WISChain: An Online Insurance System based on Blockchain and DengLu1 for Web Identity Security

Yurong Guo, Zongcheng Qi
School of Computer Sci. & Tech.
Guangdong Univ. of Technology
Guangzhou, China
867837489@qq.com

Xiangbin Xian, Hongwen Wu
Web Identity Security Lab
Guangdong Univ. of Technology
Guangzhou, China
120344408@qq.com

Zhenguo Yang, Jialong Zhang
NoPhish Technology Ltd
DengLu Technology Ltd
Hong Kong SAR, China
shawn@nophish.net

Liu Wenyin
School of Computer Sci. & Tech.
Guangdong Univ. of Technology
Guangzhou, China
liuwy@denglu.net.cn

***Abstract*—An insurance system based on blockchain is proposed for web identity security, which provides two insurance service models for personal web identity security of end users and data security of commercial websites, respectively. Claim evidences are uploaded automatically to the blockchain to keep their authenticity. Smart contracts are automatically applied between insurers and policyholders to build trust between them.**

Keywords—blockchain, insurance, web identity security.

I. INTRODUCTION

Many people on the Cyberspace have many web identities (login accounts and passwords) which have caused a severe security problem, called "Password Fatigue". Because they cannot remember all these passwords, they intend to use weak passwords, reuse the same passwords for many different websites, keep passwords unchanged for long time. To help people mitigate this sufferance, we have developed DengLu1 [1], which is a web identity authentication and management system and can help people remember and manage strong passwords and conduct automatic registration, login, and even automatic change of passwords.

However, it is very difficult to prevent all cyber-attacks, because most websites still have many unknown vulnerabilities. Hence, even though the network security technologies are greatly improved so far, it seems that data leaks (even from big and famous websites) are inevitable and all end-users will sooner or later be involved in such leaks and suffer losses in many kinds. In general, people can get compensation by purchasing insurance for such losses. However, few insurance companies so far provide this kind of insurance to compensate for the loss of information assets because it is difficult to estimate such losses due to lack of evidences. Insurance companies have concerns that the claim evidences can be fabricated. It seems that the distributed ledger and the tamper-proof nature of blockchain can solve this information inequality and counterfeiting, and hence make blockchain a promising solution to network security insurance. Claim evidences are uploaded automatically to the blockchain to keep their authenticity. Smart contracts are automatically applied between insurers and policyholders to build trust between them. It seems that web identity security insurance based on blockchain not only can facilitate insurance companies to provide insurance services safely, but also can increase the market competitiveness of websites that have purchased the insurance. Certainly, the insurance for individual users can also reduce the loss of personal account password leakage.

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

In this paper, we propose an online insurance service based on DengLu1 and blockchain for web identity security (WIS), namely, WISChain. It provides two insurance service models for personal web identity security of end users and data security of commercial websites, respectively. We also require the policyholders to use DengLu1 when accessing the Web. At least, their premiums can be greatly reduced if DengLu1 is adopted. For end-users, if they adopt DengLu1 but their passwords are still leaked, they can claim their losses and receive corresponding compensations. Another important insurance target is the databases of commercial websites. Various insurance programs can achieve automatic payment in the form of smart contracts on WISchain. We believe blockchain-based insurance models for web identity security can establish trust relations among insurance companies, security companies, websites, and individual end-users.

II. REALTED WORK

Liu et al. have ever proposed an insurance model for web services [2]. They point out the importance and practicable business models of providing insurance for web services, involving insurers, security companies, commercial websites and end users. There are two main aspects of insurance for web services. One is to provide insurance for websites, and the other is to provide insurance for specific software which needs to be connected to the Internet. The former model is that security companies sell security products to websites and provide insurance, such as 360-like security companies. The latter is provided by software developers, such as Alibaba, which provides insurance for Alipay. However, there are few independent insurance companies providing insurance for websites and software, because of the lack of professional security knowledge on assessment of websites and software security. They are even less likely to file suits against insurance fraud behaviors. Blockchain based insurance has also been proposed in certain traditional industries [3]. Etherisc also launched three pilot apps for aviation delay insurance, social security insurance and agricultural insurance [4]. However, there are still restrictions on insurance in traditional industries due to both digitalization and equivalence of claims evidences.

III. ARCHITECTURE

As we can see from Fig. 1, in addition to the blockchain as the database, WISChain involves five important parties, namely, DengLu1 server, insurance companies (Ins Co.1,2,…N), security companies (Sec Co.1,2,…N), end-users (APP1, 2,…N), and commercial websites (Website1,2,…N). The blockchain

hosts mainly the hash data of all the logs of end-users and websites. DengLu1 server and each of the security companies host a full node of the blockchain and is responsible for packing the data uploaded to the blockchain based on the consensus mechanism. Each website/end-user buys an insurance product from an insurance company, which may hire a security company to assess the security level of the potential policyholder.

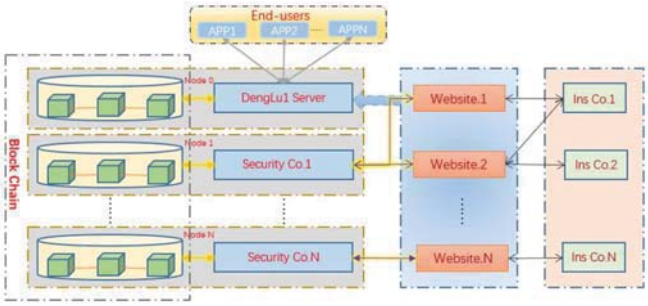

Fig. 1. Architecture of WISChain

A. Data on the Blockchain

Due to the large number of logs on the websites and the privacy of the logs, the logs cannot be stored directly on the blockchain. Only the hash data of the logs per second from each website will be uploaded and packed by a security company selected by the consensus mechanism. This ensures both security and authenticity of the logs. The DengLu1 server is responsible for uploading the hash data of all users' logs similarly.

B. The Consensus Mechanism

WISChain uses the parity POA as the consensus mechanism. WISChain also wishes to establish a decentralized, peer to peer insurance marketplace to fraud which is quite common in the insurance industry. We also uses a credit/token mechanism to reward those credit-worthy insurers and those who make other contributions, such as data packing. This award can be used as premiums to motivate users to maintain a virtuous cycle of the system for sustainable development.

C. The DengLu1 Server

The DengLu1 Server is a key component of WISChain, which is the hub of all web identities of all end users when they are used for registration/login/modification. It records all logs whose hash values are uploaded to the blockchain for checking the authenticity of the logs submitted by a policyholder to its insurance company when a claim is made.

D. Insurance Companies

Insurance companies can provide different insurance products. Their service targets can be divided into two categories: end-users and commercial websites. The insurance companies cooperating with WISchain can design different personalized insurance plans for end-users. Commercial websites can choose different insurance companies and different insurance products according to the degree of importance of their databases. In fact, most scenario-based insurance plans can be automated and quickly payable in the form of smart contracts.

E. Security Companies

When a potential policyholder wants to buy an insurance plan, a security company may be hired by the insurer to conduct a comprehensive security assessment on related website/terminal, improve its security level and reduce the risk rate. When a claim is made with a complicated situation, the security company can act as a neutral judge to detect whether the attack is within the scope of the claim. Security companies that make certain services, including judgement and data packing, to the system can receive certain token rewards.

F. End Users

Personal accounts and passwords are important insurance targets for end users. Personal participation in the insurance service of WISchain is based on the adoption of DengLu1. If a user who uses DengLu1 to manage their accounts and passwords wants to protect and buy insurance for any pair of account & password, DengLu1 can record all log data for the user's operations and their hash data are uploaded to the blockchain. If the user's account/password is stolen in certain ways, the user can get insurance compensation.

G. Commercial Websites

All related insurance terms for a website database can be predefined as smart contracts. If the password of a member is leaked from the database at the website server, the owner of the website as the enterprise user can upload the proof of leaked account, and a qualified third party (e.g., a security company) can assess it. The assessment results will be used to process the claim. When an accident triggers a claim, the smart contract automatically processes payment and reimbursement. The hash data of the logs on the blockchain can be used to verification. Consequently, commercial websites who buy insurance for their website databases can increase their competitiveness among peers, making them more attractive to users than uninsured websites, and can be less worried about data leaks.

IV. Conclusion

GDPR issued by the European Union is effective now and makes companies to pay more attention to protecting their users' data and privacy. Due to the high penalty of data leaks, the network insurance has become an urgent need. The blockchain based insurance may overturn the traditional profit model of the insurance industry with more transparent mechanisms, less premiums, and quicker settlement of claims, which can be more conducive to the promotion of network security insurance. WISChain is an attempt in this direction. It can be tested at [5]. All tests and feedbacks are welcome.

References

[1] https://www.DengLu1.cn/
[2] Liu, W et al. (2010). Business models for insurance of business web services. Service Intelligence and Service Science: Evolutionary Technologies and Challenges. 261-272. 10.4018/978-1-61520-819-7.ch014.
[3]http://finance.sina.com.cn/meeting/2018-05-21/doc-ihaturft6434356.shtml
[4] https://etherisc.com/
[5] https://wischain.denglu1.cn/