tbDEX : A Liquidity Protocol v0.2

@TBD54566975

Abstract. tbDEX is a protocol for discovering liquidity and exchanging assets (such as fiat money, real world goods, stablecoins or bitcoin)when the existence of social trust is an intractable element of managing transaction risk. The tbDEX protocol facilitates decentralized networks of exchange between assets by providing a framework for establishing social trust, utilizing decentralized identity (DID) and verifiable credentials (VCs) to establish the provenance of identity in the real world. The protocol has no opinion on anonymity as a feature or consequence of transactions. Instead, it allows willing counterparties to negotiate and establish the minimum information acceptable for the exchange. Moreover, it provides the infrastructure necessary to create a ubiquity of on-ramps and off-ramps directly between the fiat and decentralized financial systems without the need for centralized intermediaries and trust brokers. This makes currencies and decentralized financial services more accessible to everyone.

1 Introduction

We are at a crossroads in our financial system. The emergence of trustless, decentralized networks unlocks the potential for a future where commerce can happen without the permission, participation, or benefit of financial intermediaries.

Globally, 1.7 billion adults lack access to the banking system, yet two-thirds of them own a mobile phone that could help them access financial services [1]. The reasons for their exclusion vary, but the common threads are cost, risk, and lack of infrastructure. Decentralized and permissionless systems create a world that empowers individuals — one in which the right to engage in payments is neither subject to proving creditworthiness and the ability to pay account fees, nor subject to censorship when an intermediary's values do not comport with the payer or payee. It's also a world where internet access is the only fundamental infrastructure required to participate.

An open, decentralized financial system will enable all people to exchange value and transact with each other globally, securely, and at significantly lower cost and more inclusively than what traditional financial systems allow.

tbDEX was formed out of a desire to enable everyone to realize this vision of the future. The current state decentralized financial systems is still beyond the reach of everyday people, mostly requiring multiple asset transfers and transaction fees each step of the way. Aside from gatekeepers and cost, the complexity and sheer unintelligibility of this process today is a prohibitive barrier to entry for most. The tbDEX protocol is directed at this problem.

The protocol provides a framework for creating on-ramps and off-ramps from systems of fiat to digital currencies, without the need for going through centralized exchanges. The protocol affords for the secure exchange of identity and mechanisms for allowing participants to comply with laws and regulations (a feature notably absent from many efforts in the decentralized finance world).

At its core, the tbDEX protocol facilitates the formation of networks of mutual trust between counterparties that are not centrally controlled; it allows participants to negotiate trust directly with each other (or rely on mutually trusted third-parties to vouch for counterparties), and price their exchanges to account for perceived risk and specific requirements.

2. Foundational Concepts

Trust

The tbDEX protocol approaches trust differently than other decentralized exchange protocols in the sense that it does not utilize a trustless model, such as atomic swaps. At first blush, this is not optimal, especially when considering the end goal of providing access to a trustless asset like bitcoin. However, the reality is that no interface with the fiat monetary system can be trustless; the endpoints on fiat rails will always be subject to regulation, and there will exist the potential for bad behavior on the part of counterparties. This means that any exchange of value must be fundamentally based on other means of governing trust — particularly reputation.

The tbDEX protocol borrows heavily, if not completely, from well-established models of decentralizing trust, such as the public key infrastructure (PKI) that is used for securing the internet today.

Building on top of Decentralized Identifiers (DID) [2], this specification lays out a trust model in which trust is governed through disparate verifiers of trust; this is ultimately in the control of individuals, implementers of digital currency wallets, and/or delegates of trust established by either group.

The protocol itself does not rely on a federation to control permission or access to the network. There is no governance token. In its most abstract form, it is an extensible messaging protocol with the ability to form distributed trust relationships as a core design facet. The protocol itself has no opinion on what an optimal trust relationship between an individual wallet and a participating financial institution (PFI) should look like.

The nature of this trust relationship will never be universal: different jurisdictions are subject to different laws and regulations; and different individuals and institutions will have varying levels of risk tolerance, influenced by price and other incentives. It would violate the principle of trying to achieve the maximum amount of decentralization if the negotiation of trust was dictated at the protocol layer, as that would necessarily involve some form of permissioned federation.

2.1 Decentralized Identifiers (DIDs)

Decentralized identifiers (DIDs) [2] are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) determined by the controller of the DID. In contrast to typical federated identifiers, DIDs have been designed so they may be decoupled from centralized registries, identity

providers, and certificate authorities. Specifically, while other parties may be used to help enable the discovery of information related to a DID, the design enables the owner of a DID to prove control over it without requiring permission from any other

party. DIDs are Uniform Resource Identifiers (URIs) that associate a DID subject with a DID document, allowing trustworthy interactions associated with that subject.

DIDs are linked to DID Documents, a metadata file that contains two primary data elements:

1. Cryptographic material the DID owner can use to prove control over the associated DID (i.e. public keys and digital signatures)

2. Routing endpoints for locations where one may be able to contact or exchange data with the DID owner (e.g. location where PFI can be accessed)

DID Methods may be implemented in very different ways, but the following are essential attributes of exemplar Methods:

- The system must be open, public, and permissionless.
- The system must be robustly censorship resistant and tamper evasive.
- The system must produce a record that is probabilistically finalized and independently, deterministically verifiable, even in the presence of segmentation, state withholding, and collusive node conditions.
- The system must not be reliant on authorities, trusted third-parties, or entities that cannot be displaced through competitive market processes.

2.2 Verifiable Credentials (VCs)

Credentials are a part of our daily lives: driver's licenses are used to assert that we are capable of operating a vehicle; and diplomas are used to indicate the completion of degrees. In the realm of business, there exist signed receipts for payments, consumer reviews of products, and countless assertions made between individuals and non-governmental parties. While all these credentials provide benefits to us within apps, platform silos, and isolated interactions, there exists no uniform, standardized means to convey generalized digital credentials that are universally verifiable across domains, federation boundaries, and the Web at large.

The Verifiable Credentials specification provides a standard way to express credentials across the digital world in a way that is cryptographically secure, privacy respecting, and machine verifiable. The addition of zero-knowledge proof (ZKProof) [3] cryptography to VC constructions (e.g. SNARK credentials) [4] can further advance privacy and safety by preventing linkability across disclosures, reducing the amount of data disclosed, and in some cases removing the need to expose raw data values at all where legal and compliance needs do not require it.

3 Participants

3.1 Issuers of Verifiable Credentials

Issuers are the source of VCs. Both organizations and individuals (by means of their wallet) can be an Issuer. For example, a reputable organization that already conducts KYC checks could begin issuing a KYC credential to individuals. A wallet could also issue an evaluation of a PFI that it had a negative experience with and circulate this amongst their network, effectively acting as verifiable reputational feedback.

An incentive that may appeal to an Issuer is the potential to charge a PFI for the issuance of a VC used to provide a sense of credibility or legitimacy downstream. It's worth noting that verifiers, which can be a PFI, a wallet, or an individual do not have to establish an explicit or direct relationship with an Issuer in order to receive or verify credentials issued by them. Instead, a verifier need only decide whether they are willing to make a business decision based on the level of trust assurance they have in the issuer of a given credential.

3.2 Wallets

Wallets act as agents for individuals or institutions by facilitating exchanges with PFIs. More specifically, a wallet provides, though is not limited to, the following functionalities:

- Providing secure encrypted storage for VCs
- PFI discovery
- Receiving, offering, and presenting VCs
  - Note: end user consent would be required to offer VCs
- Applying digital signatures
- Storing transaction history

Wallets developed using the tbDEX protocol significantly simplify the user experience for their customers seeking to move assets between fiat and digital currencies. Individuals or organizations would no longer be required to first onboard through a separate, centralized exchange to procure digital currency assets with fiat payment instruments, before transferring those digital currency assets into the wallets. Individuals or organizations can also leverage the protocol to easily off-ramp back into fiat.

The protocol enables wallets to provide a streamlined customer experience with direct on- and off-ramps between the traditional and decentralized financial worlds. This means customers can use self-custody wallets without having to give up convenience in exchange for security or self-hosted options.

At scale, a competitive network of PFIs will also bring wallets more liquidity and competition for their customers, which means lower fees and faster transaction times.

The tbDEX protocol does not enforce any specific requirements upon wallet implementations. Wallet developers may design features and functionality that yield their desired user experience. For example, a wallet could algorithmically

select the PFI based on speed, cost, or track record — or delegate that choice to the owner of the wallet. A wallet developer could choose to pre-select which PFIs a given offer should be sent to — or choose to request and verify the credentials of various PFIs ahead of time by conducting discovery and evaluation prior to the first offer. A wallet could also choose to leave selection of PFIs entirely up to their customer. Generally speaking, we would recommend the following:

- Portability. Individuals or organizations should be able to seamlessly move all of their credentials to another wallet. The wallet should never claim or assume any sense of ownership over an individual's VCs.

- Consent-Driven. Wallet implementations must always ask for the individual's consent prior to presenting VCs to other parties, and may lean on storing their preferences to improve user experience.

3.2.2 Custodial wallets

It is reasonable to expect in institutional use cases that wallets are hosted by an organisation on behalf of a user (including private key material): this does not mean that DIDs and VCs are not able to be used to facilitate these use cases, but can still be used to discover and interact with PFIs on behalf of their users.