Meningkatkan Privasi Data pada *Online Social Networks* (OSN) Menggunakan Konsep Desentralisasi dan Kriptografi

Muhammad Yanza Hattari
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
yanza.hatta@gmail.com

Abstrak

Online Social Network (OSN) adalah suatu layanan yang dapat digunakan untuk berinteraksi dan berbagi informasi dengan orang lain secara *online.* Saat ini, banyak penyedia layanan OSN yang mengumpulkan berbagai informasi penting seperti data pribadi dan data sensitif lainnya secara terpusat (*centralized*). Hal ini dapat menjadi ancaman terhadap privasi pengguna, terutama terkait bocornya data pengguna ke pihak lain tanpa seizin pengguna. Berbagai peneliti telah mengajukan konsep desentralisasi pada OSN (biasa disebut *Decentralized Online Social Network*). Arsitektur ini dipercaya dapat memberikan privasi yang lebih baik untuk pengguna dengan menghapus otorisasi terpusat dari penyedia layanan OSN. Data-data pengguna akan tersebar di beberapa server atau didistribusikan secara penuh pada perangkat pengguna pada jaringan *peer-to-peer*. Pada makalah ini akan dibahas penggunaan layanan penyimpanan terdistribusi dan konsep desentralisasi pada *Online Social Network* yang dapat meningkatkan privasi pengguna. Selain itu, akan dibahas penerapan konsep kriptografi pada *access control* dan *blockchain* dalam *Decentralized Online Social Network* yang dapat menyelesaikan isu kepercayaan (*trust*) dan integritas data.

Kata Kunci: *Online Social Network, Privasi Pengguna, Decentralized Online Social Network, Storage, Access Control, Blockchain, Sharding, Smart Contract*

I. Pendahuluan

Online Social Network (OSN) telah menjadi bagian penting dari aktivitas pengguna internet. Melalui OSN, pengguna dapat berbagi momen melalui foto/video dan kutipan teks (biasa disebut *post*) kepada teman *online* yang dimilikinya. Facebook sebagai salah satu *platform* OSN terbesar di dunia mengklaim terdapat sekitar 2.45 miliar pengguna aktif per bulan September 2019. Pengguna ini memiliki lebih dari 125 miliar koneksi pertemanan dan dapat menghasilkan 3.2 miliar *like* dan komentar per harinya [1]. Terdapat juga berbagai *platform* OSN lain seperti Weibo, Twitter, dan lain lain yang telah menarik miliaran pengguna dari berbagai usia, budaya, kewarganegaraan dan latar belakang.

Secara umum, OSN menyediakan layanan penyimpanan yang dapat digunakan untuk menyimpan informasi digital pengguna. Selain itu, OSN juga menghubungkan pengguna dengan pengguna lain dalam jaringan. Dengan kedua hal ini, OSN dapat membantu pengguna untuk berhubungan antara satu sama lain dengan lebih mudah dan bahkan dapat membantu pengguna untuk mendapatkan teman baru. OSN juga memungkinkan pengguna untuk memberikan label/atribut kepada pengguna lain sehingga pengguna dapat mengelompokkan jaringan pertemanannya berdasarkan atribut ini.

Sebagian besar informasi (termasuk informasi personal) disimpan secara terpusat oleh pihak penyedia layanan, yang dalam suatu waktu dapat berkolaborasi dengan pihak ketiga dan menggunakan informasi ini untuk berbagai tujuan, seperti *targeted advertisement*. Iklan yang ditargetkan ini dapat menimbulkan efek manipulasi terhadap prioritas belanja pengguna dan dalam beberapa kasus dapat menyebabkan efek kecanduan belanja [2]. Penyedia layanan juga dapat membagikan atau menjual informasi user kepada pihak lain yang tidak menggunakan peraturan terkait privasi data. Hal ini dapat menyebabkan bocornya informasi pribadi di sosial media atau berbagai layanan internet lainnya yang dapat mengakibatkan terjadinya pencurian identitas, penipuan, dan pemerasan [3].

Sebagai contoh, pada tahun 2018 New York Times melaporkan sebuah perusahaan yang mendapatkan 50 juta data pengguna Facebook dengan cara ilegal [4]. Kejadian seperti ini sering terjadi dalam berbagai kepentingan. Alasan utamanya adalah arsitektur terpusat OSN yang memungkinkan penyedia layanan memiliki akses secara penuh terhadap seluruh informasi pengguna, dan pengguna hanya bisa percaya penyedia layanan melindungi informasi pribadi mereka. Dalam situasi ini, pengguna bahkan tidak dapat memastikan apakah penyedia layanan OSN benar-benar menghapus data saat pengguna tersebut memutuskan untuk menghapus akun mereka dari jaringan sosial.

Pada makalah ini, akan dibahas cara untuk mengatasi masalah di atas dengan pendekatan *Decentralized Online Social Network* (DOSN). DOSN ini diharapkan dapat meningkatkan privasi data pengguna melalui pendistribusian informasi pengguna ke server-server tertentu atau bahkan langsung ke pengguna. Akan tetapi, terdapat batasan-batasan dalam pengimplementasian DOSN seperti keamanan (*security*) dan kepercayaan (*trust*). Masalah terkait DOSN ini dapat diatasi dengan menerapkan *Blockchain* sebagai rangkaian kriptografi pada arsitektur DOSN.

Makalah ini disusun dengan sistematika berikut. Pada bagian II terdapat penjelasan tentang studi terkait privasi pada *Online Social Network* (OSN) dan juga *Blockchain*. Pada bagian III akan dijelaskan penggunaan arsitektur *Decentralized Online Social Network* (DOSN) serta manfaat *Blockchain* dalam mengatasi masalah implementasi dari arsitektur DOSN. Pada bagian III juga akan dijabarkan kelebihan dan batasan (*limitation*) pemanfaatan *Blockchain* terhadap DOSN. Sedangkan pada bagian IV akan dijabarkan kesimpulan dari makalah ini.

II. Studi Terkait

A. Privasi Data pada *Online Social Network*

Tingginya pertumbuhan dari *Online Social Network* (OSN) yang mengandung informasi pribadi pengguna menjadikan OSN sebagai target yang sangat menarik bagi orang-orang yang ingin mengambil keuntungan. Informasi pribadi ini dapat berupa informasi penting pengguna, reaksi pengguna terhadap

konten yang ada pada *timeline*, dan bahkan indikasi suasana hati pengguna dari daftar video dan daftar lagu yang mereka tonton.

Salah satu pembahasan akademik terkait potensi ancaman pada privasi individu termasuk penguntitan (*stalking*) dan pencurian identitas (*identity theft*) dikemukakan oleh Gross *et al.* [5]. Selain itu, banyak akademisi lain yang melakukan penelitian terkait dengan privasi data pada *Online Social Network*, seperti identifikasi kerentanan privasi pada *Markup Language* milik Facebook yang dapat menyebabkan *hijacking* [6], identifikasi kecacatan terhadap privasi utama Google+ [7], dan juga penemuan serangan (*attack*) pada pengguna Facebook melalui akun teman yang sudah dinonaktifkan [8].

Berbagai hasil penelitian dan banyaknya kasus *hacking* menyebabkan munculnya berbagai kampanye yang mengangkat isu kesadaran pengguna terhadap privasi data. Bahkan Presiden Amerika Serikat ke-44, Barack Obama, pernah memberikan pidato terkait dengan kehati-hatian dalam berbagi informasi di media sosial [9].

Saat ini, sudah terdapat dua model yang dapat digunakan untuk mengukur risiko terhadap privasi pengguna saat mereka membagikan informasi pribadi di media sosial [10]. Model ini memberikan pendekatan baru terkait pengukuran privasi tetapi dinilai cukup sulit untuk diterapkan. Besarnya jumlah variabel dan perhitungan yang harus dilakukan menyebabkan model ini menjadi kompleks dan memakan banyak waktu.

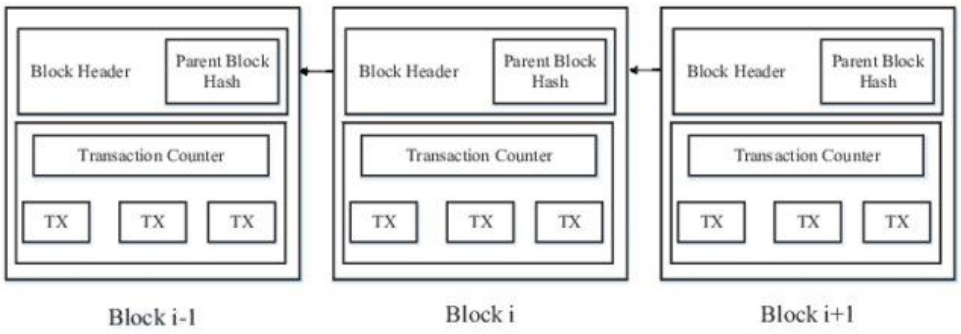
Selain itu, terdapat model lain yang menyarankan agar pengguna diberikan sebuah tampilan interaktif terkait alur perpindahan informasi pribadi dari komputer pengguna ke *cloud*, sehingga pengguna dapat memblokir alur yang mereka anggap berpotensi melanggar privasi [11] [12]. Tetapi, karena banyaknya variabel yang ada, membuat visualisasi alur data merupakan tugas yang sangat kompleks dan sulit untuk direalisasikan di dunia nyata.

B. Struktur, Mekanisme dan Skalabilitas *Blockchain*

Blockchain merupakan salah satu teknologi yang menjadi perhatian akademisi maupun praktisi saat ini. Teknologi *blockchain* ini mendasari dibentuknya Bitcoin, yang merupakan implementasi pertama dari *cryptocurrency*. Desain awal dari *blockchain* dijelaskan pertama kali oleh Satoshi Nakamoto pada Oktober 2008.

Blockchain pada dasarnya adalah sebuah catatan transaksi digital (biasa disebut *ledger*) untuk mencatat suatu transaksi dan didistribusikan secara desentralisasi [13]. *Ledger* ini akan dikelola secara simultan pada sebuah jaringan perangkat (*device*) yang disebut *node*. *Node* ini dapat berupa perangkat elektronik aktif apapun, termasuk komputer, telepon *mobile*, atau bahkan perangkat IoT (*Internet of Things*).

Secara umum, sebuah *node* bebas untuk berpartisipasi atau meninggalkan jaringan *blockchain*, dan memvalidasi, menyinkronkan serta menyimpan salinan lengkap dari *ledger.* Setiap *node* memiliki kedudukan yang sama, sehingga tidak terdapat master atau *node* pusat yang mengelola *node* lainnya.



Gambar 1. Struktur Blockchain Ledger [14]

Struktur dari *blockchain ledger* secara mudah dapat digambarkan sebagai sebuah rantai blok tempat transaksi dicatat [14] (dapat dilihat pada Gambar 1). Setiap blok akan terhubung ke blok sebelumnya (kecuali blok genesis yang merupakan blok pertama di dalam *blockchain*). Karena hal ini, setiap transaksi

yang terlibat tidak dapat diubah secara retroaktif tanpa perubahan pada seluruh blok yang terkait.

Untuk mencapai kesepakatan yang diperlukan untuk setiap transaksi, *blockchain* menerapkan mekanisme konsensus di antara *node* pada sistem [15]. Setiap *node* akan bersaing secara periodik untuk memenangkan hak untuk menambahkan transaksi baru (dalam bentuk satu blok) ke *blockchain*. Melalui mekanisme konsensus, *blockchain* dapat memutuskan *node* pemenang, dan setelah ditentukan, *node* terpilih dapat menambahkan blok ke *blockchain ledger*.

Blockchain menggunakan teknik kriptografi untuk melindungi informasi pribadi pengguna [16]. Akun pengguna akan dinyatakan dalam alamat virtual yang dihasilkan oleh *public key* yang sesuai. Karena hal ini, *blockchain* dianggap sebagai sebuah sistem yang tidak dapat dilacak (*untraceable*) dan sepenuhnya anonim. Namun, beberapa penelitian menunjukkan adanya kemungkinan untuk melacak informasi pribadi pengguna melalui analisis jaringan yang tepat. Akibatnya, beberapa pendekatan telah diusulkan untuk mengatasi anonimitas dari sistem *blockchain*. Sebagai contoh, Zcash yang merupakan salah satu mata uang digital dengan tingkat privasi tinggi, menggunakan teknologi zk-Snarks (*zero-knowledge Snarks*) untuk memfasilitasi enkripsi seluruh transaksi pada *blockchain*, sehingga sulit bagi siapapun yang ada di jaringan untuk mencari informasi detail terkait *node* tertentu [17].

Keterbatasan *blockchain* saat ini seperti *low throughput*, *high latency*, dan *resource exhausting* menyebabkan meningkatnya perhatian publik terkait dengan skalabilitas *blockchain* pada bidang industri maupun akademisi [14]. Sebagai contoh, Bitcoin hanya dapat menangani sekitar 3 hingga 7 transaksi per detik (*transaction per second*). Hal ini jauh lebih sedikit dibandingkan alat pembayaran lain seperti Visa dan Alipay.

Sebagai sebuah arsitektur dengan mekanisme paralel, *sharding technology* dianggap sebagai salah satu solusi paling menjanjikan untuk menyelesaikan permasalahan skalabilitas *blockchain* [18]. *Sharding* pada awalnya merujuk pada

suatu pendekatan *scaling* pada basis data (*database scaling approach*), yang kemudian digunakan pertama kali pada *blockchain* oleh National University of Singapore. *Sharding* pada *blockchain* akan memperluas sebuah jaringan *blockchain* menjadi beberapa sub-*blockchain* yang dapat diproses secara paralel sehingga skalabilitas horizontal tercapai. Konsep *sharding* ini juga telah digunakan sebagai salah satu metode untuk *scaling* oleh Ethereum.

C. *Smart Contract* pada *Blockchain*

Sejak munculnya *blockchain* 2.0 [19] dan diperkenalkannya *smart contract* [20], aplikasi *blockchain* dapat berjalan tanpa adanya pihak ketiga yang dipercaya. Melalui penggunaan *smart contract*, *blockchain* dapat menyediakan beberapa hal berikut.

1. *Reliable Delivery of Message*

   Pengguna dapat membaca dan menulis data pada *blockchain*, dengan jaminan data yang ditulis ke *blockchain* tidak dapat dimodifikasi. Selain itu, mekanisme *event* dari *smart contract* memungkinkan pengguna untuk dinotifikasi jika adanya data atau pesan baru [21].

2. *Account Address* (*Pseudonym*)

   Alamat pengguna pada *blockchain* biasa disebut *pseudonym*. Alamat ini biasanya berupa *hash* dari *public key* sehingga memiliki anonimitas yang tinggi. Akan sulit bagi seseorang untuk melakukan pemalsuan data menggunakan *pseudonym* orang lain tanpa memiliki *secret key* yang tepat.

3. *Transparent Third-Party Platform*

   Banyak aplikasi yang menggunakan server terpusat milik pihak ketiga untuk memfasilitasi komunikasi, tetapi hal ini menimbulkan risiko kebocoran privasi. Melalui *smart contract*, *blockchain* dapat digunakan sebagai server pusat tanpa harus menggunakan pihak ketiga lainnya.

III. Pembahasan

A. Meningkatkan Privasi Pengguna Melalui Arsitektur *Decentralized Online Social Network* (DOSN)

Decentralized Online Social Network (DOSN) adalah suatu sistem terdistribusi pada jejaring sosial (*social network*) yang tidak bergantung penuh atau bergantung secara terbatas pada infrastruktur terpusat. Arsitektur DOSN akan menggunakan sumber daya *end-user* secara *peer-to-peer* untuk melakukan berbagai fungsi layanan [22]. Banyak penelitian terkait DOSN yang berfokus pada pendistribusian penyimpanan (*storage*), kontrol akses (*access control*) dan penyediaan layanan (*services*) untuk meningkatkan privasi pengguna.

Berbagai desain DOSN memiliki mekanisme penyimpanan data dan informasi pada *node* lokal (*peer-to-peer*). Untuk memastikan *availability* dari data pengguna saat sedang *offline*, data tersebut akan disinkronkan dengan *node* lain yang masih *online* di jaringan [22]. Sebagai contoh, Supernova sebagai salah satu desain DOSN memiliki sebuah *supernode* yang akan memilih suatu *node* yang tepat bagi pengguna untuk menyimpan datanya saat pengguna tersebut *offline* [23]. Skema desain ini akan membutuhkan suatu *node* yang dapat dipercaya oleh pengguna. Akan tetapi, *node* yang ada pada DOSN biasanya tidak stabil, sehingga dibutuhkan suatu rancangan protokol untuk memastikan *availability* dari data pengguna.

Di sisi lain, beberapa desain DOSN lainnya menggunakan layanan penyimpanan yang sudah ada seperti penyimpanan terdistribusi (*distributed storage*) [24] [25] ataupun penyimpanan pada *cloud* [26] [27]. Cachet [24] dan PeerSoN [25] dirancang untuk menyimpan data pada *node* yang memiliki *distributed hash table* (DHT) sehingga sistem dapat memastikan *availability* dari data saat pengguna sedang *offline*.

Namun, desain DOSN yang menggunakan konsep DHT ini memiliki kekurangan terutama terkait kinerja sistem. Desain ini membutuhkan waktu yang

lama untuk mengambil dan menyinkronkan data dari suatu *node* ke *node* lain. Cachet [24] kemudian mencoba untuk mengimplementasikan *gossip-based social caching algorithm* yang dapat meningkatkan kinerja sistem. Akan tetapi, masih terdapat kesenjangan kinerja yang cukup besar antara desain Cachet dengan metode pengaksesan data langsung ke server terpusat. Persona [26] dan Cadros [27] kemudian mencoba mengurangi kesenjangan ini dengan menerapkan penyimpanan pada *cloud*. Saat ini, layanan penyimpanan pada *cloud* dapat diakses dengan mudah. Selain itu, layanan penyimpanan pada *cloud* ini memiliki kecepatan akses yang lebih tinggi dibandingkan dengan penyimpanan terdistribusi.

DOSN menggunakan konsep kriptografi pada *access control* untuk memastikan privasi data pengguna. Nasim dan Buchegger [28] mengusulkan kebijakan *access control* berbasis XACML yang dapat digabungkan dengan berbagai metode otentikasi lain untuk melindungi privasi pengguna. De Salve *et al.* [29] juga mengusulkan untuk menggunakan XACML dalam menentukan kebijakan privasi. Cheng *et al.* [30] mengusulkan suatu model *access control* berbasis hubungan pengguna dengan pengguna lain (*User-to-User Relationship Access Control*) yang memungkinkan pengguna memiliki kebijakan *access control* yang lebih canggih.

Akan tetapi, saat ini banyak desain DOSN yang lebih memilih untuk menggunakan *access control* berbasis enkripsi [24] [26]. Bodriagov *et al*. [31] memperkenalkan sebuah skema enkripsi berbasis predikat (*Predicate Encryption* / PE) dan menggunakannya dalam konteks DOSN. Cachet [24] dan Persona [26] menggunakan skema enkripsi berbasis atribut (*Attribute-based Encryption* / ABE) dalam menyediakan *access control* untuk pengguna.

Dari segi penyediaan layanan (*service*), PeerSoN [25] menggunakan *distributed hash table* (DHT) untuk menyediakan operasi *publish* dan *lookup* yang efisien walaupun sistem berbentuk desentralisasi. Pengguna PeerSoN ini akan menggunakan identitas mereka sendiri berupa nilai *hash* dari alamat *email* sebagai

key untuk melakukan operasi *publish* dan *lookup* data pada DHT. Selain itu, Supernova [23] menggunakan *superpeers* untuk memelihara direktori pengguna untuk membantu pengguna menemukan data teman pada DOSN berdasarkan nama atau minat. Selain itu, Supernova juga menyediakan layanan *lookup* dan penyimpanan data. Namun, seluruh layanan Supernova ini membutuhkan *superpeers* yang dapat dipercaya dan tidak mudah untuk diserang.

DOSN dapat meningkatkan privasi data pengguna dengan pemberian akses dan kontrol lebih pada informasi pribadi mereka. Selain itu, arsitektur ini menghapus otorisasi terpusat yang dimiliki oleh penyedia layanan OSN saat ini melalui mekanisme penyimpanan yang terdistribusi. Akan tetapi, penggunaan DOSN belum banyak diimplementasikan dikarenakan kinerja sistem yang belum sebaik pengaksesan langsung ke server pusat. Selain itu, terdapat masalah baru saat menerapkan DOSN, yaitu sulitnya membangun hubungan terpercaya antar *node* dan menjamin integritas data tanpa adanya pihak ketiga yang dapat dipercaya. Hal ini dapat diatasi melalui penerapan *blockchain* dalam arsitektur DOSN.

B. Penerapan *Blockchain* dalam *Decentralized Online Social Network* (DOSN)

Beberapa peneliti telah melakukan analisis penerapan *blockchain* dalam DOSN [32] [33]. Zeng *et al.* [32] mengajukan sebuah arsitektur sistem DOSN yang menggunakan *blockchain* dan konsep *sharding* untuk menyelesaikan masalah kepercayaan antar *node* dan efisiensi kinerja *blockchain*. Dari Gambar 2 dapat dilihat arsitektur DOSN yang diajukan memiliki tiga bagian yang terdiri dari:

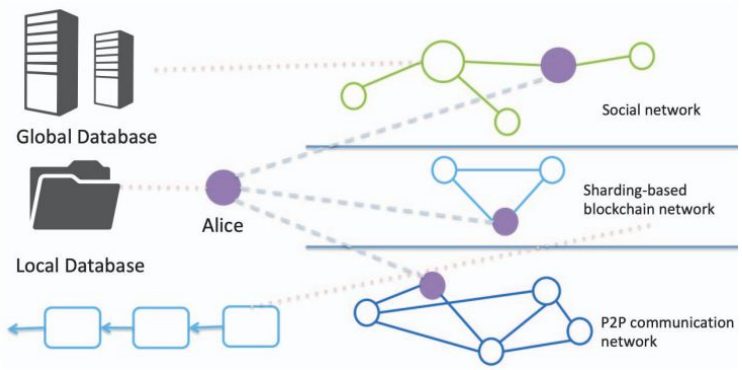
1. *Communication Network*

   Jaringan komunikasi yang didefinisikan pada arsitektur akan memiliki struktur *peer-to-peer* yang dapat memungkinkan pengguna untuk berkomunikasi satu sama lain dengan lebih cepat dan fleksibel.
2. *Blockchain Network*

Jaringan *blockchain* akan menjamin hubungan antara satu *node* dengan *node* lain sehingga sistem tidak memerlukan pihak ketiga atau pihak yang dipercaya untuk melakukan transaksi. Pada jaringan *blockchain* ini juga akan digunakan konsep *sharding*. *Blockchain* akan terdiri dari 2 lapisan, yaitu lapisan rantai utama dan lapisan sub-rantai. Penggunaan *shading* pada arsitektur dimaksudkan untuk meningkatkan skalabilitas dan efisiensi dari *blockchain* yang ada.

3. *Social Network*

   Jaringan sosial yang dimaksud adalah bagaimana hubungan suatu pengguna dengan pengguna lain dalam *Online Social Network*. Tidak terdapat perbedaan yang cukup berarti pada bagian ini dengan OSN saat ini selain layanan data dari arsitektur yang terdistribusi.



Gambar 2. Arsitektur DOSN yang memanfaatkan Blockchain [32]

Untuk meningkatkan keamanan dan privasi pengguna, Zeng *et al.* [32] juga mengajukan konsep *access control* berbasis reputasi (*reputation-based authority control*) yang akan membatasi akses pengguna di dalam sistem berdasarkan reputasi mereka dalam OSN.

Jiang dan Zhang [33] mengajukan konsep arsitektur BCOSN (*Blockchain-based Online Social Network*) yang menggunakan *blockchain* dan *smart contract* untuk meningkatkan efisiensi terhadap *access control* dan menjamin kepercayaan antar transaksi. Untuk meningkatkan privasi pengguna,

arsitektur BCOSN juga akan menggunakan *access control* berbasis enkripsi. Setiap data yang ditambahkan pada *blockchain* akan dienkripsi terlebih dahulu dan hanya orang-orang yang memiliki akses yang dapat membuka data pada *blockchain*.

Pemanfaatan *blockchain* pada DOSN akan memiliki beberapa kelebihan berikut [32] [33]:

1. *Blockchain* dapat menjamin seluruh transaksi *node* tanpa memerlukan pihak ketiga atau suatu *supernode* yang diberi otoritas lebih. Penggunaan *blockchain* akan memastikan hubungan antar *node* dapat dipercaya, sehingga arsitektur DOSN menjadi optimal.
2. Penggunaan *blockchain* dapat menghindari terjadinya *single point of failure*. Hal ini dikarenakan jaringan *blockchain* merupakan jaringan terdistribusi, sehingga kegagalan pada beberapa *node* tidak akan menyebabkan kegagalan pada DOSN.
3. *Blockchain* dapat memungkinkan pengguna untuk menyimpan dan menerima informasi tanpa takut adanya pemalsuan data. Tanpa *blockchain*, akan sulit untuk memastikan apakah data belum dimodifikasi dan belum dihapus pada DOSN.

Akan tetapi, penerapan *blockchain* pada DOSN ini juga masih memiliki beberapa batasan [32] [33], diantaranya:

1. Keamanan dari *blockchain* juga perlu mendapat perhatian tersendiri. Jika mayoritas dari *node* terkonsentrasi dalam suatu grup, maka grup tersebut dapat menyerang *blockchain* dan aplikasi-aplikasi yang terhubung (biasa disebut 51% *attack*). Akan tetapi, serangan ini memiliki *cost* yang sangat tinggi dan sudah terdapat beberapa penelitian yang mencoba menangani masalah ini [34].
2. Saat ini, biaya yang dibutuhkan untuk menerapkan *blockchain* pada DOSN masih cukup mahal, terutama jika arsitektur DOSN

mengimplementasikan *blockchain* pada berbagai *platform* yang ada saat ini. Penerapan *blockchain* akan lebih cocok untuk diimplementasikan pada jaringan independen yang sepenuhnya dibuat untuk aplikasi OSN. Jaringan independen ini akan memungkinkan DOSN untuk menyesuaikan *blockchain* dengan kebutuhan dengan harga yang lebih murah.

IV. Kesimpulan

Arsitektur *Online Social Network* (OSN) yang terpusat menyebabkan penyedia layanan memiliki akses dan kontrol penuh terhadap seluruh data dan informasi pengguna. Hal ini tentu saja dapat menimbulkan masalah terutama terkait dengan privasi pengguna. Permasalahan ini dapat diselesaikan dengan arsitektur *Decentralized Online Social Network* (DOSN). DOSN dapat meningkatkan privasi data pengguna melalui pemberian akses lebih bagi pengguna untuk mengelola informasi pribadi mereka dan penggunaan kriptografi pada informasi yang ada. Selain itu, arsitektur ini dapat menghapus otorisasi terpusat yang dimiliki oleh penyedia layanan OSN terhadap informasi pengguna melalui mekanisme penyimpanan yang terdistribusi.

Akan tetapi, DOSN masih memiliki banyak kekurangan seperti sulitnya membangun hubungan terpercaya antar *node* dan sulitnya menjamin integritas data tanpa adanya pihak ketiga yang dapat dipercaya. Hal ini dapat diatasi melalui penerapan *blockchain* dalam arsitektur DOSN. Penggunaan *blockchain* dapat menjamin seluruh transaksi *node* tanpa memerlukan pihak ketiga atau suatu *supernode* yang diberi otoritas lebih. Selain itu, *blockchain* dapat menghindari terjadinya *single point of failure* dan memungkinkan pengguna untuk menyimpan dan menerima informasi tanpa takut adanya pemalsuan data.

Referensi

[1] "Facebook Statistics," Facebook, Accessed: April 19, 2020. [Online]. Available: http://www.facebook.com/press/info.php?statistics.

[2] C. Levato, G. Linn, L. Stead, and A. Best, "Impact of tobacco advertising and promotion on increasing adolescent smoking behaviours," *Cochrane Database Syst Rev.*, vol. Vol. 4, 2003.

[3] S. Mahmood, "New privacy threats for facebook and twitter users," *in 2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. IEEE, 2012, pp. 164–169.

[4] "How Trump Consultants Exploited the Facebook Data of Millions," NYTimes, Accessed: April 21, 2020. [Online]. Available at: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[5] R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," *in WPES,* 2005, pp. 71–80.

[6] A. Felt, "Defacing facebook: A security case study," *in USENIX Security '07*, 2007.

[7] T. Bradshaw, "The first google+ privacy flaw," *in The Financial Times*, 2011.

[8] S. Mahmood and Desmedt, "Your facebook deactivated friend or a cloaked spy," *in 2012 IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE*, 2012, pp. 367– 373.

[9] "Obama advises caution in use of Facebook," Associated Press, Accessed: April 21, 2020. [Online]. Available: https://www.youtube.com/watch?v=si1gNXqH7iw.

[10] S. Mahmood and Y. Desmedt, "Two new economic models for privacy," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 4, 2013, pp. 84–89.

[11] S. Mahmood and Y. Desmedt, “Usable privacy by visual and interactive control of information flow,” *in Twentieth International Security Protocols Worksho*p, 2012.

[12] S. Mahmood, “Online social networks: Privacy threats and defenses,” *in Security and Privacy Preserving in Social Networks.* Springer, 2013, pp. 47–71.

[13] G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” *2015 IEEE Security and Privacy Workshops*, 2015.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, 2017, pp. 557-564.

[15] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *in IEEE Access*, vol. 7, 2019, pp. 22328-22370.

[16] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2016, pp. 839-858.

[17] J. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction," *in IEEE Consumer Electronics Magazine*, vol. 8, no. 5, 2019, pp. 20-25.

[18] M. Bez, G. Fornari and T. Vardanega, "The scalability challenge of ethereum: An initial quantitative analysis," *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, San Francisco East Bay, CA, USA, 2019, pp. 167-176.

[19] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. Newton, MA, USA: O’Reilly Media, Jan. 2015.

[20] N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, vol. 2, no. 9, 1997. Accessed: April 19, 2020. [Online]. Available: https://firstmonday.org/ojs/ index.php/fm/article/view/548.

[21] “Event Mechanism,” Solidity, Accessed: April 19, 2020. [Online]. Available: http://solidity.readthedocs.io/en/v0.4.21/contracts.html#events

[22] B. Guidi, T. Amft, A. De Salve, K. Graffi, and L. Ricci, “DiDuSoNet: A P2P architecture for distributed Dunbar-based social networks,” *PeerPeer Netw. Appl.*, vol. 9, no. 6, 2016, pp. 1177–1194

[23] R. Sharma and A. Datta, “SuperNova: Super-peers based architecture for decentralized online social networks,” *in Proc. IEEE Int. Conf. Commun. Syst. Netw.*, 2012, pp. 1–10.

[24] S. Nilizadeh, S. Jahid, P. Mittal, N. Borisov, and A. Kapadia, “Cachet: A decentralized architecture for privacy preserving social networking with caching,” *in Proc. ACM Int. Conf. Emerg. Netw. Exp. Technol.*, 2012, pp. 337–348.

[25] S. Buchegger, D. Schiöberg, L.-H. Vu, and A. Datta, “PeerSoN: P2P social networking: Early experiences and insights,” *in Proc. ACM Eur. Conf. Comput. Syst. Workshop Social Netw. Syst*., 2009, pp. 46–52.

[26] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, “Persona: An online social network with user-defined privacy,” *ACM SIGCOMM Comput. Commun*. Rev., vol. 39, no. 4, 2009, pp. 135–146.

[27] S. Fu et al., “Cadros: The cloud-assisted data replication in decentralized online social networks,” *in Proc. IEEE Int. Conf. Services Comput.*, 2014, pp. 43–50.

[28] R. Nasim and S. Buchegger, “XACML-based access control for decentralized online social networks,” *in Proc. IEEE Int. Conf. Utility Cloud Comput.*, 2014, pp. 671–676.

[29] A. De Salve, P. Mori, and L. Ricci, “A privacy-aware framework for decentralized online social networks,” *in Proc. Int. Conf. Database Expert Syst. Appl. Cham, Switzerland: Springer*, 2015, pp. 479–490.

[30] Y. Cheng, J. Park, and R. Sandhu, “An access control model for online social networks using user-to-user relationships,” *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 4, 2016, pp. 424–436.

[31] O. Bodriagov, G. Kreitz, and S. Buchegger, “Access control in decentralized online social networks: Applying a policy-hiding cryptographic scheme and evaluating its performance,” *in Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops*, 2014, pp. 622–628.

[32] S. Zeng, Y. Yuan and F. Wang, "A decentralized social networking architecture enhanced by blockchain," *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China*, 2019, pp. 269-273.

[33] L. Jiang and X. Zhang, "BCOSN: A Blockchain-Based Decentralized Online Social Network," *in IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, 2019, pp. 1454-1466.

[34] D. Vangulick, B. Cornélusse, and D. Ernst, “Blockchain: A novel approach for the consensus algorithm using Condorcet voting procedure,” *in Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPCON)*, 2019, pp. 1–10.