DaoLiName－Decentralized Identity as Public Key

道立名－去中心化的身份即公钥

DaoLiName Company
info@daoliname.com
https://github.com/DaoliName/daoliname

June 22, 2019

ABSTRACT

We present DaoLiName (道立名, Taoism Establishing Name) blockchain. It has a uniquely novel and useful decentralized consensus algorithm to establish an authentication assertion that a human-meaningfully low-entropy bit string is a public key. We use Good-ID to name a human-meaningfully low-entropy ID or address, Good-DID to name a Good-ID which is asserted by a decentralized consensus algorithm, and Good-DID-PK to name a Good-DID with authentication quality of being a public key. The DaoLiName blockchain offers uniquely novel and useful services of establishing Good-DID-PK.

1. INTRODUCTION

The pioneering work of BitCoin [1], and many blockchain works followed in past ten years have created useful values to users. Having been influenced, experienced, or some even been personally enjoying, the real values, more and more people with personal computing and communication devices such as smart phones become convinced that it is now technically practical to broadcast in real time all payment transactions, or more generally contracts, to a global scale online, peer-to-peer, decentralized, append only ledger. Transactions and/or contracts enter such a ledger on the basis of some trustlessly agreeable consensus algorithm which is executed by all the peering participants of the ledger system.

DaoLiName is yet another blockchain. It thus also has a part to share many best-practice accreted working principles with all previous good-intended blockchain technologies. Thanks to abundances of the previous blockchain offerings to have established knowledge pervasiveness for the area, there is little need to reinvent or re-describe this part of shared technologies of blockchain. It is worth mentioning that, as a late comer, the DaoLiName blockchain should of course respectfully make a good use of knowledge and experiences of some previous blockchain works, learn from their best practices, and avoid pitfalls. For example, in terms of consensus algorithms, knowing CPU only mining of BitCoin vs. the fairer mining approach of CPU + memory of Ethereum [2], would help the DaoLiName blockchain to choose using a more reasonable Proof-of-Work scheme. For another example, advances in Proof-of-Stake, e.g., that of Algorand [3] and EOS [4], would also provide invaluable input for the DaoLiName blockchain to consider in approaching to a fairer, more efficient, and more scalable consensus algorithm.

The present Whitepaper of the DaoLiName blockchain describes a uniquely novel and useful decentralized and consensus algorithm that we believe a blockchain technology can offer with a great value: The decentralized and consensus algorithm on inputting a human-meaningfully low-entropy bit string can output an authentication assertion on the inputting string being a public key. To our knowledge, such a function has not been previously reported.

To our knowledge, blockchain technologies appeared to date, including DaoLiName, all use some public-key algorithms for a peer participant to establish entity authentication in the peer-to-peer network. A peer upon joining the peer-to-peer network generates its private key which is necessarily random, sufficiently long and hence a high-entropy bit string. All public key algorithms use a one-way and good mixing function relate a private key to the public key, and hence the outputting public key of the peer of blockchain must also be in some high-entropy formulation. From BitCoin on, the blockchain industry name such a peer authentication public key “public address of a wallet”. So far, there seems existing no efficient or streamline decentralized and consensus algorithm to accept or output a public address of human-meaningfully low entropy. This lack of human comprehension property of any blockchain address has been conjectured as “Zooko’s Triangle” by Zooko Wilcox-O'Hearn [5], suggesting an impossibility for a blockchain identity to enjoy all the following three desirable properties of decentralization, security and human-meaningfully low entropy. The latest blockchain Whitepaper of Libra [6] states: “The Libra Blockchain is pseudonymous and allows users to hold one or more addresses that are not linked to their real-world identity.” In our view, absence of human-meaningfully low-entropy address for a blockchain is a feature only to BitCoin for its desired user spending anonymity. For all other blockchains, if this “feature” is a “have-to-have” thing, then it is a serious limitation. Considering Libra in particular, how can a nameless user establish her/his personal credit score in order to convince lenders reach a consensus decision for a loan?

The need for decentralized low-entropy name registration has been a long demand. In early and not-yet-prosper days of BitCoin, Namecoin [7] observed the need for decentralized domain name service (DNS). A domain name has a human-meaningfully low entropy to resolute to a higher-entropy IP address. The Namecoin approach is a first-come-first-serve append-only chain. To prevent DN squatting, it timestamps a DN registration request and waits for a number of other blocks before mines a block for the registration requesting DN. This consensus algorithm is obviously in a well-controlled quality. The inventors of Namecoin have abandoned their service leaving the peer-to-peer network running by a community of believers. Ethereum Name Service (ENS) [8] is also a decentralized domain name service offer. It designates some top-level domain names such as “.eth”, “.test” analogous to “.com”, “.net” in DNS to be the owners of certain “smart contract” whose execution output can bind a DN to a user requested IP. It seems that these “smart contract” owners form centralized authorities. It is not only our belief that a contract should NOT be too smart for great number of users to be able to draft themselves with confidence of understanding, only that can be some semblance of decentralization.

The need for decentralized ID (DID) being a public key is not new either. The Decentralized Public Key Infrastructure (DPKI) [9] proposal goes beyond serving DNS related names. It is essentially a blockchain era online servicing reformulation of Pretty Good Privacy Web-of-Trust (PGP-WoT [10]). Indeed, since the blockchain era is an online era, the original offline non-service based and hence amateur quality PGP should definitely try for a re-vitalization as an online service. PGP Web-of-Trust, being offline or online service, is based on third parties digitally signing public key certificates to bind a high-entropy public key to a human-meaningfully low-entropy ID. A WoT signed certificate, even assuming that the ledger-entering algorithm is decentralized as being output from some “smart contract” (DPIK requires so), in the time of use still requires the user refers to a web of third parties. This is a common inconvenience limitation of a certification, or directory-reference, based public key authentication framework. Even worse, key revocation remains being a very nasty task for certification based public key authentication framework.

The remainder of this Whitepaper describes a uniquely novel and useful decentralized and consensus algorithm to make authentication assertion that a human-meaningfully low-entropy bit string is a public key. We use Good-ID to name a human-meaningfully low-entropy ID or address of a blockchain, Good-DID to name a Good-ID which is asserted by a decentralized consensus algorithm, and Good-DID-PK to name a Good-DID with authentication quality of being a public key. The DaoLiName blockchain to be technically described below offers uniquely novel and useful services of establishing Good-DID-PK.

2. IDENTITY BASED CRYPTOGRAPHY

In 1984, Adi Shamir pioneered public key authentication to breakthrough the limitations of directory reference based framework by inventing an identity based signature scheme (Shamir's IBS [11]). In an identity based cryptography (IBC), any human-meaningfully low-entropy string can be used as a public key. This observation can remove the limitations of director-reference based public key authentication. Shamir's seminal work inspired an important research direction of IBC which flourished in the turn of the century when a number of practical IBC schemes appeared [12, 13]. These IBC schemes use a very useful cryptographic primitive called bilinear pairing which was introduced to the cryptographic community by Victor Miller [14].

A bilinear pairing is a homomorphism mapping from two additive groups of points on elliptic curve(s) to a multiplicative group of Galois Field. Let G_1 and G_2 be two bilinear pairing friendly computable elliptic additive groups of a prime order q. Let G_T be a multiplicative group of integers having the same prime order q. Let $\hat{e}$ be an asymmetric bilinear pairing mapping for which,

$$\hat{e} : G_1 \times G_2 \rightarrow G_T$$

for all elliptic curve points $U, V,$ in G_1, U', V' in G_2, the following bi-linearity equations hold and can be efficiently evaluated:

$$\hat{e}(U + V, U') = \hat{e}(U, U') \times \hat{e}(V, U')$$
$$\hat{e}(U, U' + V') = \hat{e}(U, U') \times \hat{e}(U, V')$$

Let user Alice have in possession a human-meaningfully low-entropy ID which we simply denote “Alice”, wherein quotation marking means a bit string. Let Alice be the possessor or bearer of a blockchain wallet. Let $k_{\text{Alice}} < q$ be a randomly generated integer to be of exclusive use in the function of the private key of Alice.

Let H_1 be a deterministic function mapping from an arbitrary bit string to an elliptic curve point in G_1. Let H_2 be a deterministic function mapping from an arbitrary bit string to an elliptic curve point in G_2. Thus,

$$H_1(\text{" Alice" }) \in G_1$$
$$H_2(\text{" Alice" }) \in G_2$$

are two elliptic curve points in G_1 and G_2, respectively, each is named: “ID mapping-to-curve point”.

Recommended examples of user ID for IBC include, well-known communications systems addressable identities, e.g., a mobile phone number, an email address, a social media account identity, a domain name, etc. However, in DaoLiName blockchain usecases, anything can be used in place of an ID: e.g., a photo, a birth or degree certificate, an ID card, a document file etc., since all such things can be deterministically hash mapped to unique points on the elliptic curve(s).

In addition to deterministically hash mapping Alice’s IDs to elliptic curve points, Alice’s wallet can also compute the following quadruples (these cases include special cases of $i = j$):

$$< H_1(\text{“Alice}_i\text{”}),\ [k_{\text{Alice}}]H_1(\text{“Alice}_i\text{”}) > \text{ in } G_1$$
$$< H_2(\text{“Alice}_j\text{”}),\ [k_{\text{Alice}}]H_2(\text{“Alice}_j\text{”}) > \text{ in } G_2$$

From the bi-linearity equations listed above we can derive the following “Bilinear Pairing Diffie-Hellman Quadruple” (BPDHQ) evaluation:

$$\hat{e}(H_1(\text{" Alice}_i\text{" }), [k_{\text{Alice}}]H_2(\text{" Alice}_j\text{" })) = \hat{e}([k_{\text{Alice}}]H_1(\text{" Alice}_i\text{" }), H_2(\text{" Alice}_j\text{" }))$$

since both are equal to

$$\hat{e}(H_1(\text{" Alice}_i\text{" }), H_2(\text{" Alice}_j\text{" }))^{k_{\text{Alice}}}$$

Using Miller's algorithm [14], the BPDHQ equation can be efficiently evaluated, and the evaluation does not need to know Alice's private key k_{Alice}. This property is very important in IBC since the evaluation of BPDHQ implies that the pair

$$< H_{1,2}(\text{“Alice}_j\text{”}),\ [k_{\text{Alice}}]H_{1,2}(\text{“Alice}_j\text{”}) >$$

can be used as Alice's human-meaningfully low-entropy public key! This observation forms the know-how crux for the proposed new blockchain online algorithm to output a consensus assertion that Alice's wallet can have a human-meaningfully low-entropy public key or address.

The public key cryptography worthiness of the above pair is easily demonstrable. For example, let Bob encrypt a message *m* to Alice where *m* is a bit string of length not exceeding that of a coordinate of the pairing friendly computable elliptic curve. Bob picks at random $r < q$, and computes:

$$U = [r]H_1(\text{“Alice”}),\ V = m \text{ “bit-wise-xor” } (\ x \text{ coordinate of } [r][k_{\text{Alice}}]H_1(\text{“Alice”})\ )$$

Because the pair $< U, V >$ are randomized by Bob's random value *r*, it is in general a computationally difficult to decrypt the message *m* from the pair. However, Alice can use her private key k_{Alice} to scalar multiply on the elliptic curve point *U*, to compute output the elliptic curve point $[k_{\text{Alice}}][r]H_1(\text{“Alice”})$, and then to “bit-wise-xor” the *x* coordinate of this point with *V* to decrypt the message *m*. Digitally signing a message by Alice using her private key is even easier to demonstrate in pairing cryptography, which we shall delay the demonstration to the next section.

3. DAOLINAME BLOCKCHAIN

The proposed new blockchain in its node's wallet uses bilinear pairing friendly elliptic curves. Let $G_1 \times G_2 \rightarrow G_T$ be the bilinear pairing mapping as described in Section 2. In our applications, let G_1 play the usual role of a "crypto curve" as usual as in all existing blockchain wallets. Let G_2 play a uniquely novel and useful role in blockchain technology: its usage in the new blockchain is for receiving hash mapping from Good-IDs to its coordinates as on-curve points.

Let P be a system fixed public point in G_1. Let k_{Alice} denote the private key of Alice's wallet. Alice first joins the DaoLiName blockchain anonymously as in all existing blockchains. For this normal use, she only needs using G_1; her public address is $[k_{\text{Alice}}]P$. Notice that this G_1 address is a high-entropy address. Alice can stay anonymous in the DaoLiName blockchain as in all other blockchains.

We notice that the DaoLiName blockchain will publicly fix all system parameters in trustlessly verifiable manners. For instance, let them be output from an open standard cryptographic hash function.

Some Alices may choose to become known in their Good-IDs. Such an Alice makes a G_2 transaction to link her anonymous address to her human-meaningfully low-entropy address "Alice" by broadcasting the following Trustlessly Agreeable Diffie-Hellman Quadruple (TADHQ) to all peer nodes:

$$\text{TADHQ} = <\ P,\ [k_{\text{Alice}}]P,\ H_2(\text{“Alice”}),\ [k_{\text{Alice}}]H_2(\text{“Alice”})\ >$$

We name this quadruple "Trustlessly Agreeable Diffie-Hellman Quadruple" because inputting this quadruple to the "Bilinear Pairing Diffie-Hellman Quadruple" (BPDHQ) equation (see Section 2, using a constant hash function H_1("Alice") = P in that equation) will evaluate TRUE output, and this evaluation can be publicly conducted without need of knowing Alice's private key k_{Alice}.

As in Libra blockchain or EOS blockchain, let a group of Proof-of-Stake (PoS) club member nodes verify Alice's G_2 transaction request. For instance, if "Alice" is an email address, the PoS club members should include checking email challenge to and response from that email address. Other forms of "Alice" to be hash mapping-able to G_2 include for instance: social media account, mobile phone numbers, DN registration status, etc. These are online managed identities. Some forms of "Alice" may be offline-online ones, for example: school graduation certificates, employer-employee relationship, government-citizen-servicing relationship, etc.

Let Bob denote one of such PoS nodes. Bob has stake to conduct due diligence check on Alice's transaction request. Let ID$_i$ denode ID hashed to the curve group G$_i$ (for $i = 1, 2$). The following equations are also TADHQ which are in fact Bob's digital signatures on Alice's IDs:

$$\begin{aligned}\hat{e}([k_{\text{Bob}}]\text{Alice}_1, \text{Bob}_2) &= \hat{e}(\text{Alice}_1, [k_{\text{Bob}}]\text{Bob}_2)\\ \hat{e}([k_{\text{Bob}}]\text{Bob}_1, \text{Alice}_2) &= \hat{e}(\text{Bob}_1, [k_{\text{Bob}}]\text{Alice}_2)\end{aligned}$$

These TADHQ signatures of Bob on Alice's IDs can be publicly verified by all PoS nodes. Upon reach a threshold not-ID-theft consensus, mining for Alice's TADHQ in G$_2$ block can be conducted to append Alice's TADHQ block in the append-only ledger. From now on, Alice can enjoy no-muss no-fuss use of her Good-DID-PK.

The threshold of not-ID-theft consensus signatures of PoS club members in fact constitutes an online servicing formulation of PGP WoT. What is uniquely novel and useful in this new formulation is that the TADHQ is self sufficient for authentication evaluation in the time of using public key. The PGP WoT verification only takes place in the entering G$_2$ time. The using public key time, the blockchain formulation of validity and TADHQ validity suffice to establish public key authentication for the public key users.

We notice that some blockchains, e.g., Libra, also consider making use of a form of threshold PoS signatures for consensus decision. They use aggregated signatures such as BLS signatures [15] which do not expand the size of the signature which are collectively output from a plural number of PoS nodes. Our forms of PGP WoT signatures permit a plural number of PoS nodes in a time insensitive manner, and the criterion of reaching consensus is merely dumb counting the number of PGP WoT blocks. In blockchain, the logical length can be indefinitely long, however the physical length is constantly 1, to permit simple and dumb formulation of cryptographic primitives without loss of functional beauty.

As DaoLiName Good-DID-PK is an online service, revocation of a key pair is a simple bi-product of the online service.

User anonymity in G$_1$ is a by-default property. If user anonymity in G$_2$ is also desired, bilinear pairing enables easy ways to achieve non-interactive zero-knowledge proof that Alice has in possession of her private key.

4. CONCLUSION

The DaoLiName blockchain uses bilinear pairing cryptographic primitive to enable Trustlessly Agreeable evaluation of a decision Diffie-Hellman quadruple which can deterministically link a number of human-meaningfully low-entropy identities to a high-entropy public key or blockchain wallet address. It uses a two-step entering append-only ledger to realize a decentralized consensus algorithm for achieving Good-DID-PK. It also eliminates, for the first time since the commencement of IBC nearly 20 years ago, a black-hole-ish heavy gravity center for attack and single point of failure: "Private Key Generator" (PKG) from IBC. We wish that the convenience of IBC make IBC to play its long overdue role in mainstream public key cryptographic applications.

5. REFERENCES

1. Satoshi Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2009,
url: www.bitcoin.org/bitcoin.pdf

2. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,
url: github.com/ethereum/wiki/wiki/White-Paper

3. Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich, MIT CSAIL,
url: people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf

4. EOS.IO Technical White Paper v2,
url: github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

5. Zooko's triangle,
url: en.wikipedia.org/wiki/Zooko%27s_triangle

6. An Introduction to Libra,
url: libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

7. Namecoin - Decentralized secure names,

url: namecoin.org

8. Ethereum Name Service,
url: ens.domains

9. Christopher Allen, Arthur Brock, Vitalik Buterin, Decentralized Public Key Infrastructure,
url: danubetech.com/download/dpki.pdf

10. Alfarez Abdul-Rahman, The PGP Trust Mode,
url: ldlus.org/college/WOT/The_PGP_Trust_Model.pdf

11. Adi Shamir, Identity based cryptosystems and signature schemes, Advances in Cryptology, Proceedings of CRYPTO'84, Lecture Notes in Computer Science 196, pages 48-53, Springer-Verlag, 1985

12. R. Sakai, K. Ohgishi, and M. Kasahara, Cryptosystems based on pairing, In Proceedings of 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000

13. D. Boneh and M. Franklin, Identity based encryption from the Weil pairing. Advances in Cryptology, Proceedings of CRYPTO'01, Lecture Notes in Computer Science 2139, pages 213-229, Springer-Verlag, 2001

14. Victor S. Miller, Short programs for functions on curves, Unpublished manuscript, vol. 97, pages. 101–102, 1986

15. Dan Boneh, Ben Lynn, Hovav Shacham, Short Signatures from the Weil Pairing. ASIACRYPT 2001. pages 514-532. See also J. Cryptology 17(4): 297-319 (2004)