Explain it to me like I was five - Gnosis Safe

October 2022

Explain it to me like I was 5.

The Digital Asset space is re-writing the way that we can potentially organize capital. Be it physical capital through the way that we remove the need for trusted, centralized intermediaries or human capital in the way that we can coordinate, reward, and motivate a collective to operate in a certain manner. This level of ambition, at its purest and most extreme, is difficult to get your head around for sure. Like any new theoretical construct, it is likely to be adopted in parts where it makes sense and discarded where it doesn't. No one structure or process works for all activities.

What want we wanted to do this month was to use a real-life example of how the ecosystem is adopting this new way of organizing both human and financial resources. In the spirit of one of the popular social media acronyms, "ELI5- Explain like I'm 5 (years old)", we will try to provide a simple explanation to a complex topic.

Our real-life example - Gnosis Safe (rebranded as "Safe")

The Gnosis Safe is an application that we use to store and deploy the Fort Stable Fund's digital assets across the Ethereum blockchain and the applications built on top of it. A unique feature of the way that we custody our assets in the digital asset space is that we control them completely. The record of ownership sits on the blockchain as does the record of transactions. In the traditional financial assets space, we would use a custodian which would maintain and manage the ownership of the assets in FSF's name. Historically they would hold the physical paper (a certificate of ownership) they would maintain a ledger of the owner and adjust that in their records when the ownership changed, they would also register that all with a centralized, governance body. While the process has improved and become largely digitized it still has many intermediaries involved, many which are not necessary in a digital age. While self-custody of assets provides many efficiencies and lowers costs, it presents certain security challenges which is what the SAFE application has been designed to solve.

To understand how Safe enhances security, we need to understand how addresses or accounts work on the Ethereum blockchain. There are two types of accounts on Ethereum, EOAs – Externally Owned Accounts, and SCAs – Smart Contract Accounts.

EOAs use traditional key pairs. They consist of a single private key that can be used to make transactions and sign messages. If you gain access to the private key, you gain full control of the account. Most popular wallets such as MetaMask are simple EOAs and even hardware wallets such as Ledger or Trezor are based on EOAs. This means that only your private key-a single point of failure-stands between you and your funds being lost.

SCAs – these are what Safe uses and what the Gnosis team believe are the key to mass adoption in the digital assets space. Like EOAs, SCAs each have a unique public Ethereum address and it's impossible to tell them apart by looking at an Ethereum address on Etherscan, for example. The key difference is that no single private key is used to verify transactions. Instead, logic in the smart contract determines how the account completes transactions.

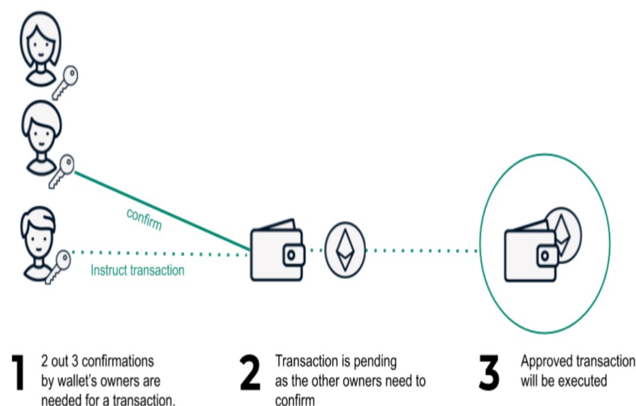
WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

So what exactly is Gnosis Safe?

It is a multi-signature (multisig) smart contract wallet. Multisig wallets are cryptocurrency wallets that require two or more private keys to sign and send a transaction. The storage method requires multiple cryptographic signatures (a private key's unique fingerprint) to access the wallet.

Multi-signature Wallets

Multi-signature wallets are contract accounts that require multiple parties to confirm a transaction before it can be executed. These parties, each represented by a unique Ethereum account address, are defined as multi-signature wallet owners in the smart contract. Only when a predefined number of these owners confirm a transaction, will the transaction be executed. Hence, the single point of failure associated with private key-controlled accounts is removed; losing or compromising a private key will no longer automatically result in a loss of all funds controlled by the account.



You can imagine the wallet as being like a bank vault or a safe that requires more than one key to open it. You can choose how many keys are allowed to open the safe as well as the minimum number of keys needed to unlock it (e.g., you could have a 2-of-3 multisig where two out of three assigned private keys are needed, 3-of-5, 5-of-7, etc.).

Some of the more notable users of multisig wallets are crypto exchanges, brokers/OTCs, investment funds and other crypto companies which use multisignature storage to secure their cold storage funds. Exchanges, brokers and the like distribute admin keys for their funds to distribute the risk; if hackers want access to their reserves, they're going to need several keys to do so. Similarly, multisig ensures no one person in a firm can unilaterally withdraw funds from the wallet. The more signatures you need to execute a transaction, the more distributed the decision-making process can be.

Other specific use cases may involve setting up a shared account among family members (for, e.g., a trust or estate) or an escrow account (for, e.g., a bet or a sale of property).

Traditional Custody enforces something akin to the above process for a fee and slows the process as a trade works through the infrastructure. The "knock" or introduced risk on self-custody is the finality of transactions. Instant and largely nonreversible transactions is indeed a feature of the process that can be daunting initially. The Positive side is increasing the speed of transactions to virtually instantaneous vs a minimum of T+2 (today plus two days) settlement. This is a huge saving in capital efficiency on the individual as well as on the macro level. This is particularly the case in a world with interest rates above zero, the concept of "the float" that is someone holding on to your money earning interest on it just to verify that you are who you say you are, you have the authority to move the funds and the destination is correct is now a real business again and a significant cost for investors.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Past performance is not indicative of future performance

An interesting event occurred earlier this month. FSF received or, in the parlance of the space, was "airdropped" approximately 4,300 SAFE tokens. These were gifted to us as an early user of the Gnosis Safe wallet. We can't attribute any monetary value to these tokens until they commence trading and a date for that has yet to be determined.

We thought that this event would serve as a useful basis for providing a brief discussion of some of the key topics coming up in crypto currently in terms of how protocols interact with their users, community and potentially also with regulators.

Airdrops, Tokens and DAOs.

Definitions:

- Airdrop – The free granting of a token that is transferrable on the designated network. They appear in your wallet at the discretion of the DAO of the protocol or product you are using
- Tokens – A programmable asset that exists on a blockchain.
- DAO – Decentralized Autonomous Organization – It's a collective who "vote" on changes any aspect of the endeavor it is linked to. The votes are cast by those who own the tokens, think of it as shareholder meeting.
- A security is defined by something called "the Howey test" – A security is "the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others."

The SAFE Token Airdrop

Why would Gnosis issue a token and why would they just Airdrop them? The conventional way to build brand is advertising through channels where potential users would be exposed to your product. Equally product placement or the payment of influencers to build a perception of momentum taking advantage of human behavior and speeding the adoption curve. As we know however one of the most effective ways to enhance adoption is personal recommendation. By financializing engagement and rewarding your early adopters who communicate the benefits of usage you can potentially accelerate your product lifecycle. Also, as these tokens are cheap (free to mint) and programmable they can be constructed to best reward your users.

The aim of the airdrop is to ensure decentralization in the newly launched SafeDAO. It is also about rewarding active users and raising awareness about Safe as a project and DAO. "By giving control over the core components of the Safe ecosystem to the SAFE Token holders, the SafeDAO is enabled to introduce value capture and reward programs that supercharge the Gnosis Safe ecosystem flywheel," Safe Co-Founder Lukas Schor revealed in the proposal

"[The February proposal] presented plans of launching a SAFE token. 5% of the total supply is allocated to reward users for their past contributions and usage. Of those 5%, half will be available immediately, and the remaining half will be vesting linearly over 4 years,"

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Safe Co-Founder Tobias Schubotz wrote, adding, "Long term, we envision the Safe as a community-driven project. It is empowering to own a part of the product they use."

Gnosis Safe had a successful funding round of $100 million in July. The company is also looking to set up the Safe Foundation in Switzerland. The foundation will oversee the intellectual property, GitHub repositories, investments, and issuance of the SAFE token.

The Gnosis Safe has users ranging from DAOs, institutions and individuals. These include ConsenSys, Aave and Synthetix. It secures more than $38 billion worth of assets.

Is the Gnosis token a security?

That's unclear and the subject of much debate for tokens in general.

Let's break it down into the components of the Howey test which is the measure by which in the USA something is determined to be a security.

- "The investment of money in a common enterprise" – well they were airdropped to us they are closer probably to a loyalty or reward scheme in this context.
- "A reasonable expectation of profits to be derived from the efforts of others." – again it's not clear what benefits the tokens will accrue. The regulators are working hard globally to try and create a framework to define exactly what a token is and where it fits in the capital stack.

One of the key questions that issuers look to create is what are referred as the Tokenomics that encourage the desired outcome and are set to differentiate them from common securities. Tokenomics are an important theme in crypto that aligns the interests of the token holders with the actual protocol. The tokenomics determine the way that the tokens are issued (free in this case) what rights they have (voting in the DAO) how many there are and the distribution schedule (vesting) and what claim they represent over any income generated (dividend). To date there has a been a conscious avoidance of registering tokens as securities and more of an attempt to avoid that classification.

So, it could be argued that under the first part of the rule these tokens aren't a security as there was no investment of money in a common enterprise. Rather it's a reward for being an early user and adopter and hopefully something that encourages us to engage with the project and evangelize it to others. The second part of the test, do we have a claim over the profits? Generally, the answer here is no as revenues and profits accumulate in DAO treasury to be re-invested in developing and advancing the project. As a token holder we have no claim over them. Employees have been rewarded and paid in these tokens also as set out under the rules of the DAO.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Successful projects such as Uniswap have amassed significant Treasuries but to date there is no plan to distribute these. Interestingly the ownership of the token doesn't have a claim on this treasury directly or indirectly. The token does, potentially, allow a vote on creating a process to redeem this treasury, however given the concentration of ownership by the creators and developers this is not something that will happen without their involvement.

Not all tokens have been issued with community building in mind. Over the "DeFi summer" we saw a rapid growth of the issuance of tokens for protocols and the establishment of highly complicated yield farming and staking structures. These were largely inflationary schemes where investors would "lock-up" the tokens for a period of time (i.e. agree not to sell) and be rewarded with the issuance of even more tokens, a "yield" of sorts. In an idealized world the structure is designed to increase engagement and traction in the underlying protocol with the view that activity would at some stage grow to the point where demand would outstrip the issuance reward. At its worst tokens for products that had a limited use case would offer unsustainable yields to attract buyers while issuing unsustainable quantities that meant that the project would have Ponzi like characteristics.

One would imagine Gnosis would equally, as it succeeds and gains traction, accumulate a treasury that they would use to further develop the product and the ecosystem. We would, with the tokens we hold, participate (by delegation) in any votes that were proposed by the DAO but these would not be related to accessing a Treasury or income stream.

Why would Gnosis create a DAO as opposed to a company?

A DAO is a way of coordinating both human and financial capital that is enforced through code. The rules of the DAO are set out at its initiation, the process for proposing votes, the process of voting and the application of the approved changes.

According to the experts, we're right now in the year of the DAO (or Decentralized Autonomous Organization). As of February 2022, there are at least 188 DAOs controlling over $12 billion in assets. These organizations have huge potential: they're digitally native, transparent by design and their community-led ethos means they can often scale faster than traditional top-down organizations.

Right now, most DAOs exist in a legal grey area- somewhere between a co-op and a small business. As DAOs continue to amass impressive treasuries and grow in number — it's becoming an imperative to protect stakeholders from legal liability and to have an appropriate structure for looming taxation. The state of Wyoming is a pioneer in this area — allowing DAOs to set up as LLCs,

One of the other reasons for selection of a DAO is the flexibility regarding the raising of capital, falling outside the regulatory regime is also clearly attractive in accelerating your growth trajectory. Issuing Tokens from an unregulated structure has been by far the cheapest and fastest way to raise capital.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Safe in Action

We will watch with interest as Safe undertakes it's mission of facilitating mass adoption in so called Web 3.

The Twitter link provides some key insights from Lukas Schor.

"There is a common misconception about Safe. As Safe is NOT a product, it is NOT a Multisig and it is NOT a DAO tool. Rather, Safe is a Web3 ecosystem built with a composable smart contract-account (Safe) at its heart." "Making every blockchain account a smart contract has been a long-lasting dream of Ethereum core developers. This effort is commonly known as "Account Abstraction (AA)".

"Benefits of smart contract accounts go far beyond just enabling Multisig wallets and powering DAOs. Bringing security and usability improvements across the board and for every user of web3."

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Disclaimer

Fort Canning Asset Management Pty Ltd (CAR) is a corporate authorised representative of Boutique Capital Pty Ltd (BCPL) AFSL 508011, CAR Number 1284461. CAR is an investment manager of the fund(s) described elsewhere in this document, or in other documentation (Fund).

To the extent to which this document contains advice it is general advice only and has been prepared by the CAR for individuals identified as wholesale investors for the purposes of providing a financial product or financial service, under Section 761G or Section 761GA of the Corporations Act 2001 (Cth).

The information herein is presented in summary form and is therefore subject to qualification and further explanation. The information in this document is not intended to be relied upon as advice to investors or potential investors and has been prepared without taking into account personal investment objectives, financial circumstances or particular needs. Recipients of this document are advised to consult their own professional advisers about legal, tax, financial or other matters relevant to the suitability of this information.

The investment summarised in this document is subject to known and unknown risks, some of which are beyond the control of CAR and their directors, employees, advisers or agents. CAR does not guarantee any particular rate of return or the performance of the Fund, nor does CAR and its directors personally guarantee the repayment of capital or any particular tax treatment. Past performance is not indicative of future performance.

The materials contained herein represent a general summary of CAR's current portfolio construction approach. CAR is not constrained with respect to any investment decision making methodologies and may vary from them materially at its sole discretion and without prior notice to investors. Depending on market conditions and trends , CAR may pursue other objectives or strategies considered appropriate and in the best interest of portfolio performance.

There are risks involved in investing in the CAR's strategy. All investments carry some level of risk, and there is typically a direct relationship between risk and return. We describe what steps we take to mitigate risk (where possible) in the Fund's Information Memorandum. It is important to note that despite taking such steps, the CAR cannot mitigate risk completely.

This document was prepared as a private communication to clients and is not intended for public circulation or publication or for the use of any third party, without the approval of CAR. Whilst this report is based on information from sources which CAR considers reliable, its accuracy and completeness cannot be guaranteed. Data is not necessarily audited or independently verified. Any opinions reflect CAR's judgment at this date and are subject to change. CAR has no obligation to provide revised assessments in the event of changed circumstances. To the extent permitted by law, BCPL, CAR and their directors and employees do not accept any liability for the results of any actions taken or not taken on the basis of information in this report, or for any negligent misstatements, errors or omissions.

This Document is informational purposes only and is not a solicitation for units in the Fund. Application for units in the Fund can only be made via the Fund's Information Memorandum and Application Form.