Verifiable

Institutional Grade On-Chain Verification

September 16th, 2021

Abstract

Decentralized blockchain applications retain properties that render them insufficient for institutional and government use cases. The core deficiency exists as a lack of verifiable, real-world identity associated with various transactions and ecosystems. The inherently obfuscatory nature of decentralized applications introduces sufficient plausible deniability. This functionality stands opposed to many jurisdictions' financial regulatory frameworks. This obfuscation of identity effectively bars regulatory compliant institutions from interacting with these revolutionary financial applications. As such, the industry requires a thoughtful approach to real-world identification that sufficiently protects a user's real-world identity while revealing essential facts about their person.

Verifiable offers users a one-of-a-kind, on-chain identity management platform. All identifying user data exists off-chain and remains protected by institutional-grade cryptography and industry best practices for cyber security. The world-class Verifiable team brings to the table a rich history of experience in cryptography, computer science, and cyber security. By encrypting user data in a secure, centralized manner and parsing only relevant, sufficiently generalized information to on-chain applications, Verifiable protects users' real-world identity while allowing decentralized applications to verify certain attributes of an individual.

Blockchain technology continues to pose a significant challenge to regulatory-compliant institutional entities. Simultaneously, this technology has presented humanity with one of the greatest opportunities for financial inclusion and accessibility thus far. As such, there exists a dire need to square the circle of the vast applicability of decentralized applications and the need to ensure regulatory compliance with the existing global financial regulatory framework. Verifiable represents the elegant solution so sorely needed by institutions, regulators, decentralized applications, and retail blockchain users.

1. Institutional Barriers to Entry

Institutions want to participate in the rapidly evolving decentralized financial revolution. As custodians of vast swaths of global wealth, institutional fund managers maintain a fiduciary responsibility to at the very least explore these opportunities on behalf of their clients. If ignored, the rise of DeFi likely entails giving up an increasingly large segment of their potential client base to more agile, technologically efficient companies. Nascent entities like BlockFi, Aave, and Compound have begun to tackle the immense web of the financial regulatory framework to offer regulatory-compliant, high-yield DeFi products. The emerging, unpreferable potential reality of dwindling market share has undoubtedly given many decision-makers in sizeable traditional financial institutions pause for concern.

Know Your Customer (KYC) regulations stand as one of the most significant challenges for any financial institution. The delicate balance of customer privacy and regulatory reporting standards entails a difficult situation of maximizing convenience while ensuring compliance. Previously, traditional financial entities enjoyed a nimble approach requiring customers to divulge significant identifying information to participate in the financial system. This process gave financial institutions immense authority and ensured aggregate consumer protection in our increasingly digital world. Simply put: no identification card, no access to the digital financial system whatsoever.

With the rise of decentralized finance, this reality now serves as a double-edged sword. The comparatively inefficient nature of centralized financial intermediaries has been laid bare for the public. Despite these short-term inefficiencies maximizing the individual user's financial security on average, it translates to a comparatively intolerable user experience overall due to the intrinsically identifying factors associated with KYC compliance. This catch-22 leaves compliant institutions in a fragile position. Despite offering the greatest levels of individual recourse in the event of a financial mishap, consumers perceive the process as an unnecessary inconvenience. In the event of user error, centralized financial institutions can mitigate most of the potential negative fallout. In a decentralized blockchain environment, the user bears the full financial cost of their error, sometimes with disastrous results.

Because of this situation, traditional financial institutions currently cannot have the best of both worlds when it comes to offering competitive yields and regulatory compliance. Despite their willingness to participate in this growing financial revolution, as evident by the numerous project incubations, partnerships, and proprietary blockchain ecosystems arising from these financial giants, existing institutions' hands remain tied. For financial entities and governments to adopt blockchain technology, they require a form of user verification that can ensure with full accuracy both the veracity of the user's identity and certain qualities relating to the given user's legal jurisdiction, restrictions, and other relevant variables. Simultaneously, rising consumer demand for identity protection and user integrity present financial institutions and governments with a dynamic challenge.

2. How Verifiable Works

Verifiable serves as a multichain third-party intermediary between users and dapps, allowing for sufficient obfuscation of a user's real-world identity while divulging relevant aspects of their personhood. This process allows dapps, decentralized exchanges (DEXs), and centralized exchanges (CEXs) to remain KYC and anti-money laundering (AML) compliant as per global financial reporting standards without requiring users to divulge their real-world identity.

Participating entities interface with Verifiable, which retrieves an internally stored list of application-specific addresses relating to the application in question. This process allows various applications to receive a binary approval or denial for a given user relative to the specific individual qualities of that user. For example, let us assume a given dapp disallows users from the jurisdiction of China from using their application. When this user attempts to access the application, the application scans a list of verified addresses stored in the Verifiable on-chain smart contract. In this case, the user will not pass the jurisdictional requirements for using the application, and Verifiable will disallow the user from creating an NFT which would otherwise allow access. By requiring users only to divulge potentially disqualifying variables via a trusted third-party intermediary, a user's identity remains unknown to the protocol. In this way, Verifiable allows the integrity of the user's real-world identity to remain intact while simultaneously parsing only relevant, disqualifying information to the protocol in question.

Verifiable uses non-fungible tokens (NFTs) to encode qualities about a given user to accomplish this feat. The lack of fungibility between user-specific assets generated by Verifiable entails an entirely unique user profile within the ecosystem. These user and dapp specific NFT binaries serve as the Verifiable ID, containing all relevant user information that can potentially be parsed to participating protocols. How Verifiable handles these user-specific NFTs ensures a seamless user experience and maximizes user security.

With Verifiable, identity theft remains nearly impossible. Verifiable NFTs parse only relevant information to participating protocols, so the granular individualization offered by current real-world identification does not exist in the ecosystem. A user seeking to co-opt another user's Verifiable ID maliciously must first co-opt the user's entire wallet and will then find only broad characteristics regarding that given user. Additionally, suppose a user either intentionally or otherwise sends this Verifiable ID to a different wallet address. In that case, the given Verifiable ID will become invalid due to the discrepancy between associated addresses. Additionally, Verifiable disallows users to send their Verifiable IDs to different addresses completely, utilizing an auto-return function in the Verifiable smart contract. Subsequently, Verifiable drastically reduces the probability of both user error and malicious activity resulting in the compromising of a user's real-world identity.

3. Becoming Verifiable

Users of Verifiable enjoy a familiar and accommodating experience when creating their Verifiable ID. The authentication process entails utilizing an email and associated password, from which Verifiable generates a unique user profile. Users can manage multiple addresses from a single profile, with initial support covering the Ethereum, Polygon, and Binance networks. The platform prompts users to upload relevant identifying documents such as national ID, passports, and other relevant items. This straightforward process allows users to utilize Verifiable as a virtual Fort Knox for their real-world identity as it pertains to decentralized applications and services.

In addition to this seamless functionality, Verifiable allows users to stake their assets directly on the platform. This process allows users to receive competitive market rates for staking their assets on the easy-to-use Verifiable dashboard. As blockchain and DeFi continue to mature, the demand for straightforward, yield generating products grows in tandem. Allowing Verifiable users to take advantage of this emerging trend easily demonstrates its resilient applicability as a verification layer and general tool for users interacting with DeFi products and services.

One of the most striking benefits arising from how Verifiable securely handles users' data comes in the form of user efficacy over said data. Currently, a myriad process of tracking tools and consumer analytic software has resulted in a haphazard process of aggregating user data and identities to optimize advertisements. Far from the desired results, this process compromises user data in several intolerable ways and results in intrusive and offputting advertisements. Companies do not allocate revenue to off-put their client base. However, the current advertising paradigm has resulted in such an absurd scenario.

With Verifiable, users can sell granularized components of their data to interested third parties. This opportunity benefits the user as their real identity remains obfuscated while pertinent qualities assist the third party in making intelligent advertisement decisions. In exchange, users enjoy the ability to profit from the sale of their data. Additionally, this configuration accrues immense benefits to businesses. Targeted marketing remains a cornerstone of an effective growth strategy. By allowing businesses to purchase specific data from a verified target audience, Verifiable enables a far more robust advertisement process when compared to existing methodologies. In this way, a second-order effect arising from sufficiently securing user data in a decentralized manner effectively solves the digital advertising crisis faced by businesses.

4. Conclusion

There exists a dire need to ensure financial regulatory compliance on the part of existing financial entities. The inability to comply when utilizing cutting-edge, yield-generating DeFi products puts the traditional financial industry at a significant disadvantage compared to emerging decentralized financial technology. Additionally, this process entails consumers taking on elevated levels of often poorly understood risk. The lack of distributed compliance tools for institutions serves as a detriment to all involved parties.

Verifiable exists as a first-of-its-kind identity management platform for institutions and the public. Verifiable's off-chain management of sensitive user data ensures maximum protection and security for crucial information by utilizing world-class data management practices. By allowing participating DeFi entities to set dynamic parameters regarding allows and disallowed users, Verifiable facilitates a form of KYC and AML compliance without divulging a given user's real-world identity. This functionality allows DeFi products to become regulatory compliant, existing financial institutions to interface with their highly desirable service offerings, and ultimately deliver elevated levels of efficacy to consumers.

Verifiable helps to close the chasm between the traditional financial industry and the rapidly growing realm of decentralized finance. As both industries continue to evolve to meet the needs of consumers, regulatory compliance assures maximum user protection. Similarly, by leveraging the best practices in securing user data while ensuring anonymity for users interacting with third parties on-chain, Verifiable facilitates the next step in the evolution of global finance.