IBE was popularised in the Boneh-Franklin Paper (Identity-Based Encryption from the Weil Pairing). Implementing a Decentralised IBE system could potentially bring some benefits to the Ethereum ecosystem. Identity Based Encryption enables public keys to be formed around representations of actual identity, building a link between existing social identities (Facebook, LinkedIn, Instagram…) and cryptographic keys. One could sign, pay and receive crypto communication, all through one (or a combination of) social user accounts.

What separates existing identification methods (uPort etc…) or name registries (Ethereum Name Service) and an IBE system is that it is "involuntary". In non-IBE systems, individuals are required to "voluntarily" sign up or bid whilst IBE systems provide a public key to everybody already registered on other platforms. This side-steps the adoption issues other identification standards face, potentially bringing greater usability and easier of adoption of the blockchain ecosystem in general.

However, there are problems with building an IBE system:

IBE systems require a trusted entity or Private Key Generator (PKGs) which hold secret parameters required to generate or map keys to existing strings

. There are research endeavours to distribute the PKGs' secret among nodes and/or prove a malicious PKG is acting nefariously. Might it be possible to build a collusion resistant/ incentivized management layer for PKGs on a smart contract?

Whom PKGs choose to distribute keys to relies heavily on existing authenticators, creating an unfortunate reliance on them.

Requiring an identity to be represented by multiple social user accounts could reduce this reliance… but could there be another method?

Lack of privacy in withdrawing a private key.

Each PKG would know whom and when an individual drew his or her key. Whilst generally this information is relatively harmless, there are certain nuanced cases where one might want this information hidden. Though unconditional anonymity maybe impossible, might we be able to introduce a mechanism that provides deniability?

There also is the method of mapping blockchain accounts (Ethereum or otherwise…) to the IBE system.

There could be a smart contract layer that translates the IBE's public private key pair on chain. Or perhaps a generation of Ethereum Public Private key pairs inside the PKG itself?

Several of us have been working on this idea and are currently architecting an IBE implementation for Ethereum. Any thoughts, ideas or feedback would be appreciated.

References:

Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In Annual international cryptology conference (pp. 213-229). Springer, Berlin, Heidelberg.

Waters, B. (2009). Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Advances in Cryptology-CRYPTO 2009 (pp. 619-636). Springer, Berlin, Heidelberg.

Goyal, V., Lu, S., Sahai, A., & Waters, B. (2008, October). Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 427-436). ACM.

Goyal, V. (2007, August). Reducing trust in the PKG in identity based cryptosystems. In Annual International Cryptology Conference (pp. 430-447). Springer, Berlin, Heidelberg.

Kate, A., & Goldberg, I. (2010, September). Distributed private-key generators for identity-based cryptography. In International Conference on Security and Cryptography for Networks (pp. 436-453). Springer, Berlin, Heidelberg.