Coconut Remote Anonymous Authentication

Bitmaintech Pte. Ltd.， 12/06/2018

Abstract——Financial organizations, including those in the blockchain industry, should comply with KYC[1] regulations while providing services to their customers. As one of the major features of blockchain is that all transaction records are public, transparent and permanent, there are concerns that organizations could potentially track and analyze customer behavior on blockchain once they have implemented KYC. This will raise serious privacy issues and obstruct the spread of blockchain. Coconut is a privacy sensitive solution for the implementation of KYC in blockchain. Coconut adopts Enhanced Privacy ID[2](Intel® EPID) to authenticate identity. It isolates the identity authentication entity from the actual business entity, allowing for identity data and business data to be managed in different organizations. Coconut protects user privacy fully, while meeting KYC requirements. Coconut finds the balance between privacy protection and regulatory compliance.

Index Terms——Blockchain, KYC regulations, Privacy, Identity authentication.

1. Introduction: Current industry problems

Applications of the blockchain technology have brought some dormant issues to the surface:

◆ Privacy issues

The core of the blockchain is a shift in bookkeeping mode. Take the most mature application - cryptocurrency - as an example. The receiving and spending of the cryptocurrency are recorded on the blockchain. If authentication is applied in all cryptocurrency transactions and the user's identity and transaction address are bound, the real-name authentication authority can easily grasp a user's financial information by tracking the transaction information on the blockchain. Therefore, most users have a resistance to real-name authentication as they hope to be anonymous throughout the transaction.

◆ Regulation issues

Most financial transactions, especially between digital currency and fiat currency, are strictly regulated by government. In many cases, relevant regulations explicitly require practitioners to identify business participants, and some also require due diligence. Therefore, to conduct business legally and compliantly, the real-name authentication and identification of users cannot be avoided.

In this respect, there is a tradeoff between privacy and supervision. The services well accepted in the market place fail to comply with regulatory requirements, while the demand-compliant services are not likely to be preferred by users. Concerning the above issues, the industry generally holds the following two attitudes：

◆ Temporary avoidance of supervision

For businesses which have no explicit regulation yet, most practitioners choose to focus on market expansion, temporarily avoiding KYC. Meanwhile, they try not to do the businesses that are strictly regulated. This attitude leads to: 1) a limit in business development ； 2) risk of subsequent regulatory regulation; 3) difficulty in defining the participant in the real world if users have disputes or do something illegal.

◆ Sacrificing anonymity

For businesses where KYC is necessary, the practitioners must sacrifice the anonymity of user, complete the user real-name authentication and securely store the relevant information. This attitude leads to: 1) loss of some users; 2) pressure to securely protect user identity information; 3) investment in many resources for KYC and data storage; 4) users having to complete a cumbersome process and provide personal information from time to time.

Although there are many identity authentication schemes in the industry, most of these schemes focus on the use of blockchain to store and verify users' identity information, or they attempt to carry out authentication in an absolute decentralized manner, which in our opinion is unrealistic. The failure of the existing schemes to address the issues today has prevented them from being adopted widely. Coconut aims to use technical means to solve the problems in the service layer instead of the network layer.

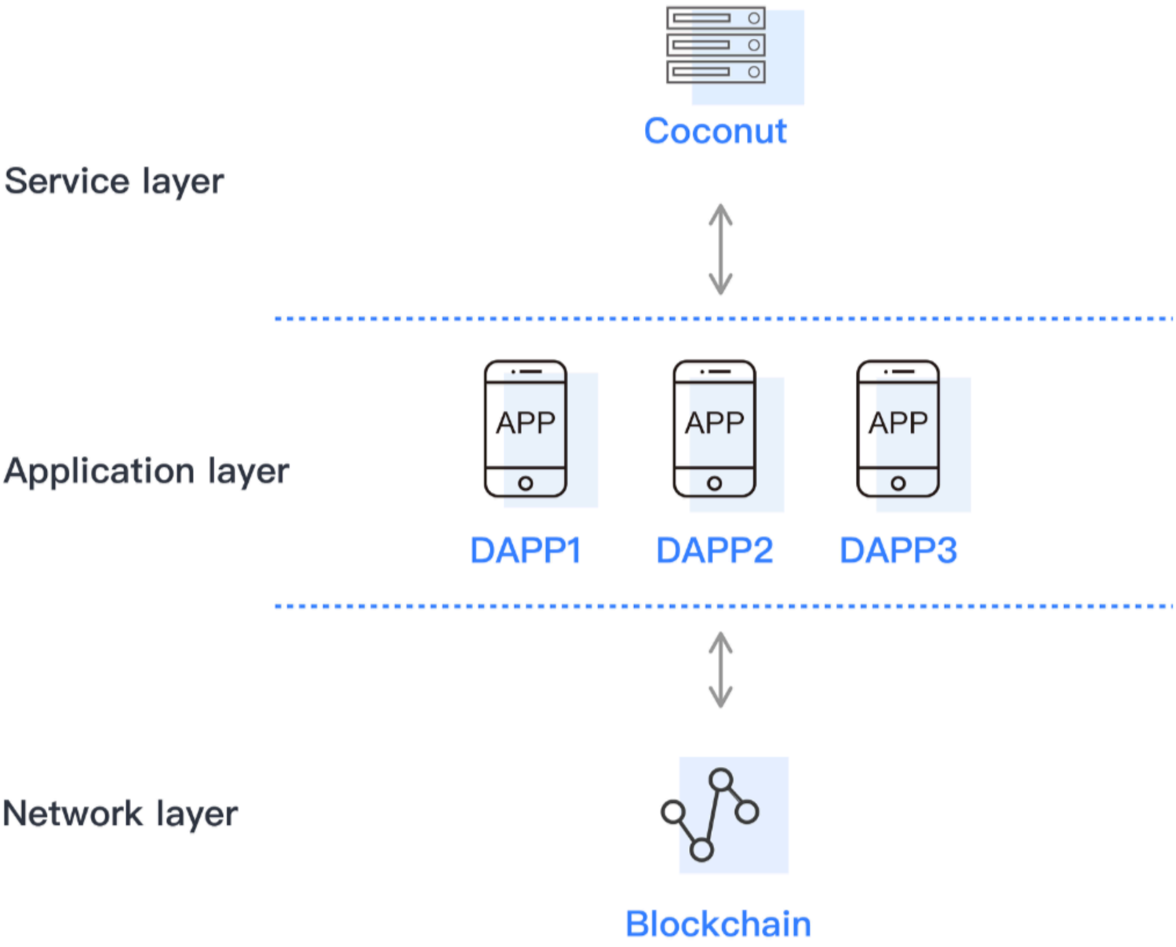

Chart-1. Position of Coconut

2. Overview

Coconut can meet regulatory requirements while fully protecting user privacy by separating the real-name authentication responsibility from business partner/platforms. After completing the identity authentication, the user obtains an EPID signing key. Practitioners can make sure the user is compliant by verifying the user's EPID signature. The EPID client signature and certificate do not permit the partner to determine the user identity.

The real-name authentication organization ("KYC service provider") must be a trusted third party and the authentication process/policy must be transparent and reliable. In general, the KYC service provider does not know what kind of services the users have participated in, and practitioners providing the financial services do not know the true identity of the users. In this way, once the users obtain an EPID certificate, they can be verified in different practitioners easily, quickly and conveniently without providing personal information many times. When the user's EPID private key is lost or copied, the valid signatures corresponding to the EPID certificate can be revoked and added to the blacklist. It effectively reduces the risk of fraudulent identity.

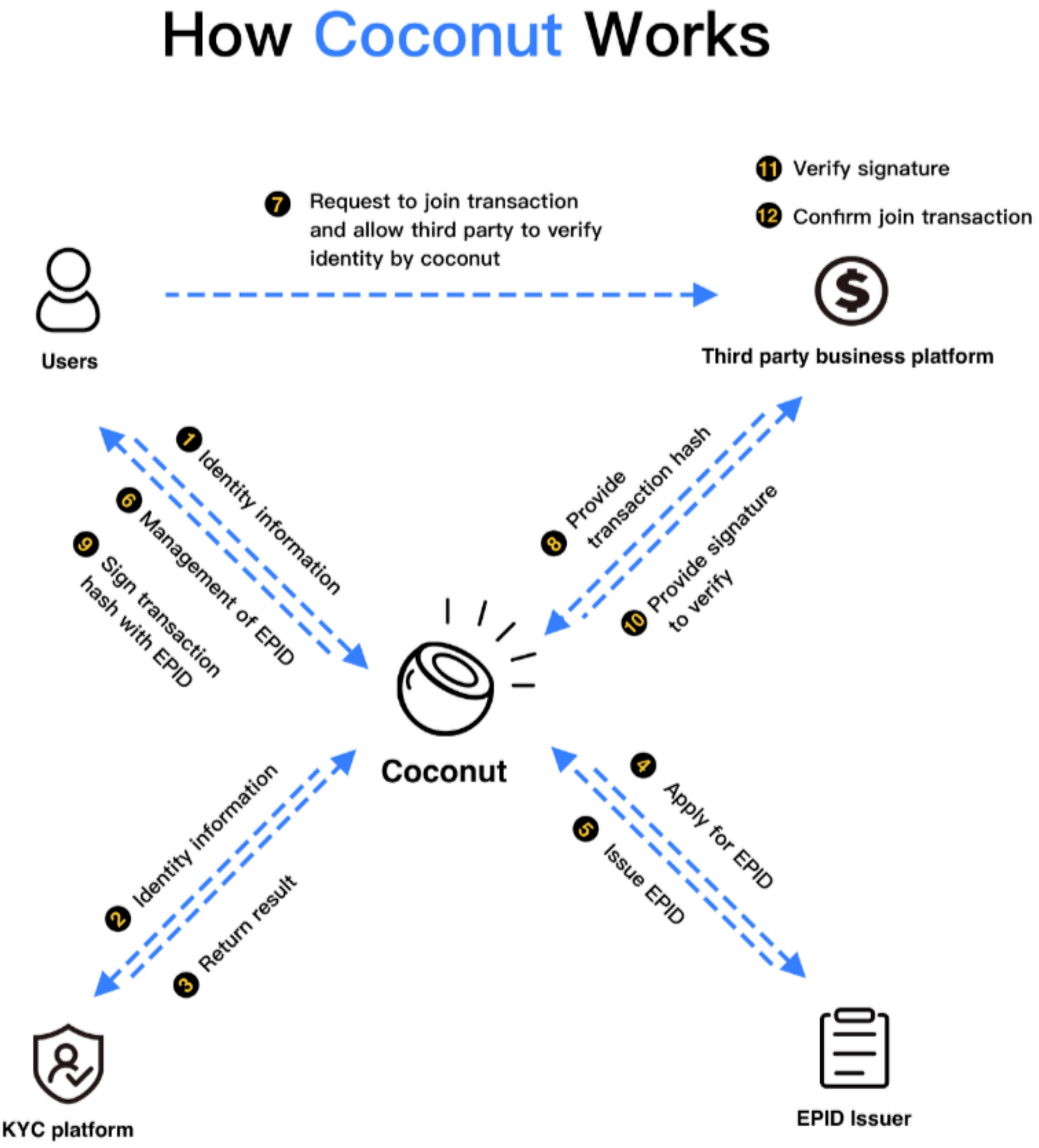
How Coconut Works
7 Request to join transaction and allow third party to verify identity by coconut
11 Verify signature
12 Confirm join transaction
Users
Third party business platform
1 Identity information
6 Management of EPID
9 Sign transaction hash with EPID
8 Provide transaction hash
10 Provide signature to verify
Coconut
2 Identity information
3 Return result
4 Apply for EPID
5 Issue EPID
KYC platform
EPID Issuer

Chart-2: Business Flow Chart

3. Remote Anonymous Authentication

In order to protect users' privacy, we incorporate a new cryptographic scheme called EPID for remote, anonymous authentication. Unlike traditional digital signature schemes, one public key in the EPID scheme corresponds to multiple private keys. There are three types of entities in an EPID scheme: issuer, members and verifiers. The issuer creates an EPID public key and issues a unique EPID private key to each member. Each member can use this private key to digitally sign a message, and the resulting signature is called an EPID signature. The verifier can use the public key to verify the correctness of a signature, that is, to verify that the EPID signature was indeed created by a group member in good standing, with a valid private key. The EPID signature, however, does not reveal any information about which unique private key was used to create the signature, within the group.

In the EPID scheme, each member chooses a unique membership key seed, f[3]. The issuer then issues a membership credential on f in a blind fashion such that the issuer does not acquire knowledge of the membership key f. The membership key and the membership credential together form the private key of the member. To sign a signature, the member proves in zero-knowledge[4] that it has a membership credential on f. To verify a group signature, the verifier verifies the zero-knowledge proof. In addition, each member chooses a base value B and computes $K = B^f$. We call B the base and K the pseudonym. To sign a signature, the member needs not only to prove that it has a valid membership credential, but also to prove that it constructs the (B, K) pair correctly, all in zero-knowledge.

In EPID, there are two options to compute the base B: the random base option and the name base option. Random base option: B is chosen randomly each time by the member. Under the decisional Diffie-Hellman assumption, no verifier can link two EPID signatures based on the (B, K) pairs in the signatures[5]. This option obviously cannot meet KYC regulations and it is noncompliant. Thus, we adopt the name base option. Note that in this option, B is predetermined; for example B= Hash("coconut"). The value K becomes a pseudonym of the member with regard to the base name, as the member will always use the same K in the EPID signature to the same B.

In Coconut, the amount and value of B are predetermined and published. The Coconut database stores all valid (B, K) pairs in the signature corresponding to the user ID. Only Coconut can tell who and which EPID private key generates the signature, and for verifier, one user can have more than one identity (the amount of identity equals to the amount of valid (B, K) pairs). It strongly enhances the anonymity of users.

To help take EPID adoption to practice, EPID technology has contributed to leading industry organizations for certification. EPID is now:

- An International Standards Organization standard for identity and privacy (ISO/IEC 20008, 20009)[6].
- A Trusted Computing Group (TCG)[7] standard for attestation (TPM 2.0 DAA).

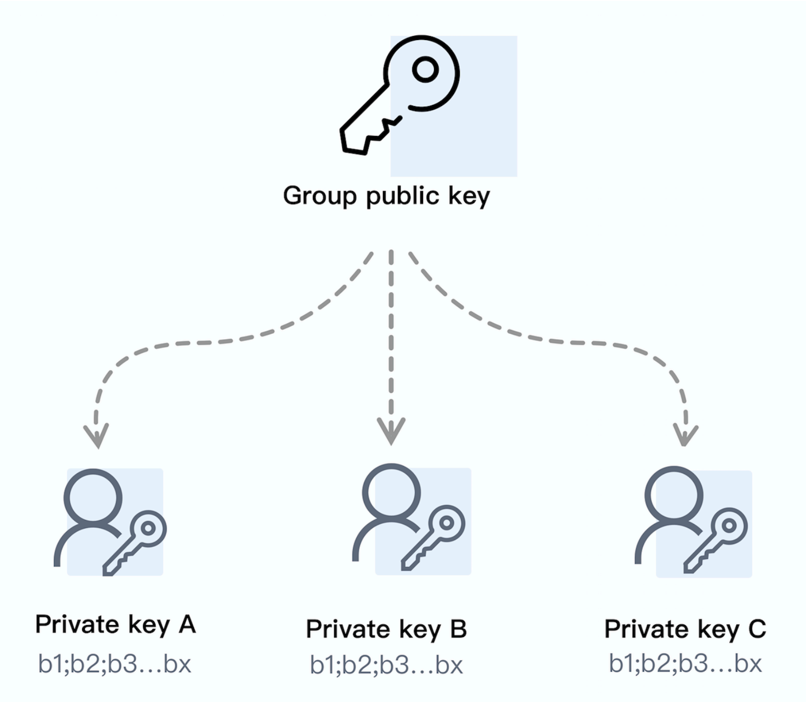

Chart-3: Relationship between group public key and EPID private key

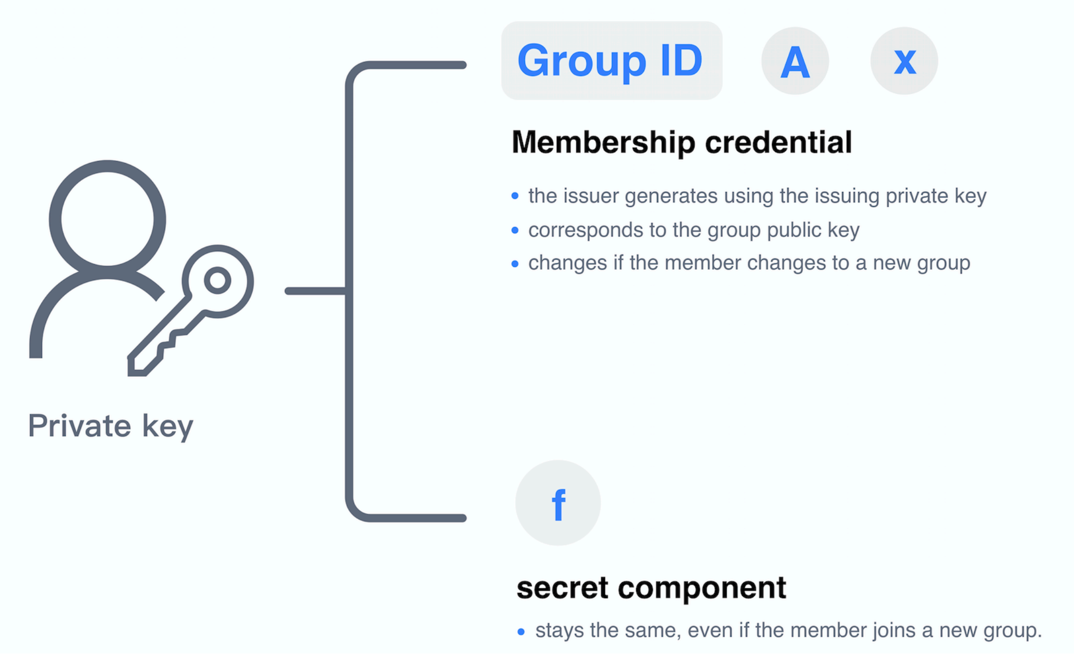
Private key
Group ID
A
x
Membership credential
the issuer generates using the issuing private key
corresponds to the group public key
changes if the member changes to a new group
f
secret component
stays the same, even if the member joins a new group.

Chart-4: component parts of EPID private key for each member

4. Roles

- User

The user is the member in *Remote Anonymous Authentication* and takes part in the business platform. Before performing a transaction, the user should complete real name authentication in Coconut and get an EPID certificate. User must keep his/her EPID private key securely. Once the EPID private key has been stolen or copied, the user should revoke the EPID certificate at Coconut as soon as possible. A user can have multiple EPID private keys.

- Coconut

Coconut is a system or application that provides the user with real name authentication entry. The user can apply for an EPID certificate from an EPID issuer by Coconut which has integrated EPID SDK. The EPID private key is generated and stored in Coconut's front end and managed by the user. The Coconut database securely stores all valid (B, K) pairs corresponding to the user ID, which is the core database to keep the relationships between real world identity of the user and the EPID signature.

Coconut is the interactive hub of users, EPID issuer, KYC service provider and business platform. All connections among these systems must be authenticated and the data must be transferred using encryption.

- EPID issuer

The issuer is responsible for generating group key pairs and issuing a membership credential to users to generate EPID private key. The issuer only provides technical services and does not participate in practical business. It can neither obtain the real identity information of the user nor the transaction information corresponding to each EPID certificate. The user interacts with the issuer through Coconut and has no perception of the issuer.

- KYC service provider

The KYC service provider is responsible for real name authentication of the user, which can be carried out by Coconut or by a trusted third-party KYC service provider. The user interacts with the KYC service provider through Coconut. Coconut provides different real-name authentication policies to meet various KYC requirements in different businesses. These KYC policies must be published to ensure that the business platform understands them accurately and accepts them.

- Business platform

The business platform is both the verifier and the relying party of the EPID certificate which provides financial services to the user and has to do KYC for the user, such as a cryptocurrency exchange. If the business platform accepts Coconut's KYC policy and process, it can judge whether the user is compliant and allowed to continue to do business in the platform by verifying the EPID signature. Coconut can support multiple business platforms at the same time.

5. Business model

Coconut can be an identity authentication app that provides EPID identity service to external multiple business platforms. In this scheme, the user identity data and the actual business data can be managed and stored separately to the greatest extent. At the same time, it helps the business platform reduce compliance costs and focus on its core business. Coconut will earn revenue by charging a verification fee based on the number of verifications.

Coconut can also be an authentication system of a risk management department in a group company. After one-time real name authentication in the system, the user can participate in all businesses under the group. The relevant business system/platform of subsidiaries or other departments can quickly judge whether the user is authenticated by verifying the EPID signature. Coconut facilitates a centralized management of user identity information, and it not only avoids duplicate development of real name authentication systems, saving resources, it also reduces the risk of user privacy leakage.

For institutions with high social credit, such as banks, in addition to internal use, their Coconut systems can be used externally as well.

6. Summary

It is undeniable that, whether the blockchain industry is able to go further and well in the future, to a considerable extent, depends on how to solve the problem of user identity authentication. How to meet regulatory requirements more conveniently and safely is an issue that has been explored for a long time. We believe that Coconut is the best scheme to balance anonymity and regulation. Besides, it can be implemented easily with consistent technical standards and it can be used extensively because of a strong feasibility.

References

1 Prof. Venkatesh U. Rajput. “Research on Know Your Customer (KYC)”. In International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013

2 E. Brickell and J. Li. “Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities.” In Proceedings of the 6th ACM Workshop on Privacy in the Electronic Society, pages 21–30, 2007.

3 E. Brickell and J. Li. “Enhanced Privacy ID from Bilinear Pairing.” Cryptology ePrint Archive, Report 2009/095, 2009.

4 O. Goldreich, S. Micali, and A. Wigderson. “Proofs that Yield Nothing but their Validity.” Journal of the ACM, Volume 38(3), pages 690-728, 1991.

5 Ernie Brickell and Jiangtao LI. “Enhanced Privacy ID: A Remote Anonymous Attestation Scheme for Hardware Devices.” Intel® Technology Journal, 2009.

6 International Standard ISO/IEC 20008-1, Information technology - Security techniques - Anonymous digital signatures, 2013.

7 Trusted Computing Group. “TCG TPM Specification 1.2,” 2003 http://www.trustedcomputinggroup.org