9-2022

Using Blockchain to Track DoD Funding and Auditing

Prithvi Prasanna

THE USE OF BLOCKCHAIN TO TRACK DOD FUNDING AND AUDITING

THESIS

Prithvi Prasanna, Contractor

AFIT-ENV-MS-22-S-161

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

THE USE OF BLOCKCHAIN TO TRACK DOD FUNDING AND AUDITING

THESIS

Presented to the Faculty

Department of Systems Engineering and Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Systems Engineering

Prithvi Prasanna, BS
Contractor, KBR

August 2022

THE USE OF BLOCKCHAIN TO TRACK DOD FUNDING AND AUDITING

Prithvi Prasanna
Contractor, KBR

Committee Membership:

Lieutenant Colonel Warren J. Connell, PhD
Chair

David R. Jacques, PhD
Member

Mark G. Reith, PhD
Member

Abstract

The Department of Defense (DoD) currently faces a significant problem when it comes to auditing and tracking financial transactions. The DoD has failed every audit since 2017 although it is gradually improving its auditable rating year after year. Concurrently, Blockchain is an emerging technology that has typically been used for cryptocurrencies but has slowly been adapted by private enterprises for their auditing and invoicing problems. This study investigates the value proposition of blockchain technology to improve DoD financial tracking and auditing. To test the hypothesis that blockchain is the optimal option for the DoD, this paper employs an industry blockchain adoption flowchart, requirements matrix for financial regulations and audit weaknesses, and a rigorous benchmark comparison chart between the current financial system and well-established private company's blockchain (which DoD could replicate). The results of the flowchart and matrix demonstrate that Permissioned Private Blockchain can track government transactions in instances where contracts between a government agency and contractor could be condensed into variables and formulas. The outcome of the comparison shows that a DoD replicated blockchain system would excel at Latency, Error Rate, Time, but not Cost Metrics when compared to other established DoD financial accounting systems.

Acknowledgements

I would like to express my sincere appreciation to my faculty advisor, Lt Col Warren Connell, for his guidance and support throughout the course of this thesis effort. A great thank you goes to all the faculty during my two years in the Systems Engineering and Management program at AFIT.

Prithvi Prasanna

Table of Contents

ABSTRACT ..... **V**

ACKNOWLEDGEMENTS ..... **VI**

TABLE OF CONTENTS ..... **VII**

I. INTRODUCTION **1**

BACKGROUND 1
PROBLEM STATEMENT 2
RESEARCH OBJECTIVES 3
INVESTIGATIVE QUESTIONS 3
METHODOLOGY 4
ASSUMPTIONS/LIMITATIONS 5
IMPLICATIONS OR EXPECTED CONTRIBUTIONS 5
PREVIEW 5

II. LITERATURE REVIEW **7**

CHAPTER OVERVIEW 7
BLOCKCHAIN BASICS 7
TYPES OF BLOCKCHAIN 9
ADVANCED BLOCKCHAIN TOPICS 11
SYSTEM ARCHITECTURE OF PERMISSIONED BLOCKCHAIN 15
CURRENT DOD SYSTEM 25
Army Financial Process *27*
United States Standard General Ledger (USSGL) *33*
Digital Dollar *35*
REAL-WORLD BLOCKCHAIN IMPLEMENTATION 35
SUMMARY 42

III. METHODOLOGY **43**

CHAPTER OVERVIEW 43
TEN STEP BLOCKCHAIN DECISION FLOWCHART 43
REGULATIONS AND WEAKNESSES REQUIREMENTS 47
Regulations Requirements *47*
Four Weaknesses in Information Technology *49*
Requirements Matrix *51*
PERFORMANCE METRICS 52
SUMMARY 53

IV. ANALYSIS AND RESULTS 54

CHAPTER OVERVIEW 54
10-STEP BLOCKCHAIN DECISION ANALYSIS 54
First Decision *54*
Second Decision *55*
Third Decision *55*
Fourth Decision *56*
Fifth Decision *59*
Sixth Decision *60*
Seventh Decision *60*
Eighth Decision *61*
Ninth Decision *61*
Tenth Decision *62*
REGULATIONS AND WEAKNESSES REQUIREMENTS ANALYSIS 64
Addressing Each Requirement *65*
Requirements Matrix Summary *71*
PERFORMANCE METRICS ANALYSIS 71
Cost Analysis *71*
Time Analysis *74*
Throughput Analysis *77*
Benchmark Analysis *79*
DOD IMPLEMENTED PERMISSIONED PRIVATE BLOCKCHAIN ..... **ERROR! BOOKMARK NOT DEFINED.**
SUMMARY 87

V. CONCLUSIONS AND RECOMMENDATIONS 89

INTRODUCTION OF RESEARCH 89
SUMMARY OF RESEARCH QUESTIONS 89
SUMMARY OF RESEARCH ANSWERS 89
What are the drawbacks of the current DoD financial systems? *89*
Does blockchain meet all requirements and remediate current drawbacks? *90*
What are DoD financial regulations and current practices? *90*
What type of blockchain are most appropriate for current DoD practices? And why? *91*
What type of transactions within the DoD can blockchain optimize? *92*
What current systems/policies would need to change to accommodate a blockchain solution? *92*
What are some challenges the DoD could face if they were to transition to a blockchain based solution? *93*
What metrics can be used to compare DoD financial systems with a possible blockchain solution *93*

Study Limitations 94
Recommendations for Action (if applicable) 94
Simplify DOD contracts *94*
Decide between COTS or In-House Implementation *95*
Recommendations for Future Research 95
Summary or Significance of Research 95
BIBLIOGRAPHY 97

I. Introduction

Background

The total spending for the United States Military is 773 billion dollars which comes out to 11% of the total 7 trillion dollars of Federal Spending [1]. Approximately 752 billion dollars of the 773 billion dollars is discretionary, which means each year a large portion of the military budget is determined by last year's transactions. With all these funds changing hands, the US Government self-audits to make sure that the funds are in accordance with established regulations. In addition, the transaction data can help create a budget for the following year.

Auditing is the act of systematically verifying all logged and unlogged financial information. Auditors require documentation for all transactions that happen within an organization to make an accurate assessment about the audit. Keeping records for the largest federal agency in the United States is a difficult task. David Norquist, Pentagon's comptroller, said "The Pentagon failed its comprehensive audit in fiscal 2020, the third year it has failed since the first audit was conducted in 2018, reflecting system and accounting problems across its vast bureaucracy that could persist until 2027" at the earliest [2]. The comptroller also said that no large-scale fraud is at fault; however, "the Army, Navy, Air Force, Marines, Special Operations, and the Transportation Command all received failing grades [3]". In the fiscal year of 2021, the DoD was unable to bring forth sufficient evidence for auditors to make an opinion, or in auditing terms, a disclaimer of opinion [4].

Blockchain technology is a distributed ledger which means everyone participating has a copy of the transactions. If every participant has a copy of the transactions, then the occurrence of malice or a mistake with a particular user's transaction can promptly be corrected from

everyone's ledger. A properly implemented blockchain's strength is that it's immutable, which means that it is nearly impossible for any sole person to manipulate data on the distributed ledger. Blockchain can be completely public, where the ledger is completely open for anyone to join. However, blockchain can also be private where only approved personnel can be added to the ledger to read or add to it. Private blockchains are generally used between organizations and don't interact with the general public at all. For example, Walmart Canada has been using private blockchain to keep track of shipping logistics with trucking companies. Walmart Canada experienced a significant drop in invoice disputes and they claimed that it has increased their payment speed and accuracy [5]. In November 2021, the United States Department of Veterans Affairs showed interest in blockchain solutions for specific areas [6]. This displays United States Government's general intrigue into this new technology.

Problem Statement

In the fiscal year 2021 report, auditors issued a disclaimer of opinion because the "DoD reporting entities that account for the majority of the DoD's balances continued to have unresolved accounting issues and material weaknesses that prevented them from providing sufficient and appropriate evidence to support the balances presented on their respective financial statements [4]". A detailed review of the material weakness and accounting issues reveals that the seven problem areas identified in the FY2020 audit report persists in the FY2021 audit report. For the scope of this thesis, the paper will look at the Information Technology problem area since the audits recommend the DoD "maintains effective controls to ensure that data flows between systems correctly and is accurately reported on the DoD's financial statements [4]". There are four key weaknesses in the Information Technology Area: Configuration and Security

Management, Access Control, Segregation of Duties and Legacy Systems [4]. Some ongoing solutions to expedite the remediation process include software consolidation and removing legacy applications. However, the Pentagon's comptroller expects that none of these solutions will be done prior to 2027 [2]. With the advance of blockchain technology, this thesis will study the extent to which blockchain technology can be used by the DoD to fix weaknesses found in the most recent report of audits.

Research Objectives

The main objective of this thesis is to determine the extent to which blockchain technology can be employed by the DoD to remediate weakness found in the 2021 Fiscal Year Audit Report.

Investigative Questions

This research will discuss the efficacy of blockchain as a possible solution to the Information Technology weakness discussed in the FY2021 Audit. This thesis will address three major questions and a few sub-questions.

- What are the drawbacks of the current DoD financial systems?
    - To what extent does blockchain meet requirements and fix current drawbacks?
- What are DoD financial regulations and current practices?
    - What type of blockchain are most appropriate for current DoD practices? And why?
    - What type of blockchain transactions is suitable for the DoD?
    - What current systems/policies would need to change to accommodate a blockchain solution?

- What are some challenges the DoD could face if they were to transition to a blockchain based solution?
    - What metrics can be used to compare current DoD financial systems with a possible blockchain application

Methodology

This thesis will apply the decision tree from the "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies" research paper to find out if blockchain is a viable fit for an organization. From the conclusion of the flowchart, we will have a better idea whether or not the DoD financial process, as a whole, is a good candidate for blockchain integration. If one gets far enough in the flowchart, they can determine which type of blockchain would be logical for the DoD financial process.

According to the Government Accountability Office (GAO), any new federal financial system migration plan should also address "Federal Financial Management Improvement Act of 1996 (FFMIA) requirements, applicable federal accounting standards, and the United States Standard General Ledger (USSGL) at the transaction level [7]". So, any new proposal to the already existing financial system should follow the same regulations as the original system. This research will use the definitions of the four financial system weaknesses and the federal accounting regulations as requirements to test blockchain validity.

The final step of the methodology will cover the performance aspects of blockchain. This part will include three different financial (two from the DoD and one Real-World Blockchain Implementation.). This section will also include the key metrics that may be used for

comparison. The comparison of two vastly different systems (DoD and blockchain systems) is not within the scope of this paper and should be saved for future works.

Assumptions/Limitations

The GAO, in their report, has outlined many ways to rectify the auditing situation with the DOD, but for the scope of this paper, we will only be looking at the Information Technology aspect of the audit weaknesses. One limitation of this thesis was availability of reliable data. This can be difficult to access data such as classified data or not available to the general public. Another way data can be difficult to access is when private companies do not share all details of their intellectual properties because of the fear of copycats in the private industry. Private companies do not need to report of their failures and only highlight their success. They may even tend to exaggerate data to win the public's interest. Finally, there is no one best way to compare two systems that differ so greatly. For this reason, we will not be comparing metrics between the systems and should be part of future works.

Implications or Expected Contributions

The purpose of this thesis is to educate the reader to the fundamentals and processes of blockchain. Secondly, this thesis can be used to convince decision makers to assess blockchain solutions. Thirdly, this paper aims to push readers to weigh the pros and cons between COTS and in-house blockchain development.

Preview

The second chapter, Literature Review, will focus on the fundamentals of blockchain technology and how the DoD operates the financial side. Methodology in the third chapter will cover the ways this paper will tackle the research objective. This includes a flowchart made for

organizations thinking about incorporating blockchain, a requirements checkbox seeing if blockchain can abide by the same rules and regulations as the other DoD systems, and finally performance metrics between the DoD systems to the real-world implementation of blockchain. The Analysis chapter systematically addresses all the ways mentioned in the methodology portion with figures, diagrams, and SysML modeling as proof. The Conclusion is the final chapter that answers each aspect of the investigative questions using the analysis as evidence and send the reader off with a call to action and a need for future works in this space.

II. Literature Review

Chapter Overview

The purpose of this chapter is to provide the reader with the base knowledge of blockchain and the current financial DoD process. For the blockchain portion, the reader will get comfortable with its attributes, different types, and end-to-end operations. As for the DoD process part, the paper shall provide examples of hierarchy and flowchart for financial activities.

Blockchain Basics

Blockchain is a distributed peer-to-peer network that has two main qualities: immutability and decentralization. Blockchains are built utilizing a SHA256 cryptographic hash algorithm. Whatever block of plaintext is used, from one word to a whole Shakespearean play, it should return a hash of a fixed length (in this case, 256 bits long). Additionally, the same input should return the same hash output every time. Even the smallest changes in the input text will result in a drastic change in the output, so attackers will not be able to see a pattern emerge. Ideally, the output hashes to be collision-free. Being a collision-free algorithm requires two different input texts not having the same output hash, which avoids confusion. SHA256 has a chance, albeit incredibly small probability, of two hashes accidentally colliding. After trying to brute-force the output hash, it should be difficult to deduce the original input texts. Brute forcing is using trial-and-error processes repeatedly to get past encryption. Lastly, it should be easy to scramble input text, but nearly impossible to reverse. The other reason it is immutable is that blockchain uses public key (asymmetric) cryptography. It is considered asymmetric, because

there are two keys, one used for encrypting while the other is used for decrypting. If blockchain uses symmetric cryptography then all a hacker would need is one key meant for encrypting and decrypting. In this cryptography, "each receiver needs a private key that can be derived from the shared public key" [8]. The asymmetric method allows the private key to be used as proof of ownership between two actors in a blockchain transaction. Finally, there are so many new transactions being added such that it is computationally infeasible to maliciously add a block(s).

Being decentralized means that there is no centralized authority making sure the data transmitted between everyone is correct. Everyone has a copy of the data table and when a new transaction is made, everyone's nodes need to make sure that they have the same data table. This is done using consensus algorithms. For example, a common cryptocurrency, Bitcoin, uses a Proof-of-Work algorithm. Proof-of-Work means that miners are brute-forcing to be the first one to solve a complex math problem. Whoever solves it correctly first adds the new transaction on the data table. For their efforts, miners are compensated per new transaction they add to the blockchain. On the other hand, Proof-of-Stake allows the person that has the most to lose to dictate the data table. A coin-owner offers a portion of their coins as collateral to become a validator. Once a validator, the coin owner will be able to validate any transactions onto the blockchain data table. If the data table the validator puts up is incorrect, then they lose their collateral. The benefits of Proof-of-Stake over Proof-of-Work is that it is more environmentally friendly, as huge mining (high electricity bills) operations are not needed. However, Proof-of-Work is much more decentralized than Proof-of-Stake as anyone with a computer can add blocks to the blockchain instead of a select group of individuals.

Proof-of-Authority is similar to Proof-of Work. Instead of the user staking a coin to add a block (transaction) to the blockchain, the user stakes their reputation or identity. Users will need to be vetted before joining the blockchain as the users can read and write blocks on the blockchain. The vetting process will include confirming their real identity and processing every potential user equally. Once the vetting process is completed the potential user becomes a validator. Since there is a team of individuals bringing validators into the fold, it needs to be addressed that Proof-of-Authority is a semi-decentralized consensus algorithm. Not everyone can become a validator, so that means a central authority is making a decision to make someone a validator. However, the central authority does not need to validate every transaction added on the blockchain, as trust is given to the validators to uphold their duty.

Types of Blockchain

The three major types of blockchain are: permissionless public, permissioned private and hybrid (permissioned public) according to the authors of "Overview of Blockchain Technology" [9]. Permissionless public blockchain is by far the most popular one. Since anyone is free to join and participate in the blockchain network, this makes the blockchain permissionless. As a benefit of this type of distributed ledger, users can read and write blocks on the public ledger. Trust within this type of blockchain is "built between peers in the network because they all have to abide by the established consensus mechanism. [10]". The most famous consensus algorithms for permissionless public blockchains are usually Proof-of-Work and Proof-of-Stake. Blocks (transactions) are added on the blockchain via "mining". Blockchain "miners" solve a series of cryptographic equations to add a transaction to the network. As a reward, miners can earn cryptocurrency. Out of the three types of blockchains, permissionless public blockchain is

hardest to hack as it is fully decentralized. All participants can keep track of transactions and look for any mistakes with the ledger.

Permissioned Private blockchains are usually controlled by a single organization. Within this permissioned blockchain, the central authority can pick who gets to have read/write access. Therefore, someone who wants to be part of the private blockchain must first get permission to join. These vetted individuals need to get further access to have read/write access for a certain blockchain ledger. All other vetted individuals that are not part authorizers for the certain blockchain ledger do not have read/write access to that certain ledger. However, they will be authorized individuals for their own blockchain ledger. Trust does not rely on the public keeping track of all the transactions, instead trust in the private blockchain is given by the central authority. This key difference makes private blockchain semi-decentralized. A common consensus algorithm for Permissioned Private Blockchain is Proof-of-Authority. There is no need for mining, as users are paid (i.e., via salary or business-to-business payment) from the organization that is in control.

Lastly, Permissioned Public blockchain (or Hybrid blockchains) are similar to private blockchain. A central authority from an organization vets potential validators. Vetted individuals may become Authorized Individuals once more screening has been done. Authorized Individuals will have read/write access while vetted individuals will have read access only. The most common place for this type of blockchain is in real estate as everyone should be able to read the price, but only a select few should be changing the price of a home based on economic factors.

Table 1. Difference between the Types of Blockchain

	Permissionless Public	**Permissioned Public**	**Permissioned Private**
Who can read/write transactions?	Everyone has read/write access	Authorized individuals have read/write access. All other vetted individuals have read access	Only Authorized individuals have read/write access. All other vetted individuals have no access
Level of Decentralization	Most Decentralized – Everyone has access therefore very far from a central authority/database	Partially Decentralized – similar to central authority as only vetted individuals have write access, but not vetted individuals can catch mistakes	Least Decentralized – closest to central authority as only vetted individuals have write access
Level of Immutability	Most Immutable - as everyone has access to read each transaction made and make sure it is correct in accordance with the consensus algorithm.	Middle Immutable - as vetted individuals may possibly be bad actors but can be kept in check by the monitoring of everyone else who has read access only.	Least Immutable - only vetted individuals can read and write making it difficult from anyone on the outside to make corrections if fault is found.

After understanding the contrasts that make up different types of blockchain, we must choose which route to take. Everyone in the public having read and write access to DoD transactions would be inadvisable. This means even foreign adversaries could have insight to the records. So, that rules out Permissionless Public blockchain. In the next chapters, we will take a closer look at Permissioned Public and Permissioned Private Blockchain.

Advanced Blockchain Topics

The next aspect of blockchain technology is smart contracts. A smart contract is a self-executing agreement with all participants of the blockchain that is written in programming code.

The smart contract will automatically execute a transaction once the conditions have been met. This type of contract has benefits over a traditional contract. A traditional contract would use pen and paper or verbal confirmation to make an agreement between client and vendor. It is difficult to enforce an agreement without consequences happening to the rule breaker. There are usually legal systems involved that help maintain the sanctity of the contract between the two parties. This is time consuming for both parties.

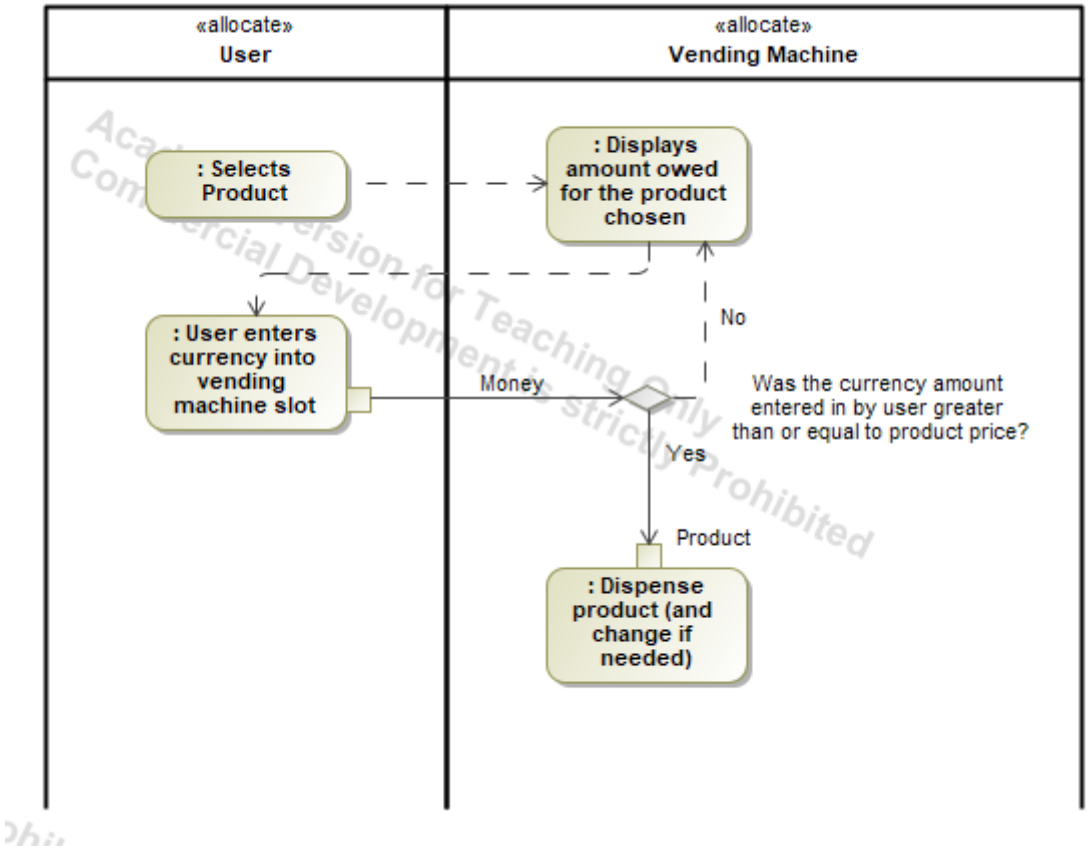


Figure 1. Vending Machine Activity Diagram

An example that is used to explain smart contracts concisely is the vending machine metaphor. As seen in Figure 1, the user of the vending machine selects a product. The vending machine displays the amount the user owes for the product. The user enters the correct amount displayed. The vending machine checks to make sure that the user has entered greater than or equal to the right amount. If the user did not meet the conditions of inputting the correct amount of currency, then the vending machine displays the monetary difference in order for the user to receive the product. Once the verification has passed, the vending machine dispenses the product the user chose.

Both parties can see the smart contract and comb it over for any malintent. This is similar to how people can inspect open-sourced applications. However, in the case of smart contracts, no one can modify them after they have been deployed. This is to make sure that the transactions are fair for both parties at all times as they have already been agreed on earlier. With smart contracts immutable, the problem arises when contracts between parties need further clarification or modification. Unfortunately, once the smart contract has been deployed (and both parties have agreed to it) then there is not much else to do with the current contract besides to "self-destruct" it and start over. "By [upon] calling this self-destruct function, a smart contract can be removed from the blockchain and all the Ethers on the contract will be transferred to a specified address [11]".

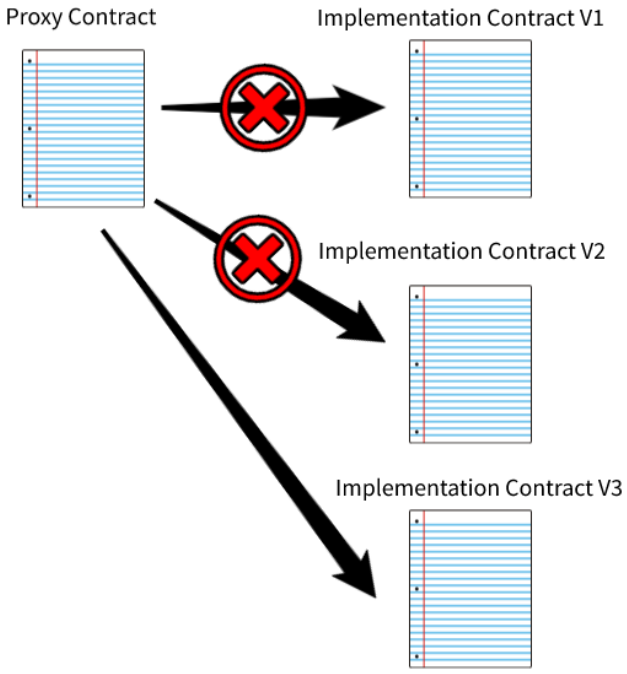


Figure 2. Proxy Contract Diagram

As blockchain knowledge improves, companies such as Open Zeppelin have been able to work with companies/clients to make a Proxy Contract that holds the state of the blockchain. The Proxy Contract points to an Implementation Contract which holds the logic for the whole agreement between company and client. Anytime there needs to be an update made to the logic of the smart contract, developers can change the Proxy Contract pointer to the new Implementation Contract. Users will use the same function name in Proxy Contract to call the function in Implementation Contract. Once a new Implementation Contract is added, the old Implementation Contract will be disregarded and the new one will take its place [12]. Changing the terms of the smart contract should only be used rarely as it breaks trust between all the users of the blockchain if smart contract adjustments are constant. Figure 2 shows the discarding of Implementation Contracts while Proxy Contract stays the same.

System Architecture of Permissioned Blockchain

From the "Blockchain Basics" section of the Literature Review, we determined that a Permissioned Blockchain (either Public or Private) would be ideal for a DoD system by ruling out Permissionless Public Blockchain. The System Architecture of Permissioned Blockchain varies slightly between platforms. The most common Permissioned Blockchain platforms include Ethereum, Quorum, MultiChain, Hyperledger Fabric, and R3 Corda [13]. Since one of this paper's case studies uses Hyperledger Fabric, we will be discussing Hyperledger Fabric when it comes to the architecture of Permissioned Blockchains.

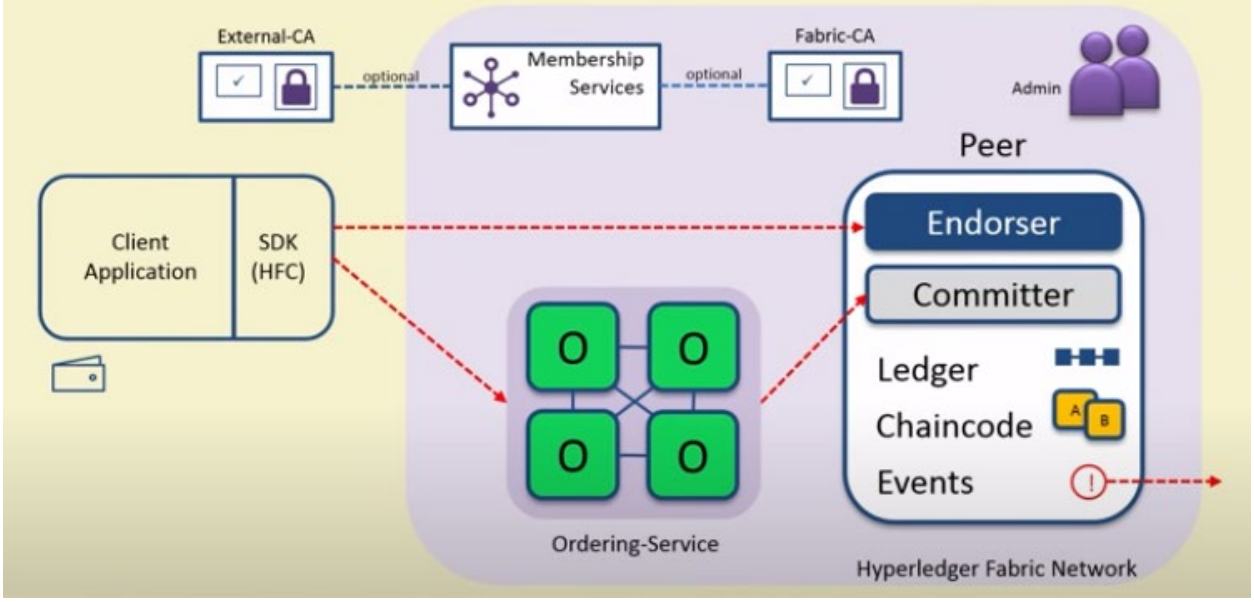
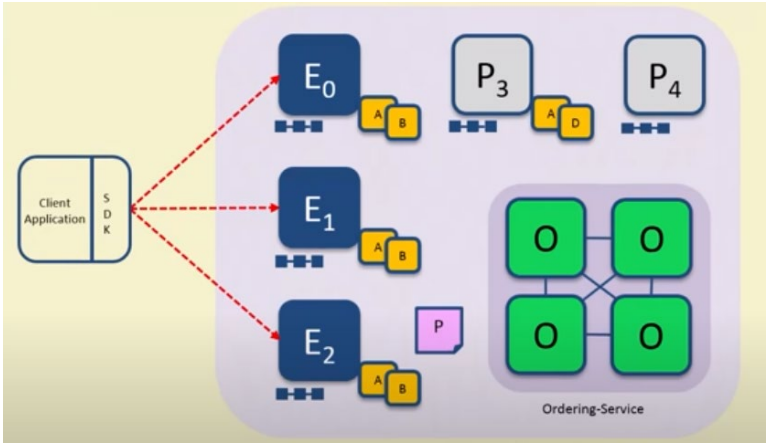


Figure 3. High Level View of Hyperledger Architecture [14]

To understand the basics, we need to understand each entity's role in the whole process. The Membership Service Provider (also known as MSP) "validates, authenticates and allows access to the network" clients by making use of Certificate Authorities [15]. These Certificate Authorities, CA, are similar to the ones used by web browsers. The CA also contains what

privileges a user has with the blockchain, as some users have more responsibilities than others. Organizations can use any MSP they prefer. There is also no limit to how many can be used for security purposes. The Client Application interacts with the Hyperledger Fabric client (HFC) which in turn performs actions on the blockchain.

Everything inside the Hyperledger Fabric Network (Purple Box in Figure 3) is part of the blockchain. An organization can have many Peers and each Peer may have a different role within that organization. The Peer can be an Endorser or a Committer. Peers maintain the ledger and world-state. The world-state is the current "snapshot" of all account balances the Peer node has access to, while the ledger only contains the sender address, receiver address and transaction amount data. They commit transactions and may hold smart contracts (in the case of Hyperledger the smart contract's name is Chaincode). An Endorsing Peer is a committing peer that also has the role of sponsoring a transaction proposal and holds a smart contract (in the case of Hyperledger it is Chaincode) [14]. Since there will be many transaction proposals happening around the same time, the Ordering Service's job is to form a coherent order for all the incoming transactions and transmit all the new orders to all Committing Peers (and Endorsing Peers) within the blockchain. The Ordering Service contains no smart contract. The Ordering Service is "plug-and-play" with whatever consensus algorithm that all parties previously agreed on. Solo is an algorithm where a single node dictates First-In-First-Out order. Another popular algorithm is the Kafka algorithm, which is known to be crash fault tolerant. Kafka assumes that some of the nodes in the Ordering Service may fail; however, even in that failure one can achieve consistent order.



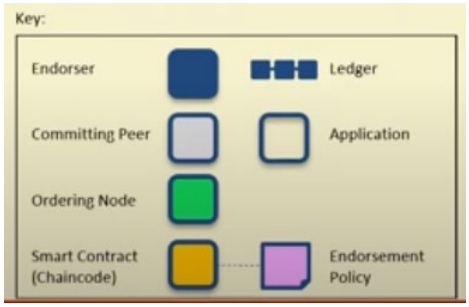


Figure 4. Step 1 for Simple Transaction on Hyperledger Architecture (left) [14]

Figure 5. The key that will be used for all the Simple Transactions on Hyperledger Architecture (right) [14]

The next aspect of understanding the Hyperledger architecture is following the process of a simple transaction that is seen by everyone in the blockchain. As seen in Figure 4, a client will propose a transaction by sending a transaction proposal to endorsing peers. The determination of how many endorsing peers the client sends to is dependent on the endorsement policy. For instance, an endorsement policy will say that "E0, E1, and E2 must endorse" or "Only two of the three between E0, E1, or E2 must endorse"

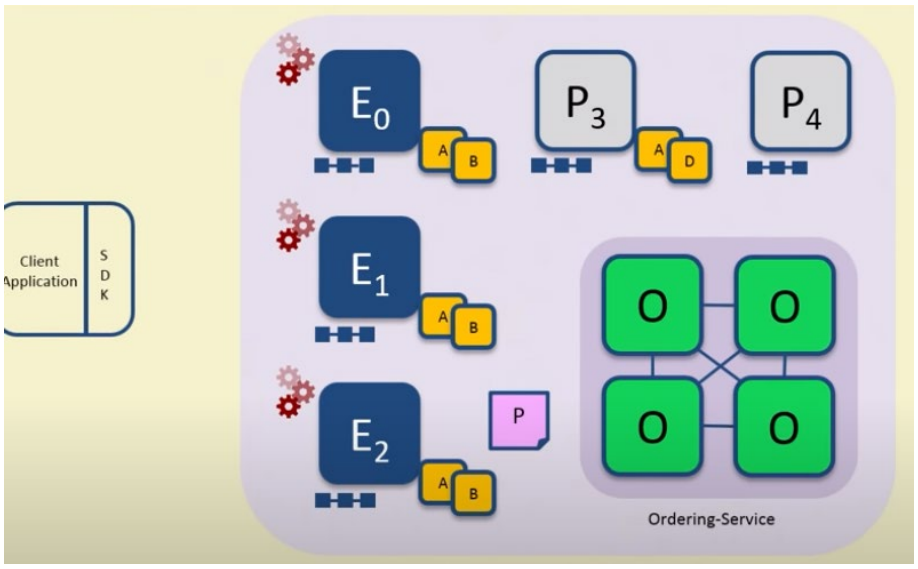


Figure 6. Step 2 for Simple Transaction on Hyperledger Architecture [14]

The second step is to execute the proposed transaction. If we take the first example as the endorsement policy, then E0, E1, and E2 all have to execute the transaction. This does not mean it will update the ledger. As part of the transaction execution each endorsing node captures the set of Read and Written data, called RW sets" [14]. The execution is signed and encrypted.

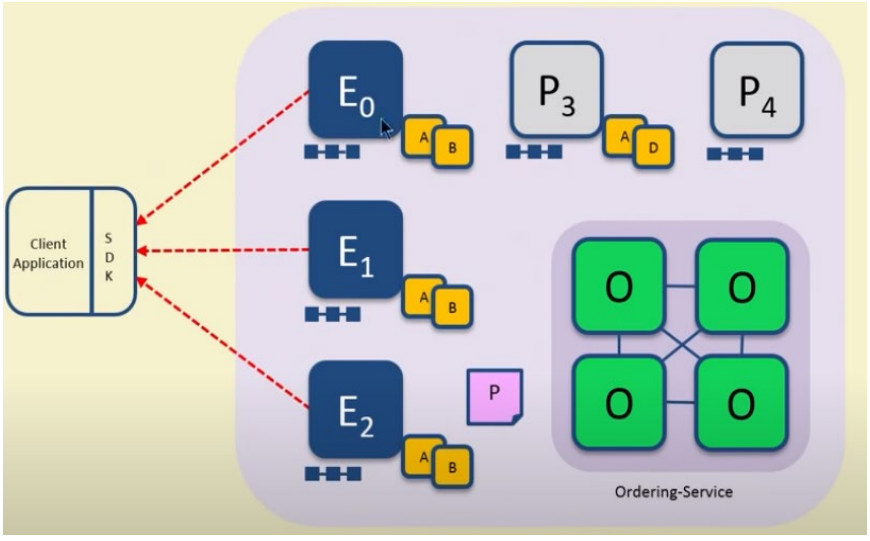


Figure 7. Step 3 for Simple Transaction on Hyperledger Architecture [14]

The RW sets are sent back to the HFC application. However, not all sets are returned at the same time. An RW set contains the signature of the endorsing peer as well as the record version number.

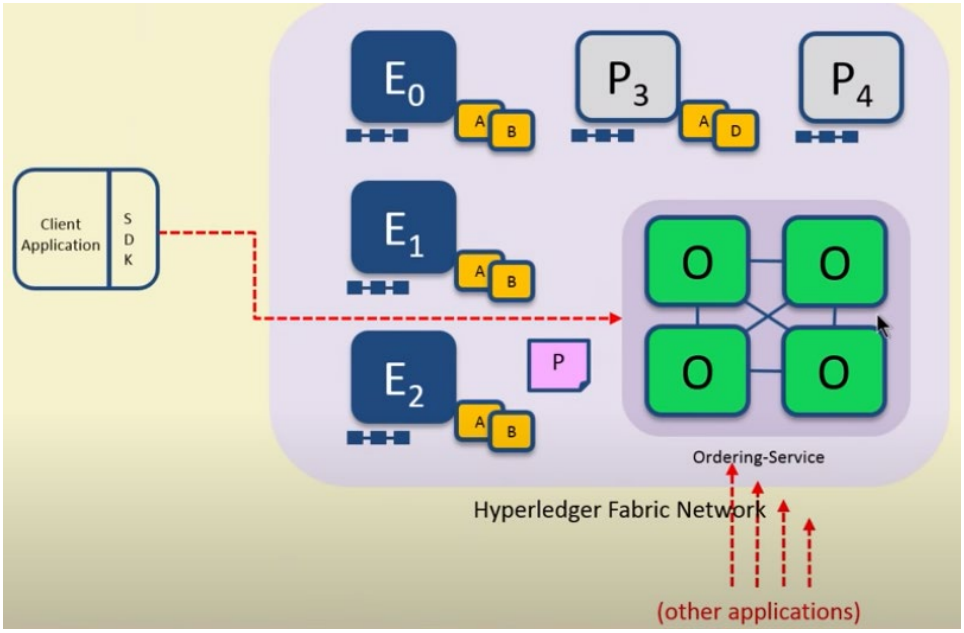


Figure 8. Step 4 for Simple Transaction on Hyperledger Architecture [14]

Step 4 shows the HFC submitting the responses from the previous step to the Ordering Service. There may be many submissions from different clients. As mentioned previously, the Ordering Service's job is to determine the order of the blockchain using whichever consensus protocol all parties have agreed on. For testing purposes, many companies use Solo, but the most common production protocol is Kafka.

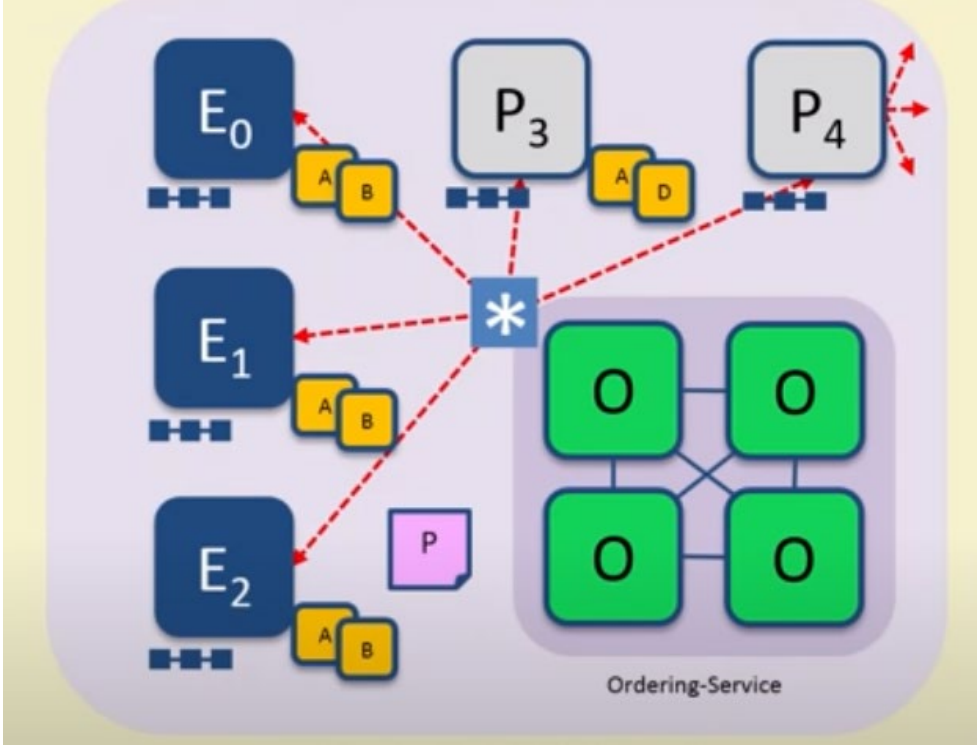


Figure 9. Step 5 for Simple Transaction on Hyperledger Architecture [14]

Step 5 shows the propagation of the block order to all peers (endorsing and committing). In Figure 9, the diagram displays the Ordering Service sending the block order to P4, which can then propagate it to other peers that are not directly connected to the Ordering Service. For instance, P4 can be the one peer that receives the block order from the Ordering Service while the other peers (that ONLY connect to P4) copies the block order from "P4".

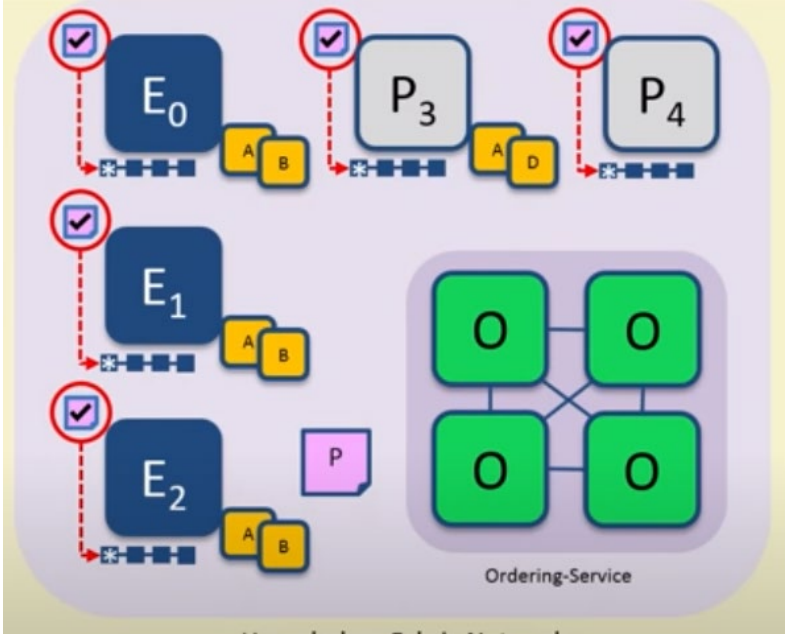


Figure 10. Step 6 for Simple Transaction on Hyperledger Architecture [14]

All Committing Peers (in the case of Figure 10: E0, E1, E2, P3, P4) now validate the newly added block against the endorsement policy. So, if a client wanted to get endorsement from E0, E1, and E2 but only got endorsed by E0 and E1, then the committing peers reject this transaction as invalid. Another check is for the RW sets. For example, the verification would check if two transactions try to update the same data. This can happen if Transaction 1 changes a variable from 100 to 200 while Transaction 2 (which happens after Transaction 1 in accordance with Ordering Service's block order) changes the variable from 100 to 50. Transaction 2 will be denied as a world state as that variable was not up to date. If it was up to date, then Transaction 2's variable would start from 200 and decrease accordingly.

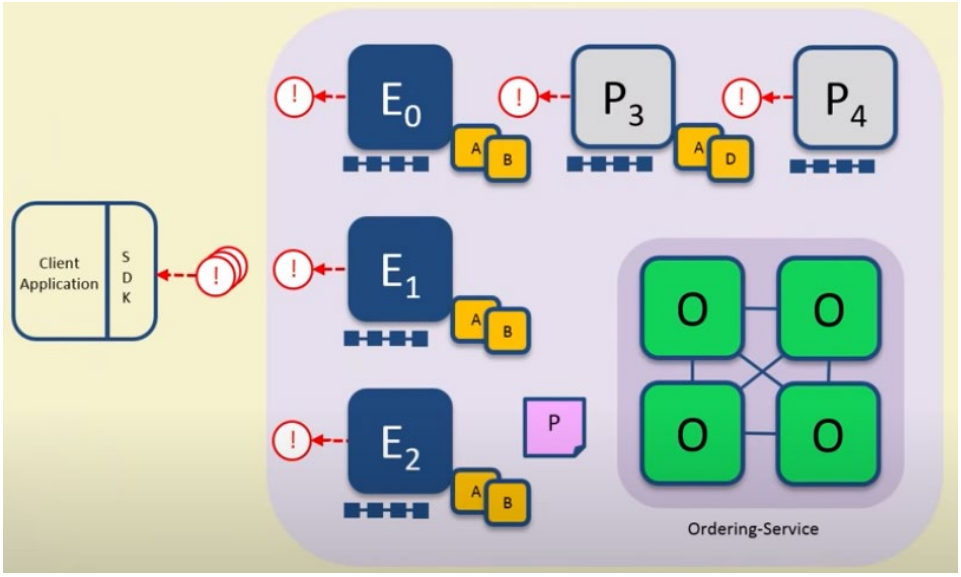


Figure 11. Step 7 for Simple Transaction on Hyperledger Architecture [14]

Finally, all the committing peers will commit the valid transactions by adding the transaction/block to the blockchain. The client is notified about the success or failure of their transaction proposal.

From the previous transaction flow, all clients have access to all of the transactions created up and until that point. This is where the difference between a Permissioned Public and Permissioned Private is shown. Since all nodes in a Public Permissioned can see every transaction, there won't be any need for Channels. With the use of Channels, Hyperledger clients can have their own mini ledger between smaller groups or two clients. Other clients will not even know the existence of these channels [16]. So, all the information above is about Permissioned Public blockchain, while the next part of this section is in reference to Permissioned Private Blockchain.

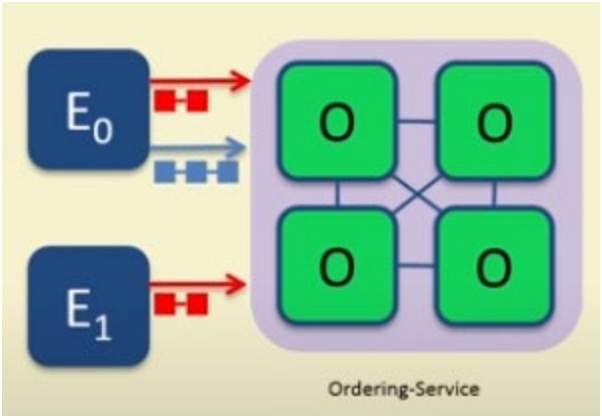


Figure 12. Diagram of Blue and Red Channel within Private Blockchain

In Figure 12, there is a red and blue ledger. E0 and E1 can endorse/commit blocks on the red ledger. However, E0 is the only Peer that can endorse/commit on the blue ledger as E1 does not know of the existence of the blue ledger. Since E0 has access to two different ledgers, the world state (current variables) and Chaincode will be different for each different ledger. Figures 4-10 represent a Single Channel Network.

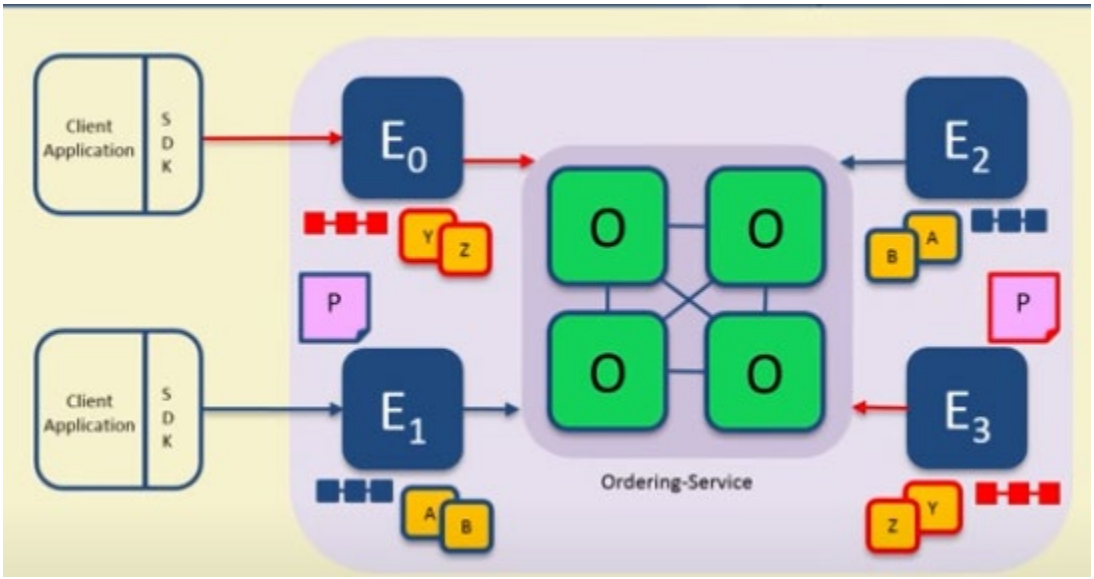


Figure 13. Multi-Chanel Network [16]

In the scenario of Figure 13, E0 and E3 endorse/commit to the red channel while E1 and E2 endorse/commit for the blue channel. The red channel uses the YZ Chaincode and with a Red Endorsement Policy. The blue channel uses the AB Chaincode with a Blue Endorsement Policy. The blue/red colorings show all the distinctions between the Channels. The commonality, in this case, is both Channels use the Ordering Service (also possible to have different Ordering Service for each Channel).

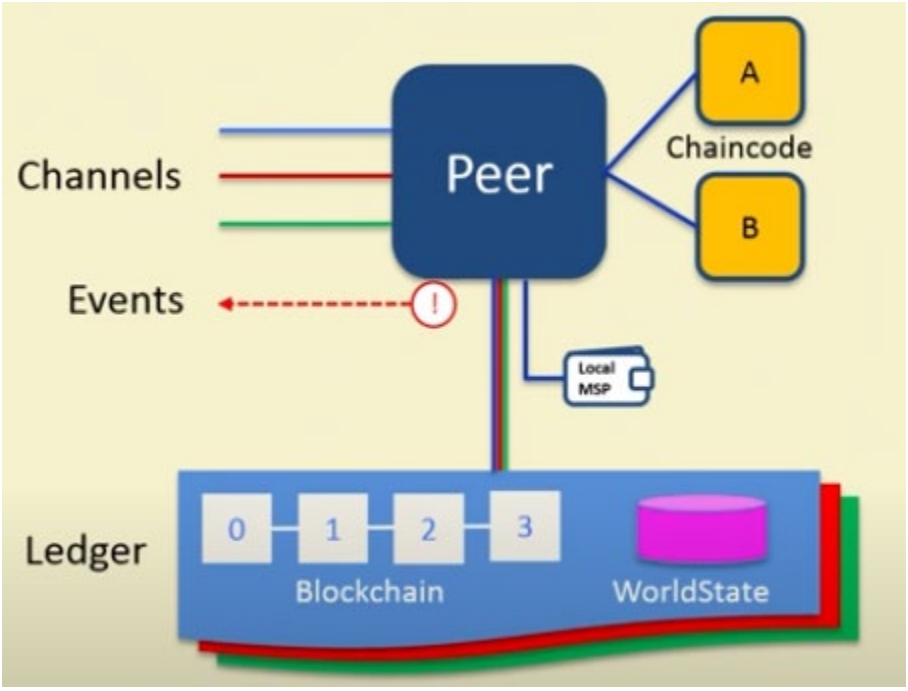


Figure 14. In-Depth look at a Peer Node [16]

As mentioned before each Peer can connect to any number of Channels (Blue, Red, and Green) where each Channel maintains a Ledger (labeled Blockchain and World-State in Figure 14). Chaincode A and B are smart contract processes that are instantiated in separate docker containers, but only one copy of the Chaincode is running at any one point. The Chaincode is shared across the channels so no state is stored in the Chaincode containers and instead stored

within the Ledger. There can be further encryption as part of the Local MSP. The emission of events is sent back to the client showing that they have successfully added a transaction on the blockchain.

Scalability of the Hyperledger Fabric is not very well documented after 30,000 transactions per second. According to Swati and Venkatesan, "throughput and latency stayed stable up to 30,000 transactions" [17]. This same paper encourages for future work to improve scalability from 30,000 transaction per second onwards.

Current DoD System

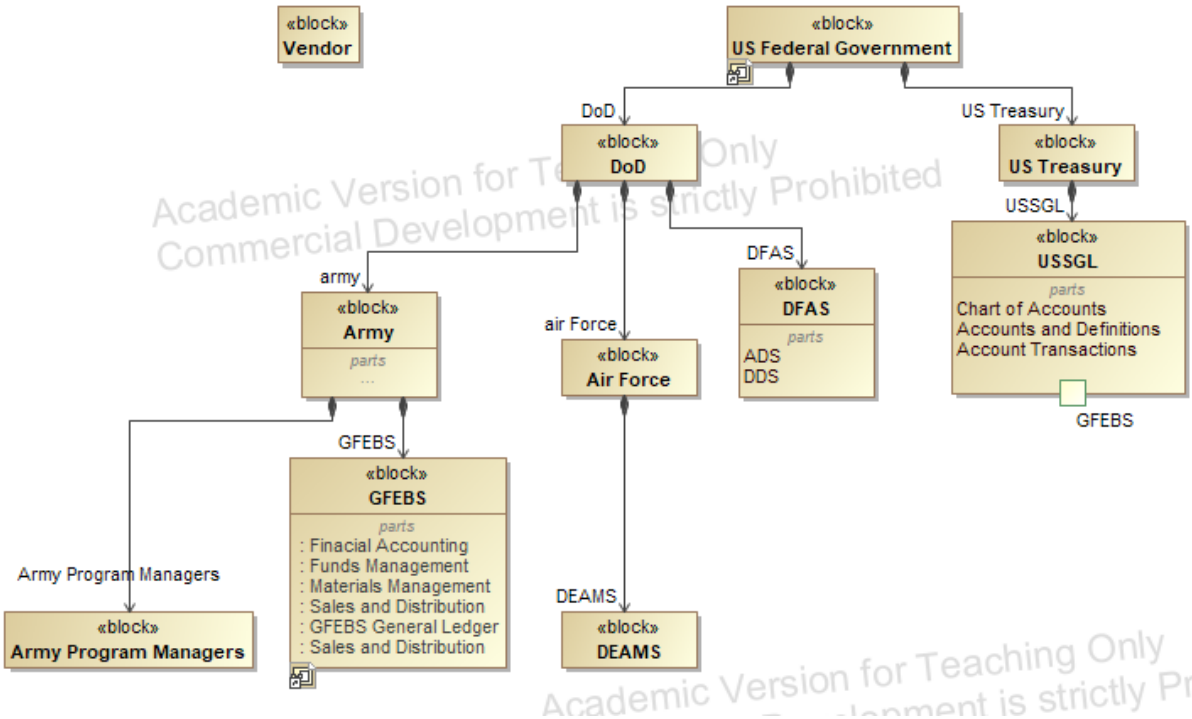


Figure 15. Block Definition Diagram of GFEBS with other DoD Systems and Vendor

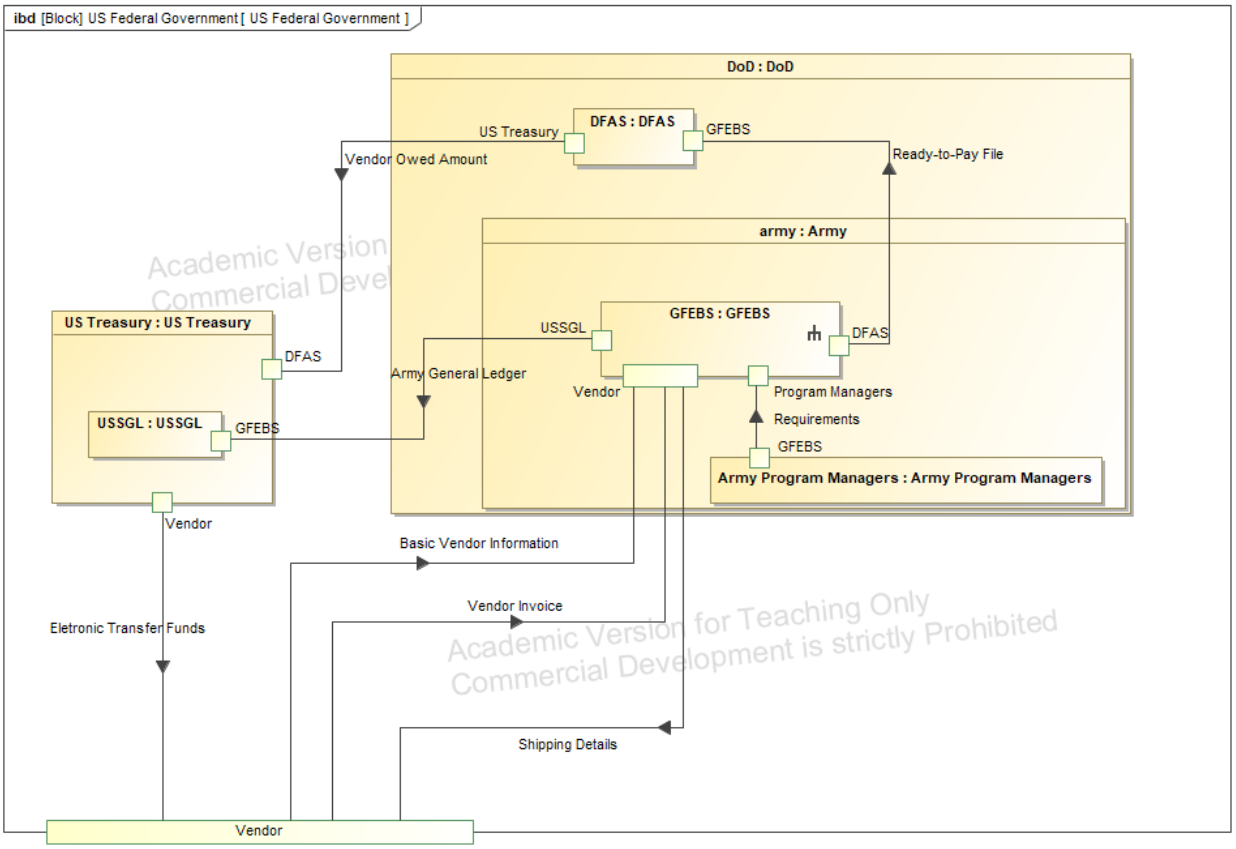


Figure 16. Internal Block Diagram of GFEBS with other DoD Systems and Vendor

Each branch of the military and agency has their own Enterprise Resource Planning (ERP). The Army uses General Fund Enterprise Business System (GFEBS), Logistics Modernized Program (LMP), and Global Combat Support System-Army (GCSS-Army). The Navy uses the Navy ERP while the Air Force is implementing Defense Enterprise Accounting and Management System (DEAMS). The Defense Logistics Agency (DLA) uses the Enterprise Business System (EBS) and finally the Defense Agency uses the Defense Agency Initiative (DAI) system [18]. The Standard Financial Information Structure was created such that there is a standardized financial reporting across DoD. The standardization allows decision makers to effectively compare programs' efficacy based on revenues and expenses [19]. As seen in Figure 15, there are parts that are not recorded as this is specific to the GFEBS payment interactions

with vendors. The interactions should be similar between the other ERPs and the federal agencies that are mentioned in the GFEBS process. This section will go over the GFEBS process in detail and discuss its connection to United States Standards General Ledger.

Army Financial Process

The Army Financial Process is the most accessible financial process out of all the military branches. We will be looking at the process where the DoD interacts with a party that is not part of the government. Vendors are a large part of the DoD budget as "$439 billion were spent on contracts for products and services" [20]. The payment process towards vendors can be split into two parts: Pre - Delivery of Goods/Services and Post Delivery of Goods/Services. We are assuming that the transactions between the Army and vendor are contractual and are to be paid on time.

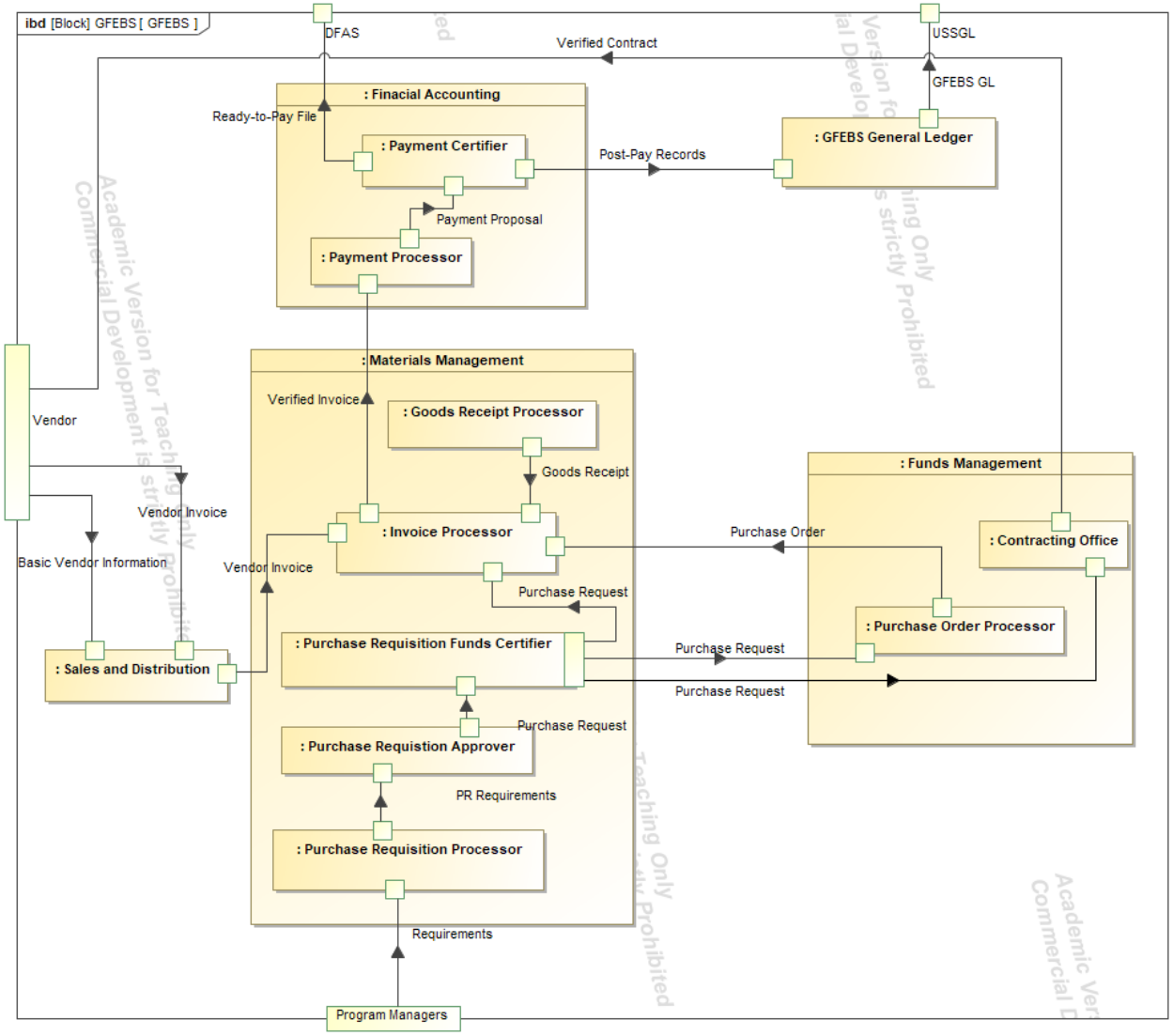


Figure 17. Internal Block Diagram of GFEBS Process [21]

Figure 17 gives a high-level view of the GFEBS process. The part of the figure that this paper will address is the top half, where financial accounting is done. Once all the information is processed in the Financial Accounting Box, a proprietary document is sent to the GFEBS General Ledger. The final step shows the ledger reporting its findings to the USSGL. In the next section, the USSGL will be discussed thoroughly with examples of Army General transactions translated over to the USSGL's Chart of Accounts. Now, in the next few paragraphs, the details of the GFEBS process shall be explained.

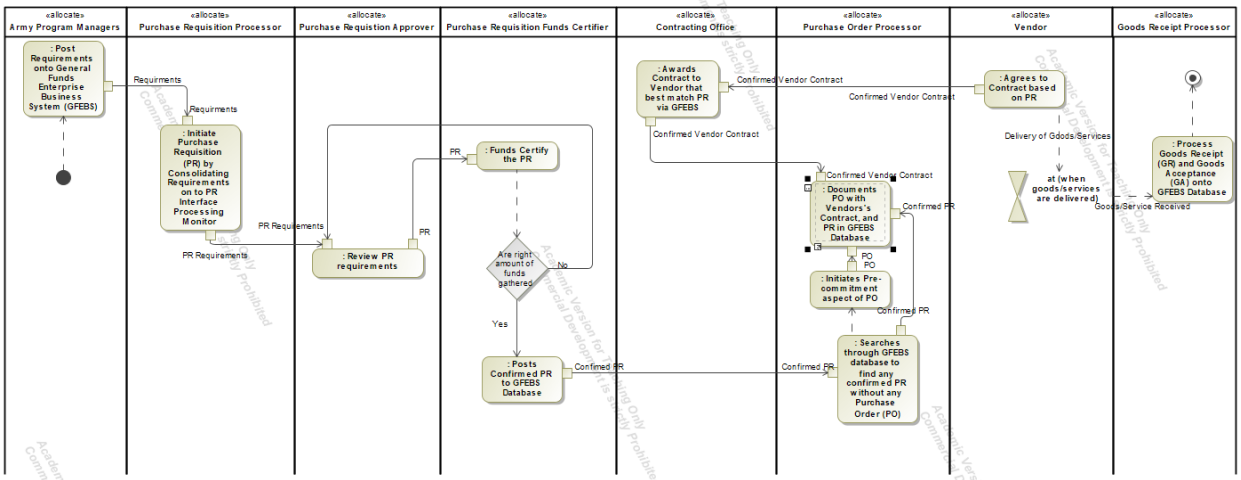


Figure 18. GFEBS Pre-Delivery Process

Before the goods/services have been delivered, there are several steps to securing funds and awarding contracts to vendors. Funds that have already been obligated are committed in the GFEBS [22]. GFEBS is the Systems Applications and Products (SAP) implementation to account for and manage the Army General Fund [23]. “GFEBS integrates several different modules to access the same database and use the same master data” [24]. This means that GFEBS uses a centralized database to read and write data.

Purchase Requisition (PR) Processors initiate the Purchase Requisition (PR) process by consolidating requirements from Program Managers. “A Purchase Requisition is a document that records the request for the purchase of goods and/or services that results in a commitment of funds" [25]. The PR requirements are reviewed by a Purchase Requisition Approver; however, the Purchase Requisition Funds Certifier confirms that the right amount of funds exists for the PR. “After a PR is fund-certified all PRs will require a Purchase Order (PO) to obligate funds" [25]. A PO is the GFEBS’s way of recording obligations from the pre-commitment records.

After a contract has been awarded the Purchase Order Processor documents the PO into the GFEBS database which represents the financial obligation of the contract. A contracting office must administer the contract to establish an agreement with the awarded vendor. An awarded contract is a legally-binding agreement between the vendor and the Army for the specific good/service at the specified price.

The Goods Receipt Processing happens when the goods/services are delivered and includes the GR and Goods Acceptance (GA) documents. GR are documents of the receiving goods/services in GFEBS, while GA are documents of the acceptance of goods/service in GFEBS. Both these records can occur simultaneously or separately. However, if they occur separately, then there is a time limit for both to be documented. As the person most involved in coordinating the GR and GA, the Goods Receipt Processor will post both documents onto GFEBS.

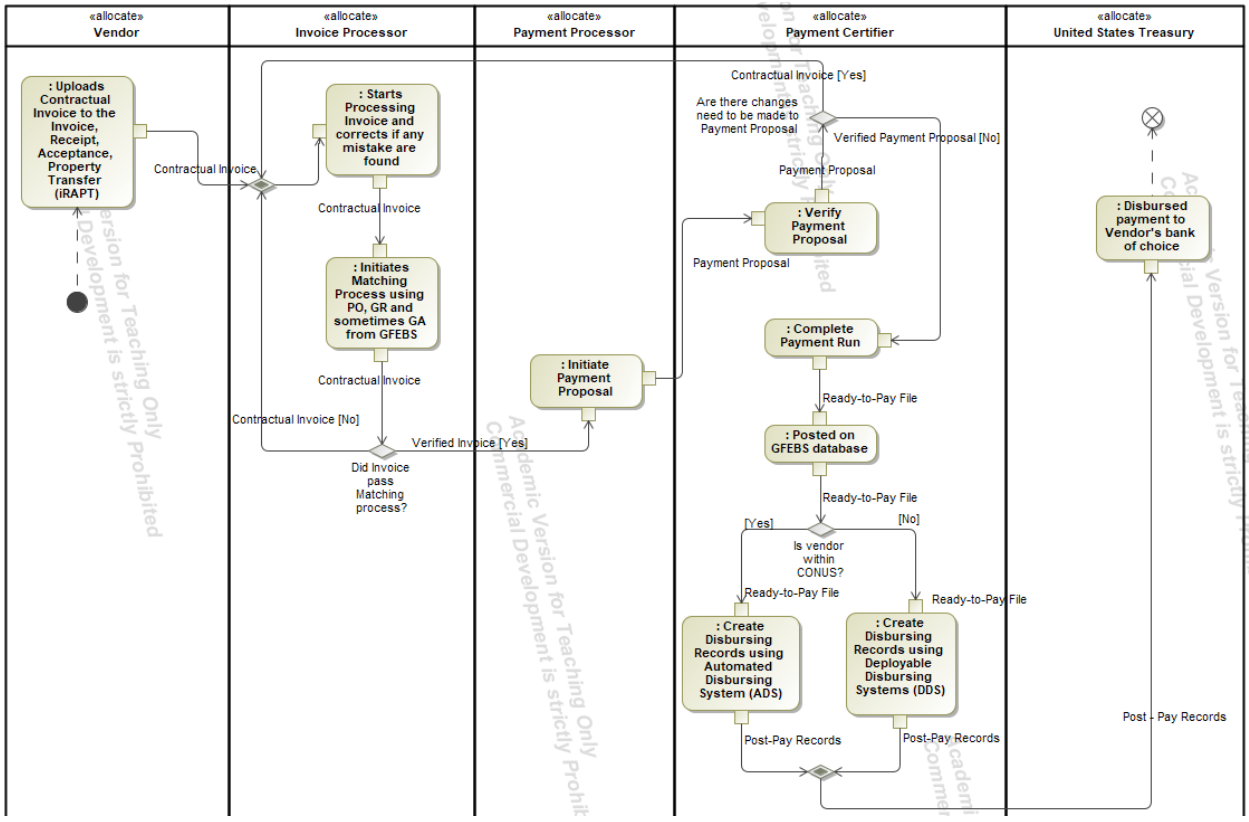


Figure 19. GFEBS Post-Delivery Process

Now after the goods/services have been delivered in accordance with the awarded contract, the vendor submits the invoice to the program Invoice, Receipt, Acceptance, Property Transfer (iRAPT) as goods or services. iRAPT was formerly known as WAWF Business Suite to consolidate many programs into one. The Invoice Processor receives, verifies, and records contractual miscellaneous payments in GFEBS at DFAS. If a mistake is found in Invoice, then the Invoice Processor will try and resolve it. After getting approval from the Invoice Processor, the Invoice is sent to the matching process. There are two types of matching processes: 3-way and 4-way. In a 3-way match, The Invoice is compared against PO and GR documents that are part of the GFEBS. The 4-way matching process is similar except that it also includes GA on top of the other two GFEBS documents mentioned previously. If the Invoice is ever less than the

Amount Obligated on the contract or amount on GR, then the process is halted and the Invoice is sent back to the Invoice Processor for further deducing.

The job of a Payment Processor is to set up parameters and fill in information from the Invoice into a Proposal File. Since there are multiple types of goods or services, the Payment Processor establishes different formats based on the Invoice type for each Proposal File. Payment Proposals display the Invoices that have been correctly matched in either a 3-way or 4-way Matching. The Payment Proposal File is sent to the Payment Certifier whose job is to verify the Payment Proposal File. If an error is found, payment is blocked by the Payment Certifier and sent back to the Invoice Processor to submit. However, if no error is found, then Payment Run is completed and the Payment Certifier creates Ready-to-Pay Files. These files include a unique Payment ID and Payment Date. The Payment Run also includes the sending Ready-To-Pay File to Automated Disbursing System (ADS) or Deployable Disbursing Systems (DDS) for payment processing. If the vendor is within Continental United States (CONUS), then the files are sent to ADS. Otherwise, the files are sent to DDS. Post-Pay File, incoming disbursement records from ADS or DDS, are confirmed with records found in GFEBS using Ready-To-Pay files as reference. Disbursement information is posted in GFEBS so anyone can view payment history. Once the Payment Run process is verified, then disbursement files are sent to the US Treasury. The US Treasury disburses the payment to the vendor's bank of choice. GFEBS general ledger account postings are processed to be compatible with the United States Standard General Ledger (USSGL). The next section will discuss the USSGL.

United States Standard General Ledger (USSGL)

The USSGL is broken up into 7 different parts: Chart of Accounts, Accounts and Definitions, Account Transactions, Account Attributes for USSGL Proprietary Account and Budgetary Account Reporting, Crosswalks to Reclassified Statements for FY 20XX (year of search) Reporting, Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS) Validations and Edits for FY 20XX (year of search) Reporting, and Crosswalks to Standard External Reports for FY 20XX (year of search) GTAS Reporting [26]. For brevity, the paper will only cover Chart of Accounts, Accounts and Definitions, and Account Transactions.

The Chart of Accounts, also known as Standard General Ledger Chart of Accounts, was established to support the consistent recording of financial events in accordance with the Office of Management and Budget (OMB) and Department of Treasury. The chart contains proprietary and budgetary accounts that are self-balancing [27]. This means that total debit is the same as total credits. Budgetary accounts are used to recognize and track budget approvals and execution. On the other hand, proprietary accounts are in reference to assets, liabilities, revenues, and expenses [28].

According to the Treasury Financial Manual, the Accounts and Definitions provides basic information about each USSGL account including: Account Title, Account Number, Balance of Account (Debit or Credit), and Account Definition" [29]. Also from the Treasury Financial Manual, Account Transactions displays the proprietary and budgetary entries that are divided in different organized categories [30].

Figure 20. Army General Ledgers Transition to USSGL [21]

In the GFEBS, the transactions that were recorded on the Army's own ledgers will be formatted so that it can be easily received and recorded in the USSGL. In Figure 20, the transactions are first recorded in Special Ledger 95 (SL-95) (Operating) as a long specific code. The next column shows another general ledger that is part of the Army, SL-Z1 (Reporting). The transactions are grouped to a new simplified code. This can be seen with the codes 6100.11B1, 6100.21T0, and 6100.2533 in the SL-95 that end up as part of group 6100.9000 in SL-Z1. Then again, the codes are simplified for USSGL purposes that only want to see the basics. This simplified coding is part of the Chart of Accounts mentioned earlier. In the same example, 6100 in USSGL will be considered an expense in their structured format. Although this is an older version of the coding, modern Chart of Accounts uses 6-digit codes instead of 4-digits. Nevertheless, it still demonstrates the transition of financial data from Army General Ledger to USSGL's Chart of Accounts.

Digital Dollar

The United States Federal Reserve is currently discussing the possibility of using a Central Bank Digital Currency (CBDC). This defined as a digital liability of a central bank that is widely available to the general public [31]. In another words, it is basically cryptocurrency that is issued by the United States Government and would equal to exactly to the United States physical currency. "CBDCs can be based on blockchain, but they do not need to be. The Federal Reserve Bank of Boston and Michigan Institute of Technology's Digital Currency Initiative found in their research that distributed ledgers could hinder the efficiency and scalability of a CBDC" [32]. The Digital Dollar Project is in its very early stages and the Federal Reserve would need to do more extensive research to see if this project could be feasible and its impact on the economy.

Real-World Blockchain Implementation

Walmart Canada has pushed blockchain far by launching the "world's largest full production blockchain solution for any industrial application" with DLT Labs [33]. Originally, Walmart was frustrated that a lot of their resources were directed to invoice disputes. It was said that "70 percent of invoices ended up as disputes and required manual investigations" [5]. This ended up costing Walmart to overpay for freight deliveries by 38% percent, since it was much easier to pay what the freight companies wanted instead of disputing [34]. The lengthy process ended up taking 6-8 weeks to close out the invoices process. The supply chain team at Walmart Canada decided to ask companies to help with their logistics nightmare. Walmart has already implemented rudimentary blockchain application where they wanted to trace produce back to the

farms where they were grown [34]. Since Walmart had experience using blockchain, they were more comfortable when one of the companies (that was asked to come up with a solution for the logistical problem) told Walmart they could implement a blockchain system in less time than a non-blockchain company. Walmart agreed to hire DLT Labs to implement a blockchain system to help with their freight logistics. Their blockchain system is called DL Freight.

Figure 21. Freight Invoice Process (Pre-DL Freight)

The configuration phase took 8 months, which is faster than normal. This is because Walmart Canada forewent their proof-of-concept process since DLT Labs were a reliable business and Walmart had some experience with blockchain already. Their first trial run with Bison Transport started immediately after with the pilot phase lasting two months. Then 17 more companies were added to the blockchain system. Within two years, all 70 of Walmart Canada's freight vendors had been added to the system. The pre-blockchain invoicing process is similar to the way DOD's ERP operates. According to Figure 21, the shipment details are shared between

Walmart and the freight company. The goods are delivered, where the shipment is either accepted or denied. If denied, then there needs to be proof as to why the shipment was not accepted. If accepted, the freight company generates an invoice. This invoice needs to match with what Walmart expects to pay for the shipment. If there is a difference between Walmart's expectations and freight company's expectations, then it gets disputed. These disputes used to take up to 6-8 weeks to resolve [35]. If the expectations match, then Walmart pays the invoice.

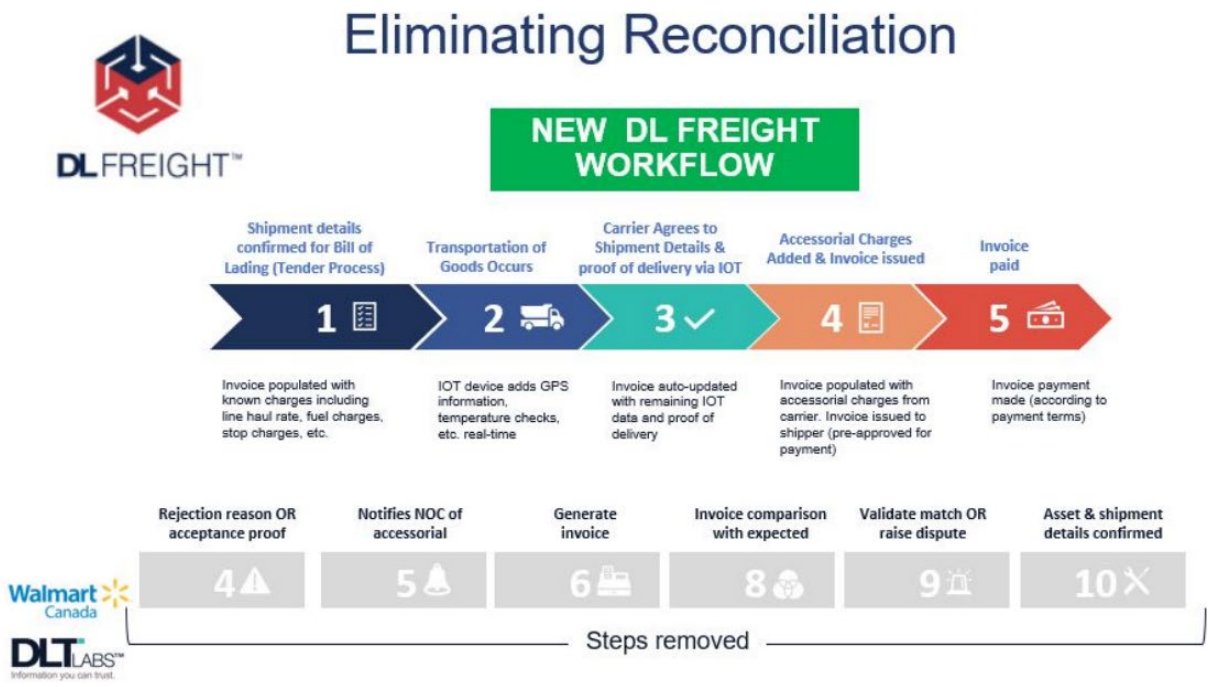


Figure 22. Freight Invoice Process (Post-DL Freight) [36]

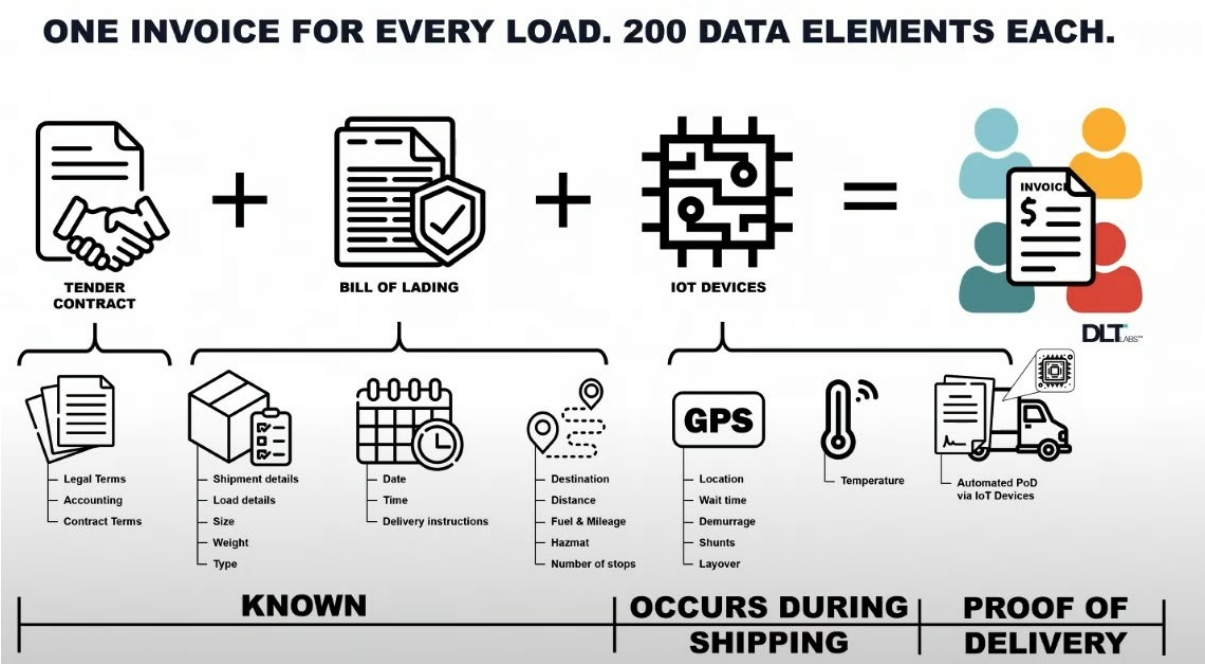


Figure 23. IoT device in conjunction with Blockchain [36]

After the implementation of the DL Freight, the workflow steps were cut in half (as seen in Figure 22). The first two steps are the same as the previous flowchart (Figure 21). In Figure 23, we see that even before shipping happens, the invoices are populated by two entities: tender contract and bill of lading. The tender contract is the same as the smart contract where both parties have already formulated the amount owed based on the variable that will be added to the invoice. The bill of lading are shipment details that includes date, load, and destination. These are subject to change for each delivery. While the shipment is being delivered, IOT devices that are part of the truck adds variable data such as GPS information, temperature checks, and other real time information to the invoice. "IoT devices are pieces of hardware, such as sensors, actuators, gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks" [37]. This means that there are temperature sensors, GPS sensors on the truck that relay information back to the blockchain. The blockchain

will consolidate all the information and add it to the invoice. After the invoice is populated with the IOT information and last-minute charges from the freight carrier, Walmart immediately pays the invoice.

This blockchain addition was able to reduce invoice disputes from 70% to 1.5% [5]. However, Shareen Hamilton, VP of Sales and Marketing at DLT Labs, explains that these "disputes" are more just discrepancies that are actively reconciled [34]. Since there are less invoice discrepancies, there is not a long list of invoices where a new disputed invoice gets added to the end. Therefore, all new discrepancies are handled quickly and timely.

DLT Labs considered many blockchain frameworks. First, they decided public blockchains were too risky for what they had in mind. For private blockchains, they had the choices of Hyperledger Fabric, Corda, and Quorum. They ended up choosing a Permissioned Private solution, Hyperledger Fabric [5]. Hyperledger Project is a non-profit organization launched by the Linux Foundation in 2015 to expand enterprise-grade blockchain across industries. There are many blockchain frameworks that are part of the Hyperledger Project; however, Fabric was chosen as it had the most success with other industries such as IBM. Fabric is an open-sourced platform which has been modified to fit the Walmart system. The Fabric model is structured as a chain of blocks and has two subsystems: 'the world state' and the 'transaction log' of all the transactions that led up to the current world state" [5]. Chaincode is the smart contract feature, employed by Fabric, that bridges the two subsystems by automating transactions and connecting outside applications to the world state ledger. The smart contract was designed in a way to be universally accepting of data of any type or any platform. Chaincode code also contains the rules and calculations that both parties must abide by. The only thing they

are inputting is the initial variables which both parties already agreed on before the shipment started. The other variables are from the IOT devices plugged into each freight.

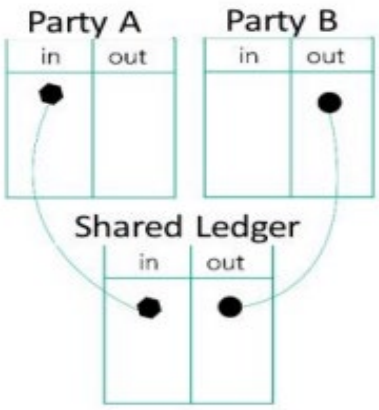


Figure 24. Triple Booking Accounting (adapted from [5])

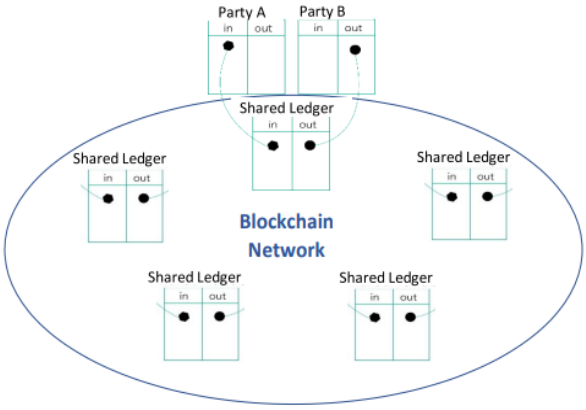


Figure 25. Triple Booking Accounting with multiple Parties (adapted from [5])

Similar to other enterprise-level blockchains, DL Freight uses the triple book accounting method. In regards to Figure 24, Party A has a credit while Party B has a debit. Party A and Party B still operate with their own internal systems; they can be synchronized as the shared ledger has both the credit (In) and debit (Out) values equaling the same amount. Figure 25 shows how different parties would be inputting their information and adding to the blockchain network.

DL Freight has 17 nodes across the network and is operated by DLT Labs, Walmart Canada and freight companies. Walmart made the conscious decision to let DLT Labs operate as a neutral party between Walmart and the freight companies [5]. This is technically not a proper private blockchain as no third parties (such as DLT Labs) would be involved. These node operators would upload data from their internal system of records to DL Freights using application programming interfaces (APIs). APIs are used to link two different applications such

that the transfer of information is possible. Virtual machines are required by DLT Labs to secure and protect the data. For another layer of security, the entire network runs without direct access to the Internet … as users have to go through a series of microservices and firewalls to connect" [5].

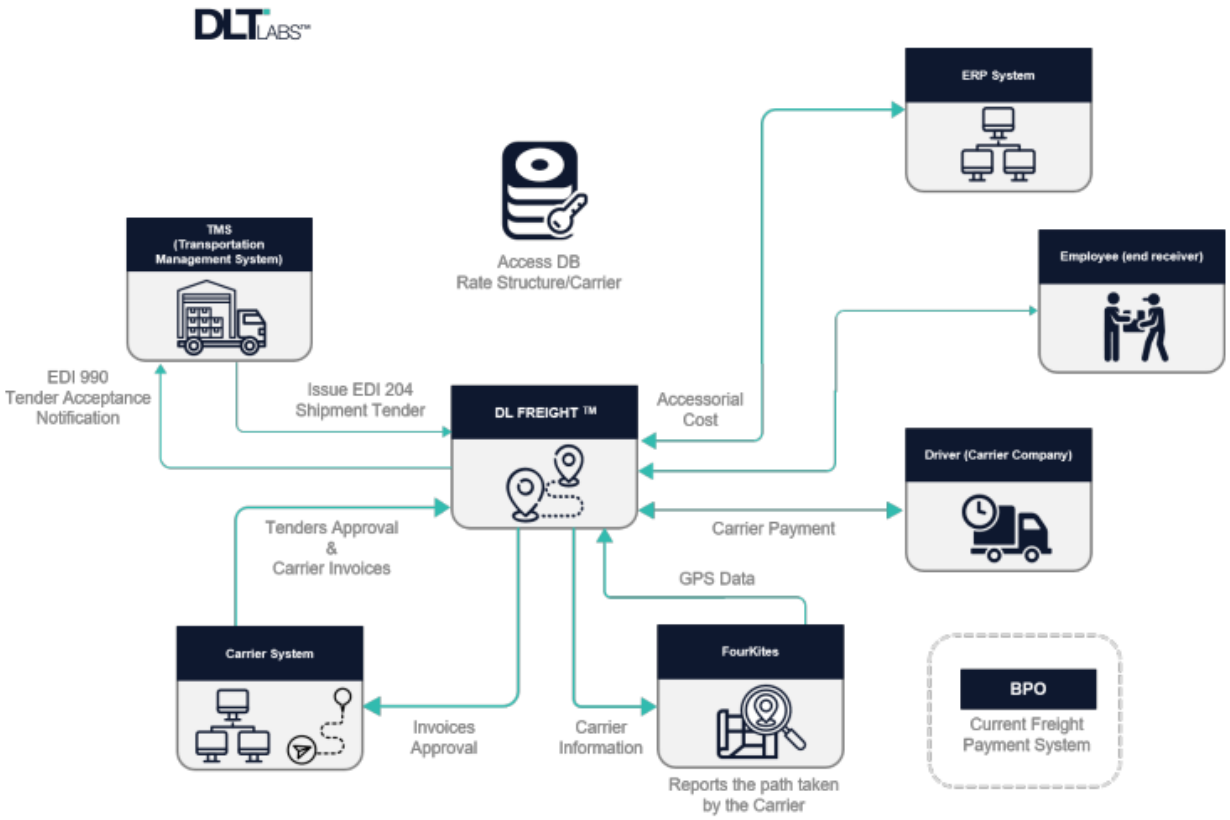


Figure 26. DL Freight's Information Process [5]

In Figure 26, the DL Freight's data process is displayed. The first aspect is the shipment tender from Walmart's Transportation Management System (TMS) being uploaded to the DL Freight platform. An acceptance notification is sent back acknowledging the request. Now, Freight Carriers will accept the shipment tender through the API. Freight Carriers would have

already connected their IOT devices to their trucks and to the DL Freight system. In this case, Walmart uses "FourKites, a system that collects and consolidates data from GPS and IoT devices from their network of [Freight] carriers" [5]. The data from the IoT devices are the variable data that was mentioned earlier. Walmart's distribution centers are connected to the DL Freights and verify the proof of delivery made by the Freight Carriers. Finally, Walmart's ERP system adds any accessory charges from the carrier (such as extra wait times or detours) and the invoice is promptly paid. In the 2021 Walton conference, Sergei Beliaev, DLT Labs EVP and Chief Strategy Officer, informs that initially the geospatial [and other variable] data was stored onto the blockchain. However, after careful consideration about the transient nature of this kind of data, they decided that it makes better sense to have the data off-chain which is directly connected to the critical information on the chain [36].

Summary

In this Literature Review, we have covered the foundation of blockchain which included its inheritance traits of immutability and decentralization, as well as different types of blockchain. In this section we also determined that Permissioned Blockchain would be a more conducive environment for blockchain than Permissionless Blockchain. The more advanced topics of blockchain include smart contracts with basic examples of blockchain in action. The final aspect of the blockchain explanation harkens back to the "Blockchain Basics" portion of the thesis and breaks down the Permissioned Blockchain using System Architecture. The next part of the Literature Review is the current process of the DoD using GFEBS as a case study. On the other hand, the last part of this section covers the real-world blockchain implementation using Walmart Canada's DL Freight as an example.

III. Methodology

Chapter Overview

The purpose of this chapter is to lay out and justify the three-point analysis plan. The first part of the chapter will cover a flowchart used by organizations that are considering blockchain. The second part of the chapter will consider and convert the established government regulations and the GAO weakness to requirements that a potential blockchain solution must satisfy. Lastly, the chapter will end with an explanation of Cost, Time, Throughput, Error Rate, and Latency Metrics between already existing DoD ERP systems and real-world blockchain implementation.

Ten Step Blockchain Decision Flowchart

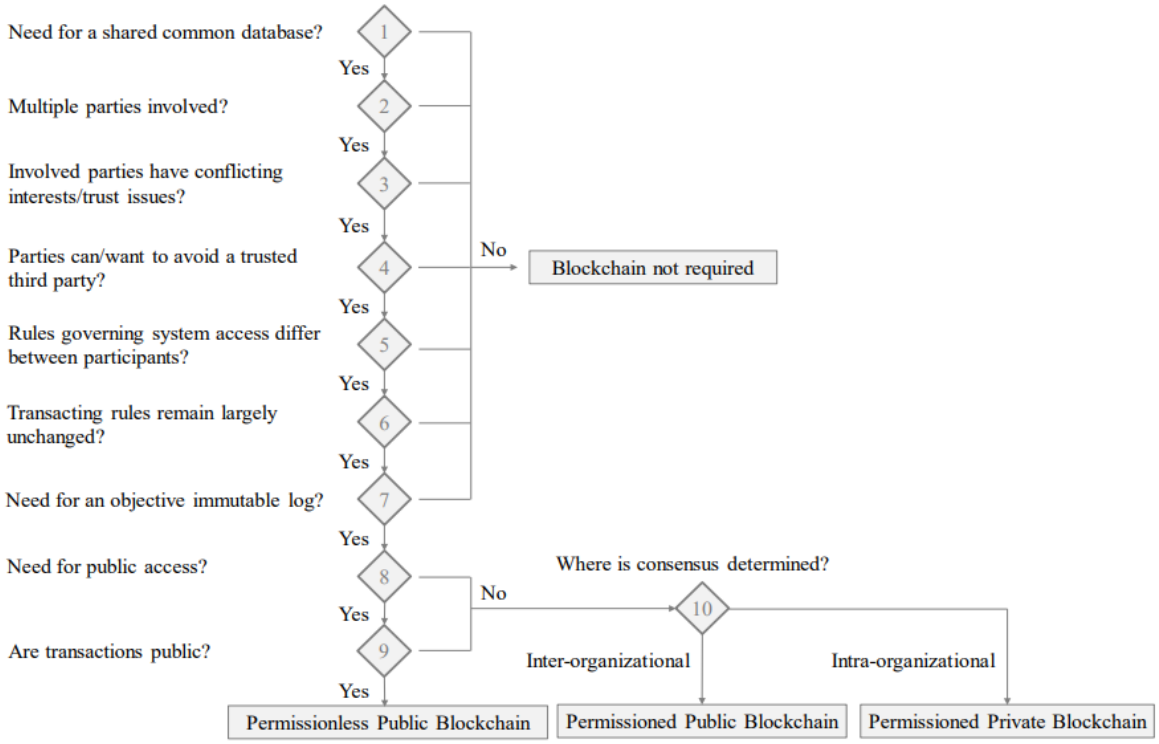


Figure 27: Ten Step Decision Path [10]

The authors of "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies" [10] compiled a simple outline of whether an organization needs blockchain. If blockchain is needed, then the authors also supplied reasoning as to which of the blockchain types (Permissionless Public Blockchain, Permissioned Blockchain, Permissioned Private Blockchain) would be the best fit for an organization. If an organization answers "Yes" to the first seven questions then blockchain may be a useful endeavor for the given organization. If no is answered to any of the first seven questions, then the organization may need to rethink if blockchain is really necessary. Questions eight through ten determine the type of blockchain that makes sense for the firm. From Figure 27, we can see that the first aspect to consider is the need for a shared common database. A shared common database implies that more than one entity would be able to view or create the data for the database. For small data sets, storing information onto the blockchain is inconsequential. However, when companies try to scale the database to larger proportions, "big-database" blockchains they will run into the problem of the blockchain being slow and expensive due to authentication timings and transaction fees, respectively. The authors have given a possible solution for the inefficient blockchain by "integrating the blockchain system with an off-chain database, or simply using a conventional database instead of a blockchain" [10].

The second question asked by the authors is if multiple parties are involved. The multiple entities may use different aspects of the database or all of it as needed. The next question refers to the trust between the parties, or lack thereof. The authors state that "a blockchain is appropriate if there are trust issues or conflicts of interest between the parties" [10]. If there is confidence amongst everyone, then a centralized database is ideal as every data entered is trusted by everyone. In blockchain, trust is determined via smart contracts. Smart Contracts are contracts

that are embedded into the blockchain via code which multiple parties have agree to ahead of time. This way all parties know whether to agree to the transparent contract.

The fourth question targets third parties. Usually, third parties are tasked with managing transactions between two parties. Since smart contracts are deployed, there is no need for a notary (to confirm a contract) or a bank (money is tied to smart contract). Fees may be incurred from the third party to the remaining participants. However, a smart contract would bypass the need for a third party. The fifth question asks if there are different rules that apply to different members of the blockchain. The author states that "If all participants have the same access rights, a relational database offers a more feasible solution than a blockchain" [10]. Administrating which entity has Peer access can play a role in this step as the guideline of the rules for each member.

The sixth question asks if the rules from the fifth question change. Once a blockchain and the smart contract have been deployed there isn't a way to change the rules of the smart contract. Otherwise, parties can modify rules to better fit their needs and it would not be fair for the parties that have been locked in a contract prior to the change. For example, if a certain threshold is met, then the smart contract (that all parties have agreed on) will disburse the money according to the contract. The seventh question takes a look at the necessity for an immutable ledger. As mentioned in the Literature Review, an immutable ledger means that the log cannot be changed once a new block (transaction) has been entered. An immutable ledger makes it simple for audits as there is only one long paper trail to follow to see every transaction made within any given timeframe. However, if an organization's ledger experiences many manual inputs, then it may lead to mistakes caused by human error. In a centralized database, one can edit a transaction,

albeit with the possibility of getting permission from someone in a higher position or more knowledgeable about the database. This is not the case on the blockchain. One cannot change the ledger once the block (transaction) is on the blockchain due to its immutability. If "Yes" is answered to any of the first seven questions, then typically blockchain is not required according to the authors of Figure 27.

The eighth question is the first part of finding out if Permissionless Public Blockchain is right for an organization. Public access means that anyone can join and no vetting process is administered. Writing and Validating blocks (transactions) to the blockchain is given to anyone that joins the open blockchain. Determining who has writing and validating access is one of the biggest demarcations between 3 major types of blockchain. If "No" is answered for the eighth question, then it automatically goes to the 10th question according to Figure 27. The ninth question is the second part if Permissionless Public is the choice for a firm. Transaction going public implies that anyone in the public blockchain can view the data. This choice determines if the organization would make sense with either a public or private blockchain. Examples of Permissionless Public Blockchain include Ethereum and Bitcoin, therefore there would need to be cryptocurrency involved with the public blockchain choice.

If the eighth or ninth question ended up being "No", then the final question asks where consensus is determined between the two permissioned blockchain. Permissioned blockchains only allow vetted individuals to the blockchain network. The two types of permissioned blockchains are decided based on how everyone on the blockchain can agree upon the validity of the block added to the blockchain. For a Permissioned Public blockchain, all vetted personnel can read the data and submit transactions; however, only authorized personnel validate those

transactions. According to the authors, incorporating this strategy encourages inter-organizational consensus [10]. On the other hand, for Permissioned Private blockchain, only authorized personnel can read, write, and validate transactions. In other words, an ideal situation to use Permissioned Private blockchain would be with only people within the organization who determine the consensus. Hyperledger is versatile such that it can be used for Permissioned Public or Permissioned Private blockchain.

Regulations and Weaknesses Requirements

The potential blockchain financial system must follow the regulations of the current financial system. According to GAO, "For federal financial management systems, a migration plan should also address Federal Financial Management Improvement Act of 1996 (FFMIA) requirements, applicable federal accounting standards, and the USSGL at the transaction level" [7]. The second section covers the GAO Weaknesses that was mentioned in the Problem Statement. The four weaknesses are translated to their requirements. A Requirement Matrix for all the requirements mentioned above will be connected to the blockchain components that satisfy them.

Regulations Requirements

1	1 Federal Financial Management Improvement Act	The system shall provide dependable and unvarying financial data while applying highest accounting standards
2	1.1 Recipients Information	The system shall capture recipient's information
3	1.2 Disbursement Term and Amounts	The system shall determine terms and accounts
4	1.3 Provide Payment Data	The system shall provide payment data to post General Ledger (GL) transactions consistent with USSGL
5	1.4 Capture GL Account	The system shall capture GL account transactions provided by supporting financial sources consistent with USSGL
6	1.5 GL Matching Codes	The system shall post GL transaction consistent with attributes codes and categories
7	1.6 Government Wide Reporting	The system shall provide GL information for consolidated government wide reporting
8	1.7 GL Agency Specific Reporting	The system shall provide GL information agency - specific finacial statement reporting
9	1.8 Cut Misuse	The system shall cut waste, loss and misuse of financial information
10	2 Federal Accounting Standards	The system shall maintain accounting data to permit reporting in accordance with the Generally Accepted Accounting Principles (GAAP)
21	3 USSGL at Transaction Level	The system shall record approved transactions in the USSGL once an approved transaction is recorded in the financial system in question
22	4 GAO Four Weaknesses	The system shall remediate the Information Technology flaws expressed by the U.S. Government Accountability Office

Figure 28. Definitions for FFMIA Requirements

Federal Financial Management Improvement Act of 1996 (FFMIA) goals are to provide dependable and unvarying financial data while applying the highest accounting standards. The Federal Financial Management System (FFMS) supports the goals of the FFMIA in three different aspects: “reliable financial reporting, effective and efficient operations, and compliance with applicable laws and regulations” [38]. The first aspect is covered by “Capture Recipients Information,” “Determine Disbursements terms and amounts,” “Provide Payment data required to post GL transactions consistent with USSGL,” “Capture GL account transactions with UGGL,” “Post GL transactions consistent with attributes codes and categories,” “Provide GL information for consolidated government wide reporting,” and “Provide GL information for agency-specific financial statement reporting.” [39]. The “effective and efficient operations” requires actions that cut waste, loss and misuse of financial information. The last part of the OMB statement is self-explanatory. Figure 28 summarizes all the requirements and definitions for the FFMIA portion.

10	2 Federal Accounting Standards	The system shall maintain accounting data to permit reporting in accordance with the Generally Accepted Accounting Principles (GAAP)
11	2.1 Principle of Regularity	The system shall adhere to GAAP rules and regulations as a standard
12	2.2 Principle of Consistency	The system shall apply same standards throughout entire reporting process
13	2.3 Principle of Sincerity	The system shall provide accurate and impartial depiction of financial situation
14	2.4 Principle of Permanence of Methods	The system shall have consistent procedures as to allow fair comparison of financial information
15	2.5 Principle of Non-Compensation	The system shall have both negatives and positives transparent reports
16	2.6 Principle of Prudence	The system shall be based on fact-based representation as to not incorporate speculation
17	2.7 Principle of Continuity	The system shall assume that the business will continue to operate while evaluating assets
18	2.8 Principle of Periodicity	The system shall distributed entries across the appropriate periods of time
19	2.9 Principle of Materiality	The system shall fully disclose all financial data and accounting information
20	2.10 Principle of Utmost Good Faith	The system shall remain honest in all transactions
21	3 USSGL at Transaction Level	The system shall record approved transactions in the USSGL once an approved transaction is recorded in the financial system in question

Figure 29. Definitions for Federal Accounting Standards and USSGL Requirements

For the Applicable Federal Accounting Standards, the “system shall maintain accounting data to permit reporting in accordance with the Generally Accepted Accounting Principles (GAAP)” [38]. 10 Principles of GAAP include Principle of Regularity, Consistency, Sincerity, Permanence of Methods, Non-Compensation, Prudence, Continuity, Periodicity, Materiality,

Utmost Good Faith [40]. Figure 29 contains all the definitions for the accounting standards' requirements.

As part of the USSGL at transaction level aspect, "each time an approved transaction is recorded in the financial management system, it will generate appropriate general ledger accounts for posting the transaction according to the rules" [38]. This requirement is the same as "Capture GL Accounts" from the FFMIA requirements.

Four Weaknesses in Information Technology

22	4 GAO Four Weaknesses	The system shall remediate the Information Technology flaws expressed by the U.S. Government Accountability Office
23	4.1 Configuration and Security Management	The system shall aid in security procedures and develop risk mitigations
24	4.1.1 Unauthorized Changes	The system shall stop unauthorized data changes
25	4.2 Access Control	The system shall control the access of information to users depending on authorization level
26	4.2.1 Reasonable Authorization	The system shall reasonably authorize personnel
27	4.2.2 Sensitive Information	The system shall prevent personnel from accessing sensitive information
28	4.3 Segregation of Duties	The system shall clearly define users role that do not conflict
29	4.3.1 Deconflict	The system shall not put users in a position where a conflict of interest for data or roles exists
30	4.4 Legacy Systems	The system shall replace legacy systems with a system that satisfies Capture Transaction Details and Auditors Documentations
31	4.4.1 Capture Transaction Details	The system shall capture transaction level details
32	4.4.2 Auditing Documentation	The system shall contain all documentation for auditors

Figure 30. Definitions for GAO Weaknesses Requirements

The GAO has recommended that the DoD should remediate four weaknesses in the Information Technology sector. These weaknesses have been identified in the FY2020 report, but have persisted in the FY2021 report as well. There are attempts at this endeavor, but according to the Pentagon's Comptroller and GAO some of them will not be fully solved until 2027 or 2036 [2], [4]. Figure 30 breaks down each of the weaknesses to the requirement definitions. The GAO defines Configuration and Security Management as the "control that prevent unauthorized changes to systems and aid in assessing risk, developing, and implementing security procedures, and monitoring effectiveness" [4]. This asks the question: Can a feature of

blockchain stop data change that hinders normal processes or triggers security measures? The two aspects of Access Control that GAO wants to tackle is to ensure that authorized roles are reasonable and prevent personnel from accessing information they are not supposed to have [4]. The Segregation of Duties weakness is defined as users having conflicting key roles and functions [4]. It is expected that this will also be tackled at the same time when Access Control will be remediated. Legacy System's weakness states that there are many internal flaws which include not being able to capture transaction-level details that satisfy accounting needs. This leads to manual reports which are hard to track down for audits. There are 140 systems that do not meet Federal requirements that have not been retired and will not be until 2036 [4]. Nine legacy systems were scheduled to retire within FY2020, but extended that deadline to 2021.

Requirements Matrix

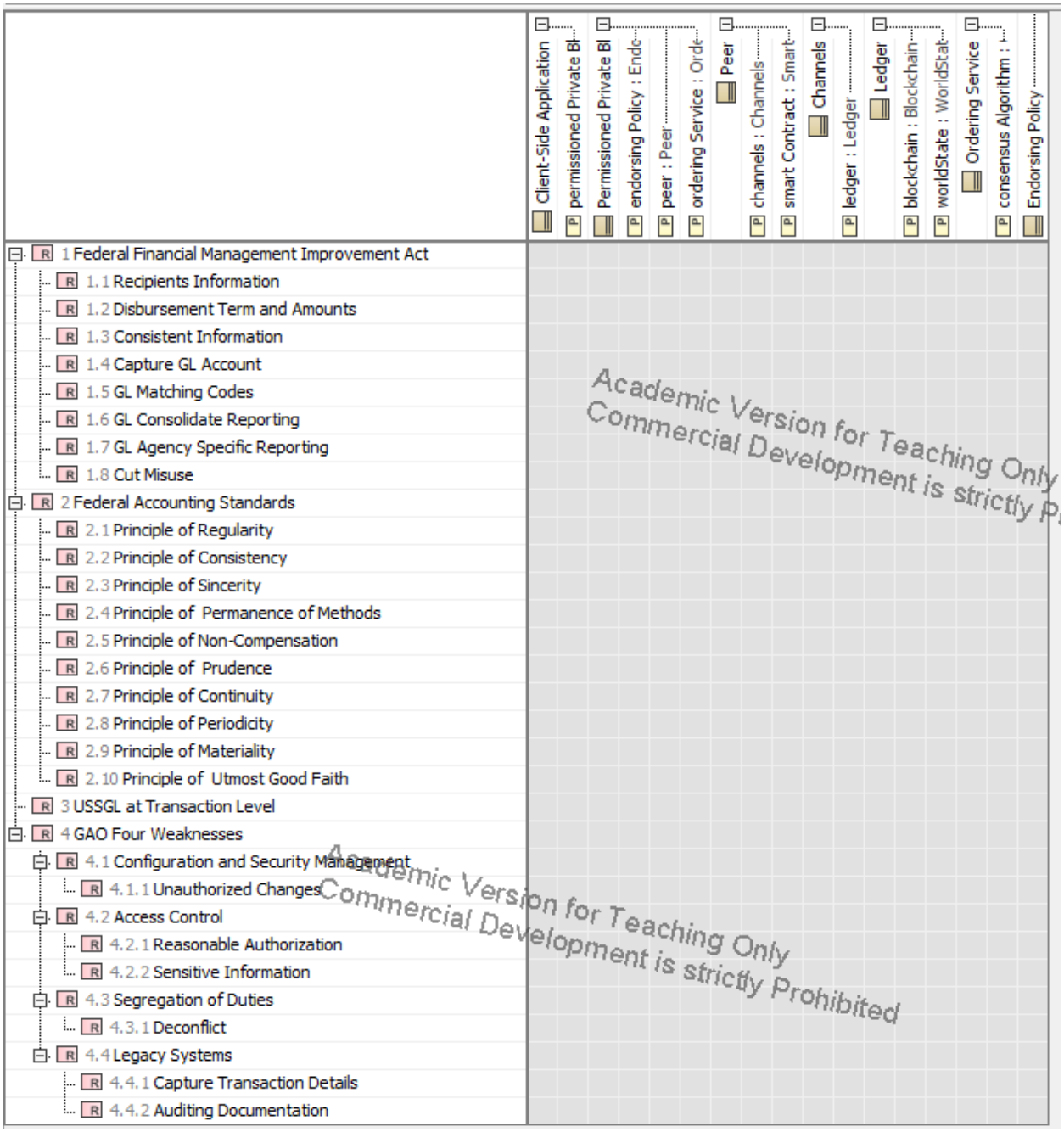


Figure 31. Requirements Satisfaction Matrix

With Figure 31 as a reference, all the requirements are listed in hierarchy order in the y-axis. Along the x -axis, the components of blockchain are also listed in hierarchy form. Some of

the GAO requirements may be administrative issues and not really an aspect of the current system's ERP. These requirements will be discussed further in the analysis portion of the thesis.

Performance Metrics

Ideally, the best way to compare two uneven systems would be to find see how one system's metrics would change based on the environment that the other system is in. This is not yet possible because the DoD has not implemented a blockchain ERP solution. Therefore, we will only be looking at the metrics of the three systems and urge for comparison research for the future.

For this paper, we will be looking at three different current systems. One current system is DEAMS. The Air Force is in the process of switching from a legacy system to a modern system. DEAMS still uses the traditional ledger system, but has been updated to keep up with current transaction infrastructure. The modernization means that there will be up-to-date data surrounding it. Many other ERP systems the military branches use have been established a long time ago and there are not many accessible sources. The other system for comparison is GFEBS. Just like DEAMS it employs a traditional ledger system. GFEBS is used because it has the most public information available. In future studies, other ERPs should be used for comparison. The analysis will include the world's largest industrial development of blockchain, Walmart Canada's DL Freight [33] as the placeholder for the potentially new blockchain. The use of Walmart DL Freight is important because it is already implemented large-scale, was established recently (in 2020), and shared a similar invoicing process to DEAMS and GFEBS.

The metrics this paper will use Cost, Time, Throughput, Latency and Error Rate. Cost will be the Life Cycle Cost for the system. In the case of DEAMS, it has not yet been fully deployed, so the most recent estimate will suffice. The Time metric is how long the system took to reach full deployment. Just like the Cost metrics, only estimates for how long DEAMS will take are available since DEAMS has not been fully deployed. Throughput, in this paper, will refer to how many invoices are processed in a year. Latency is determined on the average time of each invoice processed and the percentage of vendors who are paid on time. Being "paid on time" as a DOD vendor is under 30 days. Congress passed the Prompt Pay Act where agencies have an obligation to pay every proper invoice within 30 days after the first invoice day or else pay interest on the late payment [41]. Finally, the Error Rate is the percentage of mistakes found in the invoicing process.

Summary

The three-point plan was explained thoroughly in the methodology section. The first part explained each decision point in the flowchart to determine if blockchain is really necessary to begin with. The second portion discussed all the requirements, based on government regulations and problem areas, that a potential blockchain system should fulfill. Finally, the methodology clarified why DEAMS and GFEBS are good points of comparison for Walmart's DL Freight. It also showed how Cost, Time, Throughput, Latency, and Error Rate will be displayed for the three systems mentioned previously. The next chapter will analyze the three-point plan mentioned above.

IV. Analysis and Results

Chapter Overview

In this chapter, there will be three different analyses done to answer the investigative questions. The first analysis will be on the 10-Step Blockchain Flowchart, where each decision is carefully considered before ultimately choosing whether blockchain is right for the DoD and if so, which one. The second analysis will cover the rules, regulations, and weaknesses of the DoD using Requirements Matrices as evidence. Finally, the third analysis will cover cost, time and benchmark metrics for each of the current DoD systems and real-world implementation of blockchain.

10-Step Blockchain Decision Analysis

First Decision

The first decision in the flowchart is if there is a need for a shared common database. A shared database allows for all viewers on a team to read and write data on to it. Just within GFEBS of the Army Financial System, the Purchase Requisition (PR) Processor, PR Approver, PR Funds Certifier, Purchase Order Processor, Goods Receipt Processor, and Invoice Processor all order and vendor information so that everyone down the line of the process can use the data. Each GFEBS worker has an interfacing application that already communicates to the centralized shared database. Vendors can also see the timeline of their invoice becoming a check in their bank account. There is also a need for a shared common database as many users are reliant on it.

Second Decision

The second-choice questions if multiple parties are involved. For example, there are vendors (who are not part of any government agency) and a government agency. Another party that is involved are auditors that meticulously comb through transactions to ensure legitimacy for the transactions. In Figure 27, we can see the interactions of the parties mentioned above. The reason this question is asked is to understand that the data is not part of an internal organization. Otherwise, the database would make the most sense. However, since there are multiple parties involved, the answer is yes for this question.

Third Decision

This section will discuss the competing interests between vendors and government agencies. Since vendors are private companies, they are motivated by maximizing corporate profits and shareholder values by selling their goods/service. However, the corporation's strategy to make profits may not clearly align with United States military strategies. For example, there was a contract dispute between the DOD and Lockheed Martin about the Primer situation for the F-35's. "At the time, corrosion was found in fastener holes of F-35's being repaired at Hill Air Force Base in Utah. Lockheed and the JPO [F-35 Joint Program Office] were able to agree on a corrective action plan, one source said, and Lockheed was able to complete planned deliveries of the F-35 for 2017" [42]. Although a plan was put in place, the dispute occurred when the question of who was going to foot the bill for all the corrections. The DOD's argument was that the F-35 did not pass Lockheed Martin's Quality Assurance testing and delivered an incomplete product. Therefore, Lockheed Martin had to fix and not charge any amount to the DOD. On the flip side, Lockheed Martin's argument was that since they were correcting every fastener hole in

every F-35, they needed a lot of manhours to fix the issue. So, Lockheed Martin wanted to be paid for the labor costs. The frequency of new disputes has decreased from 2007 to 2014. In the FY 2021 annual report, "contractors docketed only 400 new appeals… for comparison, the Board docketed 497 appeals last year [2020]; 708 in FY 2014 and 624 during FY 2007… At the end of conclusion of FY 2021, the Board's total docket included 954 cases, a number which has increased slightly (up from 947) since the beginning of FY 2021" [43]. With the ever-growing list of contract disputes, we can see that there are parties with competing interests.

Fourth Decision

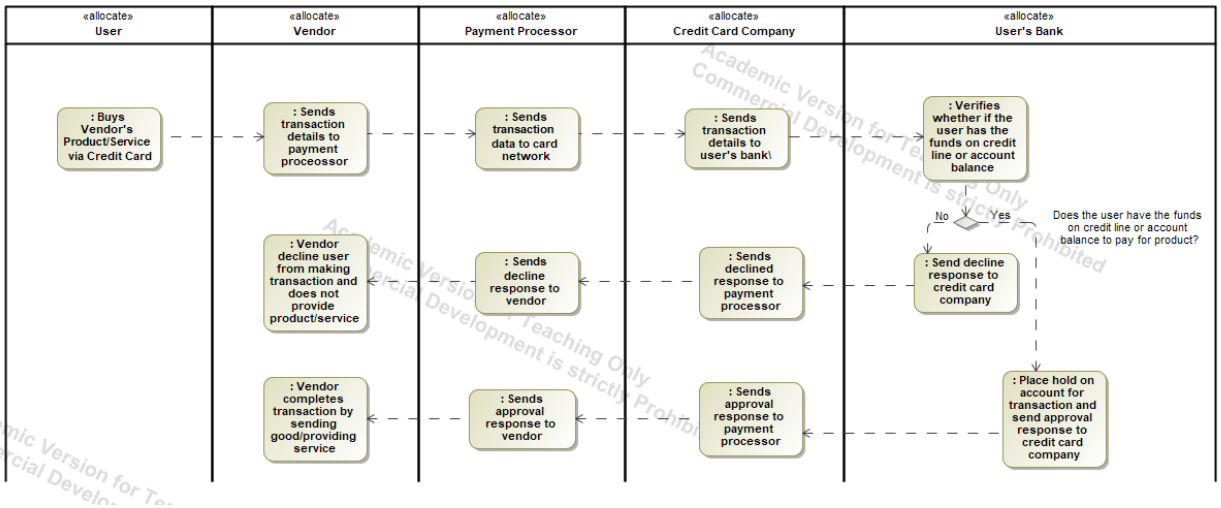


Figure 32. Credit Card Authorization Process

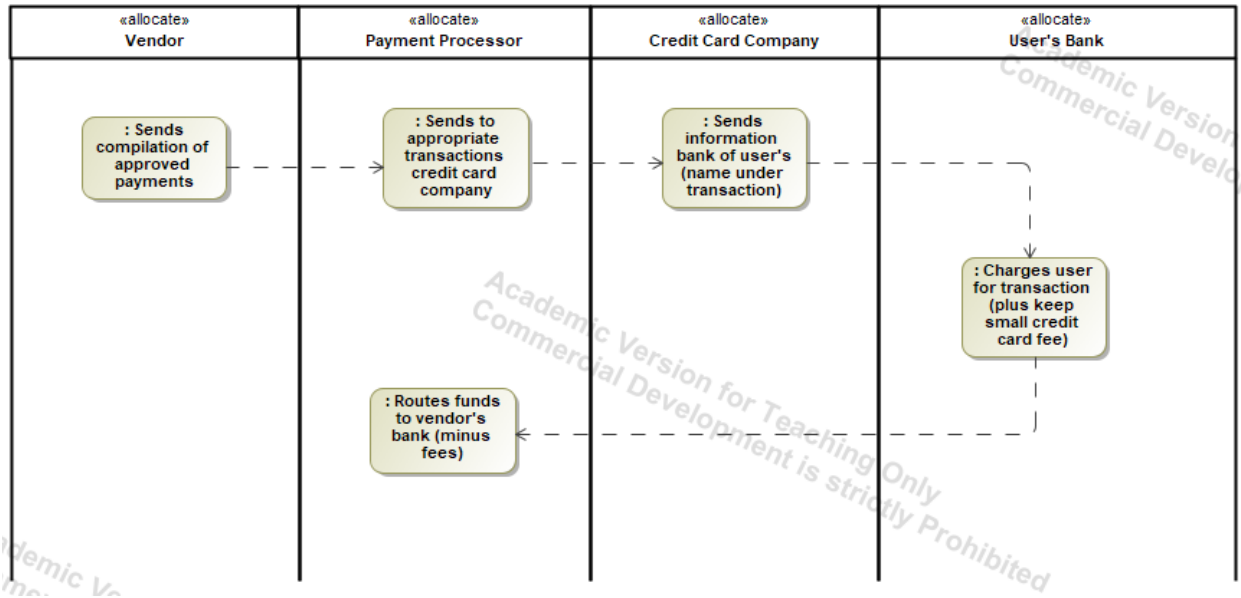


Figure 33. Credit Card Settlement Process

For the question of whether there are parties that want to avoid a trusted third party, we need to first ask if there are third parties involved at any given time. In a normal interaction for non-cryptocurrency users, the bank and credit card companies play the role of the third party. As seen in Figure 32 and Figure 33, there are two parts of the credit card process. The authorization part has 3 entities besides the user and vendor involved in the process. If we follow the flowchart, we can see that the transaction data is sent from the vendor to the payment processor. The payment processors are businesses used by vendors to process the credit card information. Common examples include Paypal and Square. The information is then sent to the User's credit card company. These would include Visa, MasterCard, or American Express. The information is then passed down to the user's bank or whomever the user holds their credit card with. Companies may include Bank of America, Chase, etc. The bank will verify if the user has enough funds on their credit line (credit card) or in their bank account (debit card). If approved, the bank will put a hold on the account for the money owed and send the approval response

through the credit card company and payment process to the vendor. However, if the bank denies the transaction, then the declined message travels the same way as the approval message to the vendor. The vendor will complete the transaction if the approval message came through or will not provide goods/service if denied messages come through the pipeline [44].

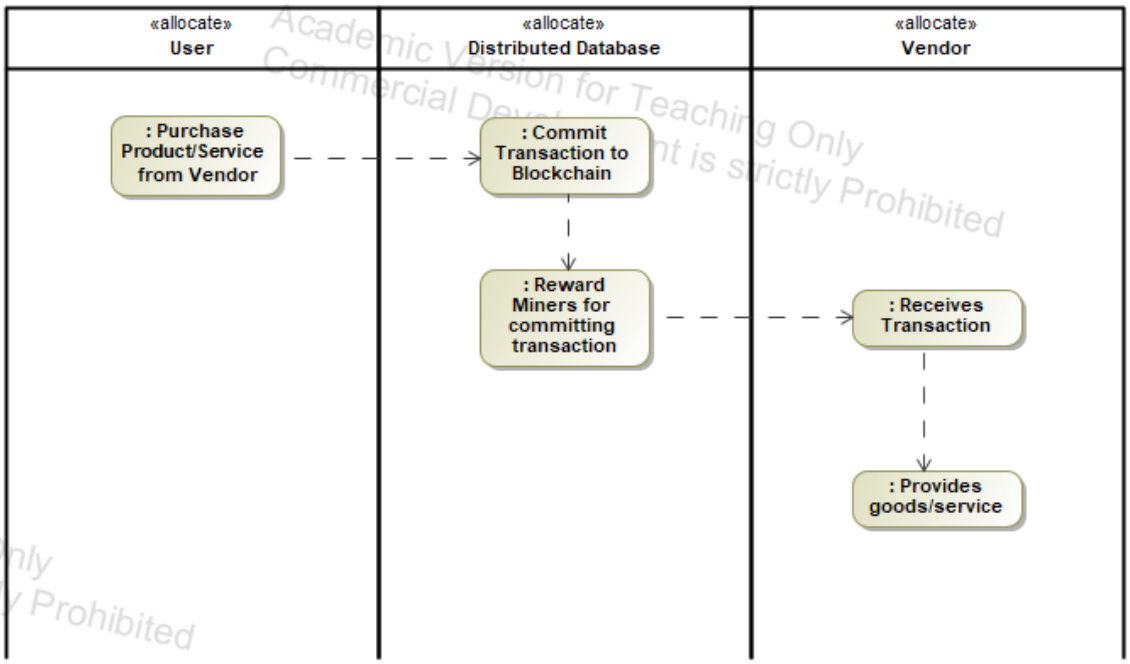


Figure 34. Simple Blockchain Transaction Process

However, the process is not fully complete. Now it is time for the Vendor to be paid out. Vendors will send the compilation of the approved payments to their payment processor (whomever they pay to use). The Payment Processor will send the appropriate transaction to the user's credit card company. The Credit card company will send that data to the user's bank. The user's bank then charges the user for the hold that they had for the transaction mentioned above. They also keep a small credit card fee. If the good/service was paid for with debit then no fee is taken. The bank then routes the funds to the vendor's bank minus more transaction fees from the

payment processor [44]. Every step of the way the vendor is not getting a full amount of money. Blockchain is planning to change this by having direct interactions between the user and the vendor. In Figure 34, the process is condensed to the user and vendor, with the distributed database holding the publicly available transaction. The user makes a purchase, then the distributed database holds the transaction. The miners are rewarded for committing the transaction and then the vendor receives the funds. The vendor just needs to provide the goods/service to finish the whole process [45].

We see how a simple blockchain was able to remove the third party from the transaction process. Is it possible to replicate blockchain for a private company and a vendor when there is no third party? Walmart and Coca Cola are private companies that have successfully implemented blockchain without having third parties in the first place [46]. So, it is feasible for DoD to implement blockchain despite not having a third party.

Fifth Decision

The next question pertains to the different rules between each participant within a system. Currently, the GFEBS process only allows one of the vendors to see their own invoice being processed. Allowing vendors to see other vendors can cause a security risk, since vendors see other transactions that the DoD has made. These transactions could be leaked to foreign adversaries. This rule would still need to be in place for the potential blockchain system which pushes us to the next question.

Sixth Decision

Will the rules be constant once they are first enacted? Since the blockchain is difficult to change once it has been deployed, all parties must agree to all the rules beforehand. This goes hand in hand with the explanation of immutable capability that blockchains possesses. The rules that everyone agrees on is part of the smart contract. So just like any other contract, it is also good business etiquette to not continuously change the contract rules.

Seventh Decision

The seventh question asks if there is a need for an objective immutable log. An immutable log will be easy to track transactions down via an audit trail as nothing can be changed once a transaction/block is added to the chain. What if there was a human error in the invoice while submitting? The GFEBS have tools to quickly correct any mistakes that happen. However, once a transaction has been entered into the blockchain, it cannot be edited or changed in any manner. "Departments and agencies having the ability to integrate transactional level control over data and write that to a blockchain make it harder to alter and easier to share. Data can be stored off chain and a hash or pointer to the data can be saved on chain, making any alteration or access apparent and traceable" [47]. Storing the "non-transactional" data off-chain creates efficient storage possibilities as the "non-transactional" data will only be hashed pointer and not the entirety of the "non-transactional" data. As mentioned before, smart contracts deploy transactions once a certain threshold is met. In the case of Walmart, the smart contract "automates all transactions and data points using GPS and IoT to track everything, including checking truck refrigeration temperatures for food shipments, said Walmart Canada, one of the country's largest employers [48]. GPS is attached to all vehicles which constantly updates the

smart contract of what is owed between Walmart and the vendor. If there is a dispute, Walmart can rely on the multiple routes taken from the trucking company as a baseline to express the price seen in the blockchain transaction. Walmart was able to reduce over 70% of invoices disputed to just 1.5% of invoices disputed after introduction to the private blockchain [35]. Since there are no humans to make human errors, blockchains are able to avoid editing with the use of smart contracts.

Eighth Decision

In the Literature Review portion of this thesis, it was determined that giving public access to potentially DOD blockchain would be unwise. Anyone, including the United States' foreign adversaries, could join the blockchain. Obviously not giving access to adversaries is highly advisable and therefore there is no need for public access.

Ninth Decision

The ninth decision would not be asked since the answer to the eight decision goes straight to the tenth decision. For sake of being thorough, let us consider if there is a need for public transactions. This would entail anyone, including foreign adversaries to read/write data onto the blockchain. For the same reasons given in the eighth decision, we see that the answer would also be "NO" to the question of "are transactions public". This solidifies that Permissionless Public Blockchain is not the right decision when it comes to a potentially DOD Blockchain. Either way, the tenth decision is the next aspect of the flowchart.

Tenth Decision

Finally, the last decision asks where the consensus is determined. The current DOD contracting system does not openly show contracting details for all vendors to see. For example, Contractor X does not see the contract information between the DOD and Contractor Y (and vice versa). Freedom of Information Act (FOIA) Exemption 4 and Trade Secrets Act prevents the disclosure of "trade secrets and commercial or financial information obtained from a person which is privileged or confidential" [49]. So, whenever a contractor learns that someone submitted a FOIA request, the contractor will use "Exemption 4 to prevent the Government from disclosing bid and proposal information, as well as other information submitted pursuant to a government contract" [50].

With a Permissioned Public Blockchain, all vendors would be able to see the transaction between other vendors and the DOD. No vendor would join this type of blockchain because contractors would use the FOIA Exemption 4 as a reason not to join. However, with a Permissioned Private Blockchain, vendors would not even know of the existence of transactions they are not privy to. As explained in the Hyperledger diagrams in the Literature Review, the Peers can be part of different blockchains and only are knowledgeable to the ones they are part of. Permissioned Private Blockchain checks all the boxes a potential DOD blockchain could be.

10-Step Blockchain Flowchart Summary

In the fifth decision, there were no third parties to remove to make Blockchain applicable. However, real-world implementation, such as Walmart's DL Freight, also did not use third parties. Although this flowchart would have ended at the fifth decision, the real-world deployment of blockchain was practical enough to continue through the flowchart. The next big

decision was determining that Permissionless Public Blockchain would not make sense for the DOD. Finally, the last decision was finding if Permissioned Public or Permissioned Private Blockchain would be ideal for DOD. With the consideration of contracts opting out of sharing private financial transactions with one another, it made the most sense for the DOD to implement a Permissioned Private Blockchain.

Regulations and Weaknesses Requirements Analysis

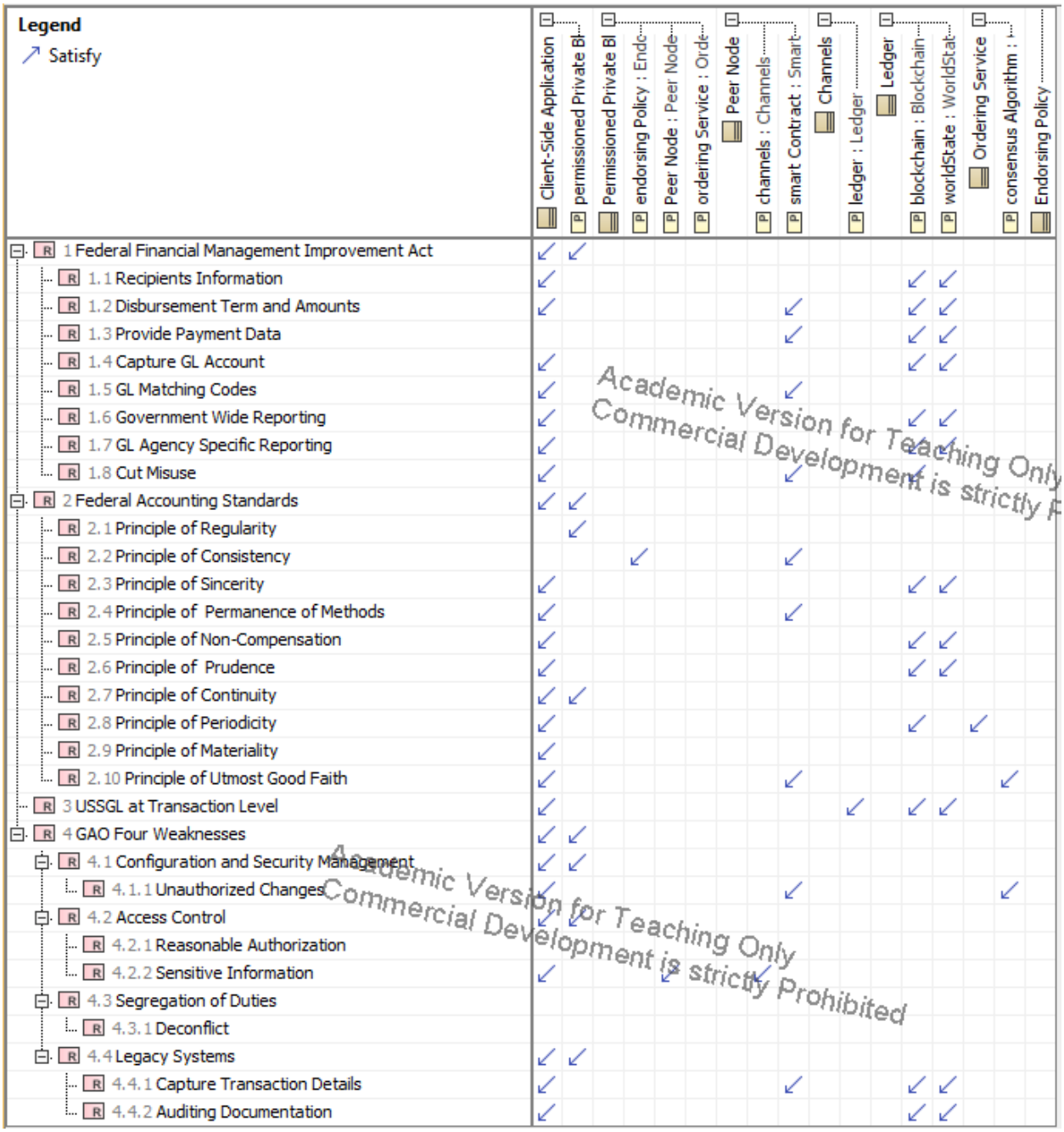


Figure 35. Regulations and Weakness Requirements Matrix (Completed)

From Figure 35, we see the Requirements Matrix filled out for the FFMIA, GAAP Principles, and GAO Weaknesses. The next few tables will give an explanation as to why a certain aspect of the private blockchain satisfies the requirements in order.

Addressing Each Requirement

Table 2. FFMIA Regulations Requirements Matrix Direct Satisfaction Explanation

FFMIA Requirements	Explanation
1.1: Recipient's information	• World State: captures the current state of the financial data for the parties involved (including recipient and donor) • Blockchain: captures all past and current GL transactions between two parties (recipients and donor) • Client-Side Application: displays recipient information for users
1.2 Determine Disbursements Terms and Amounts	• World State: captures the current state of the financial data for the parties involved • Blockchain: captures all past and current GL transactions between two parties including the disbursement amounts • Smart Contracts: captures the terms of the disbursement at all times (which has been determined by all parties prior to blockchain deployment) • Client-Side Application: displays disbursement terms and amounts for users
1.3 Provide Payment Data	• World State: captures the current state of the payment data for the parties involved • Blockchain: captures transfer of payment between two parties • Smart Contracts: automatically calculates the payment owed from one party to another based on variables for the smart contract equation

	• Client-Side Application: displays payment data and format it to align with USSGL codes
1.4 Capture GL Account	• World State: captures the current state of the party's payment account (all accounts part of GL) • Blockchain: captures all past and current GL transactions between two parties • Client-Side Application: displays GL account transactions and submits it to the USSGL (in correct format)
1.5 GL Matching Codes	• Smart Contracts: contains the necessary variables such that the transaction information can consistently be modified later to match USSGL codes • Client-Side Application: once the transaction information has been received from the private blockchain, it can be modified to fit USSGL code format at this stage
1.6 Government Wide Reporting	• World State: captures the current state of the party's payment account (all accounts part of GL) • Blockchain: captures all past and current GL transactions between two parties • Client-Side Application: once the transaction information has been received from the private blockchain, it can be modified to fit government wide reporting format at this stage
1.7 GL Agency Specific Reporting	• World State: captures the current state of the party's payment account (all accounts part of GL) • Blockchain: captures all past and current GL transactions between two parties • Client-Side Application: once the transaction information has been received from the private blockchain, it can be modified to any fit agency specific reporting format at this stage

1.8 Cut Misuse	• Blockchain: captures all past and current GL transactions between two parties, in order, so no loss of financial information • Smart Contracts: captures only the necessary variables to formulate the transaction payment • Client-Side Application: displays most up-to-date & no-loss financial information for users

Table 3. GAAP Principles Requirements (Direct Satisfaction) Matrix Explanation

GAAP Principle Requirements	Explanation
2.1 Regularity	• Permissioned Private Blockchain: all other GAAP Principle Requirements have been satisfied by some part of the Permissioned Private Blockchain
2.2 Consistency	• Smart Contracts: once the blockchain has been deployed the smart contract does not change, therefore users can rely on the contract being consistent • Endorsing Policy: This policy also is determined when the blockchain is deployed where the number and type of peers are constant
2.3 Sincerity	• World State: captures the most up-to-date account information, so it will be impartial • Blockchain: captures all transactions, so it provides impartial transaction information between all parties • Client-Side Application: displays all transaction information, therefore all the data is impartial
2.4 Permanence of Methods	• Smart Contract: When the blockchain is deployed the smart contract is set in stone and cannot be changed. This leads to fair comparison of financial data

	• Client-Side Application: displays fair comparison of financial data for users
2.5 Non-Compensation	• World State: captures the current state of the party's payment accounts which does not show bias • Blockchain: captures all past and current GL transactions between two parties. If all the information is shown then no bias can occur. • Client-Side Application: displays the raw financial data for users
2.6 Prudence	• World State: captures the current state of the party's payment accounts so no speculation is needed • Blockchain: captures all past and current GL transactions between two parties. If all the information is shown then no speculation occurs • Client-Side Application: displays non-speculated financial information for users
2.7 Continuity	• Permissioned Private Blockchain: users can read assets while others can write to assets as long as the blockchain is still deployed • Client-Side Application: front facing application continues to operate while assets are evaluated
2.8 Periodicity	• Blockchain: captures all past and current GL transactions between two parties in order. This means that authorized users can read the recorded times when transactions occurred • Ordering Service: This service distributes all the transactions in order to all the Peer Nodes, therefore showing every authorized user the recorded times when the transactions occurred • Client-Side Application: displays the recorded times when transactions occurred for users
2.9 Materiality	• Client-Side Application: disclose/displays all financial and accounting data for users

2.10 Utmost Good Faith	• Consensus Algorithm: This unchanging algorithm, that all parties have agreed on, orders data values and achieves an agreement between all the nodes. Since it is unchanging and code, it cannot be display malintent • Smart Contract: The unchanging contract has had all parties have agreed on prior to deployment of private blockchain, so no malice can occur after • Client-Side Application: displays honest transactions for users

Table 4. USSGL at Transaction Level Requirements Matrix Explanations

USSGL at Transaction Level Requirements	Explanation
3 USSGL at Transaction Level	• World State: captures the current state of the party's payment accounts when a transaction provided by supporting financial sources occurs • Blockchain: captures all past and current GL transactions between two parties • Client-Side Application: displays GL account transactions provided by supporting financial sources for users

Table 5. Four Weaknesses Requirements Matrix Explanations

Requirements	Explanation
4.1.1 Unauthorized Changes	• Consensus Algorithm: If there is typo or malintent behind a transaction then it won't get added as the consensus algorithm will read the other nodes blockchain and realize the one added does not match up with everyone else's ledger. • Smart Contract: All parties have agreed on the unchanging contract prior to deployment of private blockchain, so no malice can occur after.

	• Client-Side Application: displays authorized changes for users
4.2.1 Reasonable Authorization	No, this is an administrative requirement where people may have needed access to confidential material at a certain point, but their privileges have not been revoked yet. Another reason could be they were mistakenly given access to this sensitive information.
4.2.2 Sensitive Information	• Channels: only Peer Nodes within a Channel have access to the financial transaction. All other Peer Nodes do not know the existence of the Channel • Smart Contract • Peer Node: part of multiple channels. If a Peer Node is not part of Channel, then it will not even know it's existence. Therefore, only need-to-know financial data can be seen/written to. • Client-Side Application: displays GL account transactions for authorized users only
4.3.1 Deconflict users from key roles and function	No, this requirement requires the administration to satisfy. It is the administration's job to not put users in a position where a conflict of interest may arise. The administration would need to know the background of its users and then assign key roles. Once the key roles have been assigned then a private permissioned blockchain separate people based on authorization level
4.4.1 Capture Transaction Level Details	• World State: captures the current state of the party's payment accounts when a transaction provided by supporting financial sources occurs • Blockchain: captures all past and current GL transactions between two parties • Smart Contract: can be programmed to capture whatever details are necessary for the transaction • Client-Side Application: displays transaction level details for users

4.4.2 Contain documentation for auditors	• World State: captures the current state of the party's payment account (all accounts part of GL) • Blockchain: captures all past and current GL transactions between two parties in order such that auditors can see the transaction flow • Client-Side Application: displays/formats the Ledger of each Peer Node for auditors

Requirements Matrix Summary

A Permissioned Private Blockchain contains components to successfully tackle FFMIA Regulations and GAAP Principles. This is shown via Tables 2-4, as private blockchain satisfying all regulation between FFMIA and GAAP. Table 5 shows that there are parts of the GAO Weakness that cannot be satisfied by private permissioned blockchain alone. These include Requirements 4.2.1 and 4.3.1, where it was determined that the administration of the agency would be ones to satisfy these weaknesses' requirements. It is safe to conclude that inclusion of Permissioned Private Blockchain will not break any rules or regulations that currently stand.

Performance Metrics Analysis

Cost Analysis

The DEAMS system is divided into two stages, Increment 1 and Increment 2. DEAMS Increment 1 "uses commercial off the shelf enterprise resource planning software to provide accounting and management services" [53]. Ideally it should be able to "provide financial data to decision makers", "provide budget formulation, funds, distributions and cost modeling", "manage DOD appropriated working capital funds, and process budgetary, accounting and vendor pay transactions" [53]. Increment 1 was completed in 2020 and has added 17,000 users

across 170 different locations [7]. Increment 2, now known as DEAMS Continuous Capability Development, is on the way and is scheduled to add another 4,500 new users. Eventually the goal is to fully migrate and replace the legacy platform, GAFS-R, to DEAMS. The system has had major delays in its way of deployment which also cost more than what the original budget was set for. The GAO explains in their estimates that "in October 2010, [GAO] reported that the life cycle cost increased to about $2 billion through fiscal year 2027 with an expected full Prior Reports on DOD Financial Management deployment in fiscal year 2017—a 3-year slippage from the full deployment date reported at program initiation" [7]. As of the latest GAO reports in 2021, the cost has increased to a total life cycle cost of $3.4 billion [7].

In GAO GFEBS 2012 report, the Army estimates the life cycle cost estimate for GFEBS to be approximately $1.3 billion in 2012 money [54]. When adjusted to inflation, the amount is near $1.68 billion for the estimated total life cycle cost of GFEBS.

For the DL Freight Blockchain, there is not a comprehensive document with the cost breakdown. However, with Walmart Canada's public statements, we can get a max price of the process. Walmart announced that there would be a "$3.5 billion [Canadian dollars CAD] investment over the next five years aimed to generate significant growth and to make the online and in-store shopping experience simpler, faster and more convenient for Walmart's customers" in 2020 [55]. In the same article, Walmart mentions that $1 billion CAD will go towards remodeling and opening new stores while another $1.1 billion CAD would be spent on two new distribution centers [55]. Finally, the article mentions that DL Freight expansion will be part of the $3.5 billion, although it does not refer to how much will be spent. Since DL Freight is neither

part of remodeling or the creation of new distribution centers, we are going to assume the maximum expense of the DL Freight would be:

$$\$3.5 \text{ billion} - \$1 \text{ billion} - \$1.1 \text{ billion} = \$1.4 \text{ billion}$$

The 1.4 billion price tag may include other non-blockchain expenses. However, with little information on the breakdown of Walmart's investments, we will assume the worst-case scenario as all 1.4 billion dollars towards the blockchain effort. At the time of announcement in July of 2020, the conversion rate would change from $1.4 billion CAD to $1.03 billion USD.

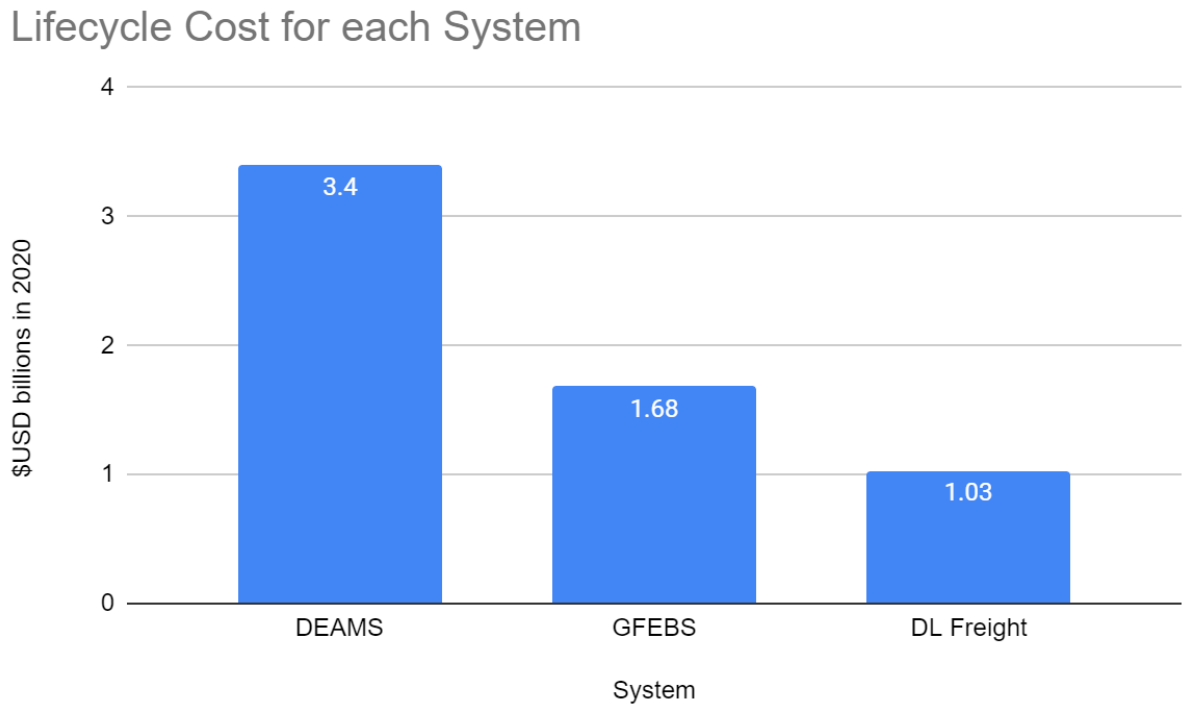


Figure 36. Life Cycle Cost of each System

Figure 36, we see the Lifecyle Cost for each system where the y-axis is the $USD billions in 2020. DL Freight cost less than both DEAMS and GFEBS. However, we do not know how

DL Freight Lifecyle Cost could change if it was put in the same DoD environment as DEAMS and GFEBS.

Time Analysis

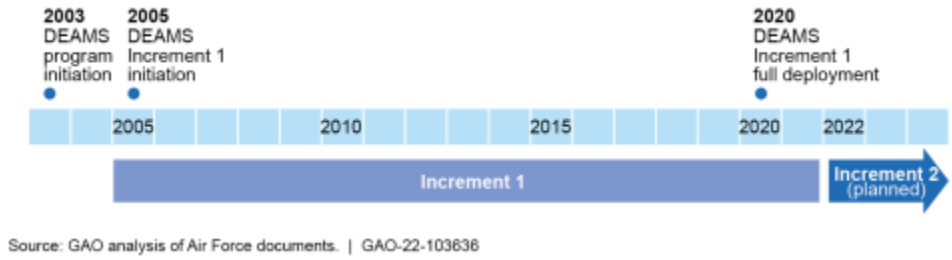


Figure 37. DEAMS's Increment 1 and Increment 2 Projected Timeline

As mentioned previously, the DEAMS system has been setback many times. In 2010, it was determined that the full deployment of Increment 1 would be in 2017. However, during 2014, it was decided that Increment 1 would not be able to finish by the 2017 deadline, and would be pushed back to 2020. Increment 2, now known as DEAMS Continuous Capability Development, is scheduled to compete by 2031. The GAO reports, "The Air Force has recently identified estimates of cost, capabilities, and schedule for the DEAMS Continuous Capability Development from fiscal years 2022 to 2031" [7]. Looking at the previous statement and Figure 37, the partial timeline completed by GAO, we can see that the whole DEAMS process, including Increment 1 and 2, is estimated to take a total of 28 years from initiation to completion.

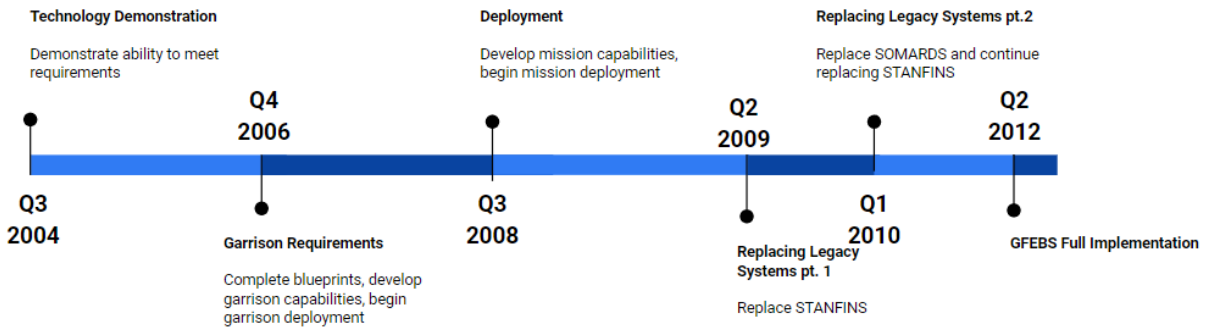


Figure 38. GFEBS Timeline

According to the GAO GFEBS 2012 report, Army started the GFEBS process in October 2004 and was "fully deployed to all intended users by July 2012" [54]. So, it took close to 8 years for GFEBS to be fully implemented. In the 2007 GFEBS Schedule PowerPoint, John Miller breaks down the first years of GFEBS timeline into Technology Demonstration from the beginning to Q4 2006, Garrison Requirements from Q4 2006 to Q3 2008, and first deployment from Q3 2008 to Q2 2009 [56]. However, the GFEBS Deployment Schedule was created in 2009 and gives a better look at the process from that point onwards. This PowerPoint dissects the timeline again by displaying Replaying Legacy Systems pt. 1 from Q2 2009 to Q1 2010 and Replaying Legacy Systems pt. 2 from Q1 2010 to Q2 2012 [57]. Finally, in Q2 2010, GFEBS would be fully implemented (seen in Figure 38).

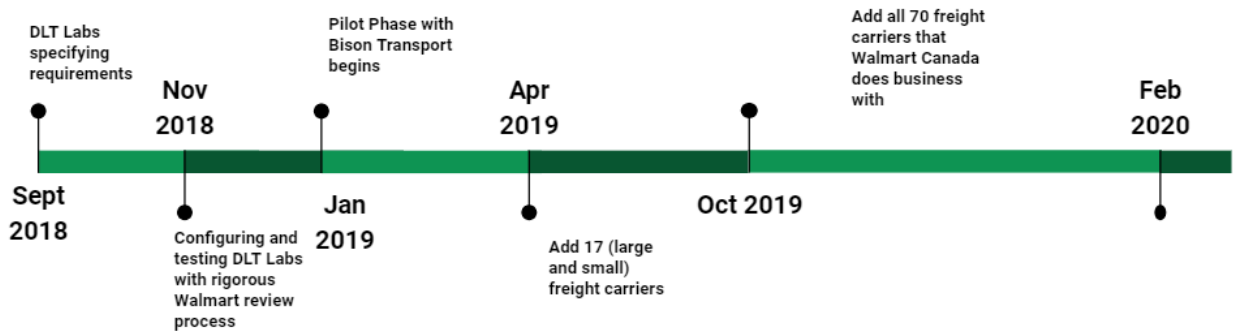


Figure 39. Walmart's DL Freight Implementation Timeline

The private blockchain system that we will be comparing the existing financial system to is Walmart's DL Freight blockchain. In 2018, their supply chain and logistics team wanted to know if there was any existing technology to help improve the invoicing problems they were dealing with. Many solutions were given; however, Walmart Canada went with DLT Labs as their provider of a blockchain platform. "The development cycle took only eight months from conception to live deployment. The first two months were spent specifying the requirements for the engagement. The next two months were spent configuring and testing DL Freight to meet specifications. The pilot phase, which included Bison Transport, one of Walmart Canada's largest freight carriers, took four months" [5]. The configuration process then only took two months which passed audits from Walmart Canada. The proof-of-concept phase was skipped as DLT Labs had proven their platform was satisfactory. In January 2019, DLT Labs went straight to the production pilot phase with Bison Transport being one of the first companies to attempt the new system. According to a Technical Communicator at DLT Labs, Abhisek Mohanty, Walmart was able to onboard the rest of the carriers (70 total) by February 2020 [58]. This means that the Known Time is 17 months. Figure 39 encapsulates all the information above in an easy-to-read timeline.

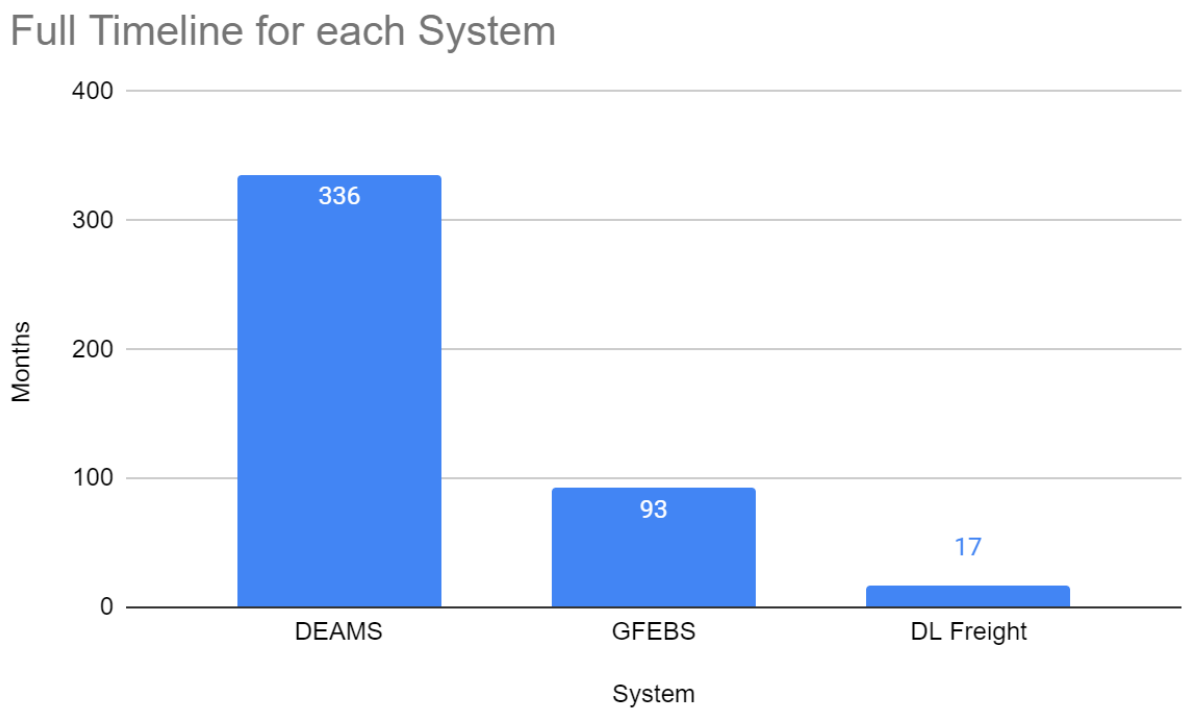


Figure 40. Full Deployment Timeline of Each System

For Figure 40, we can condense the timelines for each system and we see that DEAMS, GFEBS and DL Freight will be implemented in 336 months, 93 months, and 17 months, respectively. Once again, we are not sure how DL Freight Deployment will change based on many different DoD circumstances.

Throughput Analysis

As mentioned previously, Throughput is the number of invoices processed annually by each system. The total number of DEAMS invoices in Q1 2022 was around 70,000 [51]. If we scale the number of invoices to one year, then we get 280,000 invoices annually. It was previously mentioned that GFEBS processed $140 billion annually in 2012. At the same time, it also processed approximately 1 million transactions a day [52]. If we scale the $140 billion to

$180.7 billion dollars, then the same scaling factor means that the 1 million transactions per day would be 1.3 million transactions per day. For the DL Freight, the Hyperledger foundation case study mentions that a total of 200,000 invoices get processed over the course of 6 months [35]. Scaling it up to a year, this amounts to 400,000 invoices over 1 year.

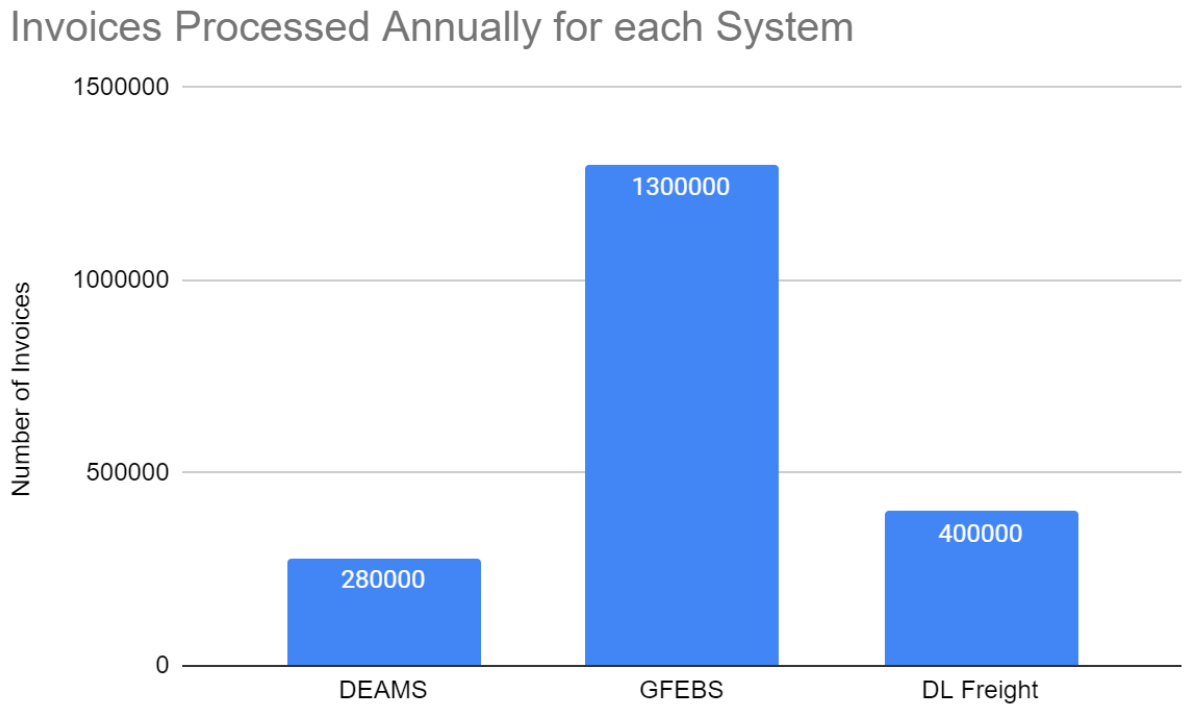


Figure 41. Throughput (Invoices) for each System

In Figure 41, GFEBS processes the greatest number of invoices which makes sense as this system has the most amount of money processed. This table does not represent the max throughput for each system, just the average throughput annually. There is not sufficient data determining the absolute limits for each system.

Benchmark Analysis

DEAMS Increment 1 improved drastically from a 2015 report. The DEAMS 2015 report talks about the 2014 Fiscal Year. In the 2014 fiscal year, DEAMS "did not meet the 95 percent threshold of balancing of timely accounts (i.e., monthly, quarterly, annually)" [59]. In the 2022 Procure-2-Pay Presentation, we see the percentage of invoices that are paid within 30 days of invoice submission date is 81% [51]. During FY2014, DEAMS was only able to balance 97.5% of Treasury funds [59]. During the FY2018, it was determined that DEAMS was now able to balance 98.8 percent of US Treasury funds [53]. This shows that DEAMS has an error rate of 1.2%. From the 2022 Procure-2-Pay Presentation, we see that the average number of days from invoice submission date to approval date is about 5 days from FY22 [51].

In accordance to a 2013 OMB report, "GFEBS consistently experiences approximately a 40% failure rate requiring invoices to be manually posted in GFEBS to correct errors" [101]. Concurrently, a pilot program called Supplier Self Services (SUS) shows the failure rate going from 40% to 7%. After that 2013 OMB report, SUS has been implemented since and no more error rate detail has been publicly available. We are going to assume that GFEBS's (with SUS implemented) error rate is at 7%. In the same Procure to Pay presentation mentioned recently, GFEBS has an average of 5 days from invoice submission to approval date. Additionally, the percentage of invoices paid within 30 days is around 79%.

Shannon Hamilton, marketing lead at DLT Labs, comments that all the invoice disputes are just easily resolved discrepancies [34]. Both parties involved wanted the manual reviews to be fresh in their minds, so investigating discrepancies immediately is done with the use of DL Freight. The average rate of approval of invoice has not been given publicly, but we do know

from the Walton presentation that if there are no discrepancies, then the invoicing is immediate [36]. For the sake of argument, let us put the average rate to be 5 minutes even though unmodified Hyperledger has the capability of close to 100 transactions per second [60]. Another reason for the 5-minute average is because DLT Labs ensures that all the invoice disputes are just quickly fixed discrepancies. All the Walmart Freight invoices were paid on time via the Walmart ERP systems as the Walton Presentations shows that "over payments/delayed payments were eliminated" [36]. All the invoice disputes dropped from 70% down to around 1.5% [35]. Since all invoices were paid on time (mentioned in this paragraph), that means that there are no errored invoices post-manual review.

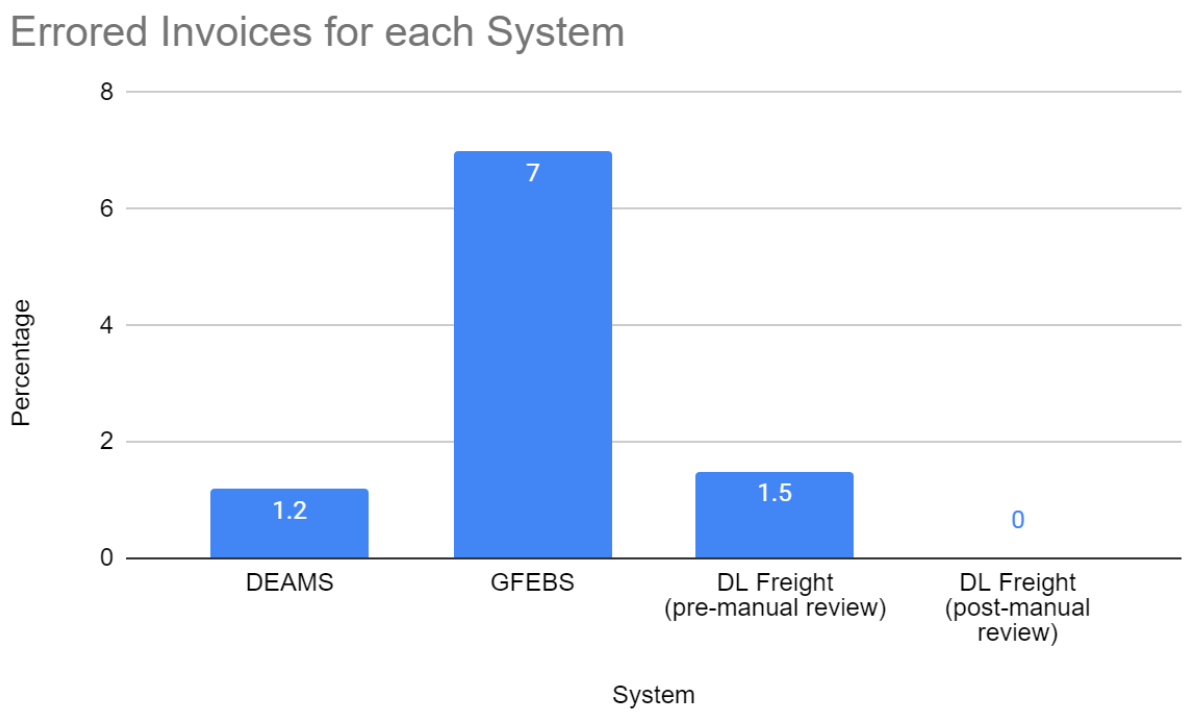


Figure 42. Error Rate (Percentage of Invoices) for each System

Figure 42, shows us the percentage of Errored Invoices for each System. pre–manual review, it appears that DL Freight has a higher rate of errors than DEAMS, but for post-manual review, DL Freight is able to drop the percentage of errors down to 0%.

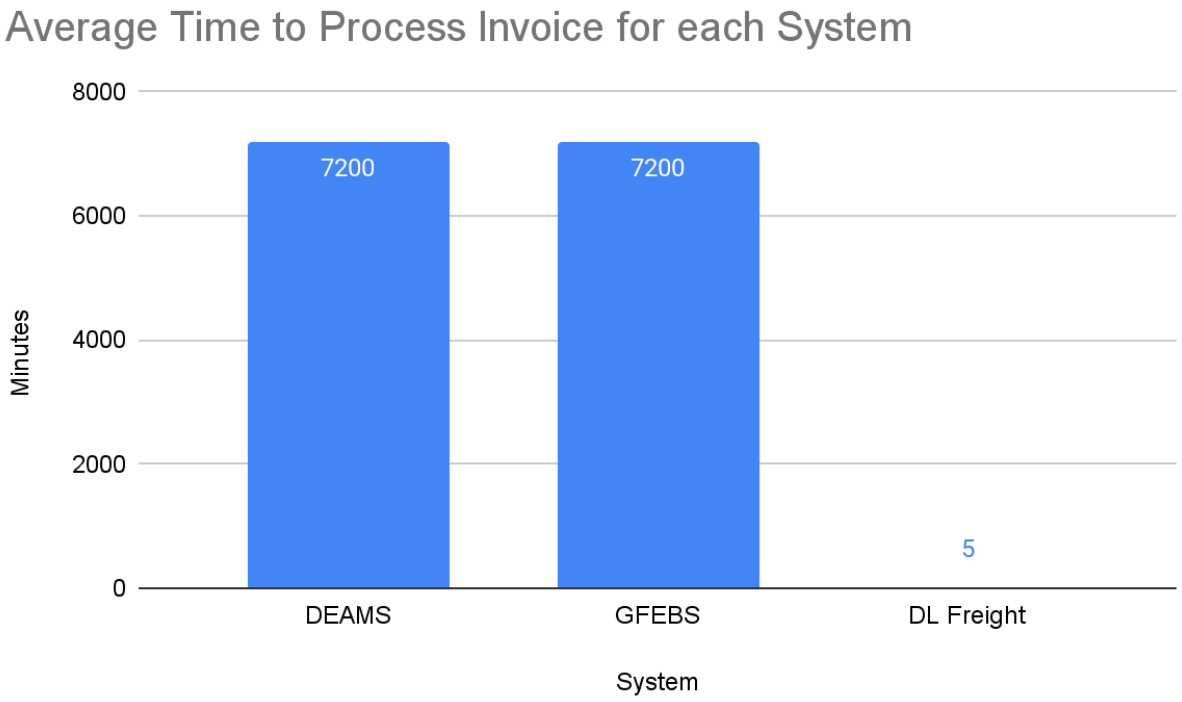


Figure 43. Latency 1 (Average Time to Process Invoice) for each System

In Graph 43, the average invoice process for both DEAMS and GFEBS are equal, but the invoices between Walmart and their vendors are nearly instant. DEAMS and GFEBS take 1440 times longer than DL Freight.

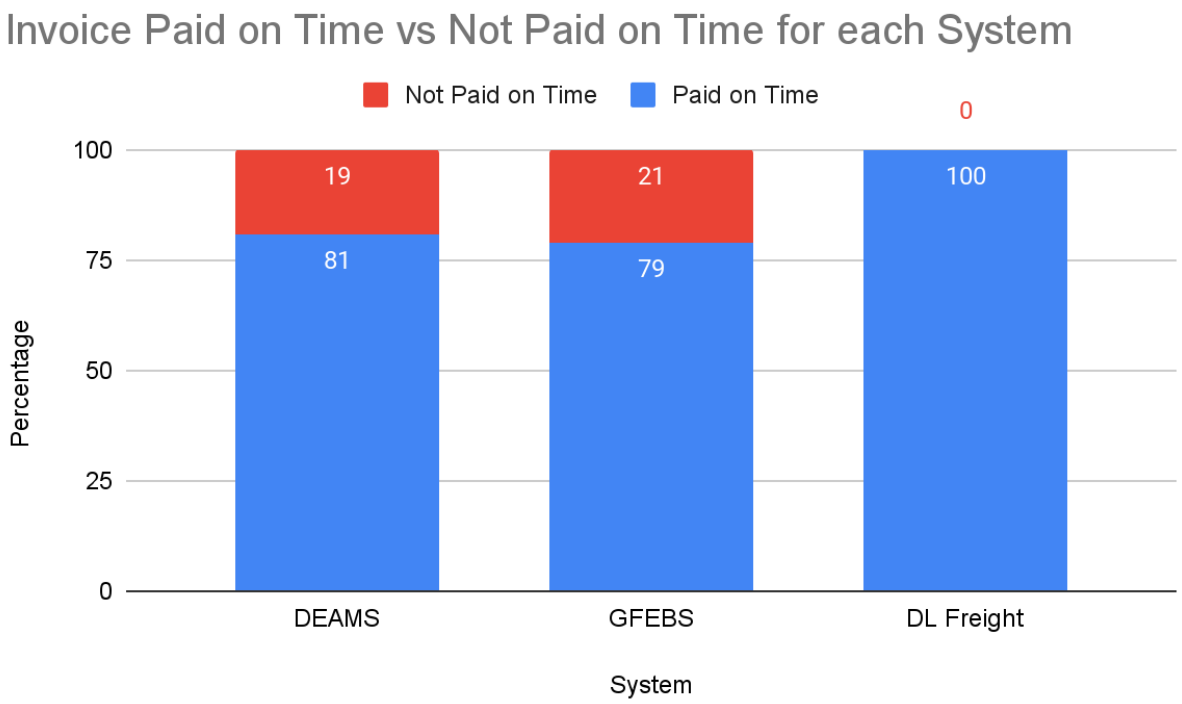


Figure 44. Latency 2 (Percentage of Invoice Paid on Time vs Not Paid on Time) for each System

In Figure 44, we see each systems invoices ratios between “paid on time” and “not paid on time”. DEAMS and GFEBS have approximately the same percentage of delayed payments while DL Freight was able to pay everything on time.

Performance Summary

Table 5. Summary of Performance Analysis

Metrics	DEAMS	GFEBS	DL Freight
Cost ($USD Billion)	3.4	1.68	1.03
Time (months)	336	93	17
Throughput (# of invoices)	280000	1300000	400000
Error Rate (%)	1.2	7	1.5
Latency 1 (min)	7200	7200	5
Latency 2 (%)	81	79	100

In Table 5, we see the summary of the Performance Analysis for three systems: DEAMS, GFEBS, and DL Freight. The Performance Analysis includes Cost, Time, Throughput, Error Rate, Latency. As mentioned previously, we do not know how DL Freight will change in theses metrics once it is implemented in an DoD environment. Therefore, we will not be comparing the Performance Metrics in this paper.

DoD Implemented Permissioned Private Blockchain

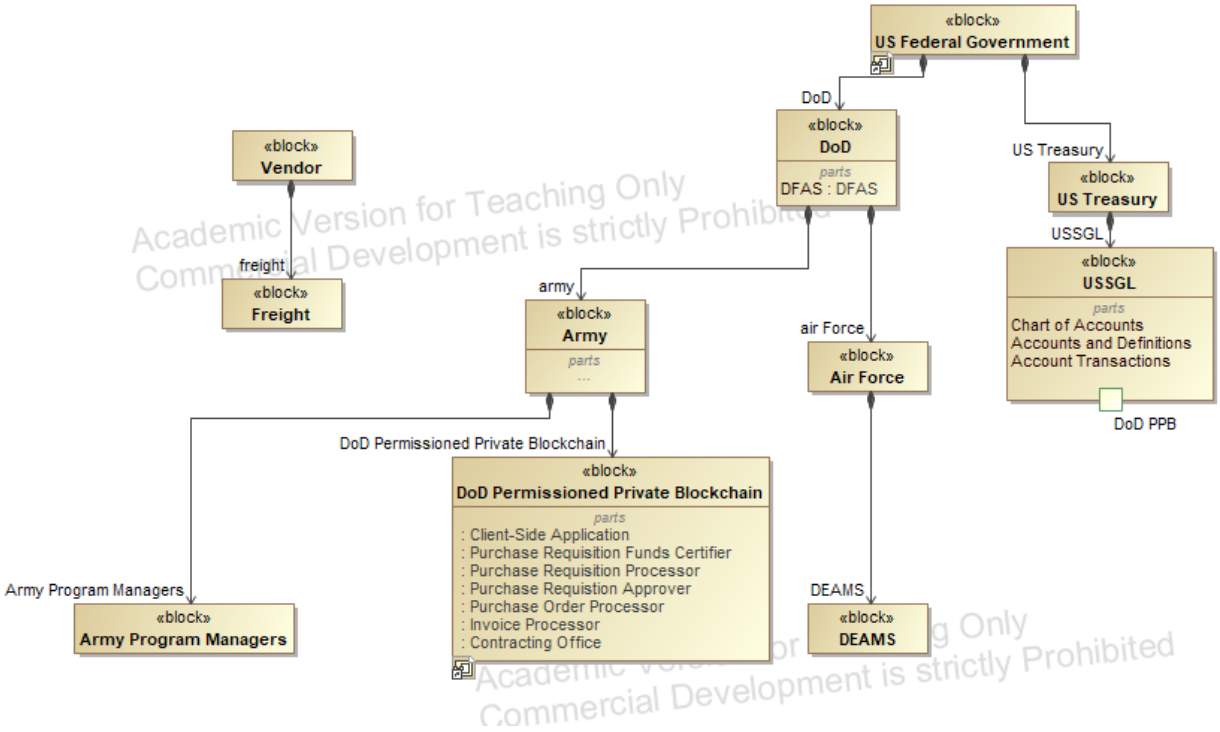


Figure 45. Block Definition Diagram of DoD Permissioned Private Blockchain with DoD systems and Vendor

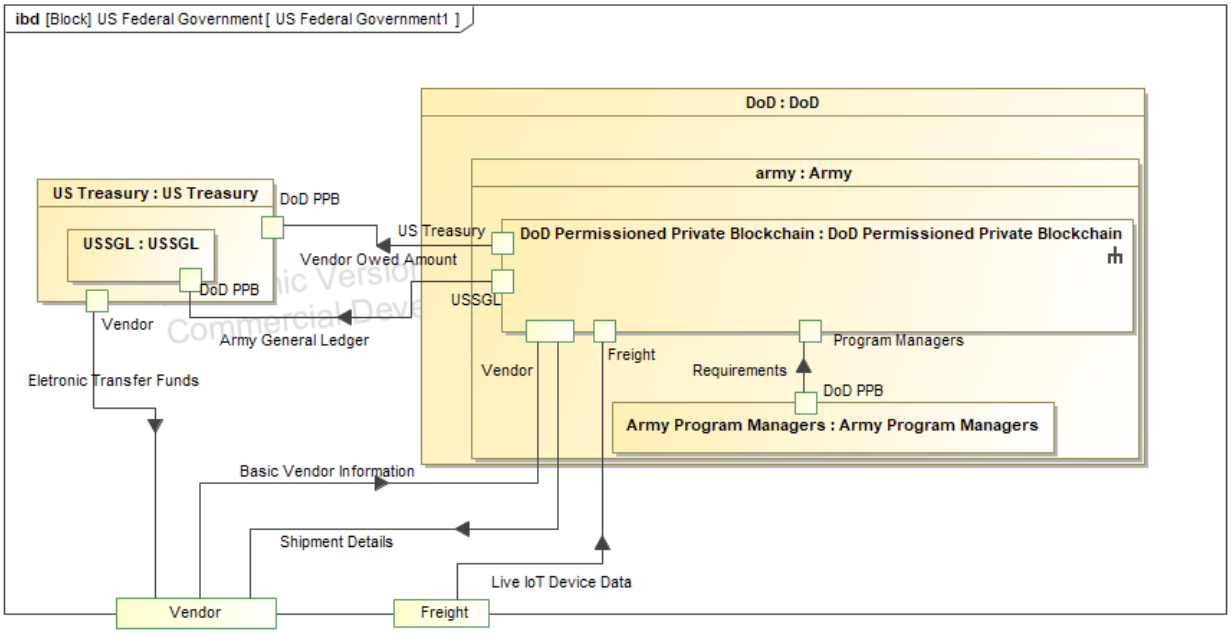


Figure 46: Internal Block Diagram including Permissioned Private Blockchain

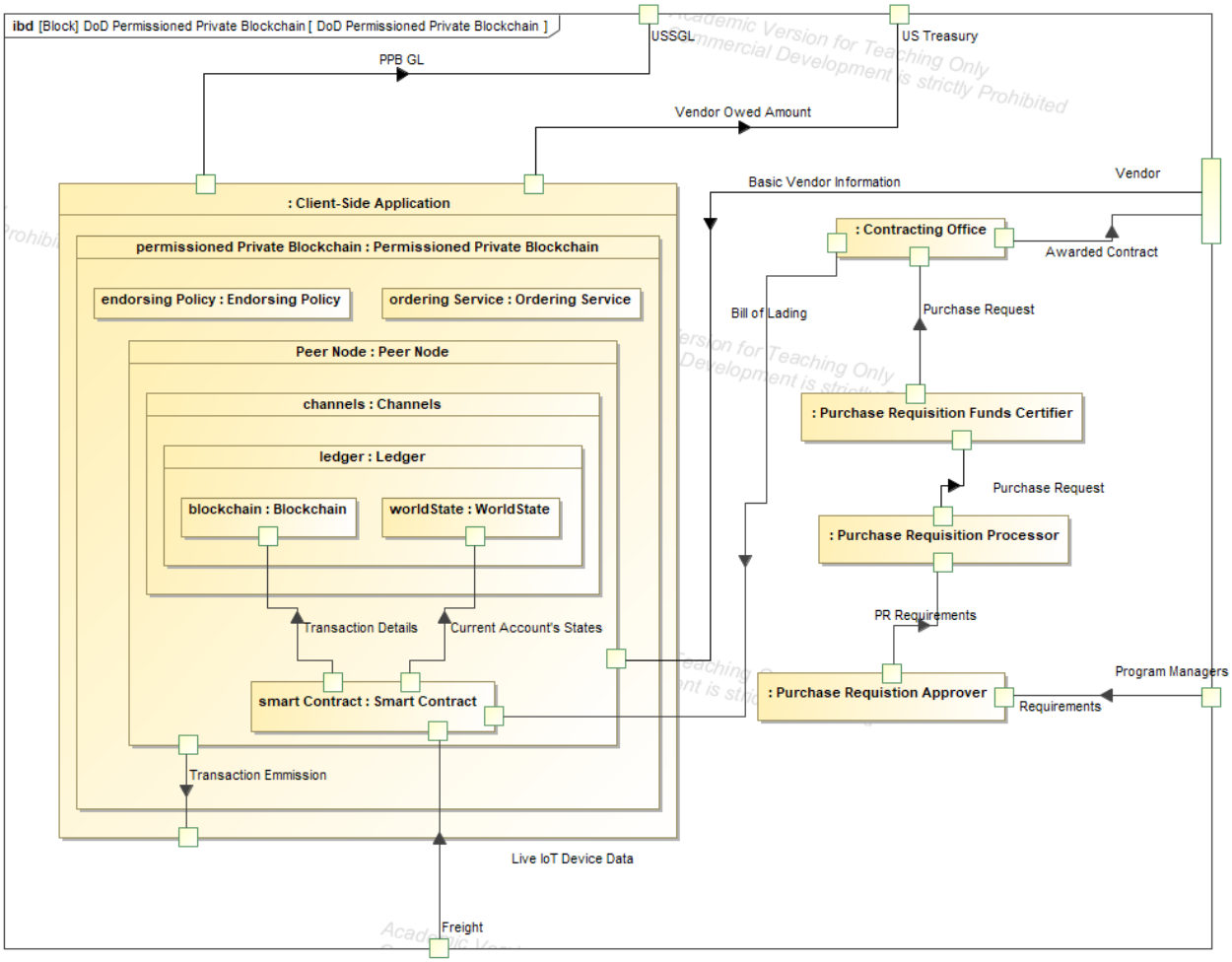


Figure 47: Internal Block Diagram of DoD Permissioned Private Blockchain

Figures 45-47 display the potential application of a Permissioned Private Blockchain in the DoD. One disclaimer for these figures is that every branch has their own way of running their ERP and the replacement of an ERP may differ between military branches. Another disclaimer is that there may be a lot of different ways of using Permissioned Private Blockchain, from minimal insertion to complete overhaul. However, Figure 45's block diagram strikes a balance. Finally, the last disclaimer is that we will be using Figure 15's GFEBS Block Diagram as the baseline for the application of Permissioned Private Blockchain. However, this paper's goal is not to replace GFEBS specifically.

Figure 36 used a majority of the established entities from the GFEBS Block Diagram (Figure 15). The parts that differ between the block diagrams is the removal of GFEBS and no longer being reliant on DFAS to pass the information over to the US Treasury to pay the vendor. In the internal block diagram (Figure 47) for "DoD Permissioned Private Blockchain", we see all the parts of the blockchain. Similar process occurs within the GFEBS internal diagram (Figure 17) as the Program Manager's Requirements are processed by Purchase Requisition Approver, Purchase Requisition Processor, and Purchase Requisition Funds Certifier. The following step, the Purchase Request will be sent to the Contracting Office who will find the best vendor for the job. Once the awarded contract has been set the next steps are where tasks differ from the original GFEBS version. The Smart Contract (shipment equation that has already been established) waits for the new Purchase Request that includes the Bill of Lading form the Contracting Office. The Smart contract is constantly taking "Live IoT Device Data" from the Vendor's Freight. This way all variables of the smart contract equation will be calculated for when the transaction is added to the blockchain. The world state (which includes all accounts' financial data) is also updated as transactions occur. The Peer Node that houses the Blockchain and World State emits the transaction such that the client-side application can display the data such that the Vendor and Contracting Office can see that there is no malice in the transaction. The Client-Side Application (CSA) is live as the new IoT data keeps updating the smart contract equation. This cuts down on all the "Payment Certifiers and Processors" and "Good Receipt Processor" as live transactions are continuously happening. Once live updates are over, indicating end of delivery, the CSA can format the Ledger to match the USSGL and US Treasury payment format. Finally, the last step is to pay the vendor via the US Treasury using Electronic Transfer similar to the GFEBS model.

A possible alternative could be the US Treasury sending CBDC instead of an Electronic Funds Transfer to the vendor. This would require the adoption of the Digital Dollar Project and further research to see if there is a major difference in the process of using CBDC instead of normal currency.

Summary

From the 10-Step Blockchain Flowchart Analysis, we determined that Permissioned Private Blockchain would be more ideal than Permissioned Public Blockchain and Permissionless Public Blockchain. In the same portion of the Analysis, we determined that smart contracts (a vital part of the Permissioned Private Blockchain) works when the contract can be broken down to an equation with variables. The variables can be updated live to constantly give the feedback for how much the vendor is owed at any given time.

In the Regulation portion of the analysis, we figured out that Permissioned Private Blockchain passed all the rules that are part of the FFMIA and GAAP Principles. In the GAO's Weakness portion of the Requirements Matrix, Requirements 4.2.1 and 4.3.1 were unable to be solved by a potential blockchain system as administrative actions could satisfy those two requirements. Other than those two requirements, the rest were able to be satisfied by different parts of the Permissioned Private Blockchain.

The Metrics portion of the Analysis, displayed the Cost, Time, Throughput, Error Rate, and Latency for the three systems: DEAMS, GFEBS, and DL Freight. A comparison would between the metrics is not in the scope of this paper. We do not know how DL Freight's Metrics will change when it is implemented in a DoD environment.

The last aspect of the Analysis is the theoretical look at a Permissioned Private Blockchain (modeled after Walmart Canada's DL Freight) within the DoD. Figures 45, 46, 47 replace GFEBS and DFAS with the Permissioned Private Blockchain, while connecting to all other major entities within the DoD. This paper chose to replace GFEBS because the breakdown of the GFEBS process was already documented in this research, making it easier for the reader to visualize changes. The replacement could be possible with any of the other DoD ERP (if necessary and appropriate). The biggest changes of the new process are the removal of "Payment Certifiers and Processors" and "Good Receipt Processor" as Freights will input smart contract variables live. The next and final section of this paper is the Conclusion which will summarize all questions and findings concisely.

V. Conclusions and Recommendations

Introduction of Research

This chapter will start with reiterating the research question mentioned at the beginning of this paper. Next, the summary of the analysis shall be discussed. Finally, this chapter will close with a recommendation of action and further research.

Summary of Research Questions

This research focused on the extent to which blockchain technology can be used by the DoD to fix weaknesses found in the most recent report of audits. There were four key areas of weakness in the Information Technology portion of the audit. This paper has answered the three major questions and few sub questions regarding the current state of the DoD financial system as well as blockchain solutions.

Summary of Research Answers

What are the drawbacks of the current DoD financial systems?

The drawbacks were highlighted when going over the GAO Weakness portion of the Methodology and Analysis. To summarize, GAO made a call to action to configure security management, control access, segregate duties, and decommission legacy systems. Configuring Security Management includes monitoring changes to avoid unauthorized adjustments. This goes along with the second weakness, Access Control. This means that users will only have access based on their authorization level. If users have the right authorization level, then ideally there would be less unauthorized changes. The next weakness is the Segregating Duties to avoid conflict of interest. Finally, according to GAO, the Legacy Systems do not do a good job

capturing transaction details. This in turn forces users of the legacy system to resort to manual recording which is hard to reproduce when auditing occurs. The goal is to fix all these weaknesses so that GAO changes the auditing from disclaimer of opinion to clean audit (free from financial misstatements).

Does blockchain meet all requirements and remediate current drawbacks?

Permissioned Private Blockchain had to satisfy the FFMIA, GAAP Principles and GAO defined Weaknesses. The requirement matrix, seen in Figure 35, shows which parts of blockchain satisfies which requirement. The blockchain was able to satisfy all aspects of the FFMIA and GAAP Principles. When it came to the weakness, the blockchain was not able to satisfy Requirements 4.2.1 and 4.3.1. These requirements were deemed to be only satisfied via administrative intervention. Besides those requirements, blockchain was able to satisfy the rest of GAO defined Weaknesses' requirements

What are DoD financial regulations and current practices?

The current practices for the DoD, in the most basic manner, are Vendors being awarded contracts based on the requirements set by Program Managers. The invoices are then sent by the Vendors once the delivery/service has been done. GFEBS operators will format the invoice one way to add to the Army General Ledger and another way as Ready-to-Pay File for DFAS. The Army General Ledger is once again reformatted for the USSGL while the Ready-to-Pay Files is sent to the US Treasury where an Electronic Payment is made for the Vendor.

The current financial regulations include following the "Federal Financial Management Improvement Act of 1996, federal accounting standards, and USSGL at the transactional level"

[7]. The FFMIA has 8 requirements. The federal accounting standards closely adheres to the ten Generally Accepted Accounting Principles (GAAP). Finally, the "USSGL at the transactional level" is similar to one of the FFMIA requirements.

What type of blockchain are most appropriate for current DoD practices? And why?

From the 10-Step Blockchain Flowchart, we determined that a Permissioned Private Blockchain would suit the DOD or any government agency the best. This decision was made over the other two popular choices for blockchain: Permissionless Public Blockchain and Permissioned Private Blockchain. It was easy to dismiss Permissionless Public Blockchain as this type of ledger would let anyone, including foreign adversaries join, read, and write on the same ledger that the DOD and its vendors/contractors would be using. The transactions would also be made public jeopardizing the integrity and confidentiality of military transactions. The reason that Permissioned Private Blockchain was chosen over Permissioned Public Blockchain is the Freedom of Information Act (FOIA) Exemption 4 which states that trade secrets and financial information between contractor and government agency can be made confidential. Contractors and vendors won't be willing to join a blockchain network where all their financial information can be read by competing contractors and vendors. This is the current (no blockchain) state of contractor/government agency relationship. In order to continue this relationship, Permissioned Private Blockchain uses Channels. These Channels allow Contractor X to do business with the DOD without even knowing the transaction happening between Contract Y and the DOD (and vice-versa). Each relationship is done on different channels recreating the same environment found in the current (no blockchain) system.

What type of transactions within the DoD can blockchain optimize?

The smart contract within all blockchains sets the rules in code where both parties agree to beforehand and adhere to at all times. Smart contract is formulaic with the use of variables (known and/or live). DL Freight, Walmart Canada's full production blockchain system, uses IoT devices within the freight trucks to send live information about temperature, GPS, etc. This information can be added on the known/consistent data (such as shipment details) to be variables where the smart contract formula produces an invoice in real time. Contract disputes like the F-35 Primer situation would not be resolved with smart contracts because putting primer on the plane cannot be broken down into a formula with variables.

What current systems/policies would need to change to accommodate a blockchain solution?

With the use of Permissioned Private Blockchain in the DoD, some parts of the GFEBS are either removed or reworked (Figures 45, 46, 47). This paper uses GFEBS as a choice of replacement, because the GFEBS process is already documented in the Literature Review making it easier for readers to follow along. The new process will see the elimination of "Payment Certifiers and Processors" and "Good Receipt Processor" as Freights as live IoT data will come from Freights to populate the smart contract's variables. If the DoD is keen on a blockchain solution, then contracts would need to be formulaic such that it can be the smart contract. However, if a contract cannot be broken down into variables, then the DoD would still need the current process to work these types of non-formulaic contracts.

What are some challenges the DoD could face if they were to transition to a blockchain based solution?

Yes, this blockchain can be used to track government transactions, in certain cases. This will be fleshed out in the next couple paragraphs. The incorporation of 10-Step Blockchain Flowchart, Regulation and Weaknesses Analysis, and Performance Metrics has led to the realization that blockchain is a solution for DOD auditing problems.

What metrics can be used to compare DoD financial systems with a possible blockchain solution

The systems chosen for comparison were: DEAMS, GFEBS, and Walmart Canada's DL Freight. DEAMS was chosen as this was the system with the most up to date data since it is currently still in progress. GFEBS was chosen as it is an already established DoD ERP that has a lot of publicly available data. Finally, DL Freight was chosen because it is an already established Permissioned Private Blockchain which could be replicated within the DoD.

The metrics this paper uses are: Cost, Time, Throughput, Error Rate and Latency. Cost Metrics observes the Lifecyle Cost for each of three systems. The Time Metrics uses the full development timeline for each system and converts into months. The Throughput Metric displays the number of invoices process annually by each system. The Error Rate is the percentage of incorrect invoices. DL Freight will have two parts: pre-manual review and post-manual review. Pre-manual review is only the blockchain running while the post-manual review takes a lot at the errors and corrects them. The Latency is divided into two parts: Average Time to Process Invoice and Percentage of Invoice Paid on Time. This way we can see how fast

Invoices are paid off and if they are paid within their respective deadlines. Table 5 shows more details of all the Metrics for each system.

Study Limitations

This study was limited by lack of data, difficulty to access data, and possible exaggerated data. There were many instances where only old versions of the data/model exist and newer models have been mentioned, but no data/model to back up the claim. Since this thesis covers the financial aspects of the DOD and vendors, many of such financial statistics will not show up as unclassified which makes it hard to get to. Another way data is difficult to access is when it is hidden behind a private company. Companies only will show the barebones of financial data for their investors, so it is hard to get a breakdown of certain expenses and profits. Private companies also may use Public Relation (PR) tricks to embellish accomplishment while downplaying failures. These companies may not report everything they have tried, so trying to find where private blockchain was unsuccessful was difficult to find. Companies only like to show off when they have done something to get a return on investment.

Recommendations for Action (if applicable)

Simplify DOD contracts

Government agencies, within the DOD, handle many different types of contracts. The call for action is to find out what DOD contracts can be simplified to variables in formulas. Similar to the DL Freight breaking down freight logistics to formulas, the DOD can do the same with its own freight logistics. Handling large scale inventory could be simplified into formulas that include IoT.

Decide between COTS or In-House Implementation

The implementation of IoT devices connecting to a Private Blockchain has already been established in private industry. This is done by blockchain development companies whose sole job is to tailor fit the blockchain to an already existing system. There are talented coders within the DOD, but not many will be experienced in coding in blockchain programming languages. The recommendation is to conduct a tradeoff analysis between blockchain developer company and DOD blockchain team to determine which group can implement a Private Blockchain.

Recommendations for Future Research

A comptroller or other high financial entity within a DOD agency conducts a formal inquiry of all the same metrics to obtain reliable first-hand (classified) data. All data obtained in this paper was unclassified, so there could be data omitted due to its classified nature. The need for a different point of view would also be of benefit because these are the same people that would be using a potential blockchain solution. Another possible future research would involve using the metrics outline in this paper and comparing DEAMS and GFEBS against DL Freight. Ideally the more DoD ERP used, the better the results would turn out.

Significance of Research

This section answered all aspects of the research question, which yielded that Private Permissioned Blockchain can be used by the government in certain transactions. It also made a call to action to simplify DoD contracts into formulas and conduct a tradeoff analysis between a COTS or in-house blockchain solution. The future research portion discussed the need for a different point of view and more firsthand data. The purpose of this paper is to better prepare the DOD to pass an audit. The process of a traceable ledger would greatly help the auditing team

track transactions. The combination of smart contracts and IoT can slim down on the amount of invoice discrepancies and delays.

Bibliography

[1] Institute for Policy Studies, "2021 Discretionary Spending," *National Priorities Project*, 2021. [Online]. Available: https://www.nationalpriorities.org.

[2] R. Sisk, "In first DoD-wide audit, every military branch failed," *We Are The Mighty*, 29-Apr-2020. [Online]. Available: https://www.wearethemighty.com/mighty-trending/dod-audit-every-branch-failed/.

[3] M. Stone, "Pentagon fails audit yet again, could pass around 2027, comptroller says," *Reuters*, Reuters, 17-Nov-2020.

[4] Inspector General of U.S. Department of Defense, "Understanding the Results of the Audit of the FY 2021 DoD Financial Statements," May 2022.

[5] M. Lacity and R. Van Hoek, "Requiem for reconciliations: DL Freight, a blockchain-enabled solution by Walmart Canada and DLT Labs," Jan. 2021.

[6] M. McSweeney, "Department of Veterans Affairs seeks contractor info on blockchain use for data sharing, supply chain optimizing," *The Block*, 26-Nov-2021. [Online]. Available: https://www.theblockcrypto.com/linked/125589/department-of-veterans-affairs-seeks-contractor-info-on-blockchain-use-for-data-sharing-supply-chain-optimizing.

[7] United States Government Accountability Office, "Air Force Needs to Improve Its System Migration Efforts," Feb. 2022.

[8] R. Tanya and B. J. Chelliah, "A Comprehensive Study on Cybersecurity Challenges and Solutions in an IoT Framework," Towards a Wireless Connected World: Achievements and New Technologies., no. 10.1007/978-3-031-04321–5_5, May 2022.

[9] J. Dattani and H. Sheth, "Overview of Blockchain Technology," *Asian Journal of Convergence in Technology*, vol. V, no. 2350-1146 I.F–5.11, 2019.

[10] A. B. Pedersen, M. Risius, and R. Beck, "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies," *MIS Quar*, vol. 18, no. 2, pp. 99–115, Jun. 2019.

[11] J. Chen, X. Xia, D. Lo, and J. Grundy, "Why do smart contracts self-destruct? Investigating the selfdestruct function on Ethereum," *ACM Trans. Softw. Eng. Methodol.*, vol. 31, no. 2, pp. 1–37, 2022.

[12] "Proxy upgrade pattern," *Openzeppelin.com*. [Online]. Available: https://docs.openzeppelin.com/upgrades-plugins/1.x/proxies.

[13] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, 2021.

[14] N.-N. Iitm, "Hyperledger Fabric – Transaction Flow," 06-May-2019. [Online]. Available: https://www.youtube.com/watch?v=nBXr7dLXAbE&list=PLyqSpQzTE6M8wy_JBTgplS_HGuOYU1qkm&index=5.

[15] V. Sumit, "Hyperledger Fabric- components and architecture," *Clairvoyant Blog*, 15-Apr-2019. [Online]. Available: https://blog.clairvoyantsoft.com/hyperledger-fabric-components-and-architecture-b874b36c4af5. [Accessed: 09-Aug-2022].

[16] N.-N. Iitm, "Hyperledger Fabric Details," 06-May-2019. [Online]. Available: https://www.youtube.com/watch?v=xjliVltyLRk&list=PLyqSpQzTE6M8wy_JBTgplS_HGuOYU1qkm&index=4.

[17] P. Swati and M. Venkatesan, "Scalability improvement and analysis of permissioned-blockchain," ICT Express, vol. 7, no. 3, pp. 269–402, Sep. 2021.

[18] P. K. Ketrick *et al.*, "Assessment of DoD Enterprise Resource Planning Business Systems," Feb. 2011.

[19] Office of the Deputy Chief Financial Officer, "STANDARD FINANCIAL INFORMATION STRUCTURE (SFIS)," *Defense.gov*. [Online]. Available: https://comptroller.defense.gov/odcfo/sfis.aspx.

[20] "DoD releases report on Defense Spending by State in Fiscal Year 2020," *U.S. Department of Defense*, 22-Oct-2021. [Online]. Available: https://www.defense.gov/News/Releases/Release/Article/2819472/dod-releases-report-on-defense-spending-by-state-in-fiscal-year-2020/.

[21] U. S. Army, "GFEBS General Ledger," 28-Feb-2012.

[22] Defense Finance and Accounting Service, "Contract Vendors," *Defense Finance and Accounting Service*. [Online]. Available: https://www.dfas.mil/contractorsvendors/.

[23] Financial Management School, "General Fund Enterprise Business System (GFEBS) Navigation Overflow."

[24] "GFEBS Spending Chain Introduction," *Army Military*. [Online]. Available: https://ssilrc.army.mil/resources/FMS/GFEBS/SpendingChain/1Introduction/html/page229645.html. [Accessed: 10-Mar-2022].

[25] "GFEBS Essentials," *Army Military*. [Online]. Available: https://ssilrc.army.mil/resources/FMS/GFEBS/Essentials/2gfebsoverview/page49713.html. [Accessed: 10-Mar-2022].

[26] "USSGL Part 1 Fiscal Year 2022 Reporting," *Treasury.gov*. [Online]. Available: https://tfm.fiscal.treasury.gov/v1/supplements/ussgl/ussgl_part_1.html. [Accessed: 09-Aug-2022].

[27] "Part 1, Section I: Chart of Accounts," *Treasury.gov*. [Online]. Available: https://tfm.fiscal.treasury.gov/v1/supplements/ussgl/ussgl_part_1/sec1_cover_2022.html. [Accessed: 09-Aug-2022].

[28] "Standard general ledger (SGL) chart of accounts," *Budget Counsel*, 16-Nov-2016. [Online]. Available: https://budgetcounsel.com/cyclopedia-budgetica/cb-standard-general-ledger-sgl-chart-of-accounts/.

[29] "Part 1, Section III: Account Transactions," *Treasury.gov*. [Online]. Available: https://tfm.fiscal.treasury.gov/v1/supplements/ussgl/ussgl_part_1/sec3_cover_2022.html. [Accessed: 09-Aug-2022].

[30] "Part 1, section II: Accounts and definitions," *Treasury.gov*. [Online]. Available: https://tfm.fiscal.treasury.gov/v1/supplements/ussgl/ussgl_part_1/sec2_cover_2022.html. [Accessed: 09-Aug-2022].

[31] Board of Governors of the Federal Reserve System, "Money and Payments: The U.S.Dollar in the Age of Digital Transformation," Jan. 2022.

[32] S. Seth, "Central Bank Digital Currency (CBDC)," Investopedia, 06-Sep-2018. [Online]. Available: https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp.

[33] K. Vitasek, "Walmart Canada and DLT Labs launch world's largest industrial blockchain application," *Forbes*, 31-Jan-2020. [Online]. Available: https://www.forbes.com/sites/katevitasek/2020/01/31/walmart-canada-and-dlt-labs-launch-worlds-largest-industrial-blockchain-application/?sh=64daf8573d2e. [Accessed: 09-Aug-2022].

[34] S. Hamilton, "The partnership between DLT labs and Walmart Canada," 23-Sep-2020.

[35] Hyperledger, "DLT Labs & Walmart Canada Transform Freight Invoice Management with Hyperledger Fabric," 2020.

[36] A. Shlykov and S. Beliaev, "Supply Chain Cost Reduction Using Enterprise Blockchain," 08-Oct-2021.

[37] "IoT Devices," *Arm*. [Online]. Available: https://www.arm.com/glossary/iot-devices.

[38] S. M. Burwell, "Appendix D to Circular No. A-123," Sep. 2013.

[39] Office of Management and Budget and Department of the Treasury, "Federal Financial Management System Requirements," May 2020.

[40] J. Fernando, "Generally accepted accounting principles (GAAP)," *Investopedia*, 19-Nov-2003. [Online]. Available: https://www.investopedia.com/terms/g/gaap.asp. [Accessed: 09-Aug-2022].

[41] C. Peckinpaugh, "How does the Prompt Payment Act work?," *FCW*, 17-Mar-1996. [Online]. Available: https://fcw.com/1996/03/how-does-the-prompt-payment-act-work/246426/. [Accessed: 09-Aug-2022].

[42] V. Insinna, "Defense Department halts F-35 deliveries amid repair bill disagreement with Lockheed," *Military Times*, 11-Apr-2018. [Online]. Available: https://www.militarytimes.com/breaking-news/2018/04/11/defense-department-halts-f-35-deliveries-amid-repair-bill-disagreement-with-lockheed/?contentQuery=%7B%22section%22%3A%22%2Fhome%22%2C%22exclude%22%3A%22%2Fnews%2Fpentagon-congress%22%2C%22from%22%3A135%2C%22size%22%3A10%7D&contentFeatureId=f0fmoahPVC2AbfL-2-1-8. [Accessed: 09-Aug-2022].

[43] M. R. Rizzo, M. E. Buxton, A. S. Ralph, D. Dharmadasa, and W. N. Alston, "TASBCA's FY 2021 Annual Report Details," *Pillsbury Law*, Nov-2021. [Online]. Available: https://www.pillsburylaw.com/en/news-and-insights/asbca-2021-report-contract-disputes.html.

[44] "Credit card payment process," *Corporate Tools*, 13-Mar-2020. [Online]. Available: https://www.corporatetools.com/credit-card-processing/payment-process/. [Accessed: 09-Aug-2022].

[45] S. Zolman, "Our prediction: Blockchain WILL replace the supplier invoice," *Netnetweb.com*. [Online]. Available: https://www.netnetweb.com/content/blog/blockchain-will-replace-the-supplier-invoice. [Accessed: 09-Aug-2022].

[46] B. Smith, J. Xiong, and D. Medlin, "Case Study of Blockchain Applications in Supply Chain ManagementOpportunities and Challenges," *Journal of information systems applied research*, vol. 14, no. 3, p. 50, Sep. 2021.

[47] Value Technology Foundation, "Potential Uses of Blockchain by the U.S. Department of Defense," Mar. 2020.

[48] E. Shein, "Walmart Canada IoT-blockchain system nearly eliminates shipping discrepancies," *TechRepublic*, 11-Sep-2020. [Online]. Available: https://www.techrepublic.com/article/walmart-canada-iot-blockchain-system-nearly-eliminates-shipping-discrepancies/. [Accessed: 09-Aug-2022].

[49] 114th Congress, "The Freedom of Information Act, 5 U.S.C. § 552," Jun. 2016.

[50] A. D. Tomaszczuk, J. E. Jensen, and A. S. Ralph, "DOJ issues new guidance on Exemption 4 to the FOIA," *Pillsbury Law*. [Online]. Available: https://www.pillsburylaw.com/en/news-and-insights/guidelines-exemption-4-foia.html. [Accessed: 09-Aug-2022].

[51] J. Bennet and D. Guinasso, "Procure-to-Pay: Handshake 5 & 6," 2022.

[52] "GFEBS completes final Wave for Full Deployment - changes way Army does business," *www.army.mil*. [Online]. Available: https://www.army.mil/article/84209/gfebs_completes_final_wave_for_full_deployment_changes_way_army_does_business. [Accessed: 09-Aug-2022].

[53] United States Air Force, "FY18 Air Force Programs: Defense Enterprise Accounting and Management System."

[54] United States Government Accountability Office, "Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals," Feb. 2012.

[55] "Walmart Canada announces major $3.5 billion investment for growth and customer experience transformation," *Corporate - Canada*. [Online]. Available: https://www.walmartcanada.ca/newsroom/2020/07/20/walmart-canada-announces-major-3-5-billion-investment-for-growth-and-customer-experience-transformation. [Accessed: 09-Aug-2022].

[56] J. L. Miller, "Army's General Fund Enterprise Business System," 10-Jan-2007.

[57] Financial Information Management, "General Fund Enterprise Business System: Army Day Workshops," 27-May-2009.

[58] A. Mohanty, "The Evolution of DL Freight," *DLT Labs*, 08-Mar-2021. [Online]. Available: https://medium.com/dlt-labs-publication/the-evolution-of-dl-freight-5ef5e80de82e.

[59] Air Force Operational Test and Evaluation Center, "Defense Enterprise Accounting and Management System Increment 1 Release 3," May 2015.

[60] A. Joshi, "Hyperledger Fabric performance benchmarking using Hyperledger Caliper," *Coinmonks*, 12-Sep-2021. [Online]. Available: https://medium.com/coinmonks/hyperledger-fabric-blockchain-performance-benchmark-using-hyperleger-capiler-66d9a9af5cce.