Huang, G.K.J. & Chiang, K.H. (2017). RegTech evolution: The TrustChain. In *Proceedings of The 17th International Conference on Electronic Business* (pp. 302-305). ICEB, Dubai, UAE, December 4-8.

RegTech Evolution: The TrustChain

(Work in Progress)

Grant K.J. Huang*, National Chengchi University, Taiwan, guanruey@icloud.com
Kuo-Huie Chiang, National Chengchi University, Taiwan, jkchiang@nccu.edu.tw

ABSTRACT

Integrity is a lifelong duty. Credit is not only given to natural persons but also to corporate citizens. In this work, we propose a blockchain-based RegTech system which helps to track the credit of organizations. The creditability of tender entity, participants and subcontractors altogether comprise the long-lasting undeniable TrustChain. The framework is scalable to all elements deemed necessary to corporate score card and referral to the developing RegTech. We expect the consistency and honesty of corporate citizens lay the foundation of a Trust society.

Keywords: RegTech, Blockchain, Smart Contract, Credit, Corporate Social Responsibility.

*Corresponding author

INTRODUCTION

Blockchain / distributed ledger or bitcoin-like technology has been regarded as an opportunity of many industries. The real innovation is not the digital coins themselves, but the trust machine that mints them (Kõlvart *et al*., 2016). The autonomous, decentralized property and comparative advantages of accountability, traceability, authenticity and non-repudiation challenge current 3rd party intermediary function as centralized authentication, and also launch the new digitalization era of financial industry, credit system, file sharing, investment tracking, and even the Internet of Things.

Accompanying the quick evolving technology, new term Regulatory technology (RegTech) appears in 2016 at governmental level in UK FCA. It reminds us of the first few years of big data and its equivalent important topics - big security. Modern regulation, like 'General Data Protection Regulation' by EU Parliament, focuses on unifying data protection for all individuals and governs the data controller of personal data. However, it is widely perceived that counting only on limited legal resources to rectification would be ineffective. We may instead expect people to behave well proactively and build a mechanism with positive reinforcement and penalty impact that is naturally persuasive and if possible, encouraging to the cumulative credit which could be regarded as an asset.

Society nowadays requires more and more corporate governance and transparency for resourceful enterprises. For the public procurement stakeholders, besides the profession and contractual capacity, play by rule of the game and do what is right, just and fair altogether help generate the solid accountability. For long, economist and computer scientists have strived to enhance the credit system by designing various mechanisms. Now we have a worthy alternative to invest. With embedded smart contracts evolving from blockchain, the gap between expectation and feasible methods gets closer. Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks (Szabo, 1997). By contrast to traditional contract, parties in smart contracts have no choice but to implement completely(Kõlvart *et al.*, 2016). After instructions are given, the predefined transaction will be self-enforcing. It largely saves the cost of supervision and eliminates the room to negotiation on payment. This confines all related parties to focus on content of agreements instead of nonperformance discount.

E-Procurement

Blockchain based system is developing quickly, however, its application in corporate regulation is rare. We select a lucrative zone to highlight the necessity of exploration. Moreover, from different perspective of the professional misconduct against public interest, people observe a smattering knowledge of the grey side of the ecosystem. To get a glance at the status of Taiwan, we conduct following analysis.

Data Preprocessing

For research purpose, we develop a web crawler to retrieve the web open data during Oct 2013 and Nov 2015 of National Procurement System, compare interim tenders (totally 108,360 cases) with the profile in Department of Commerce, MOEA by help of SheetHub.com.(Wang, 2015).

Data Analysis

After data preparation, we count the occurrences on same bidding cases. As in Figure 1, each company is a single node. If intersections of bidding on same cases are more than 5 times, the parties involved will be given an edge. Here is the example of procurement amount between NTD 20 million and NTD 100 million.

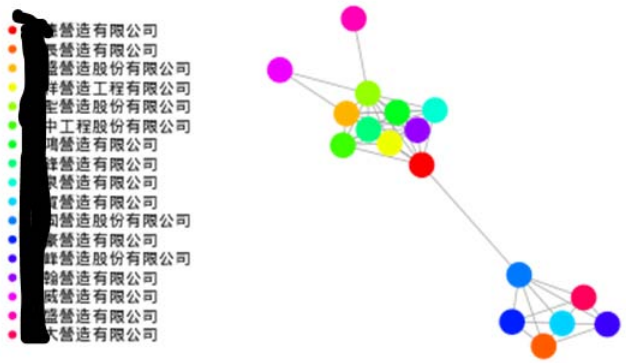

Figure 1: Bidding on same cases > 5 times

Some enterprises are inclined to meet frequently, who might be competitors of each other. However, among such intersections, there are instances that different companies bidding on same case are of the same directors. And one of them at last wins the tender. We use the Jacaard index $J(A,B) = \frac{(A \cap B)}{(A \cup B)}$ to compare the similarity and diversity of the directors of board. Table 1 and 2 exemplify such occurrences.

Table 1: Product procured: Brown Rice

Case 1	Bank of Taiwan，5,000 ton brown rice（Origins: Australia） Case size: NTD 5 million.	
Tender ID	Company name	Director of Board
70[redacted]4	A company	吳[redacted]里,周[redacted]紹,周[redacted]元,周[redacted]良
27[redacted]1	B company	吳[redacted]里,周[redacted]紹,周[redacted]元,周[redacted]良

Table 2: Product procured: Gas CO_2

Case 2	Taiwan Tabaco CO_2 500,000 kg	
ID	Company	Director of Board
5[redacted]3	A	(skip)
3[redacted]8	B	余[redacted]德,洪[redacted]芬,黃[redacted]潭,陳[redacted]銘,蔡[redacted]祥,黃[redacted]旺,洪[redacted]信,洪[redacted]三
2[redacted]9	C	(skip)
2[redacted]5	D	余[redacted]德,洪[redacted]芬,黃[redacted]潭,陳[redacted]銘,蔡[redacted]祥,黃[redacted]旺,洪[redacted]信,洪[redacted]三

The “Government Procurement Law” and “Enforcement Rules of the Government Procurement Act” regulate that at first round of open tendering procedures, there must be three or more tenderers submit their tenders. With a stretching lens to the connections of related business and their directors of board, we found that some participants indeed belong to the same owners. Such situation might be patterns of accompanying-bidding or bid rigging. No matter what reasons behind, the phenomenon may require a ledger to record for reference.

BLOCKCHAIN BASED TRUSTCHAIN

Original blockchain is a continuous ledger recorded on world distributed systems and is the Proof of Work process for bitcoin verification. Current blockchain incorporates interdisciplinary application and evolves a synthesis of distributed system, data compression, network protocol, cryptography, information theory, and game theory. To meet our requirement, in additional to nature of blockchain, we need a tokenized system capable of chaining only key value. The key needs to be distinct to connect external database of more detail requiring no computation. And the smart contract in a permissioned blockchain allows distributed encryption, fork tolerance, serialized consistency is suitable. We adopt the Ethereum Virtual Machine based smart contract, which is Turing complete to calculate everything computable we program inside.

Figure 2 illustrates the value linkage in a smart contract. Entity (government owned agency) records the value of the procurement and issue equivalent token. The token with corresponding subcontract value is given to the tender winner, and then to its subcontractors. We can trace the portion of a contract and such division will be encrypted into blockchain as a recognizer for future perusal.

Decentralized Autonomous Organizations

Selected entities are decentralized autonomous organizations (DAO), and are allowed to issue tokens when new tender is opened. These entities are full nodes, keeping complete ledgers and maintaining the hash order according to consensus algorithm. All participants in this collaborative system are known by each other. These DAOs are normally malicious-free unless being hacked. The prevention of hacking has beyond the discussion of this research, or even in current bitcoin-like systems. However, the decentralized architecture provides abundant redundancy to maintain the operation. Also, the backup service is basically remotely kept with high availability.

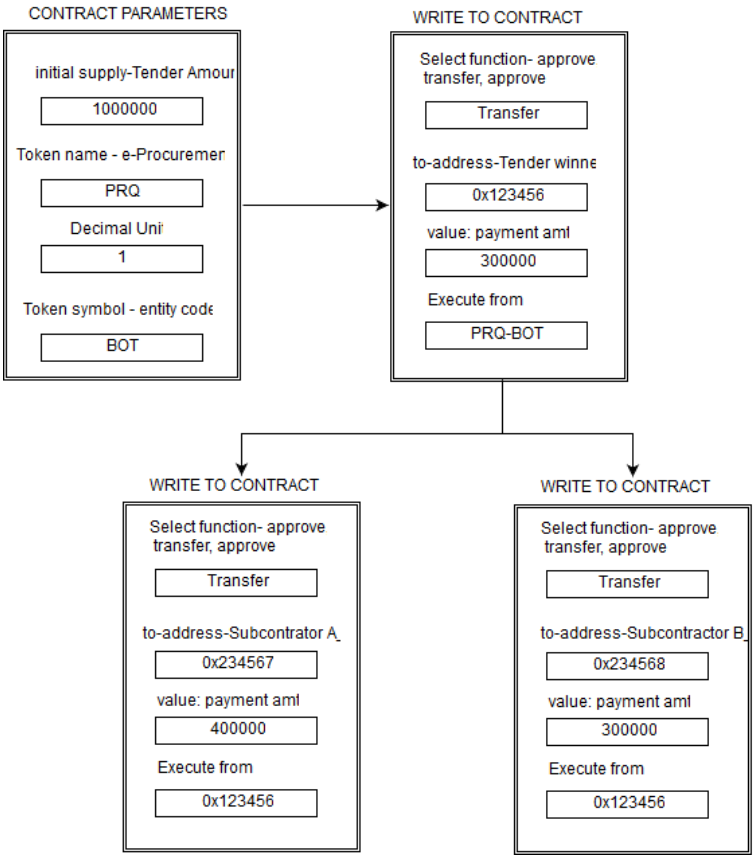

Figure 2: Smart Contract of Tenders

Byzantine Agreement Problem

This design is not Data-Race-Free as the fork tree may exist given a probability. In fact, the sibling chain is encouraged to develop to contribute the security of the main chain. The fork problem will be solved by the descendants adopting longer chain priority principle. Hence, even confronting frequent concurrent computation, the consistency can be soon reached autonomously if two thirds of members adopts (Lamport *et al*., 1982). In this agreement, new TrustBlock can be added to the longest seeable chain arbitrarily, which means that similar types of transaction could happen at the same time by any members.

Figure 3 illustrates the Merkel tree of the TrustChain. Tender winner (c) has subcontractors (a) and (b). Blockchain of execution is hashed along path of a-b-c to $H(EC_1)$. For Entity Case 1, a complete block contains also the other competitors (d) and (e), though they did not get the contract. For entity (A), it keeps all blocks of historical tenders. For the entire TrustChain, all registered entities (A, B, ..) eventually update to the root hash.

These entities are also permissioned full nodes in charge of POW. They are informative of all transactions for qualified suppliers, the tender participants of every tender and contract implementation portion. When necessary, registered entities can be the leaf node of TrustChain root to link the data in external database. All the other important data of a tender including Case Ref no, Description, Estimated Cost, Tender Category, Tender Suppliers Detail, Supplier performance can be traced back according to key value chained in block hash. The TrustChain would be a decentralized ledger extending to management performance, legal compliance, public donations and management team personal credit, by following the implementation above.

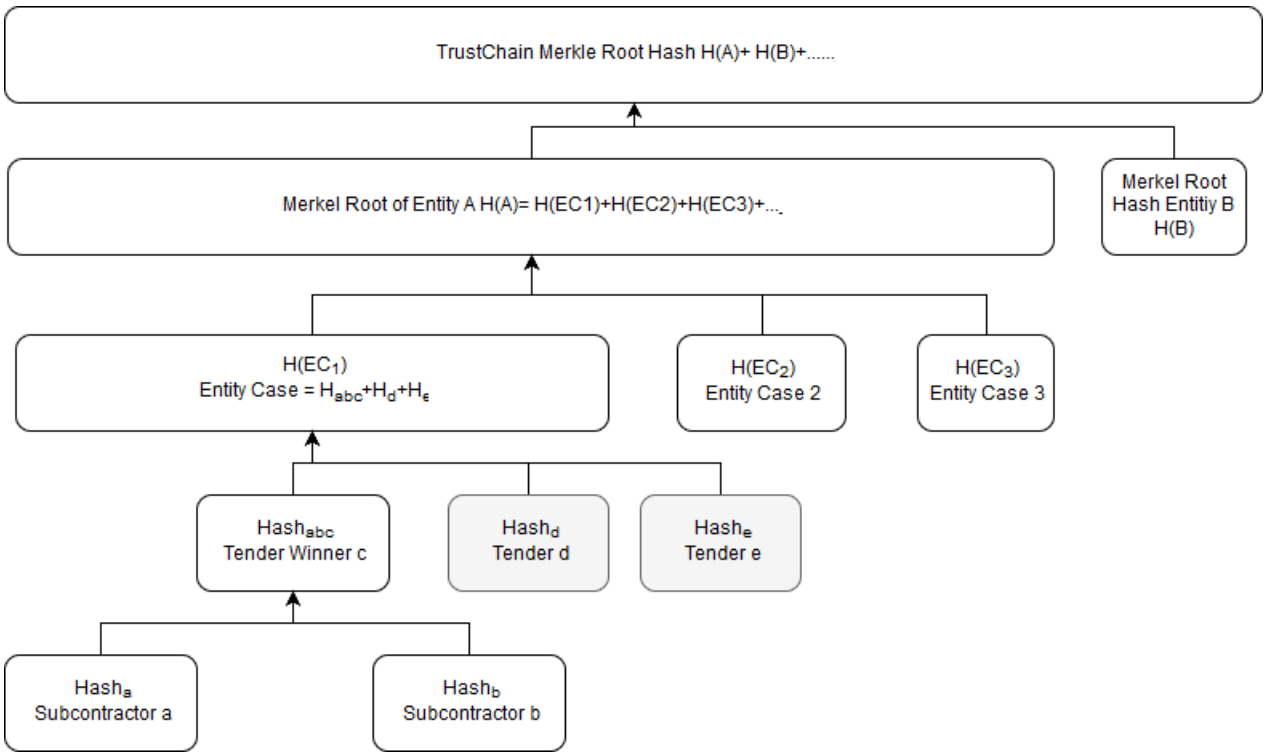

Figure 3: Merkel tree of TrustChain

CONCLUSION

Accompanying blooming Fintech, the Regtech has come to the mind of all governments, practitioners and researchers. Among the application of them, the blockchain or the distributed ledger technology have won great deal of attention. In the paper, we represent a brand new idea of creating the corporate credit network on blockchain-based smart contract that could be stacked up to higher roots to tax payment, charity donation, court sentences, dispute involvement, or owned patent, etc., and eventually complete a united TrustChain of organizations.

REFERENCES

[1] Department of Commerce of the Ministry of Economic (2017). Retrieved from http://gcis.nat.gov.tw/mainNew/English/index.jsp (1 Nov. 2017).
[2] Ethereum Foundation (2017). Retrieved from https://www.ethereum.org/ (1 Nov. 2017).
[3] Solidity (2017). Retrieved from https://solidity.readthedocs.io/en/develop/ (1 Nov. 2017).
[4] Kerikmäe, T., & Rull, A. (Eds.) (2016). *The Future of Law and Etechnologies*. Switzerland: Springer International Publishing.
[5] Lamport, L., Shostak, R. & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*, 382-401.
[6] Szabo, N. (1997). Formalizing and securing relationships on public networks', *First Monday*, Vol. 2, pp. 2-3.
[7] Wang, R. (2015). *Sheethub (Open Data Statistics)*. available at: https://sheethub.com/ (1 Nov. 2015).

APPENDIX

Settings of Experiment Environment:

- Geth https://geth.ethereum.org/

```
D:\geth
λ geth version
Geth
Version: 1.6.7-stable
Git Commit: ab5646c532292b51e319f290afccf6a44f874372
Architecture: amd64
Protocol Versions: [63 62]
Network Id: 1
Go Version: go1.8.3
Operating System: windows
```

- Blockchain language: JavaScript
- Ethereum Wallet: Mist https://github.com/ethereum/mist
- Smart Contract Standard: ERC 20
- Smart Contract compiler: Solidity http://solidity.readthedocs.io/en/latest/index.html