Enabling cost-effective, compliant access to decentralized finance (DeFi)

This article is a collaborative effort between Chainlink and Trustology. Chainlink is a blockchain company that has been pioneering smart oracle technology since pre-Ethereum Mainnet. Trustology provides high-end, secure custodial wallet solutions for institutional and individual clients.

Are you a crypto investor looking to get into DeFi but blocked by the lack of institutional features such as Know Your Customer (KYC), Anti-money Laundering (AML), and insured crypto custody capable of supporting DApps? Or are you a DApp developer looking to add such features to your project, but haven't found tangible solutions? Read on!

The crypto economy is evolving at lightning speed. Bitcoin is just over 10 years old and Ethereum emerged in 2013 promising a wider range of applications. In that short time, we progressed from a single decentralized virtual currency to smart contract-based blockchains supporting thousands of different crypto assets.

However, no economy can survive with just asset issuance and transfer. You need payments, exchange, lending, borrowing, hedging, etc. At first, this was solved by centralized systems, but that brought back old issues - the proliferation of intermediaries, the need to reconcile, lack of transparency, and reliance on central operators.

Fast forward to today and we see the emergence of DeFi applications that offer the same capabilities as current centralized ones, but now in a decentralized manner (DApps). In fact, using blockchains as back-end infrastructure to power common financial instruments is becoming one of the most popular uses for smart contract applications. The DeFi movement is gaining momentum as popular decentralized protocols like MakerDAO, Compound, and Synthetix grow user adoption with their ability to facilitate peer-to-peer capital markets.

This could only be the start as well, as DeFi is only scratching the surface in regards to unlocking capital markets. According to the Chainlink Mixicles Research Paper "The aggregate value of capital markets alone (very roughly $200Tn) dwarfs that of markets that lend themselves to basic tokenization, such as venture capital (approximately $250Bn in 2018 [53]) and gold (roughly $9Tn total value at current market price). There is potentially vast untapped value still waiting to migrate on-chain."

These apps clearly have their upsides such as offering easier access to crypto financing solutions like borrowing, lending and trading of cryptoassets. But they also have their downsides such as speed, privacy, and the old chestnut - regulation.

While individuals may be willing to use DeFi DApps without knowing the counterparty or implementing custody provisions, institutional players cannot. They are subject to the full weight of Know Your Customer (KYC), Anti-Money Laundering (AML) and Combatting the Financing of Terrorism (CFT) regulations. In other words, they need to know who they are dealing with.

Knowing identity is a crucial component from both operational and legal standpoints for real-world business processes that involve financial contracts. Given the current uncertainty around regulatory environments, it's very risky and irresponsible for financial entities with large capital allocations to interact with new DeFi instruments. While centralized solutions for KYC/AML compliance using trusted third parties or on-chain whitelisting do exist, these centralized systems require users to either trust an intermediary with their identity or incur high network costs to implement on the blockchain.

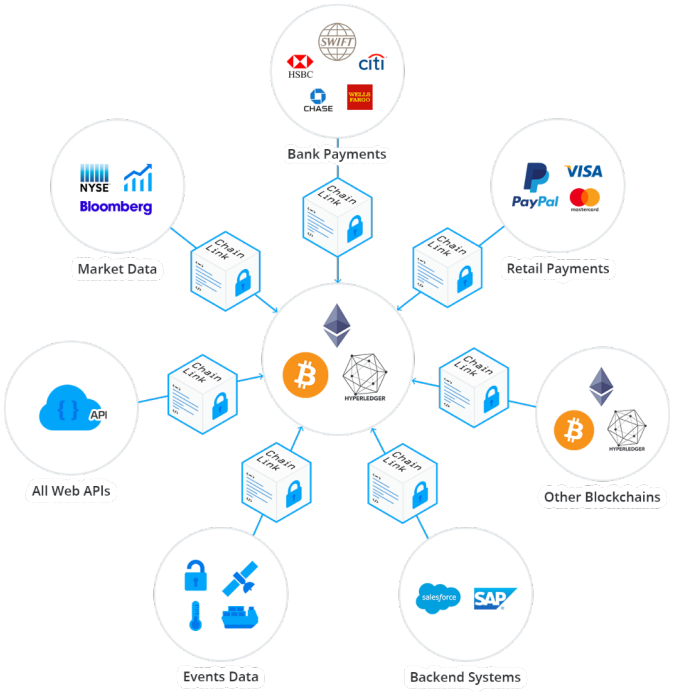
These regulatory requirements are becoming increasingly prevalent as the EU has recently updated 5AML directives that go into effect next year which creates much more stringent AML obligations for everyone, not just institutions, when dealing with crypto assets. Given the international nature of crypto and regulation, it is likely that similar changes will soon occur elsewhere around the world.

Regulation is unavoidable, so instead of fighting the inevitable, is there a way to cheaply unlock Defi for regulated players? There are a couple of options we have considered that are worth exploring in this blog.

Option 1 is to create an on-chain smart contract and pre-populate it with KYC'ed addresses, i.e. a whitelist contract. Whenever someone tries to use a DApp, the DApp contract will call the whitelist contract and proceed only if the transaction signer is on the list.

This is potentially a very expensive option, as someone has to pre-populate the list with every possible KYC'ed address. That cost is likely to be borne by either the DApp project or someone who performs KYC checks, like a custodian. For example, if a DApp has 100k users

and each update costs 10c, that's $10k off the bat for the first round of users and you still need to maintain the contract of KYC'd addresses. Some Defi DApps already employ this option, but it is expensive to preemptively maintain in terms of gas needed to upload and validate addresses, many of which might not be used or are only used once for security purposes. Additionally, there may be privacy concerns depending on how all KYC'd addresses are stored on-chain, ie encrypted vs. non-encrypted.



Instead of trying to store all the data needed to verify identities on a particular blockchain (on-chain), which is shown to be expensive, impractical, and creates network congestion, it may be most optimal for the smart contract to retrieve and return identity data from outside its network (off-chain) when needed.

Enter Option 2, using oracles and smart contracts for a cheap, yet reliable end-to-end solution.

Using oracles for off-chain connectivity

An oracle is a digital agent employed by a smart contract to retrieve and/or connect it to data and systems outside its native blockchain (off-chain). Oracles enable this off-chain connectivity for the smart contract by reformatting external connection points (APIs) so that two different software applications are compatible for data exchange. The oracle then pulls data into the smart contract and/or pushes data out based on predefined instructions and endpoints outlined in the Service Level Agreement (SLA). Under this method, DeFi smart contracts can use oracles to call off-chain APIs that possess the necessary identification data to return true/false answers to on-chain queries regarding KYC and AML.

Chainlink is a decentralized oracle network that gives smart contracts secure and reliable access to data providers, web APIs, enterprise systems, cloud providers, IoT devices, payment systems, other blockchains and much more. It features the following:

- A robust market of independent oracles providing a range of data and connections
- Flexibility to customize an oracle connection including the number of oracles, types and number of data sources, aggregation strategies, staking deposits, trusted execution environments, Mixicles and more
- A reputation framework for evaluating oracles based on on-chain metrics

It's an all-in-one network for users to customize how their contract communicates with anything off-chain using varying levels of decentralization, data aggregation, and oracle selection. Learn more by visiting the Chainlink website, Twitter or Telegram. If you're a developer, visit the developer documentation or join the technical discussion on Discord.

Having the right custodial wallet interface: a look at TrustVault

Trustology has developed an insured key and transaction management system called TrustVault. Deployed as a mobile app, TrustVault provides an easy to use interface that is accessible 24/7. Using TrustVault APIs makes it possible to create linked user and wallet accounts with which to submit blockchain transactions in a secure and controlled manner.

A user's KYC and contact data is managed at the user account level. User accounts also reference user's private keys on their registered end-user device, such as instruction keys stored in the secure enclave of an iPhone, or in a smart card.

These on-device keys let TrustVault know that the transaction has been signed by an authorized person or computer system on a secure device, i.e. offers non-repudiation and integrity guarantees. They are not the keys, however, that are used to sign on-chain transactions, as those are signed by linked on-chain policy wallet keys. So it's not a problem if a user loses their on-device keys, as new ones can be remapped to existing on-chain wallet keys.

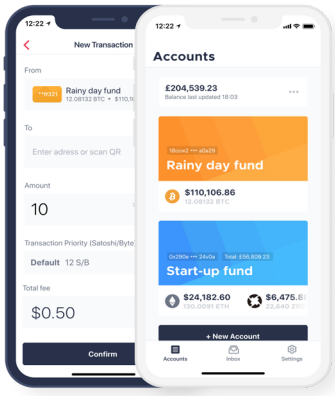
On-chain private keys are managed by a user's wallet accounts. From these keys, the wallet accounts generate BIP32 private-public key pairs and associated public addresses. Users can configure their wallets to be single or multi-signature, and have controls attached, e.g. AML, whitelists. The private keys themselves are always generated and used only by our custom firmware inside data center hosted hardware security modules (HSMs) which contain encrypted backups stored in the cloud.
With TrustVault, users can easily create BTC, ETH and

ERC-20 transfer transactions using Trustology's helper APIs. In addition, TrustVault's recent integration with MetaMask allows users to let the DApp generate the transaction in the browser or craft their own in code using their private keys. So users get all the benefits of MetaMask, without the risk of signing with in-browser keys. Alternatively, they can also benefit from the use of oracles, which send signed and unsigned transactions to TrustVault. Straight-through-processing can be achieved with signed transactions whereas unsigned transactions are more useful when there is a need for a human to sign. All submitted transactions are inspected, and if they don't pass account configured controls, e.g. AML and whitelist checks, they are rejected.

Accepted unsigned transactions are pushed to a user's inbox, which is accessible via the mobile app on the registered device. Once the transaction is signed on the device by one or more humans, as per the wallet policy settings, the transaction is sent for re-signing in the HSM.

TrustVault firmware then re-signs transactions in approximately 350ms. If all policy specified on-device key signatures are present, TrustVault HSM firmware resigns the transaction with the wallet's on-chain keys and submits it to the network-connected blockchain node.

All TrustVault wallet managed addresses are tracked by blockchain indexers. This means users can be notified whenever they receive any assets into their accounts, as well as when their transaction has been confirmed on-chain. Trustology can perform Know Your Transaction (KYT) checks for AML purposes on both inbound and outbound address transactions.



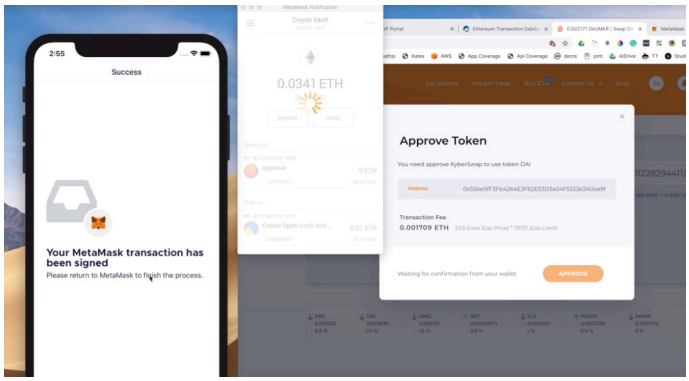
Since TrustVault generates new keys for each new wallet account and never commingles users' assets on one public address, users can use all of their favorite blockchain tools natively within the app. For example, use Etherscan to see transactions for their wallet address, CoinTracker for portfolio analysis, Cryptio for tax accounting, and Vauban for NAV reporting. Users can also conveniently view their address balance and past transactions, as well as submit and sign new ones direct from their mobile app, which also hosts the app's transaction signing inbox.

As Trustology conducts KYC on every user and maps each end-user to their private keys under our custody, we can thus interface with the Chainlink's oracle using our TrustIdentity API and return true/false to the DApp to allow or reject the transaction. For example, let's say the DApp needs to make sure that the person associated with the public address is a resident of the UK. Chainlink oracles will pick up the job, call the TrustIdentity API, which will reverse lookup the user associated with the address, check the residency value, and return a result of true if the user is indeed in the UK, or otherwise false.

Use case scenarios

Would it not be great if you could check 'just in time'? Instead of pre-populating a whitelist contract, you can use smart oracles the operate in near real-time. Here is how it could work.

The user, let's call her Alice, navigates to a DApp's web page and connects her browser wallet, e.g. MetaMask. For this to work, Alice will need to have pre-configured the TrustVault to MetaMask integration, so as to use TrustVault managed accounts.



She creates her transaction on the web page, which prompts MetaMask to sign it. A push notification is sent to the TrustVault app, and once signed by Alice, the transaction is re-signed by TrustVault and sent to the blockchain network. In other words, Alice signs the transaction with her TrustVault keys.

The DApp's contract now sends a new request to Chainlink's oracle contract, which is monitored by external smart oracles. An oracle picks up the new job, which includes Alice's TrustVault wallet address and call-back info to the originating DApp contract.

The oracle then calls TrustVault's TrustIdentity API, and asks some simple questions, e.g. is this an address that is known to you, and has it been KYC'ed to the required standard, as agreed between the DApp and Trustology.

Assuming the oracle receives a positive confirmation, the oracle calls its contract on-chain, which triggers a call-back transaction to the originating DApp contract, and the transaction completes as intended.

Conclusion

Not only does this method of using oracles for off-chain connectivity work, but it reduces upfront costs associated with pre-populated whitelists and allows for continual re-verification of the user. However, there is still the potential for oracles to be hacked, which means it's very important to have the right custodial controls in place to limit the damage. Hence, leveraging TrustVault enforces whitelists and limits controls to ensure that a hacked oracle is prevented from stealing assets from user accounts.

If you are crypto investor looking to get into DeFi but have hit a roadblock because you need KYC and AML controls and an independent custodian capable of supporting DeFi securely, or a DApp developer looking to offer KYC and AML support to your project, please do reach out to us to discuss in greater detail your needs, and see if we can build a solution to meet them.

Contact @chainlinkofficial
Join the discussion on Discord

The Chainlink network provides reliable tamper-proof inputs and outputs for complex smart contracts on any blockchain.

Contact us: info@trustology.io

Trustology's vision is to create the most compelling cryptoassets company of the 21st century. Our first focus has been securing and managing cryptoassets with our TrustVault platform technology.