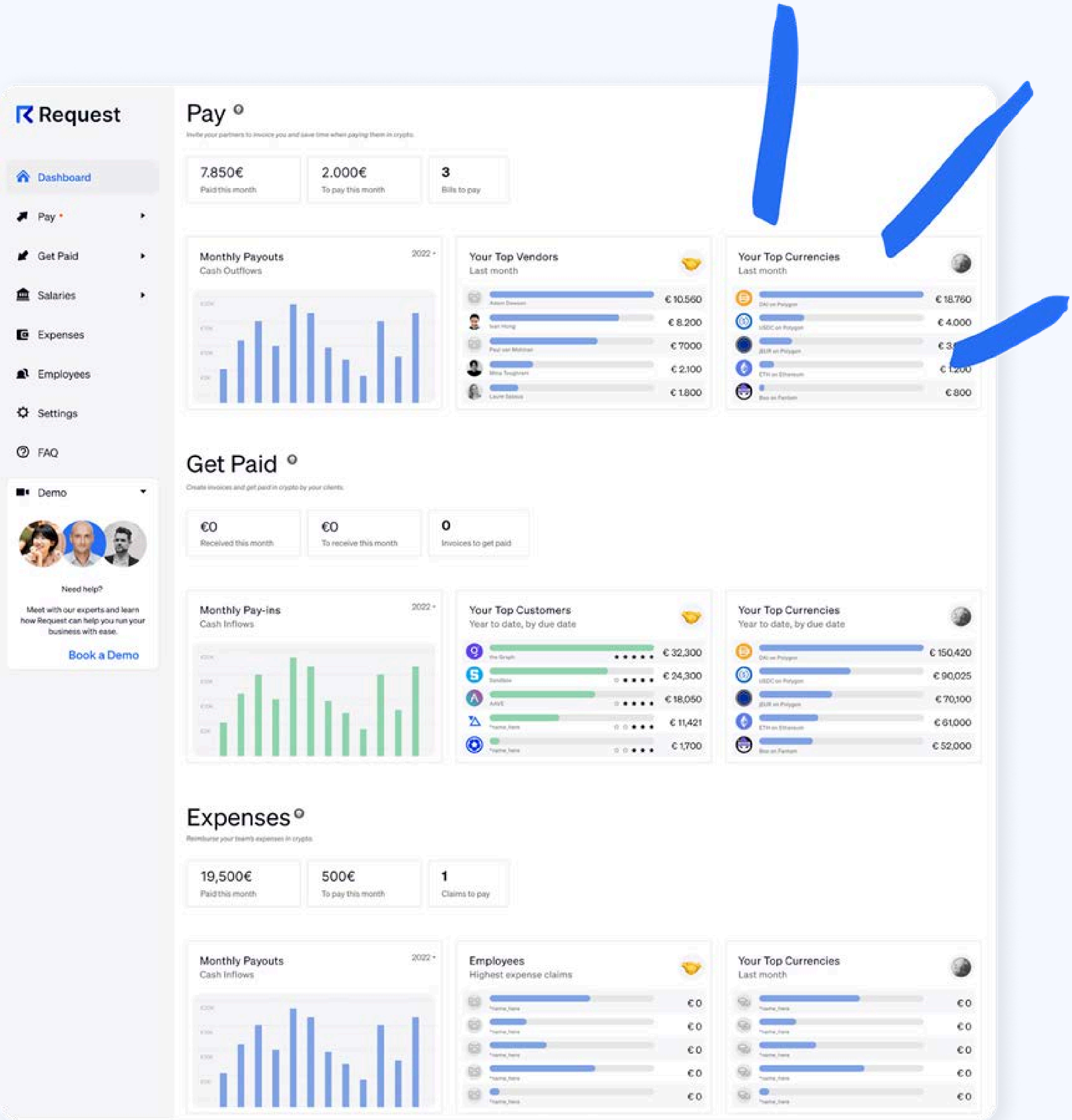
While few tools can check every item off the list, some can do more than others. This list will help you think about some of the key features of crypto payment apps that can help you enhance the efficiency of paying and getting paid in crypto.

2. STRATEGIC INSIGHTS 💡

One of the main challenges with crypto payments, or indeed enterprise payments in general, is being able to label the purpose of each transaction.

Labeling transactions allows CFOs to **code them into the organization's chart of accounts ("COA")**, which organizes finances to give interested parties, such as investors, DeFi lenders, and team members, a clearer insight into the organization's financial health.

Your crypto payment tool should also have at least simple dashboard reports that allow you to **visualize easily where your crypto transactions are coming from and going**. This way, Web3 CFOs can identify key growth areas for the organization or the main cost drivers.



3. PROCESSES & CONTROLS 🎮

As the first chapter on crypto wallets alluded to, implementing proper processes and controls is important to prevent waste, fraud, and abuse. It is not only a matter of ensuring that your organization's crypto is put to the best use possible.

For most companies in the space, a significant proportion of their treasury is sourced from invested capital.

Accountability for how investors' capital is spent is critical to the integrity of the organization and the management's reputation.

The tools you choose to manage your crypto payments should enable you to do this with features that give you the ability to:

- Maintain a clear database of employees, contractors, and other counterparties and their payment details.
- Attach proper documentation to payment requests like invoices and expense claims

.

- Review and approve payments before they are made using detailed expense policies.
- Set approval limits requiring multi-sig authentication for transactions above a certain threshold.
- Allow permissioned access to different team members. For instance, HR might be responsible for expense reimbursements.

Contact management is a commonly overlooked, yet fundamental aspect of having proper cash disbursement controls.

Does that wallet address belong to Tom from the Marketing department or the freelance graphic designer we hired last month?

To simplify managing your organization's accounts payable and accounts receivable in crypto, you need a clear way of organizing contacts and their corresponding payment details, both in crypto and fiat.

You could maintain a contact management system that will help you streamline your crypto payments.

There is nothing wrong with maintaining permissioned-access Google Sheets, but your contacts and their payment information should also ideally be integrated into your crypto payments app.

Manually pulling (read: copy-pasting) payment information from a spreadsheet into your wallet when making payments is both tedious and vulnerable to error.

Additionally, uploading CSV files to token multi-senders for batch payments can be problematic without clear version controls.

Put simply, you could make a batch payment using the wrong spreadsheet file.

4. COMPLIANCE & REPORTING 👮🏽

Lastly, they should enable you to ensure that your financial reporting complies with relevant laws concerning documenting crypto transactions for tax and anti-money laundering (AML) purposes.

The tools you choose to manage your crypto payments should enable compliance with features that give you the ability to:

- Denominate outstanding and historical crypto payments in fiat prices.
- Mark crypto payments to market values at the point of payment.
- Maintain separate records of gas fees and other transaction costs associated with crypto payments, which should be filed as operating expenses.
- Easily export historical transaction data to traditional accounting/ERP software.
- Provide readable transaction documentation, including counterparties' real-world personally identifiable information for AML reporting (such as Form 8300 for US Persons).

Starting January 1, 2024, if you're in the US and receive over $10,000 in cryptocurrency in a single transaction or related transactions, you must file Form 8300 within 15 days.

Who must file: Individuals, companies, corporations, partnerships, associations, trusts, or estates engaged in a trade or business.

What to report: Cash payments over $10,000 now include certain cryptocurrency transactions.

Deadline: File Form 8300 within 15 days of receiving the payment.

Recipients must verify and record the payer's personally identifiable information, including the payer's name, address, occupation, and taxpayer identification number; the identifying information of the person on whose behalf the transaction was conducted; and a description of the transaction and payment method.

Form 8300 filers are obligated to give written notice to every party named on the form by January 31 of the following year. Copies of the Form 8300 must also be kept on record for five years.

"Web3 feels like scaling an endless learning curve, where every new technology presents both an opportunity and a challenge."

- Fabio Mancini, CEO, TokenOps

CHAPTER 7.0

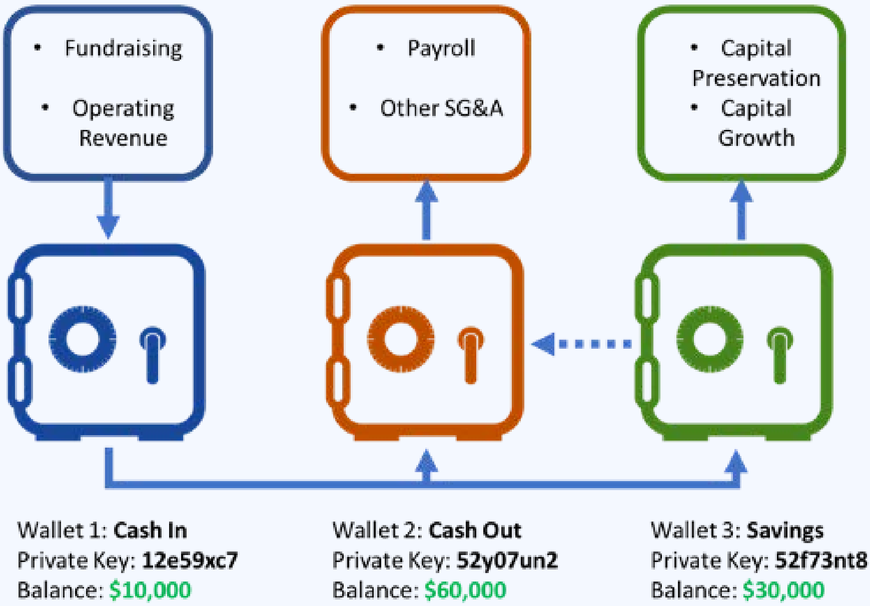
Crypto Treasury Management

The goals of a Web3 CFO's treasury allocation strategy are: capital preservation, liquidity, and income, in that order.

Treasury Management

In an earlier chapter, we explained why you should consider maintaining at least three different crypto wallets:

- one for receiving payments,
- another for paying expenses,
- and a third wallet that acts like a savings or investment account.



These accounts' assets are derived from multiple sources, primarily fundraising or operating revenue. Fundraising in crypto typically takes the form of an Initial Coin Offering ("ICO"), which lists a newly minted token for sale on a decentralized exchange to retail investors. The company receives cryptocurrencies like ETH, SOL, or stablecoins in exchange for its native token.

This fresh capital is typically directed to the treasury. Ideally, organizations or dApps with sound fundamentals will aim to generate revenue from fees. This operating revenue represents a recurring source of income for the treasury. While other ancillary sources of income may exist, this piece will focus on fundraising and operating revenue, with an ICO being the primary source of treasury capital.

Typically, in an ICO, the token issuer retains a significant portion of the supply of its native token in its treasury account. Allocated uses often include staking rewards, compensation for advisors and other core contributors, ecosystem development grants, or future working capital needs.

Often, an organization's treasury is composed largely of its native token, effectively seeking to align the interests of investors and token issuers.

Treasury Capital Allocation

BEST PRACTICES

As with a traditional finance investment strategy, proper organization treasury allocation requires a “one size fits all” solution. However, there are some best practices and a framework for approaching treasury allocation.

A16z Crypto states that “the goals are capital preservation, liquidity, and income, in precisely that order” for a Web3 CFO’s treasury asset allocation and management strategy. Building on this framework, let us dissect each component and construct a hypothetical treasury basket, assuming a profitable organization with a native token.

1. CAPITAL PRESERVATION

Large exposures to a single asset are a significant risk factor to the organization’s treasury.

Regardless of economic fundamentals, token prices are highly susceptible to exogenous shocks.

Proper asset allocation and defensive diversification are fundamental elements of traditional investing that apply to the DeFi realm as well.

An investor holding an S&P 500 ETF will almost certainly fare better than an investor holding one individual technology company stock during a tech sector bottoming such as the Dot-Com Crash.

Narrowing the focus, holding that one specific stock introduces direct, unmitigated exposure to a sole company: if it goes under, the investor goes under.

These same principles can be applied to the DeFi ecosystem and treasuries.

At its core, a treasury should be a fortress of capital, walled against market gyrations and certainly impenetrable by the malperformance of one individual asset.

However, this approach is not always taken. So, how should a treasury be composed? What is the proper asset allocation?

Capital preservation can be a challenging target, as highlighted by the cryptocurrency market's volatility and overall 2024 performance.

However, instead of focusing on an investment's market movement, an investor may consider the underlying organization's health and likelihood of survival. In other words, what is the chance of it blowing up?

Without naming specific tokens, some assets within the ecosystem are generally respected as "blue-chip" investments with the largest market caps; they are foundational to the industry; if they go under, we all go under.

Additionally, these assets have shown massive historical price appreciation since launch, which more than preserves purchasing power.

Capital preservation can also be achieved by holding industry-standard, dollar-pegged assets. For example, and not providing recommendations, Circle's USDC or SKY's USDS might fit this approach.

Assuming operations as usual, a treasury of 100% of these two assets would have the same balance in thirty years as it does today. This is essentially a "leave it under the mattress" approach.

So, which approach should we choose? While the former comes with volatility and a litany of organization-specific risks, the latter offers no possibility of price appreciation and loss of purchasing power when off-ramped to a fiat currency due to off-chain inflation.

This leads back to the basics: **Diversification**. Including a mix of both types lets an organization know its treasury will have a floor value of the dollar-pegged assets while aiming for capital gains from the industry's top coins or tokens. Capital is preserved and maintained.

"In the world of Web3, your treasury is your lifeline. Managing it wisely ensures you're ready for both today's challenges and tomorrow's opportunities."

- George Qiao, Head of Treasury at StratsX

2. LIQUIDITY 🌊

This is the cash in the checking account used to cover expenses. An organization will have a list of basic cash expenses such as compensating core contributors, audits, server hosting, marketing at events, etc. Without immediate liquidity, the project could renege on contracts or miss payments.

Going back to the need for **diversification**, an organization with 100% of its treasury in its native token would need to sell it to generate short-term liquidity.

This raises three multiple primary complications.

- **Downward pressure** on the token's market valuation. Selling large blocks into an otherwise stable market reduces the token's price, all else equal.

- **Capital loss** when selling into a down market; if the token's price has declined, selling for liquidity results in a loss.

- It invites the appearance that the organization offloading its own token has **lost faith** in its own project. Other sellers may follow, cratering the token price, or users may abandon the platform.

Liquidity exists in the form of cash. Cash, in the cryptocurrency ecosystem, exists in the form of dollar-pegged assets. Thus, liquidity is best maintained by holding a **diversified** basket of the most battle-tested such stable assets.

This selection may include the aforementioned names, USDC and USDS, or introduce other well-known dollar-pegged assets with **transparent collateral reporting.**

3. INCOME 💵

DeFi platforms can offer various treasury management services, including decentralized exchanges, lending and borrowing platforms, and yield farming opportunities. From these different avenues, a treasury may generate income through two methods:

- **Capital gains,** highlighted above, strive for the "buy low, sell high" approach. However, as seen in our investment portfolios, this approach does not guarantee positive returns and often results in massive losses. It is a high-risk strategy. That does not mean organizations must eschew asset speculation entirely; rather, they should **diversify** to protect against market or asset downturns.

- **Yield-bearing investments** present an income strategy that, if selected properly, is insulated by market dynamics.

On Lido, for example, ~$34 billion ETH is staked, earning 2.9% APR (as of 21st December 2024). Similar options exist for other proof-of-stake chains, such as Solana or Polygon.

Due to lockup periods on many staking platforms and organizations, staked assets must be appropriately balanced against available liquidity. Lido and others do afford investors the ability to sell staked assets on the secondary markets, but these assets are subject to the same risks as highlighted in the "capital gains" strategy.

A further, more stable, and often higher-yielding option is investing in a yield-generating platform such as Aave or Compound.

This type of investment relies on a pegged-dollar asset, USDC. Thus, it is a market diversification from holding an asset such as Bitcoin. Neither should comprise the entire treasury, but balancing one against the other helps mitigate risks.

This three-pronged approach to treasury management ultimately fails without proper diversification. A treasury focused 95% on capital gains income fails in capital preservation and liquidity as nearly all of its assets are in the riskiest strategy, thus putting its capital at risk and limiting dependable liquidity. Likewise, a 95% idle USDC treasury is not generating income.

"Treasury managers must focus on designing strategies that are not only attractive today but also scalable and sustainable for the future."

- Nik Pletikos, treasury and defi at Fuel Labs

Diversification is the backbone of proper treasury management. Without a diversified allocation, a treasury puts the entire organization at risk of failure.

Regardless of which chains your organization uses, there is safety in diversity. While many Web3 teams may build on specific chains and thus rely predominantly on one particular chain, Web3 CFOs should note that overexposure to one particular chain presents its own risks.

For instance, the collapse of Luna and UST wiped out many companies building dApps on Terra and holding a large proportion of their company's treasury in assets on the Terra blockchain.

Web3 CFOs owe a fiduciary responsibility to their organization's core stakeholders, especially their team, users, and investors, to protect the company's financial health—not a particular ecosystem or ill-defined sense of "community."

Balancing these three different concerns is a task that rests in part on the good judgment of Web3 CFOs, whom the management team can count on to act in the best interests of the company as a going concern. Hedging your crypto treasury's exposure should never be left to convenience, inertia, or an excess of blind optimism in any particular chain.

Chains and their ecosystems are like countries. Failed chains are like failed economies in the real world: poorly governed banana republics where no one wants to visit, invest, or build. The history of national economies and blockchain economies is littered with gravestones to both.

Blindly trusting in a particular chain or assets on that chain would be the same as deciding to move your business and all its assets into a newly-formed country in an emerging market. If doing so sounds like a risky idea, Web3 CFOs at crypto companies building on particular chains should reflect on the prudence (or lack thereof) in the DeFi world.

"Many crypto treasuries and DAOs currently suffer from the risk of overexposure, so tokenized traditional assets like MMFs will soon become a go-to diversification tool for Web3 CFOs because of their low correlation with cryptocurrencies"

\- Cloris Chen, CEO of Singularity Finance

CHAPTER 8.0

Financial Reporting in Crypto

Despite the string of crypto scandals, this presents an opportunity for new standards in financial reporting to emerge for enterprises.

Financial reporting in crypto

Blockchain's inherent transparency and real-time properties present an opportunity for new standards in financial reporting to emerge for enterprises and DAOs.

Financial reports are like a health screening for internal stakeholders like employees and management. It can be used to **align teams, and inform decisions** throughout the organization. For external stakeholders like investors, users, and regulators - financial reporting is a matter of **compliance with local laws**, but also to **inspire public confidence** in the viability and financial health of an organization.

In this chapter, we will review key issues in financial reporting in crypto like:

- **Financial Statements**
- **Proof-of-Reserves (PoR)**
- **Accounting Standards for Crypto Assets**

Financial Statements

The financial health of a web3-friendly company should be measurable through consistent financial reports and statements that **can be crafted regularly**.

Just as a traditional company would regularly bookkeep and produce monthly, quarterly, and annual financial statements, why should companies involved with crypto be any different?

If anything, CFOs can signal quality by a **proactive commitment from a Web3 firm or DAO to produce regular financial statements** internally or to investors.

However, producing financial statements can be frustrating without the right tools. Enterprise-grade crypto accounting solutions are available to integrate crypto assets into their balance sheets.

Essential tools for setting up a complete back-office system for a Web3 CFO include a solution for crypto accounting, AR/AP and payments, and payroll.

Ideally, these solutions should be integrated to maintain everything in one place.

Income Statement	
Revenue	6,355.9
Other Revenue	*18.3*
Operating Expenditure	*(5,561.4)*
Other Expenses	*(21.5)*
Net Operating Expenditure	(5,564.6)
EBITDA	**791.3**
Depreciation & Amortization	(259.6)
EBIT	**531.7**
Interest on Cash	*26.0*
Interest Expense	*(90.4)*
Net Interest Expense	(64.4)
NPBT	**467.3**
Tax Expense	(186.9)
NPAT	**280.4**

Balance Sheet	
Cash at Bank	48.3
Debtors	12.0
Other Current Assets	-
Current Assets	**60.2**
Fixed Assets	(139.0)
Other Non-Current Assets	50.0
Non-Current Assets	**(89.0)**
Total Assets	**(28.8)**
Creditors	(76.1)
Corporate Tax Payable	1.0
Interest Payable	-
Dividends Payable	9.4
Other Current Liabilities	1.6
Current Liabilities	**(64.1)**
Debt	(55.0)
Other Non-Current Liabilities	5.1
Non-Current Liabilities	**(49.9)**
Total Liabilities	**(114.0)**
Net Assets	**85.2**
Ordinary Equity	(50.0)
Other Equity	(5.0)
NPAT	*280.4*
Dividends Declared	*(140.2)*
Retained Profits	140.2
Total Equity	**85.2**

Cash Flow Statement	
Revenue	*6,355.9*
Decrease in Debtors	*(12.0)*
Other Cash Receipts	*6.3*
Cash Receipts	6,350.2
Operating Expenditure	*(5,561.4)*
Increase in Creditors	*(76.1)*
Other Cash Payments	*3.0*
Cash Payments	(5,634.5)
Interest on Cash	26.0
Interest Paid	(90.4)
Corporate Tax Paid	(185.9)
Other Operating Cash Flows	(55.8)
Operating Cash Flows	**409.7**
Capital Expenditure	(120.6)
Other Investing Cash Flows	-
Investing Cash Flows	**(120.6)**
Debt Drawdowns	-
Debt Repayments	(55.0)
Ordinary Equity Raisings	-
Ordinary Equity Buybacks	(50.0)
Dividends Paid	(130.8)
Other Financing Cash Flows	(5.0)
Financing Cash Flows	**(240.8)**
Change in Cash Held	**48.3**

Fig 14. - Example illustrating links between the financial statements

As mentioned in the introduction to the Web3 CFO Guide, most CFOs working at Web3 organizations have prior experience.

For simplicity, the most basic financial reporting consists of three statements: an income statement, a balance sheet, and a cash flow statement (Fig. 14).

Populating the content within the financial statements then involves systematically linking information from each area within the model, starting with revenue and working through expenses, debtors, creditors, assets, etc.

Maintaining consistency in creating regular financial statements and thorough financial reports will prepare Web3 companies for auditors when they come knocking at the door.

Alternatively, Web3 CFOs at smaller organizations lacking the in-house capabilities to manage financial reporting can consider outsourcing the work to crypto-native corporate service providers like BlockOffice.

"Delegating accounting and tax matters to professionals helps CFOs to focus on the business operations."

- Christian Corrigan, CFO, BlockOffice

Proof of Reserves

Proof-of-Reserves ("PoR") is an independent audit performed by a third party to validate that a centralized entity's or smart contract platform assets equal clients' funds. PoR allows the market to verify that industry giants are acting honestly and are solvent.

A competitive advantage can be achieved by an on-chain PoR that matches assets against liabilities and details equity. The same is true for decentralized stablecoins. It's not enough to list assets.

PoR should detail cryptographic proof of client balances and wallet control. The public should also be able to see the sum of client liabilities, user-verifiable cryptographic proof that all wallets were included, and signatures showing a custodian has control.

Currently, PoR is most popular among exchanges and other centralized **deposit-taking institutions or platforms,** given that crypto assets are often opaquely held in these centralized entities.

Of the largest centralized exchanges, Kraken Digital Asset Exchange is known and respected for its PoR. Binance also regularly shares PoR on its website.

PoR should be an industry standard for DeFi, especially stablecoins & real-world assets (RWA). If individuals/entities can't be certain that a protocol or stablecoin is backed as it claims to be, the market remains susceptible to systemic risks that harm DeFi adoption & innovation.

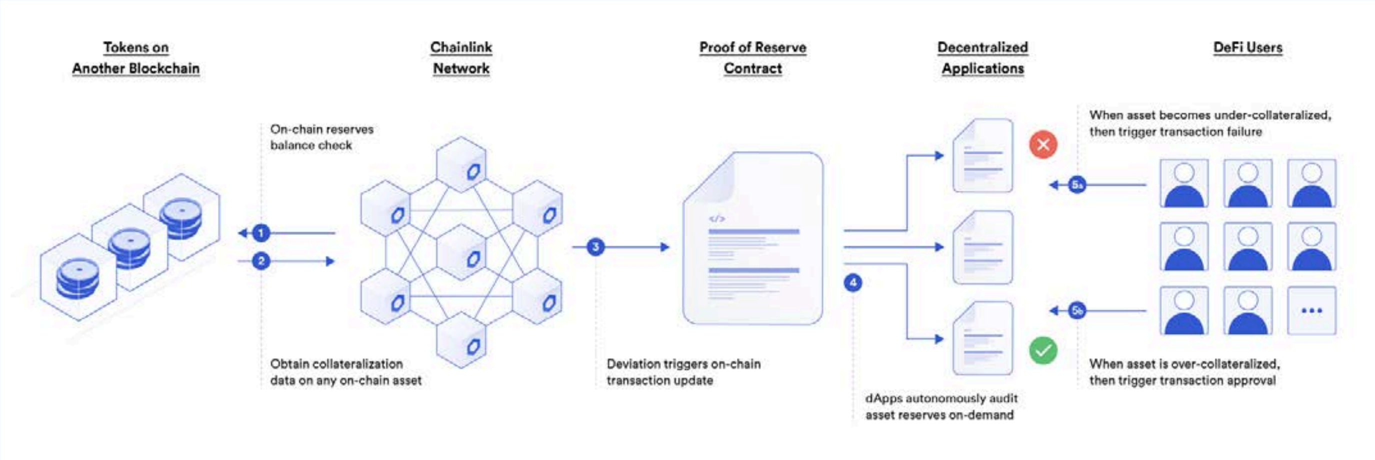


Fig 15. - Chainlink's PoR for auditing multi-asset collateralized tokens

For example, Chainlink's PoR service provides smart contracts with the data to assess collateralization of any on-chain asset backed by both (i) off-chain and (ii) cross-chain reserves. Operated by a decentralized network of oracles, it enables the autonomous auditing of collateral in real-time rather than forcing users to trust paper guarantees made by custodians. This can give DeFi platform users transparency into an asset's underlying collateralization (Fig. 15)

Accounting Standards

Accounting for crypto assets remains a highly debated topic among bookkeepers and investors today.

While innovation in the crypto space is moving rapidly, standard setters in the accounting industry have not had the same stamina to keep up. **With new crypto assets emerging constantly with varying properties, the task is monumental**, to say the least.

Current accounting standards were not written with crypto assets in mind, so one must examine them and apply a principles-based approach.

The two **prominent standard setters today are the IASB and FASB**, which are responsible for developing and publishing International Financial Reporting Standards (IFRS) and US GAAP accounting standards, respectively. While both seek to improve the transparency of financial reporting, **the accounting treatment of crypto assets will slightly differ under IFRS and US GAAP** and should be applied according to the jurisdiction of the underlying entity.

In this guide, we aim to provide the salient approach under both frameworks for the following;

- **Initial recognition and subsequent measurement of crypto assets**
- **Fair value measurement of crypto assets**
- **Tax: calculating capital gains/losses**
- **Disclosure of crypto assets**

Note: this guide focuses on the accounting treatments when crypto assets are held under one’s own account rather than on behalf of third parties.

INITIAL RECOGNITION & SUBSEQUENT MEASUREMENT OF CRYPTO ASSETS

One of the main differences between accounting for crypto assets under IFRS and US GAAP is that IFRS allows for accounting under Intangibles or Inventory, while under US GAAP, crypto assets can only be accounted under Intangibles.

The reasoning for concluding was to examine the nature of a crypto asset.

- **Is it cash?**

Cash must be used as a medium of exchange and a monetary unit for pricing goods and services.

Also, cryptocurrencies are not legal tender and are mostly not issued or backed by any government or state. Hence, they cannot be recognized as cash. Bitcoin in El Salvador is the exception here.

- **Is it a financial asset?**

To be recognized as a financial asset, there must be a contractual right to receive cash or another asset. Again, crypto-assets do not meet this definition.

However, the exception would be for stablecoins, as explained under the below conditions.

- **Is it a fixed asset?**

No, cryptocurrency is not tangible in nature but digital.

- **Is it an inventory?**

Inventories are not required to be in physical form, but inventory should consist of assets held for sale in the ordinary business. (IFRS - IAS2 'Inventories')

Therefore, if your entity holds the crypto asset for an extended period and investment purposes, it would likely not meet the definition of inventory.

- **Is it an intangible asset?**

If crypto assets are acquired for investment purposes only, they fall under intangibles.

(IFRS - IAS 38 'Intangible Assets,' US GAAP - ASC 350 'Intangibles, Goodwill and other')

THE CURIOUS CASE OF STABLECOINS

While most crypto assets would fall under either intangibles or inventory, as outlined above, many stablecoins are not accounted for as crypto intangible assets. This is because stablecoins meet the definition of a financial asset if the contractual arrangement includes a right to receive cash from the issuer.

Understanding the redemption rights is essential to making this assessment, and classification under a financial asset would depend on the following non-exhaustive list;

- Legal form of the stablecoin,
- Existence and enforceability of redemption rights and,
- Collateralization supporting the stablecoin's value.

DIFFERENT ACCOUNTING TREATMENTS UNDER IFRS AND US GAAP

Given the nature of many crypto assets, they will mostly have an indefinite useful life and are not amortized. Instead, they are tested for impairment annually (or more frequently if impairment indicators exist).

Under intangibles, if the fair value of a crypto asset falls below its carrying amount, an impairment loss equal to the difference must be recognized. This impairment loss cannot be reversed, even if the fair value increases later.

The gains are only recorded until the time of sale when they are realized. (that's the most controversial debate around recognizing crypto assets under intangibles)

Also, you are not allowed to combine the acquisition amounts of the same crypto assets across multiple dates to carry out an impairment test; rather, you should track the individual cost basis of each purchased crypto.

Tracking your impairment movements is important as it would show differing final results in your financial statements. The example below provides the entries when an entity tracks impairment instead of not tracking.

DAY 1: You buy 1 ETH for $4,000

Dr ETH - Cost basis $4,000
    Cr - Cash $4,000

DAY 2: Price of ETH rises to $4,600

No entry

DAY 3: Price of ETH drops to $3,750

Dr Impairment exp. $250
 Cr - ETH - Cost basis $250

DAY 4: Price of ETH rises to $3,900, and you sell the 1 ETH

Entry **with** previous impairment

Dr Cash $3900
    Cr - ETH - Cost basis $3,750
        Cr - Trading gain $150

Entry **without** previous impairment

Dr Cash $3,900
Dr Trading loss $100
    Cr - ETH - Cost basis $4,000

DIFFERENT ACCOUNTING TREATMENTS UNDER IFRS AND US GAAP

Based on what we discussed above, below is a summary of the different accounting treatments allowed under IFRS and US GAAP:

Applicable Standard	Framework	Initial Measurement	Subsequent Measurement	Movements in carrying amounts
Inventory	IFRS (IAS 2)	Cost	Lower of cost and net realisable value	Movements above cost - N/A Movements below cost - Profit and loss
Intangible assets - Revaluation model (Requires existence of active market)	IFRS (IAS 38)	Cost	Fair value less any accumulated impairment	Movements above cost - Other comprehensive income Movements below cost - Profit and loss
Intangible assets - Cost model	IFRS (IAS 38)	Cost	Cost less any accumulated impairment	Movements above cost - N/A Movements below cost - Profit and loss
Intangible assets	US GAAP (ASC 350 ‘Intangibles, Goodwill and Other)	Cost	Fair value less any accumulated impairment	Movements above cost - N/A Movements below cost - Profit and loss

“Web3 CFOs need diverse skills to provide financial strategic oversight, navigate evolving regulations, collaborate with technical teams, build robust processes, and align leadership with complex financial and accounting challenges.”

- Raymond Shuai - CrunchSpark

FAIR VALUE MEASUREMENT OF CRYPTO ASSETS

Under IFRS and US GAAP, the fair value is "the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date." *(IFRS 13, US GAAP ASC 820)*

FAIR VALUE HIERARCHY

Fair values are divided into a three-level fair value hierarchy based on the lowest level of significant inputs used in valuation models, as follows:

- **Level 1:** quoted prices in active markets for identical assets or liabilities that the entity can access at the measurement date;
- **Level 2:** observable inputs other than level 1 inputs; and
- **Level 3:** unobservable inputs.

CHALLENGES

Determining the fair value of crypto assets and providing a reliable and consistent audit trail can be challenging as the crypto asset markets;

- **Remain open 24/7**
- **Are not regulated**
- **Vary as the volume and frequency of trades.**

With different exchanges quoting different prices, it's important that you **maintain a consistent approach regarding the pricing source of your crypto assets** where the greatest volume is being traded. Given that markets never close, the recommended practice would be to **use the same time to price the assets**.

Crypto assets like Bitcoin, Ethereum, and Solana are actively traded and, therefore, will have an active principal market. An active market is one in which **transactions for the asset or liability take place with sufficient frequency and volume** to provide pricing information on an ongoing basis. The accounting standards do not define specific thresholds that need to be exceeded in frequency and volume to determine if an active market exists. As such, the determination is subject to professional judgment.

Therefore, if an active market exists for that crypto asset at the measurement date, a Level 1 valuation can be performed. In the absence of an active market, the prescribed guidance is to use a valuation model that can be applied consistently from period to period.

TAX: CALCULATING CAPITAL GAINS & LOSSES

Most finance managers actively track the unrealized gains/losses of their digital assets to make more informed investments and better manage risk.

Calculating capital gains or losses may also be relevant when **taxation on capital gains** is levied. **Capital losses may sometimes be used to offset your tax liabilities**. Typically, only realized gains are relevant for tax reporting purposes.

Capital gains are usually calculated by subtracting the fair market value at the time of sale from the cost basis at which the crypto asset was acquired.

Thus, if your organization is domiciled in a jurisdiction where capital gains taxes are levied on crypto assets, it is important to understand how to assess your cost bases (i.e., what did it cost to acquire the asset) when calculating the profit or loss of transferring, selling, or spending a digital asset.

COST BASIS CALCUATIONS 🧮

There are several methods to calculate cost basis, including:

- First In, First Out (FIFO)
- Weighted average cost (WAC)
- Last In, First Out (LIFO)
- Highest in, first out (HIFO)

These are summarized in the table below:

Cost-basis method	Explanation	Some countries that recognise this method.
First In, First Out (**FIFO**)	Assets acquired first are sold first.	Most commonly recognised method, including countries such as USA, Australia, Germany, Austria, Norway, Switzerland, Singapore
Weighted average cost (**WAC**)	Average price paid for all tokens of that cryptocurrency.	Second most frequently recognised method, including Canada, UK, France, Singapore
Last In, First Out (**LIFO**)	Assets acquired last are sold first.	LIFO is not a standard method for financial reporting of crypto assets but may be used for tax purposes in some countries
Highest in, first out (**HIFO**)	Highest price assets are sold first.	HIFO is not recognized under official accounting standards like US GAAP or IFRS, but may be used for tax purposes in some countries.

Below, we will illustrate these methods' impact on the gains/losses. It is important to note that the explanation below **refers to fungible cryptocurrencies**.

Consider the following example of Janet Saylor, CFO of MacroTactics, a Web3 fund:

- Janet bought 1 BTC in Jan 2017 for $1,000 per BTC
- Janet bought 2 BTC in Jan 2018 for $14,000 per BTC
- Janet bought 5 BTC in Jan 2019 for $3,500 per BTC
- Janet sells 2 BTC in Dec 2024 for $100,000 per BTC

With **FIFO method**, Janet would set her cost basis for the 2024's sale as $15,000:

- Capital gains on 2024's sale = ($100,000 x 2) - $15,000 = $185,000

With **WAC method**, Janet would set her cost basis for the 2024's sale as $11,625:

- Capital gains on 2024's sale = ($100,000 x 2) - $11,625 = $ 188,375

With **LIFO method**, Janet would set her cost basis for the 2024's sale as $7,000:

- Capital gains on 2024's sale = ($100,000 x 2) - $7,000 = $193,000

With **HIFO method**, Janet would set her cost basis for the 2024's sale as $28,000:

- Capital gains on 2024's sale = ($100,000 x 2) - $28,000 = $172,000

As seen above, HIFO often leads to the **lowest capital gains** and tax liabilities. However, the FIFO methodology is the **most widely accepted** cost-basis method. This is because it accounts for the frequent points of purchases and sale of crypto assets across accounting cycles. Discuss with your professional accountant when deciding on your preferred cost-basis method.

OBTAINING CLEAN DATA FOR YOUR COST-BASIS CALCULATIONS

When maintaining your ledger of digital assets transactions, it is essential to review the following data points across each wallet type:

- Transaction fees
- Timestamping of transactions

Not accounting for these may result in erroneous data being used to calculate the cost basis of your team's digital assets.

1. TRANSACTION FEES

When calculating the cost basis of your digital assets, it is essential to account for the fees incurred in the transaction. It is essential to deduct the transaction fees when determining the cost of the said digital asset. Some of these fees include:

1. Gas fees charged by the blockchain protocol
2. Fees imposed by the wallet provider (usually by centralized wallets)

It is important to understand and account for the relevant fees involved in each of these activities. See the table below.

Activity	Explanation	Relevant fees
Revenue	Crypto being used as a payment method.	No fees if the tokens are automatically received into your wallet.
Deposits	Receiving tokens from another party.	No fees as the receiver of the deposit.
Withdrawal (from self-custody wallet)	Transferring tokens out from your team's wallet to another.	Gas fees are incurred by the blockchain that the decentralized exchange is being built on.
Withdrawal (from centralised custody wallet or exchange)		Withdrawal fees charged by the centralised wallet or exchange.
Swap (on a centralised exchange)	The exchange of token types between two parties via a centralised exchange.	Fees charged by the centralised exchange for executing the swap.
Swap (on a decentralised exchange)	The exchange of token types between two parties via a decentralised exchange.	Fees charged by the decentralized exchange are usually programmed in the exchange's smart contract and automatically executed at the swap instance.
Yield Farming (a.k.a. Staking)	Obtaining additional crypto assets due to locking up crypto assets, i.e. staking, in a decentralised protocol or application.	Fees charged by the decentralised protocol. Gas fees charged at the point of withdrawing the rewards earned from the yield tenure.
Airdrop	Obtaining crypto assets due to being a qualified recipient in a campaign	If the airdrop needs to be redeemed, the blockchain on which the airdrop DApp is being built incurs gas fees.

2. TIMESTAMPING OF TRANSACTIONS ⏱️

It is common for Web3 finance teams to have transactions involving both centralized exchanges and self-custody wallets. The good news is that users can quickly export their transaction records (e.g., via the central exchange's records or block explorers such as Etherscan) for both.

However, **centralized exchanges and block explorers often mark the timestamp of transactions in different time zones**.

When compiling a chronological record of transactions across centralized and self-custody wallets, finance managers must ensure the transactions are in the same time zone before compiling them into a master journal. This matters because cost-basis methods such as FIFO require an accurate chronological order of transactions.

It is best to **keep all transactions in the same time zone**, be it UTC or the local time zone of the entity for which financial statements are prepared.

Here are the default time zones for popular block explorers and centralized exchanges. (Updated as of Dec 2024)

Exchange or wallet that the transaction was made from	Source of transaction records & default timezone for transaction records
Self-custody wallets such as MetaMask, Ledger, Coinbase Wallet, Exodus, Phantom, Trust WalletMPC wallets such as Fireblocks, Qredo, FORDefi	Block explorers EtherScan: UTC BscScan: UTC Solscan: UTC SolanaFM: UTC PolygonScan: UTC
Centralised exchanges such as Binance, Coinbase, Coinhako, Gemini, OKX	Binance: local time following IP address Coinbase: UTC Coinhako: local time following IP address Gemini: UTC OKX: local time following IP address

When choosing crypto-native accounting software, ensure that these adjustments for fees and timestamps are accounted for.

DISCLOSURE FOR CRYPTO ASSETS

As there are no explicit IFRS and US GAAP standards for crypto assets, the presentation and disclosure of crypto assets and crypto asset transactions should follow the entity's approach regarding the accounting model to apply to the crypto asset, i.e., as an intangible asset, inventory, a financial asset, or otherwise.

However, such **disclosures require significant judgment** and a thorough understanding of the underlying facts and circumstances.

For example, below are the summarized disclosure details of Microstrategy for their Bitcoin holdings in their most recent annual report;

- The Company determines the fair value based on quoted prices on the Coinbase exchange, the active exchange that the Company has determined is its principal market,

- The Company performs an analysis each quarter to identify indicators for impairment,

In determining if an impairment has occurred, the Company considers the lowest price of 1 Bitcoin quoted on the active exchange at any time since acquiring the specific Bitcoin held by the Company.

"In the fast-evolving crypto landscape, clear and comprehensive asset disclosure helps users of information better understand the value of crypto assets held both in centralised and decentralised finance projects."

- Luis Machado, Head of Finance at CoW Protocol

Financial reporting in crypto

BEST PRACTICES

Maintaining transparency and openness in financial reporting will help to build trust with investors, regulators, and other stakeholders.

Below are four tips on optimizing corporate financial reporting.

By following these best practices, CFOs can ensure that their company's financial reporting is accurate, compliant, and transparent when using cryptocurrencies in its financial operations.

1. LEVERAGE TECHNOLOGY 💪

Implement robust accounting and tax systems that are capable of handling cryptocurrency transactions.

This may include **integrating specialized software or hiring external experts** like the ones in the web3 finance club, to assist with cryptocurrency transactions' accounting and tax reporting.

Enterprises can use accounting software such as QuickBooks, Netsuite, or Sage Intacct to manage their corporate financial reporting.

This software will allow companies to handle their accounts payable, accounts receivable, and payroll quickly and efficiently.

This can include using cloud-based crypto accounting platforms like Request Accounting, data analytics to gain insights, and crypto-powered AR/AP and payment solutions like Request Finance.

Corporate-level financial solutions designed for web3 in the marketplace can be evaluated by their cross-functionality capability between applications.

The right tools can dramatically simplify financial reporting in crypto for Web3 CFOs.

Crypto financial reporting and tax compliance are very difficult to accomplish at scale without a practical crypto bookkeeping solution that consolidates cryptocurrency transactions in one place.

Sophisticated back-office solutions exist for Web3 enterprises to enable scalable crypto financial reporting and compliance.

The core requirement for producing meaningful financial reports from a corporate-level crypto operation is through **a bookkeeping solution designed specifically for cryptocurrency transactions**.

Tracking cryptocurrency transactions is an entire challenge due to the complexities of blockchain and its technical diversity.

This means such a solution would need to be capable of tracking transactions and other crypto data from the following sources:

- Exchanges
- Blockchains
- DEXs
- Defi Protocols
- NFTs
- Neobanks
- Crypto Payments & AR/AP
- MPC-enabled Custody Solutions

With the data sources being supported, the next challenge is data injection. This means that the back-office bookkeeping solution can actually receive the data itself in a secure Read-Only way while having the required dataset for a comprehensive ledger.

Three possible data injection methods need to be supported in order to support every crypto data source available.

- Read-Only APIs
- Blockchain support (more chains, the better)
- CSV support (including a solution native template)

If the above data injections are all available within the back-office crypto accounting solution, there will always be a way to inject the data.

"BE GAAP's silence on digital assets leaves Belgian businesses at a disadvantage, forcing them to interpret ambiguous rules while other jurisdictions like the US and IFRS regions advance their standards. I would love to see advisory bodies step up, acknowledging the urgency to modernize accounting frameworks for the crypto economy"

- Koen Masschelein, Makofisc BV

2. DEVELOP A FINANCIAL STRATEGY 🎯

- Companies should create a comprehensive financial strategy that outlines their goals, objectives, and strategies for managing their corporate financial reporting. This strategy should cover budgeting, cash flow, taxes, and financial forecasting.

- Regularly review and update the company's financial reporting processes and policies to ensure compliance with the latest regulations and best practices. This may include conducting regular internal audits and consulting with external experts as needed.

3. ASSIGN RESPONSIBILITIES 👷

- Companies should assign specific financial reporting responsibilities to members of their organization. This will ensure that all financial documents are accurate and timely.

- Stay informed about the latest cryptocurrency developments and regulations in your country and region. This will ensure that your financial reporting complies with the law and avoid potential penalties or fines.

- Consider implementing a risk management framework to identify, assess, and mitigate potential risks associated with specific cryptocurrencies and platforms.

4. REVIEW FINANCIAL STATEMENTS 🔎

- Companies should review their financial statements regularly to ensure they are accurate and up-to-date. Doing so will enable them to make informed financial decisions and identify potential issues.

- Track the current market value of cryptocurrencies held by the company and adjust the value of the assets in the financial statements accordingly. This will help accurately reflect the company's financial position and avoid potential reporting errors.

- Ensure all cryptocurrency transactions are properly documented and recorded in the company's financial records. This includes keeping track of the date, amount, and type of transaction, as well as the relevant wallet addresses and transaction IDs.

Concluding Thoughts

As we look back on the events of 2024, it's clear that significant challenges and opportunities lie ahead for CFOs leading crypto-friendly organizations.

First, 2024 saw **the continued growth and adoption of DeFi platforms**. We can expect to see more companies and individuals using these platforms to manage their financial assets and conduct transactions without the need for traditional financial intermediaries.

We have also seen the **continued development of broader Web3 technologies**, which enable users to interact more seamlessly with decentralized applications and protocols.

2025 will certainly present challenges and opportunities for Web3 CFOs. One of the biggest challenges will be understanding **the complex and rapidly evolving landscape** of Web3, crypto, and DeFi.

CFOs must develop a deep understanding of these technologies and their potential implications to make informed decisions.

Another challenge for Web3 CFOs will be ensuring compliance with **increasingly complex and varied regulatory frameworks** worldwide.

Despite these challenges, there are also significant opportunities for Web3 CFOs. One of the biggest opportunities has been and will continue to be the ability to **access new liquidity and funding sources** through DeFi platforms. CFOs can use these platforms to raise capital and manage their financial assets in new and innovative ways.

Perhaps most of all, **a natively global system of finance and commerce** can allow Web3 projects and teams to hire, operate, and grow at a scale and reach unprecedented in economic history.

By staying up to date with the latest developments, developing a deep understanding of these technologies, and working closely with legal and compliance teams, Web3 CFOs can navigate the challenges and take advantage of the opportunities.

THE REQUEST FINANCE TEAM

Get in touch

EDITORIAL & CONTENT ✍️

Simran Agarwal, Ecosystem Manager

simran.agarwal@request.finance

CUSTOMER OPERATIONS 💌

Sebastien Pussiau, Regional COO (Europe)

sebastien.pussiau@request.finance

Eduardo, Regional COO (Americas)

eduardo.carvalho@request.finance

Mashudi S, Regional COO (Asia)

mashudi.swidjojo@request.finance

Thomas Barbey, COO (EMEA)

thomas.barbey@request.finance

BUSINESS DEVELOPMENT & PARTNERSHIPS 🤝

Jacob Kobler, Head of Partnerships (Global)

jakob.kobler@request.finance

Interested to hear more?

Reach out to us

simran.agarwal@request.finance
twitter.com/requestfinance
linkedin.com/company/request-finance/

BOOK A DEMO