Eliminating capital projects cost flow fraud using distributed ledger technology (DLT)[1]

Dr Lalamani Budeli

Abstract

It is estimated that organizations loss 5% of their annual revenue to capital project cost flow fraud performed by employee, consultants, auditors, and suppliers. During project execution, completion certificates are used to trigger payments of suppliers' consultants and contractors signed by internal parties involved in a specific work package completed. A completion certificate is a document that is awarded, after the inspection of a project task (work package), stating that it has been constructed according to the approved plan and that it meets all the necessary standards set by the organization, authority, or municipal corporation. Cost flow is commonly defined as an internal flow of money within the organization until the money is paid out of the organization which is referred to as cash flow. In most organization capital projects, cost flow happens daily while cash flow happened after 30 days.

In this article, Distributed ledger technology (DLT) was compared to traditional governance tools aimed to prevent cost flow fraud to determine the best method that can be used in capital projects. The result indicates that distributed ledger technologies (DLT) outperformed other traditional methods and governance requirements put in place by the organization to combat cost flow fraud. Its advantage is the transparency of payments to stakeholders directly involved with the task and activities performed other than all other methods centralized to a project coordinator. This will prevent all completion certificates that are fraudulent not being processed by finance as due diligence is performed by technical teams involved in the specific work package. This approach will assist project organizations to save billions of money per annum.

Keywords: Capital project, Cost flow Fraud, Distributed ledger technology (DLT)

Introduction

Project cost fraud and corruption especially in the procurement systems is one of the major contributors of annual losses for both private companies and governments throughout the world. Stolfo et al (2000:130) said that this fraud is mostly routed to project monitoring and control where progress misrepresentations are made to sign the work package completion certificate which triggers cash flow to the organization who performed the task. Bach et al (2020:81) indicated that this differs significantly from one country to another as it is also dependent on contract type, culture, religion, societal norms, and values. Donegan et al (2017:170) alleged that When project owners, both in the public and private sector, fail to impose the right policies and procedures to deter fraud on their projects, they are indirectly

[1] How to cite this work: Budeli, L. (2021). Eliminating capital projects cost flow fraud using distributed ledger technology (DLT), *PM World Journal*, Vol. X, Issue VI, June.

encouraging those involved in their projects to commit actions that would lead to project fraud. Van Eenennaam et al (2021:92) whispered that these actions would increase the chances of project failure because they will increase the project cost, delaying the project completion, reducing the project quality, failing to meet stakeholders' objectives among others. Hu et al (2019:1140) specified that, while cost management is viewed as a continuous process, the function is normally split into four steps which are resource planning, estimation, budgeting, and control.

Literature review

Howell et all (2019:23) held that the DLT courses of action can be planned in various manners and can uphold a few or all pieces of an exchange stream. Romero (2018:18) whispered that such game plans commonly include a few key specialized plan ideas that indicate the data to be kept on the record and how the record is to be refreshed.

- Maintaining Ledger information - Records keep up either a past filled with all exchanges or a bunch of records adjusts. In payment, clearing and settlement use cases, a dispersed record is utilized to record possession or equilibriums of computerized resources or advanced portrayals of actual resources. Distributed ledger may act as a central repository for financial contracts by retaining the terms of an actual contract or a copy of it. Some DLT arrangements go a step further and allow for "automated contract tools" which permit users to include self-executing code on the ledger to automate the fulfilment of contract terms. Examples include the execution of interest and principal payments on certain dates, collection or distribution of funds based on certain events occurring, or automatic termination of contracts based on agreed-upon terms. This type of functionality is often referred to by the industry as a "smart contract. Bouras (2020:480)

- Ledger update - An eminent property of DLT is the conveyance of duties regarding refreshing the record by different hubs. These hubs can be conveyed across various destinations, foundations or even purviews, as talked about later. all the nodes are connected and have their identical copy of the ledger and changes to the ledger can be reflected in all copies within a certain period (latency).

- Payment consensus validation - To refresh a synchronized disseminated record, a game plan ordinarily utilizes various conventions for correspondence among hubs and for working with agreement among hubs about the present status of the record just as its chronicled record. Cryptographic tools, such as public-key cryptography play an important role in DLT by identifying and authenticating approved participants, confirming data records, and facilitating consensus on ledger updates. Participants proposing changes to the ledger, authenticate themselves by providing their cryptographic digital signatures for the proposed change. Validators will use cryptographic tools to verify whether the participant has the proper credentials to do so. The consensus mechanism is the process by which the nodes in a network agree on a common state of the ledger.

> This process typically relies on cryptographic tools, a set of rules or procedures reflected in the protocol, and either economic incentives which generally involve validation and agreement on ledger updates. Nodes in the network may play a variety of technical roles as the system administrator, Validator, auditor, asset issuer, and Proposer. Chapman (2017:59)

DLT for capital project milestone payment, clearing, and settlement activities can be designed in several ways and perform different functions. To highlight how the concepts of distributed node, ledger, and consensus could be used in a payment transaction.

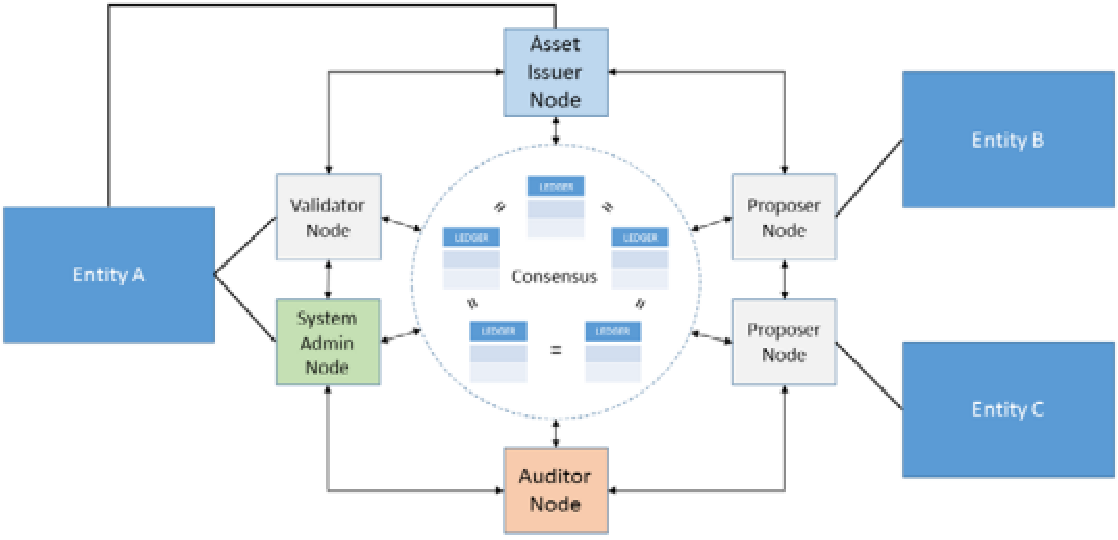

Figure 1 Capital project process flow of a DLT-based payment system

Shabsigh, et al (2020:45) said that assigning particular roles to a broad range of entities and their nodes may introduce other important issues. if only certain nodes are delegated to achieve consensus, it may be easier (and faster) to reach consensus on the state of the ledger; however, it may also be easier for any one of these nodes to compromise the integrity of the ledger. Increasing the number of nodes may improve the overall resilience of the network but it may also lengthen latency. DLT arrangements characterized by a larger number of distributed roles may raise important questions related to governance, settlement, and operational risk management.

Research method

The learning task here is quite straightforward. Given a set of "labeled transactions", T = {tI = < f1,.....,fn>, compute a model or classifier, C, by some learning algorithm L, that predicts from the features < f1,...,fn-1> the target class label fn, "fraud" or "legitimate". Hence, C = L(T)   where L is a learning algorithm. Each element t eT is a vector of features, where we denote f1 as the "transaction amount" (*tranamt*), and fn as the target class label, denoted fraud t = 0 (legitimate transaction) or t = 1 (a fraudulent transaction). Given a "new unseen" transaction, x, with unknown class label, we compute fn (x) = C(x). C serves as our fraud detector. WP represents the work package. We define for a set of transactions S, a fixed overhead amount, and a fraud detector (or classifier) C:

$$WP\ cummulative\ cost\ (C, S, overhead) = \sum_{teS}^{n} WP\ Cost\ C, t\ overhead$$

And

$$\text{Average WP cost (C,S,overhead)} = \frac{cummulative\ WP\ cost\ (C,S,overhead)}{n}$$

Since it takes time and personnel to investigate a potentially fraudulent transaction, a fixed overhead value is incurred for each investigation. That is, if the amount of a transaction is smaller than the overhead, it is not worthwhile to investigate the transaction even if it is suspicious. For example, if it takes ten dollars to investigate a potential loss of one dollar, it is more economical not to investigate. Assuming a fixed overhead, we devised the cost model for each transaction t and classifier C, showed in Table 1. (Recall, F1 (t) = tranamt(t)

Table 1 Cost Model for Transaction

Outcome	**Cost (t, overhead)**	
Miss (False Negative, FN)	Tranamt(t)	
False Alarm (False Positive, FP)	overhead	if tranamt(t) > overhead
	0	if tranamt(t) = < overhead
Hit (True Positive, TP)	overhead	if tranamt(t) > overhead
	Tranamt(t)	if tranamt(t) = < overhead
Normal (True Negative, TN)	0	

In describing our results, we report the maximum savings (or stop loss in bank parlance), as the total rands amount saved from detection under this cost model. The total potential rounds loss for a (test) set of transactions (S) is defined as the total dollar amount of all fraudulent transactions:

$$TotalPotentialLoss(S) = \sum_{te\&fraud=true}^{0} tranamt\ (t)$$

The important lesson here is that the data mining problem is a straightforward cost optimization problem, namely to capture or recover the *TotalPotentialLoss* due to fraud. That is, given a test set of transactions, S, a fraud model C*overhead*, and the *overhead*, the *TotalCostSavings* is defined as:

TotalCostSavings overheadoverhead (S,C overheadoverhead) =TotalPotentialLoss(S,C overhead overhead) – CumulativeCost(S,C overheadoverhead)

Five work packages from five different project were selected for evaluation purposes (case study)

Results

The final stage of our experiments on the credit card data involved the exchange of base classifiers between the two methods.

Table 2 DLT Performance results for the Capital project cost flow fraud detection data set.

Type of Classification Model	Size	Accuracy	TP - FP	Savings
COTS scoring system from Chase	1	97.2%	0.689	R 9.5 M
Best base classifier over one subset	1	95.23%	0.614	R 8.4 M
Best base classifier over entire set	1	98.9%	0.794	R 12.5 M
Meta-classifier	50	99.2%	0.831	R 15.5 M

Table 3 Traditional methods Performance results for the Capital project cost flow fraud detection data set

Type of Classification Model	Size	Accuracy	TP - FP	Savings
COTS scoring system	1	85.4 %	0.524	R 6.82M
Best base classifier over one subset	1	85.8%	0.614	R 7.68M
Best base classifier over entire set	1	87.7%	0.615	R 7.96M
Meta-classifier	50	88.9%	0.721	R 8.98M

The result shows that using DLT has a high accuracy of detecting and eliminating cost flow fraud which will results in huge cost servings monthly. This will assist the organization to efficiently and effectively manage their limited financial resources while improving capital project cost performance.

Discussion

DLT may profoundly change how project resources are kept up and put away, commitments are released, contracts are upheld, and dangers are overseen. Defenders of the innovation feature its capacity to change monetary administrations and markets by:

(I) lessening intricacy;
(II) Improving start to finish handling velocity and hence the accessibility of resources and assets;
(III) Diminishing the requirement for compromise across numerous record-keeping foundations;
(IV) Expanding straightforwardness and permanence in exchange record keeping;
(V) Improving organization flexibility through disseminated information to the executives; and
(VI) Decreasing operational and monetary risks.

DLT may likewise ensure capital project cost flow straightforwardness if data contained on the record is shared comprehensively with members, specialists, and different partners.

Conclusion

The results showed us that DLT can facilitate a solution to a cost flow fraud problem in capital projects or improve upon existing services or processes. This technology can simplify processes, improve information flows, reduce operational costs, expand access to financial services information and improve financial inclusion in projects. The technology may reduce the need for human involvement through automation, thus increasing the efficiency and accuracy of cost flow management in capital projects.

References

1. Bach, M.P., Dumičić, K., Žmuk, B., Ćurlin, T. and Zoroja, J., 2020. Data mining approach to internal fraud in a project-based organization. *SciKA-Association for Promotion and Dissemination of Scientific Knowledge*, *8*(2), pp.81-101.

2. Bouras, M.A., Lu, Q., Zhang, F., Wan, Y., Zhang, T. and Ning, H., 2020. Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. Sensors, 20(2), p.483.

3. Chapman, J., Garratt, R., Hendry, S., McCormack, A. and McMahon, W., 2017. Project Jasper: Are distributed wholesale payment systems feasible yet. *Financial System*, *59*.

4. Donegan, J., Ganon, M. and Johnson, Z., 2017. Influencers of earnings management fraud: Coercion, project stage, and ethics. *Journal of Managerial Issues*, pp.169-188.

5. Fiergbor, D.D., 2020. Managing Projects Using Forensic Accounting in Detection and Prevention of Fraud in Ghana. *Global Economics Science*, pp.44-49.

6. Howell, B.E., Potgieter, P.H. and Sadowski, B.M., 2019. Governance of blockchain and distributed ledger technology projects. Available at SSRN 3365519.

7. Hu, H., Dou, B. and Wang, A., 2019. Corporate Social Responsibility Information Disclosure and Corporate Fraud—"Risk Reduction" Effect or "Window Dressing" Effect?. *Sustainability*, *11*(4), p.1141.

8. Stolfo, S.J., Fan, W., Lee, W., Prodromidis, A. and Chan, P.K., 2000, January. Cost-based modeling for fraud and intrusion detection: Results from the JAM project. In Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00 (Vol. 2, pp. 130-144). IEEE.

9. Shabsigh, M.G., Khiaonarong, M.T. and Leinonen, M.H., 2020. *Distributed Ledger Technology Experiments in Payments and Settlements*. International Monetary Fund.

10. Romero Ugarte, J.L., 2018. Distributed ledger technology (DLT): introduction. *Banco de Espana Article*, *19*, p.18.

11. Van Eenennaam, F. and Michel, H., 2021. Fraud Governance Case. In *New Living Cases on Corporate Governance* (pp. 91-93). Springer, Cham.

About the Author

Dr Lalamani Budeli

South Africa

Dr Lalamani Budeli obtained his degree in Electrical Engineering at the Vaal University (VUT), BSc honors in Engineering Technology Management at University of Pretoria (UP), Master in engineering development and Management at North West University (NWU), Master of business administration at Regent Business School (RBS) and a Doctor of Philosophy in Engineering Development and Management at North West University (NWU), Potchefstroom, South Africa. Currently, he is a managing director of BLIT, an engineering, research, and project management company based in South Africa.

His research interests include project portfolio management, agile project management, plant life cycle management, advanced systems analytics, project early warning system, and the use of artificial intelligence in project management. Currently, he is spending most of the time on research that is looking at the development of system and application that uses the latest technology like block chain, internet of things (IoT), Big data, and artificial intelligence. Lalamani Budeli can be contacted at budelil@blit.co.za.

To view other works by Dr. Budeli, visit his author showcase in the PM World Library at https://pmworldlibrary.net/authors/lalamani-budeli/