Ushare: user controlled social media based on blockchain

Antorweep Chakravorty
Department of Computer Science & Electrical Engineering
University of Stavanger
4036 Stavanger, Norway
antorweep.chakravorty@uis.no

Chunming Rong
Department of Computer Science & Electrical Engineering
University of Stavanger
4036 Stavanger, Norway
chunming.rong@uis.no

ABSTRACT

This paper presents the potential for blockchain based solutions to disrupt the world of social networking. We offer *Ushare*, a user centric blockchain supported social media network that enables users to control, trace and claim ownership of every piece of content they share. Harnessing peer-to-peer capabilities of the blockchain technology allows a truly decentralized, secure, anonymous and traceable content distribution network. *Ushare* consists of four key components: the blockchain, a hash table with encrypted content shared by a user, a Turing complete relationship system to control the the maximum number of shares performed by user's circle members and a local personal certificate authority that manages the user's circles and encrypts data to be shared before it is broadcasted to the network.

CCS Concepts

•**Human-centered computing** → **Social networking sites; Social tagging systems;** *Reputation systems;* Collaborative and social computing devices; •**Security and privacy** → *Cryptography;* Database and storage security; •**Computing methodologies** → *Parallel computing methodologies;*

Keywords

blockchain; ownership; traceability; control; sharing; social network

1. INTRODUCTION

The modern world is increasingly becoming driven by data. This is not just limited to Internet of Things (IoT), ubiquitous mobile computing, smart energy grids and cities, but more so in social media. Users and corporations are now connected, interacting and sharing data among themselves at an increasing pace. The infrastructure of such services has been traditionally supported by centralized networks. However, lack of trust, transparency and control over organizations that furnish such networks has brought to light the adverse aspects of centralization [13, 3, 15]. The emergence of disruptive innovations has led the computing space towards a decentralized, autonomous, and distributed paradigm [4, 22, 21, 8]. Users are also becoming conscious of their online presence and expect to have more control, traceability, accountability and ownership of their data.

The first generation of blockchain based technologies [22, 16] is widely documented to have demonstrated the merits of decentralization, disintermediation, anonymity and censorship resistance in the financial industry. Blockchain technologies, through its second iteration, have not only enabled simple transactions, but also complex computation on a network [7, 12, 14, 28, 19]. These advances are not just limited to the financial sector, but new internet applications can also harness these building blocks to empower users to take control of their online footprint.

In this paper we propose *Ushare*: a novel blockchain for social networks that models its state transition system on data shares. It would enable users to create a secure, permanent and unbreakable link with their data. They would be able to share their data with their circle of friends, family and others. Using a scriptable *Relationship System* on the blockchain, the traceability and the ownership of the data would be maintained, even when their data are shared further down the social network. It would be able to control the number of further shares members in a user's circles can perform. We also introduce a *Personal Certificate Authority (PCA)* for each user, that would remains outside the blockchain in their personal space as a client software. The PCA would issue certificates based on the circles created by a user to share their data. This allows only members belonging to a user's particular circle to view the content shared with that circle from the blockchain. The PCA would also maintain a revocation list for members of a user's circle who have been removed and their rights to view future content would be voided. The proposed blockchain social network would not only allow ownership of content to be verified, tracked and controlled, but also secure their content from any central authority, third parties or individuals who do not have rights to view the content.

The rest of the paper is structured as follows: Section 2, provides an overview on aspects of blockchain technology that would enable realization of the proposed solution. Section 3, discusses the existing notion of data ownership, traceability and security for blockchains. The proposed solution is detailed in section 4. In section 5, frameworks that could be used to build the solution are discussed. Finally, in sec-

IMCOM '17, January 05-07, 2017, Beppu, Japan
© 2017 ACM. ISBN 978-1-4503-4888-1/17/01...$15.00
DOI: http://dx.doi.org/10.1145/3022227.3022325

tion 6 we present the related work on similar approaches using blockchains for social networking and we conclude with section 7.

2. BACKGROUND

The sub-sections in this part introduce some of the technologies that could be used to build *Ushare*. We give an overview of blockchains, their types, types of validations for blocks, incentives that could be provided to participating nodes in the network and smart contracts. *Ushare* could be built as a permissioned blockchain because it would require users in its network to be validated. It could use proof of stake as a validation scheme since it allows for better utilization of resources and would suit in a permissioned setting. Incentive scheme for *Ushare* could be access to the social network and ability to share their data in a secure, annonymized and decentralized manner. Finally, its relationship system could also draw upon the contributions from smart contracts.

Blockchains could be defined as a chronological database of transactions grouped in a block and validated by a network of computers, with multiple blocks added one after another in a chain. The current iteration of blockchain is based on the cryptocurrency Bitcoin [22]. Since then, multiple blockchain based new internet applications that take advantage of its decentralization, traceability, accountability and security have emerged.

Blockchains can be grouped as permissioned and permissionless. In addition, there are two key mechanisms: Proof of Work and Proof of Stake for validation and acceptance of blocks that are added to a blockchain. Finally, computers in a network are incentivised to do some form of work in terms of computation to validate these blocks. Each of these concepts are described bellow.

2.1 Blockchains

The main differentiator for the type of blockchain is based on the authorization requirements for nodes in a network to act as validators and have access to the blockchain data [26].

2.1.1 Permissionless

Permissionless blockchains are public and allow anonymous users to participate and contribute their computational power.

2.1.2 Permissioned

Permissioned blockchains are restricted and users participate after verification from a centralized third party. This kind of blockchains is usually private.

2.2 Block Validation

Transactions that are broadcasted to a blockchain are grouped into blocks and these blocks are validated by a competing network of peer nodes. The node that first validates a block of transactions is rewarded in some form. The mechanisms used for validating blocks can be described as proof of work and proof of stake. Any blockchain could use these mechanisms to validate its blocks.

2.2.1 Proof of Work

The early blockchains were built around the concept of proof of work [22]. The amount of work performed is measured in terms of computational contributions, also called as mining. All nodes in the network compete to mine for a new block by solving for some partial collision using hash functions. The miner that computes it first is rewarded. However, this form of validation could be extremely inefficient in term of energy and, therefore, also very expensive as the work done by miners that do not get validated first are wasted. This incentivises nodes to centralize the hashing power into pools, which obviously is not desirable for a network whose goal is to minimize the need to trust third parties [25].

2.2.2 Proof of Stake

Proof of stake [11, 17, 29] validates blocks by randomly choosing nodes to contribute their block to the chain. This form of validation chooses a node based on their stake or reputation, randomness, or through distributed voting.

2.3 Incentives

The nodes in a blockchain network are incentivised to contribute their computing power. Each time a node verifies a block and it is accepted into the blockchain, they get some form of reward. In the cryptocurrency world, they are rewarded in those currencies either by materializing a coin, providing a percentage of the transaction or allocating the unspent transactions. This facilitates the activeness and decentralization of the blockchain network.

2.4 Smart Contracts

Multiple efforts [2, 6, 24] have been undertaken to improve the rudimentary scripting system proposed in [22]. Additionally, there are others [30] that have proposed extension of such scripting system into what are termed as Smart Contracts. Smart Contracts consists of a program code, a storage file and an account value. It allows any user to create a contract by broadcasting a transaction. Once a contract gets created it cannot be altered.

3. DATA OWNERSHIP, TRACEABILITY, INTEGRITY & SECURITY

Blockchains are designed to operate without the need of a central authority. It builds consensus based on the peers in the network who validate the transactions and their lineage. It becomes particularly suitable for authentication of ownership rights as all history of transactions are validated, accepted and added to the blockchain by the whole network allowing ownership to be forever validated and traced.

Data confidentiality, availability and integrity are other key features of blockchains. Permissioned blockchains protect unauthorized disclosures as the blockchain remains private and transactions are accountable. Blockchains are peer-to-peer systems with each participating node possessing the complete blockchain or parts of it. Availability of data in such a decentralized system remains high, even with a catastrophic failure, as there would always be some nodes possessing the blockchain. Data integrity ensures that data accepted or available in the blockchain is protected from invalid modification, insertion or deletion. Mechanisms such as proof of work and proof of stake are key in ensuring that the data integrity is maintained. Blockchains inherently preserve data integrity as any malicious activity on the blockchain needs control of more than half of the network's computing power.

The decentralized nature of the blockchain could often lead to a counter intuitive notion about data security since the whole network would have access to the blockchain. However, innovations on such problems have led to strong encryption methods and zero knowledge proofs to store and access data in a much more secure manner.

4. PROPOSED SOLUTION

Ushare would allow users to have control over their social interactions. It introduces a unique blockchain that describes assets as data shared or broadcasted to the network. Unlike regular state transition systems that describe ownership status of assets, it will describe a state as a depletion of a token value that determines the number of transactions or shares that can be performed with that asset. A Turing complete Relationship System would handle the transition of the states through validation of the tokens until they get completely depleted. Finally, a client based Personal Certificate Authority (PCA) would maintain a user's relationships and ensure that the encrypted assets that have been shared are viewable by only the intended circle of members. Further, the solution would be completely anonymous and secure as all stored data would be encrypted off-sight before storing it in the blockchain or any accompanying system.

4.1 *Ushare*

Ushare can be classified as a permissioned blockchain as actors in the network need to be named to develop consistency, accountability and traceability of shared data. It can have a set of third parties to carry out the verification of each new user who joins the network, providing them with a unique identity.

A transaction is made between a user and the members belonging to the user's circle. The PCA creates a encrypted version of the data with the circle's public key and stores it into a distributed hash table. Since, multiple users might encrypt the data to share among their own circles, the hash table contains three columns. The first being the hash of the encrypted data item shared with them, the second being hash of the data item decrypted and re-encrypted using their circle's public key for further shares and the third column stores this data item that they encrypted. The genesis transaction of the data item has the same hash for both the first two columns. The user shares the hash id of the data they encrypted with each member of their circle. This enables maintainability of precise traceability and control over shareability. Transactions are broadcasted to the blockchain with the user identity and the data hash id to record the trails. It also contains a token value, set by the data owner that specifies the allowed number of additional shares. Whenever a transaction is broadcasted, the Relationship System is invoked and it verifies that the share is allowed by checking the token value. It decrements the token value for any further shares by a member of the user's circle. Transactions with the data item are disallowed when the token value becomes zero.

In the following sub-sections, we describe these two key modules of *Ushare*.

4.1.1 Distributed Hash Table

The hash table would act as a distributed data store similar to that proposed for BigTable [10]. Blockchains are inherently decentralized, but not distributed. Data items that a user shares could be of type image or video. These are files of large sizes and need to be stored in a distributed manner for efficient storage, indexing and traversals. The blockchain itself would contain the transactions in terms of user shares, referring to the shared hash id of a file. The lineage of a file is recorded in the hash table with an old and new hash ids. The old hash refers to the file encrypted by the user who shares it and the new hash represents the file decrypted and re-encrypted by the user with whom the file was shared.

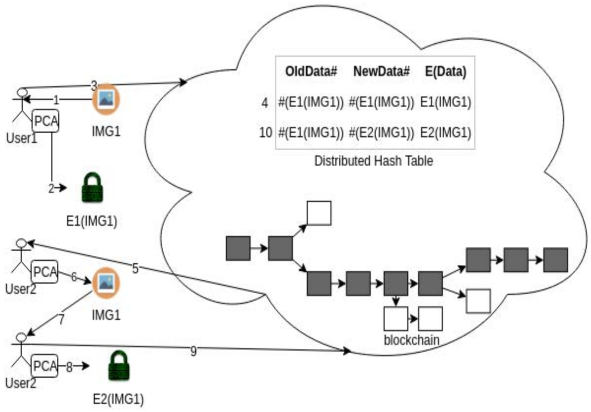

Figure 1: Hash Table Workflow

Figure 1, shows the workflow for creating the hash table. A user, User1 gets an image IMG1(1) and encrypts it with the public key of the circle with whom it will be shared using the PCA(2). The user then stores the encrypted image into *Ushare*'s hash table(3) with the hash of his encrypted image as OldData# and NewData#(4). Since the user is the owner of the image, both the old and new hash keys are the same. Another user, User2 is a member of the circle who has access to the shared image. After traversing the blockchain, the user can access the image from the hash table(3) and decrypt it(6). This user now re-shares this image(7) with its circle by encrypting it with the public key of the circle(8). This encrypted image gets stored in the hash table(10) with the hash key of the previous encryption as oldData# and its new hash as NewData#.

Maintaining a separate hash table for storing the data outside the blockchain allows a predictable growth of the blockchain. Since validation of blocks usually needs downloading of the complete chain by the participating nodes, larger blockchains would put considerable computing constrains.

4.1.2 Blockchain

A user wishing to share a data item with its circle creates the first broadcast as a transaction with its identity as "from" and the hash key of the encrypted data item as "to" address. The transaction also contains a "token value" that specifies the number of allowed shares with that data item. Next, the user broadcasts multiple transactions, each containing the encrypted data hash key as from address and identity of the members of the circle as to address. The value of the token is also present in the transaction. Any shares made with this data item make another transaction with the new user's identity as from address and the hash

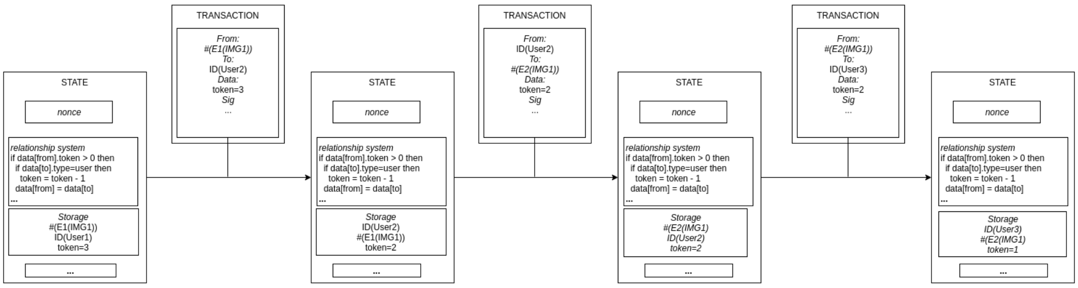

Figure 2: State Transitions

key of the data encrypted with this new user's circle key as to address. Following this, multiple transactions are again made for members of that user's circle with the new hash key as from and the identity of members of the user's circle as to address.

Figure 2, shows the state transitions. A transaction contains a from address, a to address, the data value and a digital signature. A state contains a cryptographic nonce which is an arbitrary number that may only be used once. An executable code using the relationship system verifies whether a transaction is valid in terms of the allowed number of shares. If the transaction is allowed, it decrements the token value by one. A data storage is also present, containing the trails of the shares and its token value.

Ushare would inherit the technicalities from established blockchains for validation of blocks, proof of work, proof of stake, maintenance of the decentralized database, incentives for mining and other procedures. Please refer to section 2 for details.

4.2 Relationship System

The relationship system would be a Turing complete programmable unit which remains a part of the blockchain. It can feature loops, internal states and can even make transactions with other actors. The computation would be executed on every participating node in the network. The main goal of this system is to verify that shared transactions are valid. Prior to creating a state, it verifies the token value and decrements it. Whenever a token value reaches zero, it reverts to the previous state and does not allow any future share of that data item.

4.3 Personal Certificate Authority (PCA)

The PCA is a client software that manages a user's circles, securely shares the private keys of the circles with its members, keeps records of keys shared with it and encrypts any data shared with a circle with its public key. It ensures that any data stored in *Ushare*'s hash table is encrypted before it is broadcasted. It also maintains a revocation list that revokes rights of a member of a user's circle.

The key management for PCA could be built upon the existing Bitcoin Wallet solution[1]. There are multiple applications that aim at providing identity management for blockchains using symmetric keys. ShoCard[2], offers solutions for creating digital identities that protect consumer privacy. Uniquid[3], offers blockchain access management for digitally connected assets inside a network of smart devices and people. Healthnautica [5], tries to maintain secure medical records and audit trails. Insights could be gained from these applications that would add to the development of *Ushare*.

However, with the growth of the blockchain with multiple circles and members, the key management issues could have a major impact on security and performance. Alternative to symmetric encryption, solutions such as [27], could also be used. It relates to a system for protecting an encrypted information unit, with the unit being encrypted by applying an encryption key on the information unit. A chosen number of system users have encryption subkeys and the system comprises a calculation means for calculating the encryption key from the encryptions subkeys provided by said users based on a predetermined mathematical function.

5. FRAMEWORKS

The proposed *Ushare* solution could be built from scratch as a new blockchain like other permissioned blockchains which include Eris[4], ripple[5]. Alternatively, *Ushare* could also be built upon existing blockchains. A popular framework on which this solution can be built is Ethereum [30]. It supports a built-in blockchain with a fully fledge Turing complete programming language [7]. Enigma [31] from MIT is another decentralized computational blockchain framework with guaranteed privacy. MultiChain [23] provides a rapid framework for designing, deploying and operating distributed ledgers. IBM offers the Hyperledger [9] project which is a collaborative effort in creating advance blockchain technologies. Openchain[6] is an open source distributed ledger allowing management of digital assets in a robust, secure and scalable way. BlockStack [1] provides a blockchain application stack to build decentralized, server-less apps by plugging into its services for identity, naming, storage, and authentication. DECENT [20] is a decentralized blockchain based peer-to-peer content distribution network.

In due course, all these platforms, including developing a framework from scratch, would be evaluated to determine the best suited approach for *Ushare*.

6. RELATED WORK

Akasha[7], Synereo [18] and Ascribe[8] are projects that ex-

[1] https://blockchain.info/wallet/#/
[2] https://shocard.com/
[3] http://uniquid.com/
[4] https://erisindustries.com
[5] https://ripple.com
[6] https://www.openchain.org/
[7] http://akasha.world/
[8] https://www.ascribe.io/

plore blockchains for social media. All of these solutions are in their infancy with an alpha release. Akasha is built on top of Ethereum and it aims to build a knowledge architecture for social human advocacy in the context of social networks, freedom of expression, creative perpetuity and privacy for a better Internet in service of humanity. Synereo presents a decentralized and distributed social network designed for an attention economy. It offers a platform more as a social market place. Ascribe leverages blockchain technologies to transfer, cosign or loan digital currencies.

These solutions remain in their early phase of inception and are not available for evaluation. Their design principles, methods, technology and aims are quite different to *Ushare*. Unlike these solutions, *Ushare* positions a user in the core of its philosophy. Its goals are to provide a distributed, decentralized, secure and anonymous platform so that users can share their content with whom they want. Further, all content stored on the *Ushare* platform remains encrypted with all keys managed by the PCA that remain on the users local devices.

7. CONCLUSION

A conceptual solution for creating a user centric social network that would enable users to control, trace and securely share content was presented in this paper. It was argued that the decentralization, anonymity, traceability and censorship resistance of blockchains could support such a platform. *Ushare*, the proposed platform would enable these and more. It would also support offsite encryption of data and mechanisms to share them through the blockchain. The functionalities would be delivered through four core components: the blockchain that would keep record of ownership of data items and number of shares made, a relationship system that would enable programmable code to be executed on the blockchain and control the number of allowed shares for a data item, a hash table that stores encrypted data that user shares and, finally, a local personal certificate authority that manages a user's circles, encryption keys and controls access to content.

Frameworks that would support the development of *Ushare* would be evaluated in the future. Scripting capabilities for such frameworks would be assessed in order to establish the relationship system. Various applications for identity management for blockchains would be another area of investigation. Overall having a user centric approach in controlling social network activities with guarantees on privacy, security, ownership, anonymity and traceability would be the key philosophy behind *Ushare*.

8. REFERENCES

[1] M. Ali, J. Nelson, R. Shea, and M. J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *2016 USENIX Annual Technical Conference (USENIX ATC 16)*, 2016.

[2] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek. Secure multiparty computations on bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 443–458. IEEE, 2014.

[3] J. Ball. Nsas prism surveillance program: how it works and what it can do. *The Guardian*, 8, 2013.

[4] J. P. Barlow. A declarationof the independence of cyberspace, 1996.

[5] G. Baxendale. Can blockchain revolutionise eprs? *ITNOW*, 58(1):38–39, 2016.

[6] I. Bentov and R. Kumaresan. How to use bitcoin to design fair protocols. In *International Cryptology Conference*, pages 421–439. Springer, 2014.

[7] V. Buterin. A next-generation smart contract and decentralized application platform. *white paper*, 2014.

[8] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*, 25(6):599–616, 2009.

[9] C. Cachin. Architecture of the hyperledger blockchain fabric. 2016.

[10] F. Chang, J. Dean, S. Ghemawat, W. C. Hsieh, D. A. Wallach, M. Burrows, T. Chandra, A. Fikes, and R. E. Gruber. Bigtable: A distributed storage system for structured data. *ACM Transactions on Computer Systems (TOCS)*, 26(2):4, 2008.

[11] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Proceedings on Advances in cryptology*, pages 319–327. Springer-Verlag New York, Inc., 1990.

[12] P. Devanbu, M. Gertz, C. Martel, and S. G. Stubblebine. Authentic third-party data publication. In *Data and Application Security*, pages 101–112. Springer, 2002.

[13] V. Goel. Facebook tinkers with users emotions in news feed experiment, stirring outcry. *The New York Times*, 2014.

[14] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 491–500. ACM, 2011.

[15] B. Hardekopf. The big data breaches of 2014. *Forbes, January*, 13, 2015.

[16] A. Hayes. Evidence for bitcoin. *Altcoin Price Efficiency: Miners' Arbitrage in Cryptocurrency Markets*, 2014.

[17] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, 19, 2012.

[18] D. Konforty, Y. Adam, D. Estrada, and L. G. Meredith. Synereo: The decentralized and distributed social network. 2015.

[19] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *University of Maryland and Cornell University*, 2015.

[20] P. Linder. Decryption contract enforcement tool (decent): A practical alternative to government decryption backdoors.

[21] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. H. Byers. Big data: The next frontier for innovation, competition, and productivity. 2011.

[22] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[23] S. D. Norberhuis. *MultiChain: A cybercurrency for cooperation*. PhD thesis, TU Delft, Delft University of

Technology, 2015.

[24] R. Pass et al. Micropayments for decentralized currencies. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 207–218. ACM, 2015.

[25] M. Peck. The bitcoin arms race is on! *IEEE Spectrum*, 6(50), 2013.

[26] G. W. Peters and E. Panayi. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *Available at SSRN 2692487*, 2015.

[27] C. Rong and G. Zhao. System for protecting an encrypted information unit, Oct. 7 2014. US Patent 8,855,317.

[28] M. Swan. *Blockchain: Blueprint for a new economy.* " O'Reilly Media, Inc.", 2015.

[29] P. Vasin. Blackcoins proof-of-stake protocol v2, 2014.

[30] G. Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 2014.

[31] G. Zyskind, O. Nathan, and A. Pentland. Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*, 2015.