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, storage and communication devices such as desktops and 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. Such a ledger can even be physically materialized by these personal devices orgainized in Decentralized Autonomous Organization (DAO). Transactions and/or contracts enter an append-only ledger on the basis of some trustlessly agreeable consensus algorithm which is executed by all the peering nodes of the ledger system.

DaoLiName is yet another blockchain. It thus also has a part to share with or inhere from practices accreted working principles from many previous blockchains. Thanks to the abundance of the previous blockchain offerings to have established knowledge pervasiveness for the area, there is little need to reinvent or re-describe that part of the shared or inhered blockchain technologies. It is nevertheless 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 blockchains, learn from their best practices, and avoid pitfalls some may have met. For example, in terms of consensus algorithms, knowing CPU only mining approach of, e.g., BitCoin vs. fairer mining approach of computing, memory and even storage resources of, e.g., Ethereum [2], certainly helps the DaoLiName blockchain to choose using a more reasonable Proof-of-Work (PoW) scheme. For another example, advances in Proof-of-Stake (PoS), e.g., those of Algorand [3] and EOS [4], also provide invaluable input for the DaoLiName blockchain to consider improving efficiency and scalability for blockchain technologies.

The DaoLiName blockchain that we propose in the present Whitepaper, however, would like to focus on a uniquely novel decentralized and consensus algorithm that we believe to be very useful. The new decentralized and consensus algorithm on inputting a human-meaningfully low-entropy bit string can output an authentication assertion that the inputting low-entropy string is a wallet public key or address. To our knowledge, a blockchain node address of this quality has not been seen in the previous blockchain technologies appeared so far.

Blockchain technologies to date, including DaoLiName, all use some public-key algorithms for a peer node to establish entity authentication in the peer-to-peer network. A peer node 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-WoT, 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 PGP-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 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 a 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], which qualifies one-way and good-mixing properties of public key algorithms, the BPDHQ equation can be efficiently evaluated, and the evaluation does not need to know Alice's private key k_{Alice}. This astonishing property of Miller's algorithm is very important to 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 computationally infeasible to extract 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 enabled cryptography, which we shall delay the demonstration to the next section.

3. DAOLINAME BLOCKCHAIN

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

Let P be a system fixed public point of the prime-order q 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 the Libra blockchain or the 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, for $i = 1, 2$, denode ID hashed to the curve points in the group G_i. The following equations are also TADHQ which are in fact Bob's digital signatures on Alice's IDi:

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

These TADHQ signatures of Bob on Alice's IDi can be publicly verified by all peer nodes. Upon reach a threshold of no-ID-theft consensus, mining for Alice's Good-DID-PK block containing TADHQ = < Alice_1, $[k_{\text{Alice}}]\text{Alice}_1$, Alice_2, $[k_{\text{Alice}}]\text{Alice}_2$ > can be conducted to append Alice's Good-DID-PK 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 no-ID-theft consensus in the form of PoS club members adding their TADGQ blocks as their signatures on Alice's verified ID_i to the append-only ledger in fact constitutes an online servicing formulation of PGP WoT. What is uniquely novel and useful in this new formulation is that a TADHQ block is self sufficient for authentication evaluation in the time of using the Good-DID-PK. The PGP WoT verification only takes place in the time of Good-DID-PK entering ledger's G_2 leg. In the time of using Good-DID-PK by users in security applications, the blockchain consensus rule and the TADHQ validity suffice to establish Good-

DID-PK authentication for the users. No any reference to any third party's trust certification is needed in the time of using a Good-ID-PK. The unavoidable need of referencing to a third-party's certification in the time of using a PGP-WoT certified public key is unfortunately a non-decentralization flaw in all known DPKI approaches.

We notice that some blockchains, e.g., Libra, are also considering making use of a form of threshold PoS signatures in their consensus algorithms. They use some aggregation of signatures, like that of the BLS signature [15] in which a collectively signed signature by a plural number of PoS nodes does not expand the size of the output signature. Our formulation of PGP WoT signatures permit a plural number of PoS nodes to append their signature block in the ledger in a time insensitive manner, and the criterion of consensus ignition is merely dumb counting the number of PGP WoT blocks. Because verification of ID guarding against ID theft may involve offline steps, a time-insensitive ignition of consensus is necessary. Fortunately, in the blockchain technology, although the logical length can be indefinitely long, the physical length is constantly 1. The simple formulation of PGP WoT threshold ignition of consensus of the DaoLiName blockchain, although looking not so smart, nevertheless in an elegant manner serves the needed online-offline verification function of true ID ownership.

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 and abundant ways to achieve non-interactive zero-knowledge proof that Alice has in possession of her private key.

4. CONCLUSION

1. The DaoLiName blockchain uses the bilinear pairing cryptographic primitive to enable Trustlessly Agreeable evaluation of a decision Diffie-Hellman quadruple to deterministically link any number of human-meaningfully low-entropy bit strings to a high-entropy public key or blockchain wallet address.

2. The DaoLiName blockchian uses a two-step online-offline entering append-only ledger to realize a decentralized consensus algorithm for achieving Good-DID-PK authentication.

3. For the first time since the commencement of the IBC notion in the 1980s, a so-called "Private Key Generator" PKG, which is a black-hole-ish heavy gravity center for attack and single point of failure, is forever eliminated from IBC.

4. We wish that IBC in the blockchain era would play its long overdue role in the 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)