HALF EPSILON

DIGITAL ASSET CUSTODY AND TRANSFER SOLUTION

JOIN THE INTER-CUSTODIAN NETWORK TO TRANSFER DIGITAL ASSETS INSTANTLY WITH COMPLIANCE AND CONFIDENTIALITY

WHITE PAPER v 1.1

January, 2021

Contact: hello@halfepsilon.com

AUDIENCE AND PURPOSE

The audience of this white paper includes security architects, technical leaders and business leaders in the Virtual Asset Service Providers (VASPs) industry considering new and better approaches to help secure Digital Assets, reduce transfer costs, maintain confidentiality of their transactions and comply with upcoming regulations for the VASP industry, specifically FATF's Travel Rule.

In addition to providing best in class custody of Digital Assets, Half Epsilon Digital Asset Custody and Transfer Solution (DACTS) enables a fundamental change to how assets are transferred between VASPs. It allows direct inter-VASP transfers of Digital Assets without the transactions being submitted to a blockchain. The transfers are instant, confidential and Travel Rule compliant. They also do not suffer from variable transaction fees.

EXECUTIVE SUMMARY

VASP concerns can be grouped into three categories; concerns related to storage of Digital Assets, concerns related to transfers of Digital Assets, and concerns related to tokenization.

Storage Related Concerns

- How do we store Digital Assets securely?
- How to protect against insider theft?

Transfer Related Concerns

- How to transfer Digital Assets instantly?
- How to maintain confidentiality of Digital Asset transfers?
- How to deal with variable transaction fees offered by blockchains?
- How to comply with regulations, specifically FATF's Travel Rule?

Tokenization Related Concerns

- How to jointly enforce confidentiality, security and compliance of inter-institution token transfers while ensuring decentralization?

Custody solutions in the market today do address storage related concerns to a large extent. But concerns related to Digital Asset transfers remain unaddressed. Half Epsilon DACTS offers a holistic solution to both types of concerns. VASPs on the Inter-custodian Network can transfer Digital Assets to each other in a peer-to-peer fashion without any intermediaries.

INTRODUCTION

Over the last few years, we have seen a historic migration of Digital Assets from individuals to VASPs. VASPs fall in one or more of several categories. There are Exchanges, Lending Desks, Market Makers, Hedge Funds, and OTC and Brokerage firms. In addition, both neo and established banks are getting into custody and servicing of Digital Assets globally.

All these entities have common concerns regarding storage and transfer of Digital Assets. Thefts are commonplace, both by outsiders and insiders. According to Forbes [1], hackers stole $4 Billion worth of Digital Assets by mid-August, 2019. The Hardware Security Module (HSM) industry has responded with products that protect against outsider threats by ensuring secure management and use of private keys. Some HSM providers also address insider threats by enabling policy-based quorum approvals for allowing Digital Asset transfers. There are also some Multi Party Computation (MPC) based solutions in the market today that rely on a group of entities to engage with each other and jointly sign transactions.

VASPs are also concerned about the speed at which transactions are settled on blockchains. Depending on the blockchain, transactions may take hours to settle. When transferring large values, VASPs often send out a small valued transaction first to ensure that the blockchain address has been correctly shared and that the end-to-end transfer is possible before sending out the large value. This doubles settlement latencies.

Very few blockchains protect confidentiality. In most cases, transaction graph analysis is possible and originator and beneficiary VASPs can be readily identified from publicly recorded information. Financial institutions do not publicly share competitive information and only reveal it to the correct authorities. VASPs suffer on this account because of the nature of their business and no practical solution to this problem exists today.

Popular blockchains are often congested and overwhelmed with traffic. This has led to a steady increase in transaction fees. As blockchains become popular, transaction fees rise. Also, the transaction fees are variable and depend on the real-time demand for the blockchain resource. This imposes a steadily increasing yet unpredictably variable cost to VASPs. Often, this cost is transferred to the customers of VASPs. VASPs and their customers would benefit tremendously with predictable costs of Digital Asset transfers.

VASPs also have to contend with regulatory compliance of their Digital Asset transfers. National governing bodies heed advice from global bodies such as the Financial Action Task Force (FATF) in order to arrive at regulations for VASPs in their jurisdiction. A particularly damning regulation for the VASP industry is the mandate that they have to comply with FATF's Travel Rule. The Travel Rule mandates that the information of payer and payee should travel with the payment message. At the time of this writing, the VASP industry is struggling to adhere to this mandate. In recent times, an inter-VASP messaging standard has been proposed [2] and also a few implementations of the same exist [3, 4]. These solutions offer an overlay solution for Travel Rule compliance. An ideal solution would be one where the

payer-payee information travels with the settlement message itself. However, no such solution exists today.

A critical component of Half Epsilon DACTS is the One Time Spend Machine (OTSM). Half Epsilon OTSM is an industry grade HSM with custom logic that prevents it from spending the same Digital Asset more than once. OTSM can be used to create *Digital Asset Titles* for locked up Digital Assets. These titles can be transferred from one OTSM to another in peer-to-peer fashion without intermediaries. A VASP has the option of transferring a Digital Asset Title to another VASP or to claim ownership of the locked up Digital Asset. Payer and payee information flows along with an ownership title. The transfers are instant, confidential and do not incur any transaction fees. Given the nature of transfers, there is no upper limit on the transaction throughput of the Half Epsilon inter-VASP network.

In the following section, we describe the Half Epsilon OTSM. Then, we describe the custodian smart contract where Digital Assets are securely stored until they are redeemed. Then, we describe Half Epsilon DACTS. After that, we describe the architecture of the Half Epsilon inter-VASP Network. Finally, we describe the unique use cases that our technology enables and conclude the white paper.

ONE TIME SPEND MACHINE

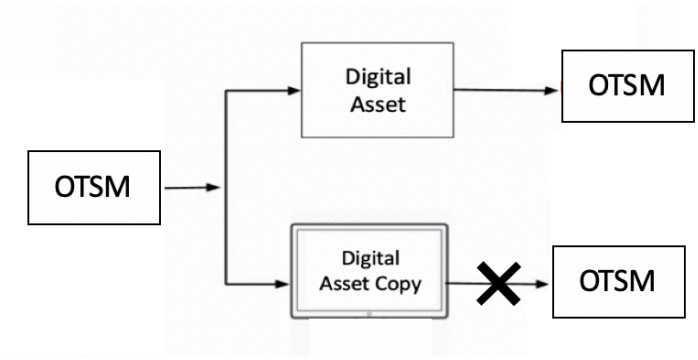

Figure 1: Half Epsilon OTSM cannot transfer a Digital Asset more than once.

Half Epsilon OTSM is a blockchain HSM. Its base functionalities are similar to those of other blockchain HSMs in the market.

- Like other blockchain HSMs, it provides secure and resilient key management for Digital Assets. This protects against outsider attacks as the private keys are never available outside the secure HSM environment.

- Like some other blockchain HSMs, it provides the ability to enable quorum approvals to authorize Digital Asset transfers. This protects against malicious insiders.

In addition, Half Epsilon OTSM offers API to facilitate the management of Digital Asset Title.

- *lockDA()*: This API creates a blockchain transaction to lock up a Digital Asset in the custodian smart contract.

- *createTitle()*: This API creates a new Digital Asset Title for the locked up Digital Asset.

- *transferTitle()*: This API transfers the title to another VASP on the Inter-custodian Network.

- *destroyTitle()*: This API destroys a Digital Asset Title and returns a cryptographically verifiable proof of the fact.

- *unlockDA()*: This API creates a blockchain transaction to unlock a Digital Asset from the custodian smart contract.

Half Epsilon OTSM provides the basic capabilities required for DACTS.

SOFTWARE ONLY OTSM

Several practical scenarios require that a physical HSM may not be used. It may be considered impractical from a cost effectiveness or a management overhead point of view. Companies such as Fireblocks [5] and Curv [6] are coming in with newer approaches to digital asset custody which involves Multi-Party Computations (MPC). It is possible to build OTSM leveraging the MPC approach.

CUSTODIAN SMART CONTRACT

The custodian smart contract operates on a blockchain. It provides two capabilities:

- *lock()*: This function allows a VASP to lock Digital Assets into the smart contract.

- *unlock()*: This function allows a VASP to provide a cryptographic proof of having destroyed a Digital Asset Title and to reclaim the corresponding locked up Digital Asset.

The custodian smart contract has been audited by well-known auditors for security and efficiency.

REGULATED CUSTODIANS

In addition to the custodian smart contract, regulated custodians can maintain custody of Digital Assets and issue their own digital IOUs as Digital Asset Titles. Digital Assets need not just be crypto-currencies. They may represent claims on equities, fiat currencies, bonds, or any other financial instrument.

DIGITAL ASSET CUSTODY AND TRANSFER SOLUTION

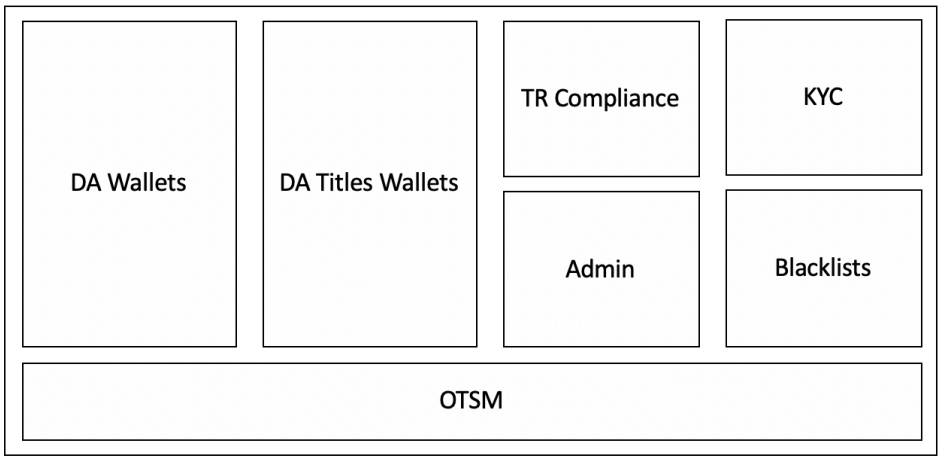

Figure 2: Components of Half Epsilon DACTS.

Apart from the OTSM, DACTS includes several other components.

- **Digital Asset Wallets:** These are wallets for blockchain native crypto-currencies. A user is able to transfer these to anyone with a blockchain address; not just someone on the Inter-custodian Network. A user is also able to convert these to Digital Asset Titles.

- **Digital Asset Title Wallets:** These are wallets for Digital Asset Titles. Digital Asset Titles can be transferred in a peer-to-peer manner without any intermediaries among VASP users in the Inter-custodian Network. A user is also able to convert Digital Asset Titles to blockchain Digital Assets.

- **Travel Rule Compliance Module:** This module brings Travel Rule compliance to the Inter-custodian Network. Both Digital Assets and Digital Asset Titles are transferred with Travel Rule compliance. We follow the IVMS-101 messaging standard.

- **KYC Module:** Each VASP maintains KYC information about its customers. This information is useful for Travel Rule compliance.

- **Admin Module:** Administrators get to add and manage users. They also get to manage relations with other VASPs.

- **Blacklists Module:** Admins can choose to blacklist individual users, even those belonging to other VASPs. Admins can also blacklist other VASPs. Transfers to blacklisted users and VASPs are blocked.

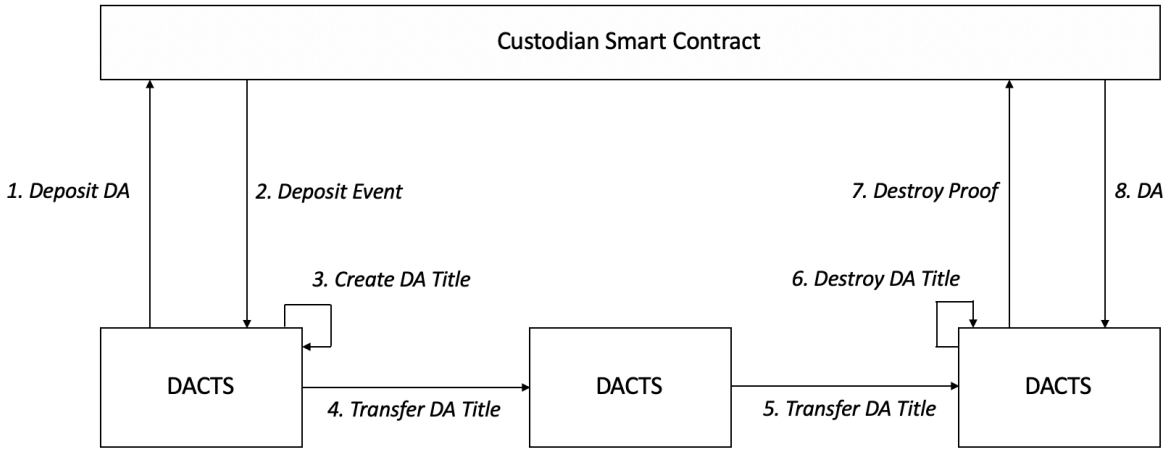

Figure 3: DACTS can convert a blockchain Digital Asset to a Digital Asset Title. The title can be transferred between VASPS. A VASP may choose to destroy a title and redeem the locked up Digital Asset.

A user is able to login into DACTS and transfer Digital Assets by submitting transactions to the blockchain as usual, convert them to Digital Asset Titles, transfer titles on the Inter-custodian Network by simply selecting them and choosing a payee. They can also convert Digital Asset Titles back to Digital Assets.

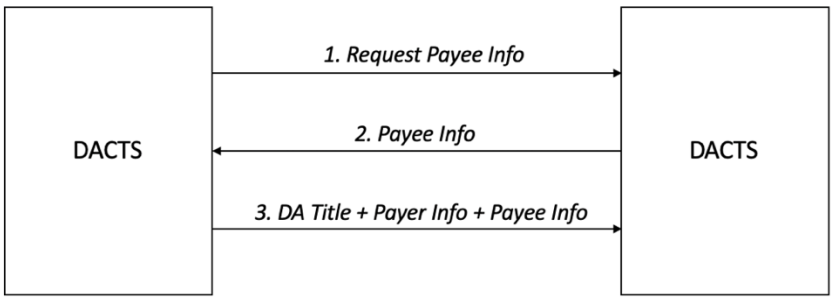

Figure 4: Travel Rule Compliant Digital Asset Title transfers.

Before executing a transfer over the Inter-custodian Network, an originator VASP queries the beneficiary VASP for KYC information of the payee, and adds the payer and payee's KYC information to the payment message before transferring the Digital Asset Title to the beneficiary VASP.

INTER-VASP NETWORK

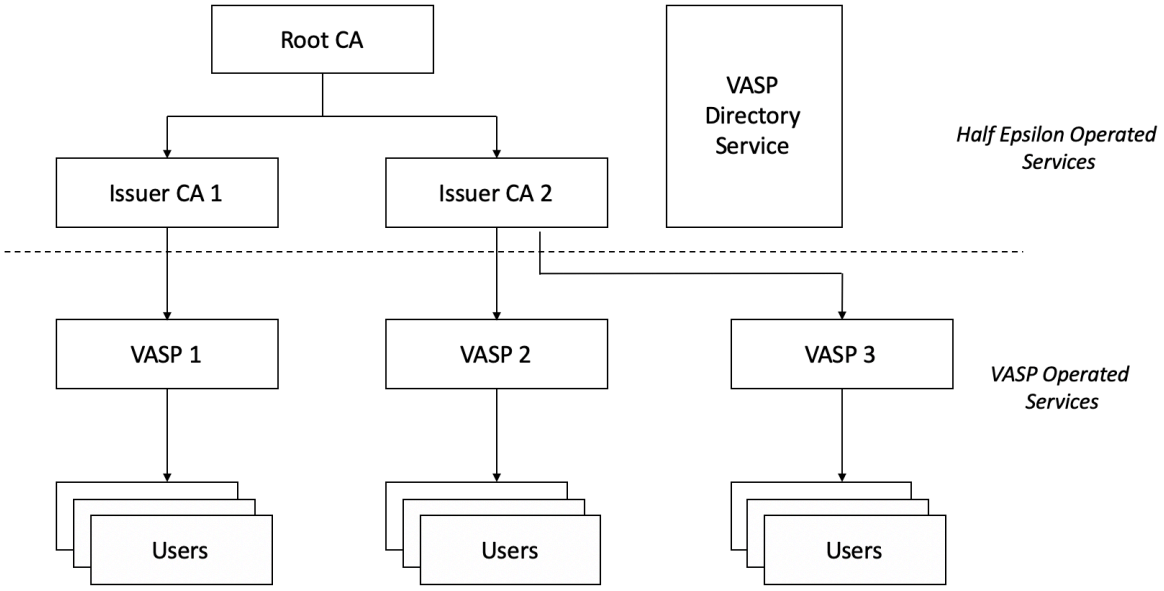

Figure 5: Overall Architecture of the VASP Network.

Half Epsilon operates a Root CA, several intermediate CAs and a VASP directory. VASPs are admitted to the VASP network after proper Know Your VASP (KYV) procedures. Each VASP has a certificate issued by an intermediate CA. In turn, a VASP issues certificates to its users. A user in the VASP network can transfer ownership titles to any other user in the VASP network.

Beyond issuing certificates to admit VASPs, Half Epsilon does not play any role in peer-to-peer transactions. The VASP directory is used by VASPs to find network addresses of other VASPs and to find the correct end-points to query them for KYC information and for making transfers.

USE CASES

The Half Epsilon Inter-VASP Network facilitates novel use cases.

GLOBAL ELECTRONIC CASH

VASPs on the Inter-custodian Network can facilitate the transfer of stable-priced Digital Assets (rather their titles) at low or no cost. The transfers will be instant and regulation compliant. Transferring small values across borders has always been a challenge and the Inter-custodian Network can facilitate this use case.

TRUE OTC

OTC trades have never truly been peer-to-peer. Intermediaries have always been involved. For the first time, it is possible for VASPs (and in the future traditional financial institutions) to truly trade OTC while avoiding charges imposed by trading desks.

CONFIDENTIAL DE-FI

It is possible to develop confidential versions of various DeFi protocols. In addition to confidential payments, the Half Epsilon Network can support the flow of various other DeFi instruments, e.g., AMM pool shares.

CENTRAL BANK DIGITAL CURRENCIES

The Inter-custodian Network can extend to banks and central banks. It is the perfect Digital Asset transfer system for CBDCs and other bank issued settlement coins or financial instruments.

OTHER FINANCIAL INSTRUMENTS

Banks and Financial Institutions have experimented with Blockchains, Permissioned Blockchains and Distributed Ledger Technology (DLT) as the transfer mechanism for tokenized financial instruments such as bonds, equities, and real estate tokens. Each of these technologies have their shortcomings. Blockchains are too public and often there is no guarantee that tokens will flow within regulated environments. Permissioned Blockchains compromise confidentiality and incur huge liabilities on reputed institutions that have to maintain transaction data that does not belong to them. DLTs often employ centralized transaction ordering systems and this is often unacceptable. The technology presented in this white paper uniquely achieves the four critical properties of (i) maintaining confidentiality of transfers, (ii) ensuring security of transfers with proper double-spend prevention, (iii) adhering to compliance requirements, and (iv) decentralization, i.e., there is no centralized control or visibility over transaction processing.

CONCLUSIONS

Modern day VASPs have several common challenges when it comes to storage and transfers of Digital Assets. Half Epsilon provides a holistic solution to these challenges. Our technology enables cost effective, confidential, are regulation compliant operations for VASPs. It also opens up the opportunity for novel use cases ranging from global electronic cash to Central Bank Digital Currencies. OTSM, our core technical contribution, can be developed either as a Blockchain HSM or a software only component leveraging MPC.

REFERENCES

[1] “Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018”, Forbes, August 15, 2019.
[2] InterVASP Messaging. URL: intervasp.org
[3] TRISA. URL: trisacrypto.github.io
[4] SYGNA. URL: sygna.io
[5] fireblocks.com
[6] curv.co