

GM-X[™] ERP for Blockchain White Paper

By: Nelson M. Nones CPIM

Founder and CEO, Geoprise Technologies Corporation



INTRODUCTION

GM-X is the first and only ERP application in the world to combine proven blockchain technology with strong encryption.

GM-X for Blockchain enhances mutual trust and security between trading partners when business-to-business collaboration is a strategic imperative.

Enterprise resources planning (ERP) systems have been around for thirty years or more, and thousands upon thousands of legacy ERP systems are well entrenched today within small, medium and large enterprises across the globe. “If it isn’t broke, don’t fix it” being a generally accepted rationale for leaving things as they are, it seems improbable that those systems could be displaced anytime soon by something new. Yet a compelling event, the rapidly accelerating incidence of catastrophic security breaches affecting enterprises of all sizes across all industries, is drawing urgent attention to the security vulnerabilities those legacy systems expose, as enterprises face increasing pressure to gain competitive advantages through enhanced business-to-business collaboration.

Blockchain, a disruptive technology which has emerged only within the past decade, is widely seen as a panacea for security breaches and their consequences. Until now, no one has stepped forward with pragmatic solutions to leverage this new technology for the benefit of supply chains, which are the core focus of most ERP systems.

This white paper introduces GM-X ERP for Blockchain, a new offering from Geoprise Technologies which is the first of its kind to incorporate proven blockchain and encryption technologies to enhance mutual trust and security between trading partners when business-to-business collaboration is a strategic imperative.

SECURITY BREACHES ARE A GLOBAL PANDEMIC

Information security vulnerabilities have become a cause for alarm as news of major security breaches and hacking attacks continues to break nearly every week. In the United States alone, reported data breaches are on pace to surpass 1,300 during 2017, up 21% from the previous year—exceeding the 19% compound annual growth rate (CAGR) of U.S. data breaches since 2005 by two points.

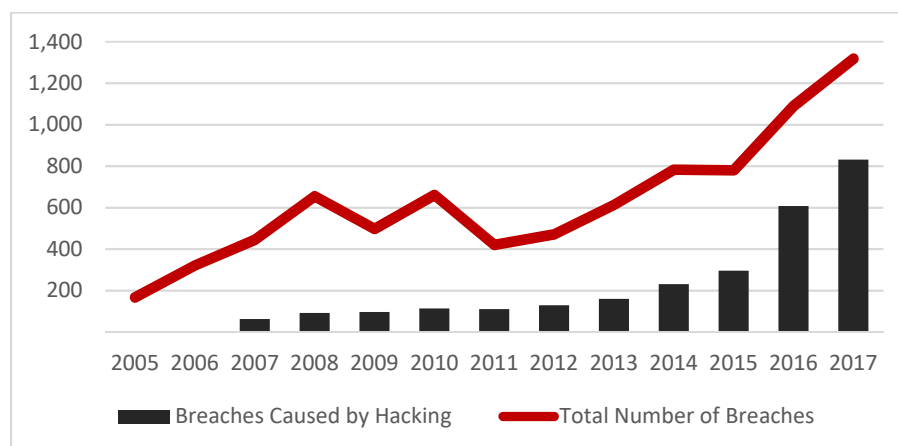


Figure 1 – Data Breaches Reported in the United States, 2005-2017

Source: Identity Theft Resource Center (ITRC), December 2017 (annualized 2017 data)

The causes of data breaches have evolved rapidly within the past two years. Hacking includes phishing, ransomware, malware and skimming attacks perpetrated by pranksters, advertisers, Internet trolls, cyber criminals and nation states. These were responsible for just 14% of U.S. data breaches in 2007, well behind the loss or theft of information in transit which caused 28%. But hacking caused 63% of U.S. data breaches during the first half of 2017, surpassing every other category by six-fold or more. According to the Identity Theft Resource Center, a U.S. non-profit organization sponsored by foundations and corporations including Google® to support victims of identity theft, “Within the hacking category, phishing was involved in nearly half (47.7 percent) of these attacks. Ransomware/malware, newly added in 2017, was present in 18.5 percent of the hacking attacks.”

The business, finance, health and medical sectors have been hit hardest so far in 2017, reporting 83% of U.S. data breaches, far ahead of educational institutions, government and the military which reported 17% of breaches. As with causes, the targets of attacks have shifted significantly since 2005, when educational, government and military entities reported 61% of breaches while the business, finance, health and medical sectors reported 39%.

RAPID ADOPTION OF CENTRALIZED CLOUD SERVICES IS FUELING THE PANDEMIC

It is no coincidence that recent shifts in both the causes and targets of data breaches took place at a time when businesses and consumers were rapidly adopting cloud services. Skyhigh Networks reports that in mid-2013, the average enterprise used 397 cloud services while the average consumer used 148. By mid-2016, cloud service usage grew to 1,018 per enterprise and 409 per consumer—a CAGR of anywhere from 37% to 40%. This furious growth has been propelled by a multitude of factors including convenience and speed as well as significant cost savings, but the underlying driver was the proliferation of smartphones and other mobile devices which has grown at a fairly consistent 22% CAGR globally over the past decade.

Recent data breaches are a direct consequence of increasing reliance on public cloud services. These include Software-as-a-Service (SaaS) offerings which are convenient and economical; but are also centralized in the public cloud and therefore vulnerable to phishing and malware attacks directed toward SaaS end users.

By their very nature, mobile devices rely on cloud services accessed via the public Internet to a far greater degree than desktop and laptop computers tethered to internal corporate networks. This means they expose a significantly higher attack surface. A 2016 study by the Pew Research Center revealed that 28% of Americans did not lock their smartphones, and 40% say they performed updates—including security updates—only when it’s convenient. The same survey found that 54% of Internet users accessed public Wi-Fi networks which are susceptible to session sniffing attacks, and many of them did so when performing sensitive activities such online shopping (21%) or online banking (20%).

To capitalize on new market opportunities, public cloud service providers have generally focused on delivering speed and convenience at the expense of security. The main business driver is unrelenting competitive pressure to release powerful yet simple, friendly and easy to use applications as quickly and inexpensively as possible. Best security practices, on the other hand, tend to reduce competitiveness by erecting as many obstacles as possible in order to thwart intruders. Considering these priorities, most application designers and developers instinctively don’t think like hackers. They are passionate about all the good things they envision their cloud services can do, but cannot easily conceptualize a hacker’s nefarious motives or modes of attack.

In the headlong rush to market, the easiest and least expensive way to make cloud services fast and convenient was to centralize them—meaning that data sent and retrieved by users of those services is stored in centrally-managed databases maintained exclusively by the service provider—and grant access to them by way of old-fashioned user IDs and passwords. Many of these services were built on the cheap using immature technologies, and rolled out hastily, in a manner that wasn't sufficiently hardened or administered to ward off clever phishing expeditions or “back door” intrusions. This broadened the attack surface yet again, because an attacker who successfully penetrates a centralized system can gain access to all the data it holds.

THE TRADEOFF BETWEEN CONVENIENCE AND SECURITY HAS REACHED A TIPPING POINT

In addition to revealing lax cybersecurity habits, the Pew Research Center's 2016 survey found that roughly half of Americans did not trust the Federal government or social media sites to protect their data, and over one third did not trust the companies or retailers with whom they did business to do so. Considering the rapidly accelerating pace of well publicized data breaches since then, it is quite likely that the proportion of Americans who do not trust those entities to protect their data has grown to an absolute majority today, and will continue to increase unless and until enterprises and cloud service providers are able to staunch the data breach pandemic.

As hacking by cyber-criminals and state-sponsored entities grows ever more frequent and sophisticated, “hardening” existing systems has become a never-ending, costly and ultimately futile effort. Businesses and consumers no longer trust the patchwork approach to adequately protect their information assets.

Some service providers, like Microsoft®, have begun to act aggressively to stop the bleeding using conventional technologies and approaches, but at considerable cost of convenience. In the end, though, these tactics won't suffice. As journalist John Beban said in 2016, “If you build a 30-foot wall, all it's going to do is create a market for 31-foot ladders.”

But the current state of affairs doesn't have to carry on this way. Two technologies, strong encryption and blockchain, are available right now but haven't been widely adopted yet due to the daunting complexities and costs of re-engineering legacy software applications and cloud services to take advantage of them.

Through its foresight and the flexible design of GM-X, its flagship enterprise resources planning (ERP) application suite, Geoprise Technologies has successfully incorporated strong encryption and blockchain technologies into a Web application which enterprises can quickly, economically and securely deploy today.

SECURITY REQUIRES BILATERAL TRUST

The security vulnerabilities of centralized systems, including most cloud services, arise from the inherent concentration of control in one place—the servers which host those systems, and the organizations which run those servers. Those organizations could legally or contractually qualify as trusted third parties but, in reality, at best they can only be fully trusted when their systems aren't hacked. Lacking absolute enforcement power, outside parties are powerless to control their own identities, financial assets and intellectual property which may reside or pass through those systems. This may not be much of an issue when the host organization is a trusted third party which abides by the law and honors its contractual commitments, but it can rapidly disintegrate into a disaster should a nefarious hacker succeed in stealing those identities or assets.

Geoprise recognized this fundamental problem long ago, and first proposed a bilateral trust model to deal with it back in 2005. We wrote, “A bilateral trust model ... puts absolute enforcement power in the hands of the respective parties according to the terms of a mutually-agreed contract. For example, your contract with [a] service provider might give you the right to declare certain information ‘private’, after which the service provider has no right to see [it] without your explicit permission, obtained according to your rules. You can enforce your rights by encrypting this information, and issuing the [decryption] key only when you’ve authorized someone to see it.”

At that time, strong encryption technology was widely available; however, blockchain technology did not exist. It would be disclosed for the first time in 2008, three years later.

Blockchain technology facilitates bilateral trust among a system’s users, by enabling multiple parties to directly and securely share a single ledger comprising all the transactions which have ever occurred since the blockchain’s inception, up to the present. None of the data in the ledger is stored centrally. Instead, the ledger is shared among all parties, who store, read and write to it using their own systems. This is known as “disintermediation.”

Each party uses its own system, or “node”, to hold its copy of the ledger. Data automatically propagates between nodes in a peer-to-peer fashion. Instead of using their browsers or mobile devices to access a centralized application and its databases, participants must access their own systems using whatever credentials those systems require. This architecture exposes no central attack surface through which one of the participants or an external hacker could alter the data. As a side benefit, it also provides redundancy and fault protection for all parties.

BLOCKCHAIN TECHNOLOGY MAKES SHARED INFORMATION PERMANENT, TAMPER-PROOF AND VERIFIABLE

Each item of data written to a blockchain forms a separate transaction. Transactions, in turn, are chronologically grouped into blocks forming chains, and each block is linked to its predecessor all the way back to the original or “genesis” block.

Each copy of the ledger in a blockchain network is permanent, tamper-proof and readily verifiable.

When a block is first created, its contents are “hashed” using a cryptographic function which converts the block’s data into a unique identifier comprising a combination of characters. For example, the SHA-256 hashing algorithm converts a block of any size into a unique combination of letters and numbers that is always 64 characters long and represents exactly 256 bits. Hashes are self-certifying identifiers which are irreversible, making it impossible to reconstruct the data from its hash, but the hash can be reconstructed from the same data. Next comes a built-in process known as “consensus”. In public and anonymous blockchains, consensus is achieved through “proof of work” (POW) which requires an independent party known as a “miner” to solve an excruciatingly difficult mathematical problem sooner than anyone else; but alternative consensus algorithms can be utilized, such as round-robin schedules which require miners to wait their turn in the rotation before they are able to prove any valid blocks. These are far less intensive computationally but are suitable only for private, permissioned networks. Whatever the algorithm, consensus is possible for a new block only after all its predecessors have been similarly proven.

As soon as consensus is reached for a new block, the block is sent to all the other nodes. Blockchain technology assures permanent data integrity by allowing participants at those nodes to verify the block before accepting it. Verification is done by examining whether or not the block has

been proven through the consensus mechanism; then by hashing the data in the block, and comparing the result to the hash value sent with the block. The block will be rejected if it isn't proven or the hash values don't match; otherwise the new block will be accepted and appended to the recipient's copy of the blockchain. This procedure makes it impossible for a participant or external hacker to alter or tamper with a block.

Blockchain technology, therefore, provides a trustworthy mechanism for avoiding disputes between parties who may not fully trust one another, while eliminating the need for mutually trusted third parties and their vulnerable centralized systems to do the job. Illustration 1, below, shows a simplified working example.

Illustration 1

This illustration is a simplified demonstration of how blockchain technology makes shared information permanent, tamper-proof and verifiable.

Assume that an honest seller has quoted the price 1,017.43 to a buyer using an XML message like this:

```
<update_quote_header>
<quote_id>8859658868000000000000000000000000000026743</quote_id>
<quote_type_id>QUOT</quote_type_id>
<quote_desc>PLACARD INSTALLATION</quote_desc>
<quote_status_type_id>SUB1</quote_status_type_id>
<valid_from_date>2018-01-26</valid_from_date>
<valid_to_date>2018-02-09</valid_to_date>
<quote_value>1017.43</quote_value>
<item_count>1</item_count>
<currency_code>USD</currency_code>
<child_tables>
  <quote_item>
    <quote_id>8859658868000000000000000000000000000026743</quote_id>
    <quote_item_seq_no>1</quote_item_seq_no>
    <quote_item_desc>PLACARD INSTALLATION</quote_item_desc>
    <quote_item_status_type_id>SUB1</quote_item_status_type_id>
    <estimated_delivery_date>2018-02-02</estimated_delivery_date>
    <quote_quantity>1</quote_quantity>
    <unit_price>1017.43</unit_price>
  </quote_item>
</child_tables>
</update_quote_header>
```

This message is compressed into a new transaction like this which is written to a block in clear text:

```
update_quote_header<quote_id>85965886800000000000000000000000026743</quote_id><quote_type_id>QUOT</quote_type_id><quote_desc>PLA  
CARD INSTALLATION</quote_desc><quote_status_type_id>SUB1</quote_status_type_id><valid_from_date>2018-01-26</valid_from_date><val  
id_to_date>2018-02-09</valid_to_date><quote_value>1017.43</quote_value><item_count>1</item_count><currency_code>USD</currency_co  
de><child_tables><quote_item><quote_id>88596588680000000000000000000000026743</quote_id><quote_item_seq_no>1</quote_item_seq_no>  
quote_item_desc>PLACARD INSTALLATION</quote_item_desc><quote_item_status_type_id>SUB1</quote_item_status_type_id><estimated_deliv  
ery_date>2018-02-02</estimated_delivery_date><quote_quantity>1</quote_quantity><unit_price>1017.43</unit_price></quote_item></ch  
ild_tables></update_quote_header>
```

The transaction's SHA-256 hash value is:

2B928B441629CBADC56AAFFA447727DF04772AD8EFA924832C779155E398BA88

After consensus is reached for this block, a dishonest competitor who is a participant in the same blockchain tries to alter the data by changing the first seller's price quotation to 2,017.43—in hopes of profitably undercutting the first seller's quotation:

```
<update_quote_header><quote_id>885965886800000000000000000000000026743</quote_id><quote_type_id>QUOT</quote_type_id><quote_desc>PLA  
CARD INSTALLATION</quote_desc><quote_status_type_id>SUB1</quote_status_type_id><valid_from_date>2018-01-26</valid_from_date><val  
id_to_date>2018-02-09</valid_to_date><quote_value>1017.43</quote_value><item_count>1</item_count><currency_code>USD</currency_co  
de><child_tables><quote_item><quote_id>885965886800000000000000000000000026743</quote_id><quote_item_seq_no>1</quote_item_seq_no><q  
uote_item_desc>PLACARD INSTALLATION</quote_item_desc><quote_item_status_type_id>SUB1</quote_item_status_type_id><estimated_deliv  
ery_date>2018-02-02</estimated_delivery_date><quote_quantity>1</quote_quantity><unit_price>2017.43</unit_price></quote_item></ch  
ild_tables></update_quote_header>
```

It's important to note that a dishonest competitor cannot change the block's hash value, because that value is also the block's unique identifier in the blockchain. In other words, changing a block's hash value will always create a new block, and can never alter an existing one.

When the altered block arrives at the buyer's node, the buyer attempts to verify it by calculating a SHA-256 hash value from the transaction data:

E3A0753FABBD280370D5327CBF704C413FFF005ED18D7832E42B2B524B274AC0

Verification fails because this result is not the same as the transaction's hash value. The buyer rejects the block, thwarting the dishonest seller's gambit.

Illustration 2

This illustration demonstrates how encryption technology gives parties complete control over their information assets.

In Illustration 1, all participants in the blockchain can see the data for each transaction, which is transmitted in clear text. In reality, sellers will want to keep their price quotations confidential, and allow only the buyer to see them.

All the blockchain's participants generate key pairs consisting of a private and a public key. Assume that the buyer's key pair is:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDl+gh7qNntWxFOl/0Y9txqnxMYV+4WbuiU7ISM/wBM8Hb0wCUL2Xm+dFus5mHeM/zCGCjovHpKuw+Q2NZahDHu0o8FXZVm9ybd3lF3Sfr20++sAyNm
ul+5qB8m6mycw/3o78dyLPoiIJPe9lB8knrZE2LB1A5HjaYil4IfHwQjNQIDAQAABAGBAJfgvVN1Wp7PQqMBNcQT29MqRQERqPH1wvH/FUf4JimpsNXIQ28E68rkq1qP
N1j4ulcwf2vcdWL/ELOXEFDs9s/ChkXnM1WT2VU07CU526IFFWsMXqtTBCwOCnaluHps/Q7h4XFvNw8ZmsFayXqITXg9esJ6MWBm3a92xVCZGA/BakeA9nEAlNF4c3SA
aAuWgQxqBbqubegh2B3B7kA/dzHnaD2ja+JoKpkhCdQya0Xg5zke1FzhwvLtjMWSWRCOTqdB IhQJBA071jBbW/BT9QmFf6LFYKLM7jg65qqnLDh+X1qvSohu3sM0jgcVd
1HIGTaQ03ruvIrrGKbrS8wulU6+rU5FxeCQew7vpNKjPkiE8qbuvi0mtUSTsEcNu6sM/zne5QSKYtUw0/dzueLOMuef5HG0BMWshbNfcq8KL4RwI4Jf0H5nUUCQt/
W0RDxPbk52PntnVmyBmuqQuyfDsFJeHNYn06sLtsMuB8I8G/Au+0KmqwLLGjogvymM2bf2YHaCQg5PcdqUECQDkKIYqHPkmZG0gvZ9k3J5YJWdo3Gx0FkU/V1COK30Ba
r6LKAK7sWw5A19tpkox8xJmyxgr08YEDzOBMC6F13Ue
-----END RSA PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDl+gh7qNntWxFOl/0Y9txqnxMYV+4WbuiU7ISM/wBM8Hb0wCUL2Xm+dFus5mHeM/zCGCjovHpKuw+Q2NZahDHu0o8F
XZVm9ybd3lF3Sfr20++sAyNmUl+5qB8m6mycw/3o78dyLPoiIJPe9lB8knrZE2LB1A5HjaYil4IfHwQjNQIDAQAAB
-----END PUBLIC KEY-----
```

Further assume that the dishonest seller's key pair is:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgHyagDhyUp5jY24lwIMRlGyn/nR87aPKx7Vr0CKBJKNpvtTCP1vQ4IQFQxrsW2+1GRca8nmfC8JiWa36Yg4j4UUbEX6H9H+5ETax9NeXmqFnK/g66anyG
WSFDY8jUWCNDnAc4105LFKx1sn16fcbLNQ181/81B/DzC4853wPoZLGzAgMBAAEgcYBdGyBKS5WQXbXHydStwIBAMwDx+56NQbnh/LkMm7b70QnkiK61vUQozTLONPKi
AWG58ADtP5Cg2v/wIH1U3UQGrF0QN7EtKwxxUXUHNb/2APAFbwRX/xQ20LF9zMTUmUnEyJpG8PaCUwW2mbzQcpRcztiuyLwrCU4fntiHe+ewQJBAOpsAN9zgECovtH8
1VG1PrFF7ORhxezkt++gJmYSiRo79YtpCTJ2zB14bDskz7XaLRUGU3LW1XEEYQb652JgzYKCCQCIERNGEH/qRa7b03j5JIN5dbnnrd9GGAJif9bD12SPa+Rzn0qhXSETQ
xN/YgU5i+Z+htX2gc17WY953r8r7SBJbAkeAJdyGOrM+7eIweAs1XJj+M4EEFbr/scwuGdDDKj/Gtnn61fZc2xZ82rq7tcG06daZumcaWQWyrCAXKYdr8o4BJYQJAFEE/
TXqhAcPvpLkQj/WwzQFw+po/SikPmV3rNvU3w9d8lRhBprqpA0zLxwXki09PkbhGYU2z0QJGRGA7ecJqJAArD2HQntW2LET8jZ2642s0P5SIOVORAQOqrTOrJS62XZ9
yHbJREsIn/v6IU6RVQPKyicamODFUVoHyWfNBQ2wA==
-----END RSA PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgHyagDhyUp5jY24lwIMRlGyn/nR87aPKx7Vr0CKBJKNpvtTCP1vQ4IQFQxrsW2+1GRca8nmfC8JiWa36Yg4j4UUbEX6H9
H+5ETax9NeXmqFnK/g66anyGWSFDY8jUWCNDnAc4105LFKx1sn16fcbLNQ181/81B/DzC4853wPoZLGzAgMBAAE=
-----END PUBLIC KEY-----
```

Both participants distribute their public keys to all the other participants in the blockchain (including the honest seller), but it's vitally important for them to keep their private keys to themselves!

The honest seller wants to transmit a price quotation to the buyer in confidence, so generates a random password for the price:

25308688476921129611344912306488980886

The honest seller then encrypts the transaction data using this password. The result might look like this:

```
-----BEGIN MESSAGE-----
Encryption-Info: AES-256,CBC,PKCS5 Padding
Key-Info: MD5,PBKDF2 HmacSHA1

DHPEfpSLygtN2VETKSRqgDi/fHj8P/eSXUuBsaWHEmeodjN5aL9NYiTT2ksgkaiwHMKMvY0u3TMqmCa1MgAobIdTQ5msM8YDdpIcyoKINp677UoDp8+sYEi5GXs3xiX9
Kd6VqWi4EJEj/lrVQ8/hc5BM3Rrj+rxr+JMj2Twy6YbA/G215QAbC089q8t+V3jsm+xbcgJbvFWgW03YhZ1b8uZ7PdBpaRQvKRoNBAXuaAQpPy1ToMmNAxW43Aia9qa9a
ejHAFKQCrB4SAm9hCwCI3wVTLMptPKupUeGSpWG/wIzMcNqhpR8aFPybyungrFnhmjCTbbCPHYqSWMGn/vXk1mlzVoBaxZmwTEeycmY/fM0v2bFBAIcusjZRQ3STARPe
SJO1sGseHqkjq2DcEJCtn4L8g7cz5E06lxReBsxg4rz4oj5+ieiYSZ2RVvqB0/5RlvqgUrE0n3LvxQeS+bdqxPOXh0ITJP2MSFuXWcumahg2s6RJTVhnrK40tVK24L
xmcQwsQ13NJ4PERIO7gGc67351978nbag5NJ4V2UpEjNr61PWnOhreKofVHWf05DV8hgjhFhfrJmF9M/05G25dBj7t8hammFG51dnZkLYkNT1VLiZeFvVdxrklr0FF
IL+eb6i2msKnm7mcPXNwsT/iHrIsUa/+1k1JLYnWESWQpJe1Qi5+eQLQNY0AwcBKA6Ae0PnUT6mpPQEZxcck+i3Di00faXaC63bxbnhKAQZRC83evVMTVupJy1simfV
aT9Rr+W9Nx55eDPeR2Xtpt0ijHTpx+31lsU+LBI/XYEzmVzi79nGcCC5VoNp13E0mt0YEae1ZMEjj/tNGGDHkWszzjPzG/jsoMrk0kYQxV0RrxZMK8Dnw4TB6Df+2Pha
gaRFg7Opioi5qAHi6a+72dpuEmJt8pow1j1P62s7pnKVL/SYxuqCOPint+m5W44pNyopRnDxT4MngUfqyFY8kbzwhr9s/Ul3P1+WzQ/eWftI7DkqSBF6YLK2X+euCyN7
Xwj0Gzha3E/zeL78rB4crrxncTJvnNzBX2F5Kw9HLXUiRjH4Ptv6Gv0w7uJ0FCFN
-----END MESSAGE-----
```

The honest seller's encrypted data will be visible to all participants in the blockchain, but is unintelligible to any participant who does not hold the password. Note that when an encrypted transaction is added to a block rather than clear text, the block's SHA-256 hash value will differ as well, because it will be generated using the encrypted text instead of the clear text. This does not affect a recipient's ability to verify the block; only on their ability to comprehend it.

Next, the honest seller encrypts the password using the buyer's public key, with the following result:

```
TJPqk6AmZxtXzWu0JUrqC8kaPpuCa0bC+RNi1TGULeAaJHHDCECekt1mG4L9ttrIQBWvw+aohWj3GImD+uiX8dBmu52gBa7A3yz/MRDXRD2tOC4BmJQrc+Dh0NuJC
4csj8mHNnmVB8iLLUSmMxYoIHQz57Fex3K+RT0EEP4=
```

The honest seller provides the encrypted password to the buyer—which is be done by adding a separate access stream for the transaction data written to the block. The password can be decrypted using the buyer's private key. The buyer can then use the decrypted password to decrypt the transaction data, revealing the honest seller's price quotation.

Other participants, including the dishonest seller, will fail to decrypt the password using their private keys. Because they cannot decrypt the password, they cannot decrypt and see the honest seller's price quotation.

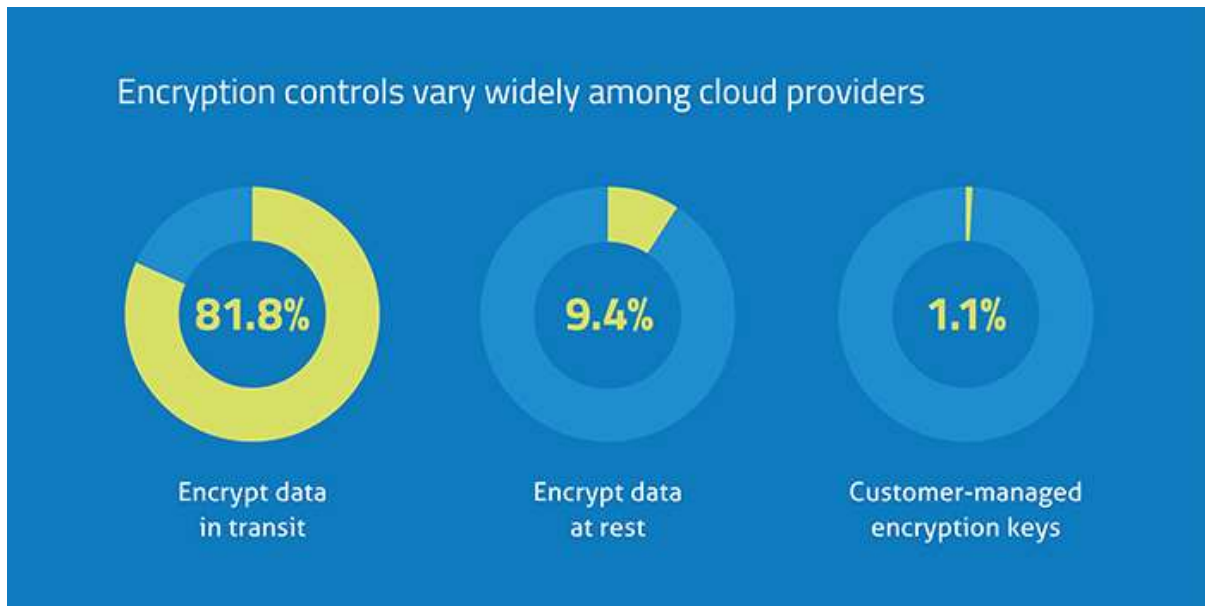


Figure 2 – Availability of Encryption Controls for SaaS Offerings

Source: Skyhigh Networks

“Encryption makes data indecipherable to anyone without access to the encryption keys, but when a cloud provider encrypts your data, administrators at the provider can view your data. The cloud provider may also be compelled by law to provide copies of your data to various governments around the world without notifying you. And in the event of a breach, a cyber-criminal who has compromised the encryption keys of a cloud provider can decrypt the stolen data. Encrypting data using your own encryption keys can prevent these scenarios, but just 1.1% of cloud providers support tenant-managed encryption keys.”

– Skyhigh Networks

ENCRYPTION TECHNOLOGY GIVES PARTIES COMPLETE CONTROL OVER THEIR INFORMATION ASSETS

Keeping the data in a blockchain confidential requires it to be encrypted before it is written to the chain. It also requires each party to create a key pair comprising a private and a public key, and to distribute the public key to all other parties. Before a participant publishes data to the blockchain, the data is encrypted using a randomly generated password. That password, in turn, is encrypted using the public keys of all other parties who have the publisher’s permission to read the data.

In this way, even though the entire ledger is visible to all participants—a necessity for enabling each participant to verify each block as discussed earlier—the data linked to each transaction is visible only to participants who are able to decrypt the password using their own private key.

This mechanism, in short, allows parties to create a “valve” for each item of data they publish to the blockchain. Only parties to whom the publisher has granted explicit permission can open the valve, by supplying a valid password. Permissions are enforced by encrypting the passwords in a manner that only permitted subscribers are able to decrypt. Illustration 2 on the previous page shows a working example.

GM-X ERP ENABLES REAL TIME COLLABORATION BETWEEN EMPLOYEES, CUSTOMERS AND SUPPLIERS

GM-X from Geoprise Technologies is a Web ERP application suite that addresses the ever-growing need to transact business beyond the confines of traditional offices and facilities. It is a robust enterprise-class application that facilitates business operations anywhere in the world at top speed, reliability and efficiency. GM-X presently consists of 17 integrated subsystems covering security and audit, master data and content management, business process management, sales force automation (SFA) and supplier relationship management (SRM), logistics execution, and project and activity execution functions as illustrated in Figure 3.



Figure 3 – GM-X Application Suite Capabilities

Unlike other ERP applications which are suitable for internal use only, GM-X enables real time collaboration between employees, customers and suppliers by bridging the gaps between external operations and internal systems:

- Manages trading relationships with customers, suppliers, third-party logistics providers (3PLs), contract manufacturers and staff on demand;
- Integrates product data management and Web content management;
- Manages inventories;
- Tracks and audits in-transit, consignment, field and trunk stock;
- Provides self-service portals for customers, suppliers and contractors;
- Manages electronic exchange of requirements, RFPs, RFQs and quotations;
- Issues and tracks supplier and contract manufacturing purchase orders;
- Receives, tracks, fulfils and invoices customer orders;
- Tracks shipments and deliveries of materials and finished goods;
- Manages project scheduling and tracks project execution;
- Monitors work effort and tracks schedules, timesheets and expenses;
- Provides personnel tracking, applicant tracking, performance reviews and learning management; and
- Automatically monitors quality, availability and on-time delivery performance.

In collaborative business scenarios involving an enterprise and third parties such as customers, suppliers, 3PLs, contract manufacturers or staff on demand, the traditional way of deploying GM-X requires one of those parties to host a centralized GM-X application and database. The application is typically deployed within a demilitarized zone (DMZ) or classified military zone (CMZ) so it can be conveniently accessed by internal employees and third parties alike using the public Internet. Alternatively, for greater security the application could be deployed behind the host party's internal firewall and the other parties could access it using a virtual private network (VPN). Either way, the GM-X database is deployed inside the host party's internal firewall to keep the data secure.

In one such scenario, an organization ("Buyer" in Figure 4, below) which procures goods and services from multiple suppliers ("Seller" in Figure 4, below) can host the GM-X application and allow participating suppliers to access the GM-X Supplier Portal to receive requests for quotations (RFQs) and submit quotes. The Seller who is awarded the business can access the same GM-X Supplier Portal to receive the Buyer's purchase order (PO), submit a sales order acknowledgment to the Buyer, and submit advance shipment notifications (ASNs) and invoices to the Buyer when the products or services are shipped. The Buyer, in turn, can confirm the delivery of these shipments to the Seller.

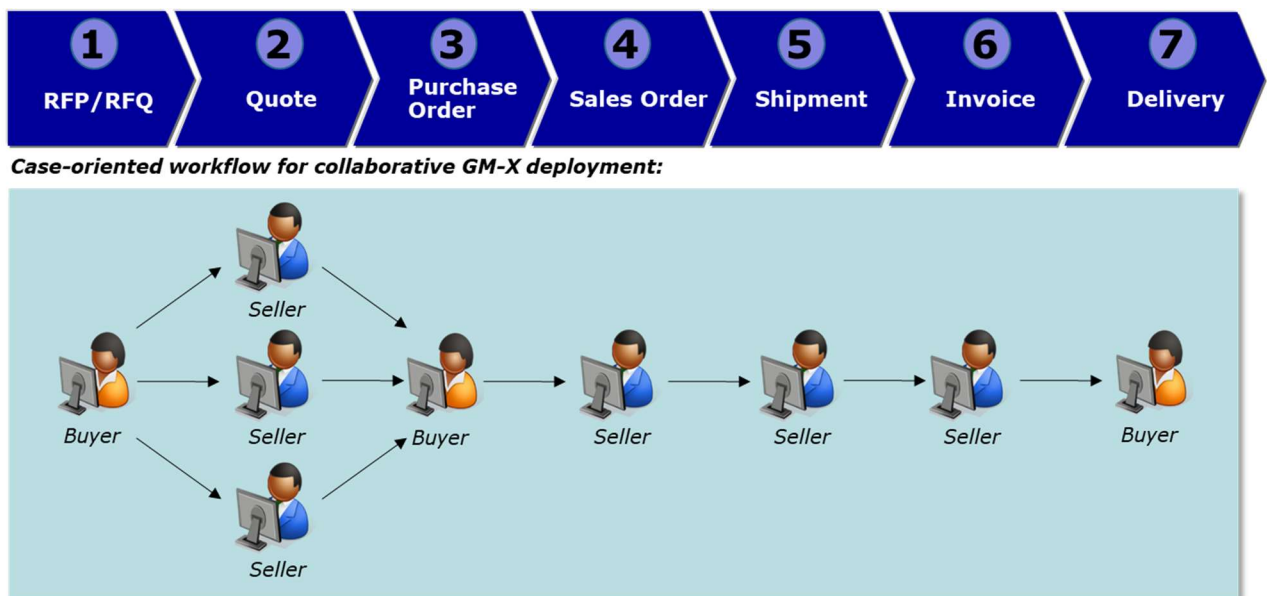


Figure 4 – Collaborative Business-to-Business Procurement Scenario

The GM-X Supplier Portal benefits Buyer and Sellers alike in support of this procurement scenario:

- Automates RFQ preparation based on the Buyer's requirements or purchase requisitions;
- Automates the selection of Sellers who are invited to bid, using criteria such as supplier pre-qualification or characteristics, long-term purchase agreements and supplier performance history;
- Provides invited as well as successful Sellers immediate access to relevant supplementary content for each RFQ, such as engineering drawings, computer-aided design (CAD) models, specifications and related documentation;
- Saves time and eliminates data entry errors by eliminating the manual re-entry of quotes received from Sellers into the Buyer's ERP system;

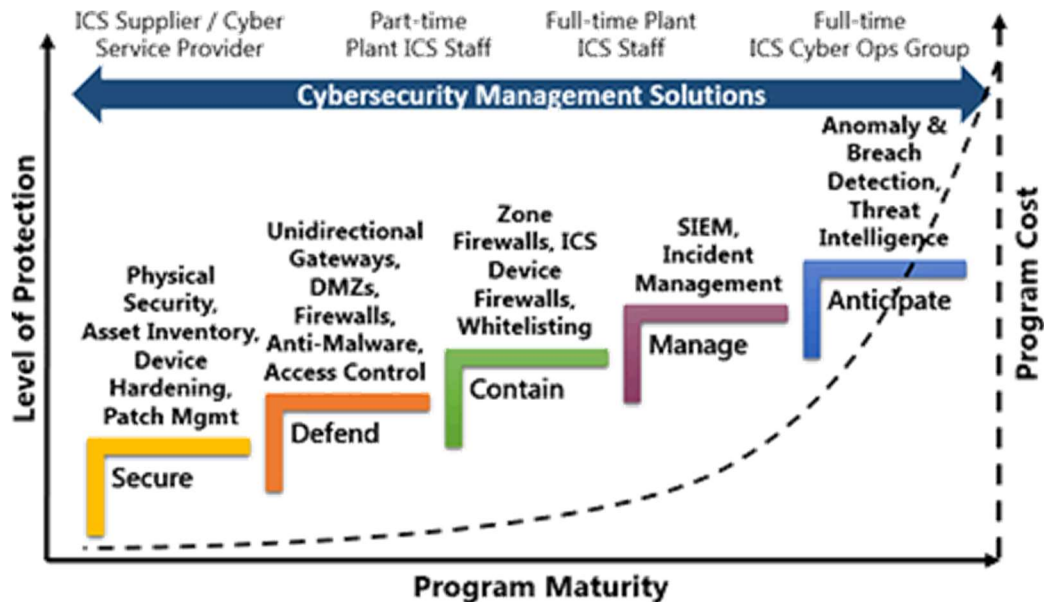
- Expedites the evaluation of quotes received from Sellers by ranking them according to price, availability and commercial terms offered;
- Reduces order fulfilment cycle times by instantly transmitting POs from Buyer to Seller, and sales order acknowledgments from Seller to Buyer;
- Provides Buyers with immediate visibility of shipment status and tracking;
- Provides Sellers with immediate visibility of shipment arrivals and receipts by Buyer;
- Eliminates the time and cost of verifying Seller's invoices using three-way matching between the PO, receiver and invoice;
- Sellers do not need to invest in any hardware or software, other than wired or wireless high-speed Internet connections and devices running popular browser software including desktop and laptop personal computers (PCs), tablets or smartphones; and
- Provides the benefits of electronic data interchange (EDI) in lower-volume trading relationships which do not justify the cost of implementing EDI.

CENTRALIZED DEPLOYMENT OF GM-X ERP IS CONVENIENT, BUT DOESN'T ADDRESS ALL SECURITY AND TRUST ISSUES

The GM-X ERP application suite embodies best information security practices and methods, and has been successfully deployed by organizations having military-grade information security requirements, policies and procedures. Key GM-X security features include:

- Authentication by user ID and password, or by two-factor authentication (TFA);
- Ability to temporarily disable user accounts, or restrict account validity to a date range;
- Enforces an organization's security policy through configurable account lockout after failed logon attempts; configurable password rotation, length and format rules; password strength meter; password change confirmation; encryption of stored passwords and secure HTTP (HTTPS) password transmission;
- Ability to restrict user access to authorized devices, based on static Internet protocol (IP) address;
- Ability to restrict user access to authorized time periods;
- Fully configurable role-based access controls at both task and field levels;
- Row-level security option;
- Database access credentials can be encrypted and stored outside the GM-X Application's Web server root;
- Options to use HTTPS requests and responses for designated pages within the GM-X application, or all pages;
- The GM-X application remains fully functional even when scripts are disabled as a security precaution through individual browser settings or an organization's group policy objects (GPO);
- All GM-X program code is encoded to prevent code injection attacks on the GM-X application server;
- All GM-X program code is hardened to incorporate best practices and methods for preventing session fixation, session hijacking, cross-site request forgery (CSRF), code injection, SQL injection and cross-site scripting (XSS) attacks;
- To prevent data leakage, data is never passed between browsers and the GM-X application server by way of the application's uniform resource locator (URL); and
- The GM-X application can run on the latest versions of operating systems, system software and relational database management systems (RDBMS), to incorporate the latest available security updates and enhancements.

These features are capable of providing the highest level of information security possible for a Web application. Unfortunately, however, they can't guarantee complete security. That's because security is only as good as a host organization's cybersecurity management program, as illustrated in Figure 5, below.



Source: ARC Advisory Group

Figure 5 – Industrial Cybersecurity Model

Centralized deployment of the GM-X Application Suite may also raise specific ethical and information security concerns which no software package or cybersecurity management program, no matter how hardened or mature, can completely address when arm's length parties collaborate using a centrally-managed application and database.

For the procurement scenario described above, an honest Seller's concerns might include:

- How can I keep my quotes confidential—and prevent them from leaking to my competitors—after I submit them to the Buyer?
- How can I prevent a dishonest competitor (or dishonest employees of the Buyer) from altering or tampering with the quotes, sales order acknowledgments, ASNs and invoices that I submit through the Supplier Portal?

An honest Buyer may have ethical and information security concerns as well, even if it hosts the centralized application:

- How can I keep my RFQs, POs and intellectual property—engineering drawings, CAD models, specification and other information—confidential and prevent them from leaking to my competitors or dishonest suppliers, after I make them available to Sellers?
- How can I prevent dishonest Sellers from hacking into the database to inflate prices quoted by their honest competitors?

Concerns like these demonstrate how storing confidential information in a centralized database creates a significant security challenge which can erode the trust which is required between Buyer and Sellers. Someone within or outside the Buyer's organization could hack into the database, or access the database using legitimate credentials, to change the data; for example, to alter a Seller's quote. This might be done by an insider who has valid access credentials and is secretly colluding with the Seller's competitor in return for kickbacks. It could also be done by Seller's competitor, if the competitor is able to hack into the database. Additionally, Buyer's or Sellers' competitors could hack into the centralized database to steal valuable intellectual property or confidential information.

All these concerns arise from the centralized database's inherent concentration of control in one place—the Buyer's information technology (IT) infrastructure, for this procurement scenario.

In the past, the only way to preserve the trust required between parties was to invest in expensive and time-consuming mechanisms for verifying the data kept in the centralized database, and reconciling it with the data independently kept by each of the Sellers. The GM-X Audit subsystem can facilitate such verification, but it doesn't (and cannot) automate the verification and reconciliation processes.

HOW GM-X LEVERAGES BLOCKCHAIN AND ENCRYPTION TECHNOLOGIES TO ENHANCE TRUST AND SECURITY

GM-X is the world's first ERP system which can be deployed as part of a private, permissioned blockchain. In such deployments, each participant in the blockchain runs its own server node comprising:

- The blockchain server bundled with the GM-X Application Suite, connected to the public Internet or a private wide-area network (WAN);
- The GM-X Application Server, accessed from any browser as shown in Figure 6, below;
- An RDBMS of the participant's choice, which is licensed separately (GM-X supports Oracle®, Microsoft SQL Server®, MySQL® and PostgreSQL); and
- A local area network (LAN), Intranet or corporate WAN.

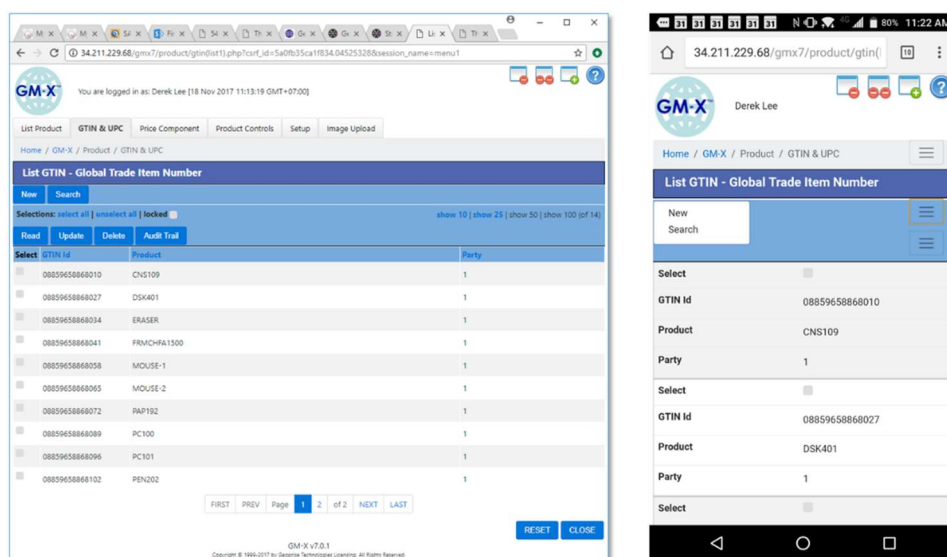


Figure 6 – Fluid, Responsive Web Design Works on Desktop PCs, Laptops, Tablets and Smartphones

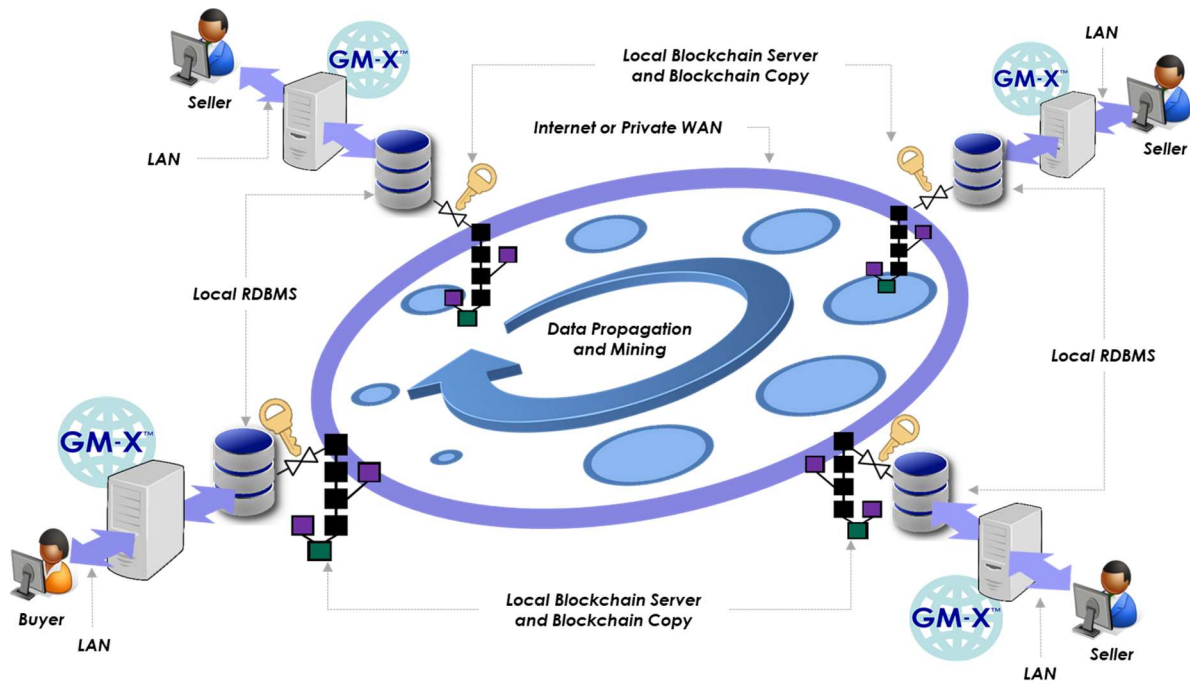


Figure 7 – GM-X ERP Blockchain Deployment

Figure 7, above, illustrates the entire blockchain for the collaborative business-to-business procurement scenario shown earlier in Figure 4.

For maximum security the GM-X server and RDBMS at each of the four server nodes shown in Figure 7 can be deployed behind the participant's internal firewall, while the blockchain server would typically be deployed behind a perimeter firewall in a DMZ or CMZ, as shown in Figure 8, below. Authorized users at each node connect directly to the participant's LAN, Intranet or corporate WAN, or establish secure VPN connections over the Internet. Connections can be made using Ethernet cable, or through wireless access points.

The servers at each node can be clustered in various configurations for load balancing and high availability, and can be hosted in any manner the participant chooses; for example:

- Physical machines hosted on premises or at a dedicated data center;
- Virtual machines provisioned within a private cloud hosted on premises or at a dedicated data center; or
- Virtual machines provisioned by infrastructure-as-a-service (IaaS) such as Amazon Web Services® (AWS®) or Microsoft Azure®.

The blockchain itself propagates across the public internet or private WAN, forming a peer-to-peer network depicted as the large oval ring at the center of Figure 7. This means that the blockchain server at each node maintains its own copy of the entire blockchain at all times. Blockchain servers and their current copies of the blockchain are shown by the blockchain symbols in Figure 7.

Like the GM-X Application itself, the blockchain server bundled with GM-X may run on either Microsoft Windows® or Linux/UNIX operating systems. It can process up to 1,000 transactions per second on a network of mid-range servers without the costly and time-consuming proof-of-work mining associated with public blockchains. These servers can also be clustered at each node for load

balancing and high availability. As shown in Figure 8, below, each blockchain server provides Federated Blockchain Manager and Data Valve services for the node where it is situated.

Federated Blockchain Manager Services

Collectively, the blockchain servers in the network are responsible for:

- Restricting blockchain access to permitted users only, using cryptographic signatures;
- Allowing access to multiple blockchains from a single server node, with permission;
- Conferring privileges within the network, including each participant's mining rights and rights to administer the privileges of other users, in addition to the rights to send (write) and/or receive (read) transactions;
- Enforcing the voting protocol for reaching consensus among the blockchain's administrators on any change to a participant's rights;
- Accepting new transactions from permitted participants, organizing them into new blocks and sending them to all the other participants (propagation);
- Receiving new blocks arriving from the other participants;
- Mining new blocks by proving a permitted miner's cryptographic block signature;
- Enforcing a diversity policy which requires permitted miners to wait for their turns in the rotation. This mechanism prevents a participant from mining any more blocks until a minimum number of consecutive blocks has been mined by the other permitted participants; and
- Verifying the validity of mined blocks.

The propagation and mining of blocks is visually depicted by the spinner image at the center of Figure 7.

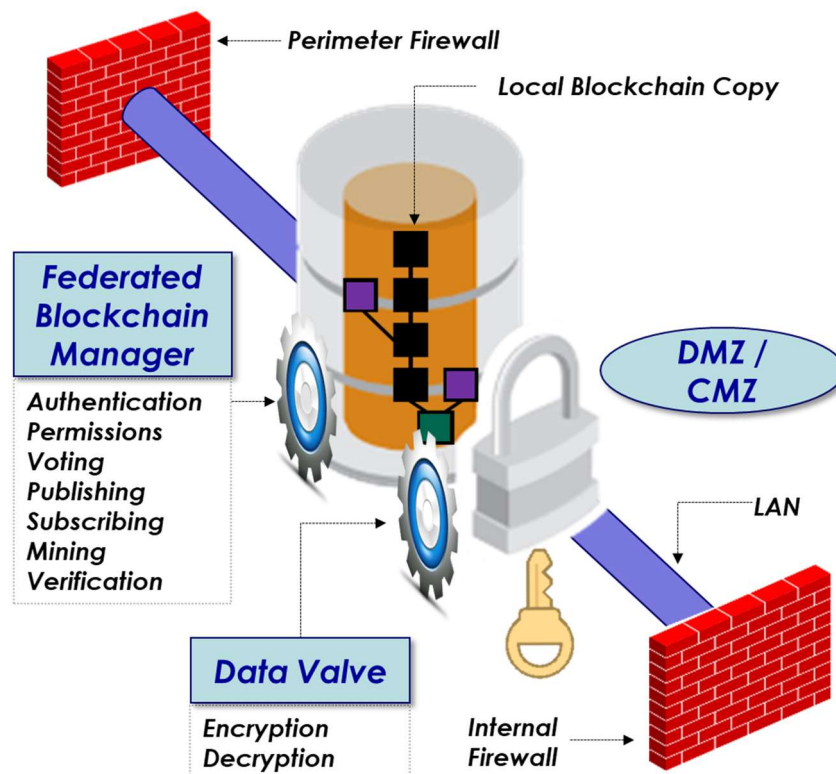


Figure 8 – GM-X Blockchain Server

To avoid needless waste of resources, GM-X does not require proof of work (POW).

The purpose of the diversity policy is to prevent a “51% attack” wherein one participant, or a group of colluding participants, monopolizes the mining process to alter or tamper with a group of transactions in the blockchain’s history. The

diversity policy is configurable, and may vary from completely lenient (every permitted participant can mine any block without waiting) to very strict (a permitted participant can mine only one block per turn, and must wait until all the other permitted miners take their turns). The optimal policy for a particular network should reflect a trade-off between the risk of malicious data alteration on the one hand, and network performance on the other. A very strict policy will fully mitigate the risk of a 51% attack, but might cause the network to freeze if a permitted miner goes offline. On the other hand, a policy of complete leniency will keep the network from freezing, but won’t prevent a 51% attack. It also won’t help the system to automatically resolve forks in the blockchain caused by communication failures which temporarily prevent some participants from receiving blocks sent by the others. In this situation a stricter diversity policy allows the fork with the longer blockchain to be adopted as the global consensus when the network is reunited. In the absence of a specific risk assessment, the default policy is to restrict each participant from mining any more consecutive blocks per turn than half the number of permitted participants.

Data Valve Services

Each blockchain server is also responsible for protecting the visibility and confidentiality of data propagated across the network. This function is represented by the valves and keys depicted in Figure 7, and performs the following at each network node:

- Generates a Rivest-Shamir-Adleman (RSA) key pair, and publishes the public key to the other participants;
- Receives transactions as streams containing data, or a combination of data and files, from the GM-X Application Server running at the sender’s node;
- Generates a random 48-digit base 64 password for each transaction at the sender’s node, and then uses this password and the Advanced Encryption Standard (AES) algorithm to encrypt the transaction before propagating it to the other participants;
- Maintains a password directory for transactions at the sender’s node;
- Using the RSA algorithm, encrypts the password once for each public key published by the other participants who are authorized to see the transaction, and adds the encrypted passwords to the access stream for the transaction it protects; and
- At each authorized participant’ node, attempts to decrypt the password using that participant’s private key. If the password is successfully decrypted, uses the decrypted password to decrypt the transaction data, or combination of data and files; and then passes the decrypted transaction data, or combination of data and files, to the GM-X Application Server running at the node. Otherwise, the transaction will be ignored if the participant isn’t authorized to see it, or the password cannot be decrypted using the participant’s private key.

This approach does not impair any other participant’s ability to mine or verify the validity of blocks containing encrypted transactions, even when a participant is unable to decrypt the data. When transactions are encrypted, all participants will receive them because all participants maintain the same copy of the blockchain. Mining and verification will utilize hash values generated from the encrypted transactions. These hash values are just as functional for mining and verification purposes as hashes generated from clear text.

HOW GM-X SELECTS AND EXCHANGES DATA BETWEEN BLOCKCHAIN PARTICIPANTS

Because blockchains are meant to be permanent and tamper-proof, new blocks can only ever be appended to an existing blockchain. No transactions or blocks should ever be removed from a blockchain, nor should the contents of any block be altered. The GM-X blockchain server's consensus mechanism and diversity policy fulfil this requirement as described earlier.

This means that blockchains continually grow in size over time. For this reason, they should be as compact as possible to minimize network traffic as well as storage capacity requirements at each node's blockchain server. Moreover, a participant will gain no benefit—and may needlessly invite data leakage risks—by publishing information to a blockchain that isn't required by at least one of the other participants.

GM-X addresses these requirements by allowing participants to configure their GM-X servers exactly as needed to collaborate effectively with the other participants, according to their respective roles. Configuration consists of activating specific GM-X database tables to be published to each blockchain.

For example, to support the collaborative procurement scenario described in this white paper, Buyers will at minimum need to activate the GM-X tables containing RFQs (REQUEST), purchase orders (ORDER HEADER), shipment receipts and rejections (PACKAGE IN CONTENT), non-conformance reports (NON CONFORMANCE REPORT) and also possibly files containing engineering drawings, CAD models and specifications together with their metadata (CONTENT TYPE).

Sellers, on the other hand, will at minimum need to activate the GM-X tables containing quotes (QUOTE HEADER), advance shipment notices (SUPPLIER SHIPMENT), invoices (INVOICE HEADER) and returned material authorizations (RETURN MATL AUTH HDR).

Each participant can configure GM-X to publish only the information it initiates by way of the roles it plays in the collaboration scenario that a particular blockchain supports. This approach promotes information sharing while keeping the blockchain as compact as possible, and prevents leakage of information that is intended for internal use only.

One of the participant nodes—usually, the node belonging to the organization which sponsors the blockchain—is designated as the “parent node” and the GM-X server configuration for this node can activate additional GM-X tables which are published to all the other participant nodes. Additional tables may include, for example, master data such as currency codes and units of measure which should be standardized to facilitate optimal communication between participants. Because these data are non-confidential, the data valve services described earlier aren't needed or utilized.

Any participant can choose to publish data to one or more of the other participants by selecting a suitable GM-X table as the distribution list. For example, the RESPONDING PARTY table allows a Buyer to identify all the Sellers who have been invited to submit quotes in response to a specific RFQ, and the QUOTE ROLE table identifies the Buyer to whom a specific quote is submitted. When the RFQ is published, it is considered confidential and visible only to the invited Sellers. Data valve services will be utilized and passwords will be encrypted using each invited Seller's public key. A quote is considered confidential and visible only to the Buyer who requested it. Data valve services will be utilized and a password will be encrypted using only the Buyer's public key.

Alternatively, participants can choose to publish data exclusively to the parent node. These data are intended to be confidential and visible only to the GM-X server at the parent node.

Accordingly, data value services will be utilized but passwords will only ever be encrypted using the parent node's public key. To support the collaborative procurement scenario described in this white paper, for example, this configuration would be useful only when the parent node belongs to a single Buyer, and all the other participant nodes belong to its Sellers.

The GM-X Blockchain Subsystem also provides the following additional capabilities:

- Guarantee of globally unique identification keys;
- Proof of participant identity;
- Preservation of referential integrity in blockchain transactions;
- Event-driven release of data to the blockchain;
- Retrieval of data from the blockchain; and
- Integration of other ERP applications.

Guarantee of Globally Unique Identification Keys

Many GM-X tables, including the QUOTE HEADER, PARTY, REQUEST and WORK EFFORT tables, have auto-incrementing primary keys (also known as “technical keys”) causing the underlying RDBMS or GM-X application programs to issue new values by adding 1 to the greatest existing primary key value when inserting new records into these tables. Whenever a table is propagated over the blockchain network, these values must be globally unique to prevent collisions at other participant nodes. But there can be no guarantee of global uniqueness when multiple systems—the GM-X Application and RDBMS servers shown in Figure 7—are issuing numeric identification keys independently from one another.

To solve this problem, Geoprise has enhanced most GM-X auto-incrementing primary keys to contain a maximum of 38 numeric digits divided into 2 implicit segments. The most significant segment, which may contain anywhere from 1 from 12 significant digits, is reserved for a globally unique participant identifier (the “Participant ID”); and the least significant segment contains auto-incrementing values that are left-padded with zeroes, if necessary, to form a fixed precision of 26 digits. Whenever a participant's GM-X system issues a new key value, it auto-increments the least significant segment by 1 and then prepends the Participant ID. This strategy completely avoids data collisions at other participant nodes by guaranteeing that all key values propagated to the blockchain are globally unique. It also theoretically enables the GM-X Application running at each participant node to insert one short of 100 octillion ($10^{26} - 1$) of its own database rows in each table, which far exceeds the capacity of any commercial ERP system on the market today.

GM-X is the world's first and only ERP system to natively incorporate all GS1 Class 1 Identification Keys standards into its database and application design.

It is therefore completely fluent in the global language of business.

This may seem like a purely technical matter, but astute readers will have already noticed a much broader supply chain implication. Today a variety of national and international standards exist for specifying unique identifiers for collaborative business processes. The most comprehensive of these, the GS1 Class 1 Identification Keys standards, have been promulgated for a wide variety of business objects including products and services (GTIN), parties and locations (GLN), logistics units (SSCC), returnable assets (GRAI), assets (GIAI), service provider and recipient relationships (GSRN), documents (GDTI), consignments (GINC), shipments (GSIN), digital coupons (GCN) and components

or parts (GPID). All of these identification systems achieve the goal of global uniqueness by prepending a globally-unique company prefix to each identification key. The GS1 company prefix, in turn, may be anywhere from 3 to 12 digits long, and the resulting identification keys may contain as few as a single numeric digit (GTIN, GLN, GRAI, GIAI, GDTI, GINC, GCN and CPID) to as many as 26 (GIAI, GINC and CPID). Using current versions of the Oracle, Microsoft SQL Server, MySQL and PostgreSQL databases, the design of GM-X auto-incrementing keys accommodates all these GS1 standards with no possibility of data collisions between blockchain network participants.

For this reason, an organization which has already licensed a GS1 company prefix number can use it as its Participant ID when joining a GM-X blockchain network.

In a blockchain, each participant's ERP must guarantee the avoidance of data collisions.

Many business organizations, however, have not adopted the GS1 Identification Keys standards and therefore haven't licensed a GS1 company prefix number. Many of them, especially those located in the U.S., may have a randomly-assigned 9-digit Data Universal Numbering System (D-U-N-S®) number issued by Dun & Bradstreet, but those numbers could collide with GS1 company prefix numbers. The GM-X application solves this problem by prepending the prefix 027 to each D-U-N-S number when constructing the Participant ID. The resulting range of Participant ID values accommodates any D-U-N-S number using exactly 12 numeric digits. According to GS1 standards, prefixes beginning with 02 are reserved for Restricted Circulation Numbers (RCNs) issued by companies. Any company in the world may use GS1 prefixes beginning with 02 for any purpose as long as the keys beginning with this prefix are kept within a restricted environment. This is the case for any GM-X blockchain network, which is restricted to its invited participants.

Other business organizations which join a GM-X blockchain may not have a GS1 company prefix or D-U-N-S number. For them, Geoprise prepends the prefix 028 to a randomly-generated number up to 9 digits long. The resulting range of Participant ID values accommodates one less than a billion ($10^9 - 1$) unique identities using Participant IDs varying in length from 4 to 9 digits. As for D-U-N-S numbers, this solution is fully compliant with the GS1 standard because any company in the world may use GS1 prefixes beginning with 02 for any purpose.

Proof of Participant Identity

As noted earlier, a variety of consensus mechanisms exist for verifying the validity of mined blocks in a blockchain. It is well established that proof of work (POW) is only useful when trustless consensus is required, as is the case with public, unpermissioned and anonymous (or pseudonymous) blockchains; otherwise it is a needless waste of resources. That's because a private or permissioned blockchain is not a trustless environment; even if the participants in a private or permissioned blockchain don't fully trust one another, they must nevertheless be accredited or trusted *enough* to have been invited in the first place.

Any trustworthiness assessment or accreditation of a person or organization requires proof of identity. As we also wrote in 2005, "Proof of identity is of course the crux of any bilateral trust model. That's because each party's ability to enforce its end of the contract depends, in turn, upon its ability to tell the difference between a legitimate representative of the other party, and an impostor. The usual ways of establishing identity on-line are the good old user ID and password, and digital certificates ... [but] in no way does a valid combination of [a user ID and password] prove a user's identity (in legalese, it's not 'probative evidence of identity')."

The ability to use GS1 company prefixes or D-U-N-S numbers as Participant IDs in a GM-X blockchain provides a powerful mechanism for proving the identity of each participant. To obtain a GS1 company prefix, for instance, it's necessary to submit an application to a GS1 Member Organization (MO), each of which serves a specific country and establishes country-specific criteria to qualify for the assignment of a company prefix. As an example, corporations or partnerships applying to Thailand's GS1 MO must present—along with their application form and payment—a certified copy of the Thailand Certificate of Business Registration issued by the Thailand Ministry of Commerce within the past 90 days, a certified copy of the firm's Tax Identification card or Value Added Tax registration certificate issued by the Thailand Revenue Department, a profit and loss statement certified by the firm's registered auditor, and an example of a company product or picture with authorized signature and company stamp. All these documents must bear an authorized signature and company stamp. In addition, corporations need to assign a person as their authorized officer by providing a letter of power of attorney (with Thailand stamp duty paid), and a certified copy of either an attorney's ID or the representative's national ID card. These documents offer probative evidence of the corporation's or partnership's identity as well as the identity of its authorized representative. If Thailand's GS1 MO is satisfied with the presented proof, it will issue a unique GS1 company prefix beginning with 885, which is the GS1 prefix for Thailand (the GS1 company prefix might therefore look something like "885513600"). It will also add the newly-issued prefix to the Global Electronic Party Information Registry (GEPIR), a free, anonymous and publicly accessible Web service which gives access to basic contact information for GS1 registrants. Other blockchain participants can use such resources to verify a prospective participant's identity during the participant onboarding process, as illustrated in Figure 9, below.

Toggle Column: [Company Prefix](#) - [Key Licensee GLN](#) [Expand all](#) | [Collapse all](#)

Show entries Search:

Key Licensee GLN	Co. Name	City	State	Province
8855136009999	Charoen Pokphand Foods PCL	Songkhla	--	--
GS1 Company Prefix				
GS1 Company Prefix	885513600			
Last Change Date	Oct. 25, 2016			
Party Data Language	en			
Return Code	Query Successful [RC-0]			
GS1 Company Prefix Licensee				
Party Name	Charoen Pokphand Foods PCL			
GLN	8855136009999			
GS1 Key Licensee				
Party Name	Charoen Pokphand Foods PCL			
GLN	8855136009999			
Address				
Company Name	Charoen Pokphand Foods PCL			
Street Address	No 79 Moo 10 Sub District Thabon District Ranod			
City	Songkhla			
City Code	90140			
Country Code	TH			
Contact				
Telephone	+667458755669			
Information Provider				
GLN	885888099997			

Figure 9 – Sample GEPIR Query

Source: GS1

This example demonstrates that it would be very difficult indeed for an impostor to obtain a GS1 company prefix in Thailand. Dun & Bradstreet follows similar procedures before issuing D-U-N-S numbers. For its part, Geoprise Technologies will only ever issue a Participant ID to a firm which:

- Demonstrates that it has not licensed a GS1 company prefix and does not have a D-U-N-S number;
- Has executed a GM-X Application Software License Agreement conferring a license to use the blockchain server bundled with the GM-X Application Suite, and which is currently in full force and effect; and
- Complies in full with Geoprise's "know your customer" (KYC) policies and procedures in a manner which provides compelling probative proof of identity to Geoprise.

Proof of identity is the crux of bilateral trust. Each party's ability to enforce its end of a contract depends upon its ability to tell the difference between a legitimate representative of the opposite party, and an impostor.

Because their true identities are also known to the other participants in a GM-X blockchain, those who are responsible for mining (validating) transactions, but perform malicious acts, can be expelled and perhaps prosecuted or sued for their transgressions. The possibility of recourse for malicious acts means that consensus can be achieved without the need for POW. As a result, transactions can be confirmed much faster, and the GM-X blockchain is exponentially more scalable.

Whenever a participant licenses GM-X for Blockchain software, the copy of the software which Geoprise ships to the licensee is permanently embossed with the unique Participant ID. In this way, each GM-X Application Server installation will only ever have one Participant ID: the one belonging to its licensee. The licensee's GM-X Application Server will use this Participant ID to construct all auto-incrementing primary key values ever inserted into the local GM-X database from sources other than the blockchain server (which is to say, that GM-X server, the participant's human GM-X users and any other computerized systems which integrate with the GM-X server).

As noted earlier, the blockchain server bundled with GM-X allows access to multiple GM-X blockchains from a single server node. It is therefore possible for a single participant to join two or more GM-X blockchains, each of which supports a different collaboration scenario. The other participants in any one of those blockchains need not be the same as those belonging to the other blockchains. However, a participant who joins two or more GM-X blockchains will run a single GM-X Application Server instance and use a single Participant ID for all those blockchains. This way, the data propagated to each blockchain always comes from a single source (the participant's GM-X Application and local database) and bears the same globally unique identification keys.

It's important to note that the GM-X Participant ID is not the same thing as the participant's blockchain address. Using the above example, GS1 company prefix 885513600 is a human-readable Participant ID which is visible in all auto-incrementing primary keys generated by the participant's GM-X server. A blockchain address looks like `1Yu2BuptuZSiBWfr2Qy4a1c6qEVnwPWrdkHPEc` which is the public key of the participant's digital signature and is the result of hashing the public key of an Elliptic Curve Digital Signature Algorithm (ECDSA) public-private key pair multiple times along with a blockchain version and checksum. This process is designed to ensure that addresses created on one GM-X blockchain are extremely unlikely to be valid on a second blockchain.

Preservation of Referential Integrity in Blockchain Transactions

When each participant sets up their GM-X system, all of an activated table's parents and children can be automatically activated as well, based on parent and child relationships defined by the table's class. This is necessary to preserve the referential integrity of propagated data. Thus, for example, if the GM-X Request Subsystem's QUOTE HEADER table is activated by a participant for propagation over the blockchain network then the parent CURRENCY CODE, QUOTE STATUS TYPE and QUOTE TYPE tables will be automatically activated also, together with the child QUOTE HEADER EXTRA VALUES, QUOTE ITEM, QUOTE ROLE, QUOTE STATUS HIST, QUOTE TERMS and RESPONDING PARTY tables. Figure 10, below, illustrates some of these data relationships.

The parent and child relationships defined by a table's class don't necessarily address all referential integrity requirements for a particular scenario. For example, the CURRENCY CODE table, which is a parent of the QUOTE HEADER table, has 1 parent table (UOM CATEGORY) and 12 child tables; and those tables—together with all their ancestors as well as the ancestors and descendants of all the other child tables referenced by the QUOTE HEADER table—can also be automatically activated when each participant sets up their GM-X system. To accelerate the setup procedure, the automatic activation settings can be accepted without any modifications, and indeed no performance penalty will be incurred by activating tables which are never actually used, since no data for these tables will ever propagate through the network.

However, it may be desirable to manually adjust the automatic activation settings under certain circumstances. For QUOTE ITEMS, all the PRODUCT table's 42 children, including the GM-X tables which hold bill of material details, will be activated automatically. This may or may not be necessary, depending on whether or not Sellers must reveal bills of material to Buyers for quoted products. If they are, then the automatic activation settings should not be changed; otherwise it would be prudent to deactivate the bill of material tables. This will prevent the propagation of useless information across the network, and make the blockchain more compact.

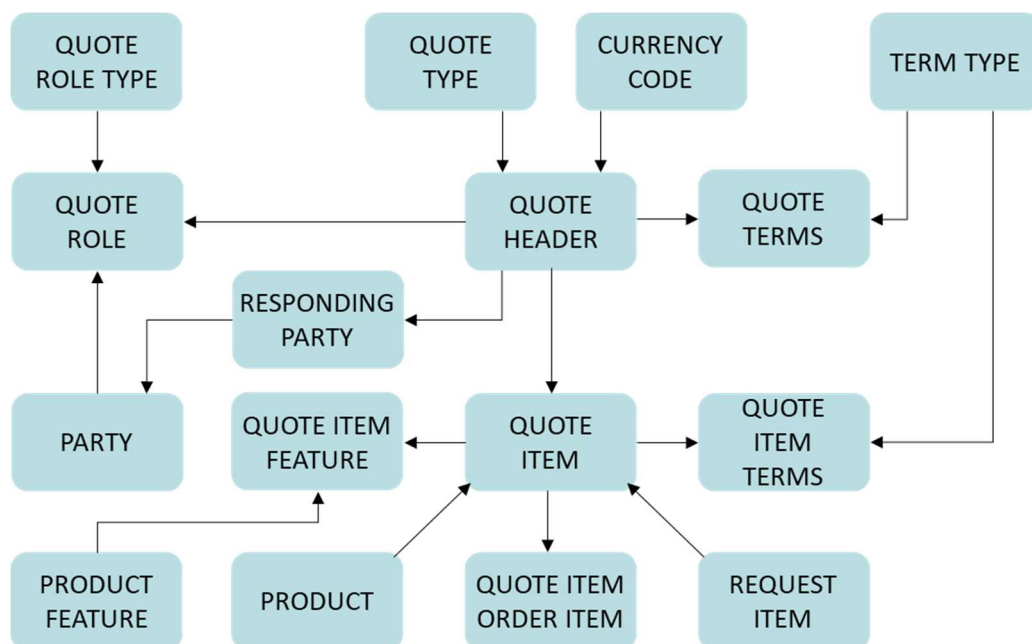


Figure 10 – Partial GM-X Relational Data Model for Quote Headers and Line Items

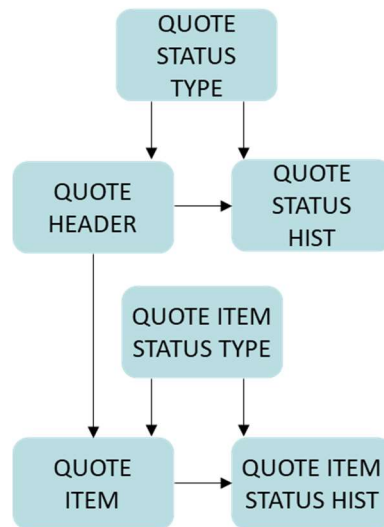


Figure 11 – GM-X Relational Data Model for Status Lifecycles of Quote Headers and Line Items

Event-Driven Release of Data to the Blockchain

A great many GM-X objects have built-in status lifecycles. For example, each Seller quote has a current status such as ‘Pending’, ‘Submitted’, ‘Acknowledged’, ‘Withdrawn’, ‘In Review’, ‘Returned’, ‘On Hold’, ‘Rejected’ or ‘Accepted.’ One or more of these status values can be designated as lifecycle states which trigger the propagation of transaction data to the other participants in the network.

If ‘Submitted’ is designated as a lifecycle state for propagation then a Seller who has not yet decided to submit a quote can leave its status as ‘Pending’, which retains the quote exclusively on the Seller’s local GM-X database server.

As soon as the Seller changes the status of the quote to ‘Submitted’, all the data related to that quote is appended to the blockchain and propagates through the network as a ‘Submitted’ quote. The process is completely analogous to saving an email that you are currently drafting in the ‘Drafts’ folder of your local email client, and then hitting the ‘Send’ button only when you’ve completed and reviewed the draft.

If the Seller later decides to withdraw the quote, and has also designated ‘Withdrawn’ as a lifecycle state for propagation, the updated quote will also be appended to the blockchain and propagates through the network as a ‘Withdrawn’ quote.

Retrieval of Data from the Blockchain

As explained earlier, the blockchain server bundled with GM-X is responsible for passing each new transaction to the GM-X Application Server running at each recipient’s node. This happens immediately after the transaction is decrypted, if the transaction is encrypted and the recipient is authorized to see it. The method for writing new transactions to the local GM-X database is triggered automatically and performs inserts, updates or deletions based on the current state of the GM-X database and file system at the recipient’s node, regardless of whether an insert, update or deletion originally occurred at the sender’s node. No human intervention is required for error-free transactions. Any errors encountered are written to an error log.

Integration of Other ERP Applications

Should a GM-X blockchain participant wish to use a bespoke or commercial off-the-shelf (COTS) legacy ERP package instead of the GM-X Application locally, that system must be adapted to send unencrypted data to the blockchain in a manner similar to the clear text shown in Illustration 1, and also to receive unencrypted data from the blockchain as described above. Crucially, to maintain data integrity and prevent data collisions, the legacy ERP package may also need to be modified to preserve referential integrity and support globally unique auto-incrementing keys within the legacy database.

Those modifications would generally utilize whatever systems integration technology or application program interfaces (APIs) the legacy ERP system supports to access a set of standard APIs exposed by the blockchain server bundled with the GM-X Application. Figure 12, below, illustrates a major consultancy's view of how such integration would work.

To send unencrypted data to the blockchain after it is organized and formatted as shown in Illustration 1, the GM-X Application's blockchain server exposes a set of JavaScript Object Notation Remote Procedure Call Application Programming Interface (JSON-RPC API) commands for:

- Creating new data streams on the blockchain; and
- Publishing transactions to streams.

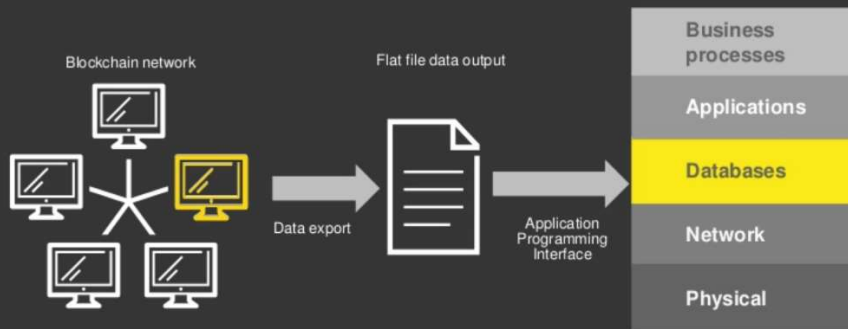
The blockchain server also exposes additional JSON-RPC API commands for:

- Subscribing to streams;
- Unsubscribing from streams;
- Listing all transactions within streams or specific blocks;
- Listing transactions within streams or specific blocks having a given key value;
- Listing transactions within streams or specific blocks from a specific publisher node; and
- Retrieving specific transactions from streams.

Additional C#, Go, Java, JavaScript, PHP, Python and Ruby wrappers for the JSON-RPC API commands are also available from third parties.

Do enterprises need to replace their ERP systems to reap the benefits of blockchain technology?

Blockchain resides at the edges of ERP applications, enabling enterprises fully to utilize blockchain's benefits without changing their existing ERP infrastructure. This can be accomplished easily by establishing an Application Programming Interface layer between the node and the database. Each participant or node on the network maintains its own copy of the transaction ledger, which can be used as an input on the database layer.



Page 16

EY Global Blockchain Summit



Figure 12 – A Major Consultancy's View of Integrating Blockchain with Legacy ERP Systems

Source: Ernst & Young (EY Global Blockchain Summit, April 2017)

Deploying and running the GM-X ERP Application Server and database locally may be a simpler and more cost-effective approach, even when it is necessary to continue using a legacy ERP system, because no development would be required to send data to the blockchain, or receive data from it. Instead, as illustrated in Figure 13, below, the local GM-X ERP Application Server could be deployed as a middleware engine to store data in the GM-X database according to the native and normalized GM-X enterprise data model; and then utilize conventional extract, transform and load (ETL) processes and APIs to transfer data between GM-X and the legacy ERP system.

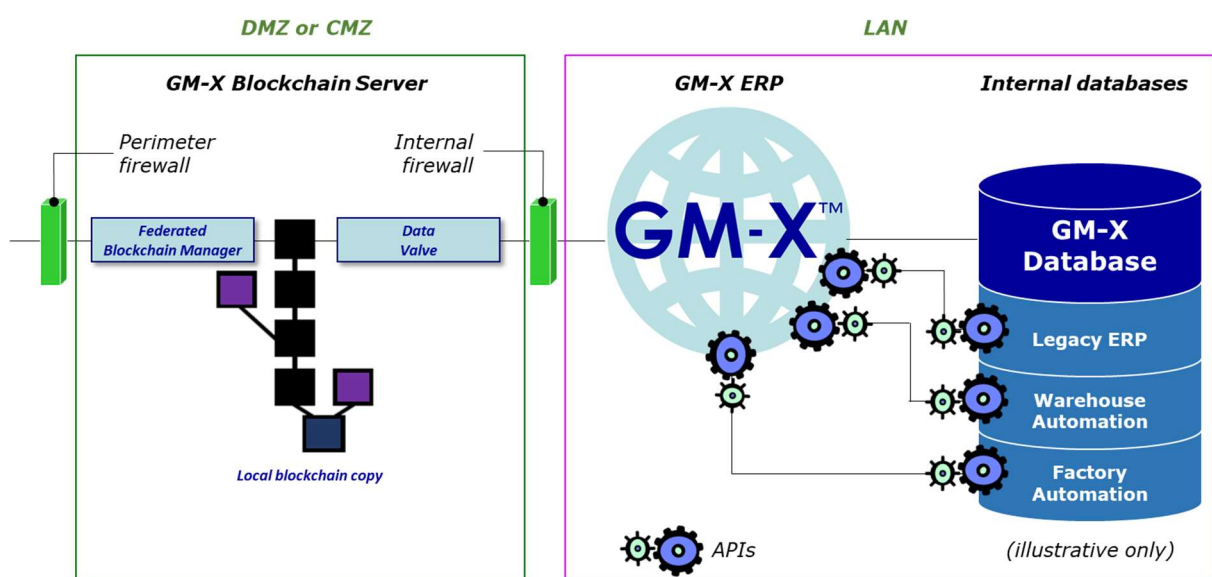


Figure 13 – Deploying GM-X ERP as a Middleware Engine Between a Blockchain and Legacy ERP

STRATEGIC IMPLICATIONS FOR ENTERPRISES

“Some predict that the peer-to-peer nature of the blockchain could transform ERP and business processes fundamentally. Currently, the ERP business model is centered around individual enterprises. Blockchain technology allows an ecosystem of companies to organize and share data where the primary metric is the performance of the ecosystem and not the individual enterprise. [ERP] might evolve and eventually include ecosystem resource planning, in other words. While this may or may not be the direction of things for ERP systems, what is more clear is that blockchain technology within ERP is just around the corner. ‘By the end of 2017, there will be blockchain-enabled ERP applications in production at many companies in several industries,’ says Jack Shaw at American Blockchain Council. ‘Supply chain and logistics will be the most widely used at first. By 2020, use of Blockchain-enabled ERP will be widespread.’”

– Peter Kowalke, Ziff Davis

The collaborative procurement scenario described in this white paper is by no means the only scenario for which the GM-X ERP system could be deployed as part of a private, permissioned blockchain. Other scenarios are illustrated in Figure 14, below, and include:

- Collaborative supplier qualification and audit;
- Collaborative sales, distribution and invoicing;
- Collaborative shipment tracking;
- Execution of projects when resources are provided by multiple organizations or teams, both internal and external;
- Collaborative customer feedback;
- Global inventory management across multiple warehouses as well as in-transit, consignment, field and trunk stock, without having to reconcile stock;
- Archive and records management;
- Provenance tracking (“track-and-trace”), which is tracking the origin and movement of items across a supply chain, such as safety-critical automotive components, pharmaceuticals, luxury goods, apparel, food products, cosmetics and electronics; and
- Collective recording and notarizing of supply chain data between organizations, to eliminate reconciliation time, effort and cost.

Returning to the introductory theme of this white paper, it’s instructive to go back in time to the last great transformation from mainframe to three-tier client/server computing which occurred during the 1990s. To be sure, this transformation was motivated by the emergence of two new technologies which were disruptive for their time: the Internet, and “smart” PCs sporting fancy graphical user interfaces instead of dumb “green-screen” terminals. But it was propelled by an even more compelling event, which was the coming millennium and the urgent need to fix or replace systems which were vulnerable to the so-called “millennium bug” (also known as the “Y2K bug”), to avoid disruption of business operations.

Confronting this compelling event, and motivated by the availability of new technologies, most enterprises opted to replace their existing ERP systems instead of patching them.

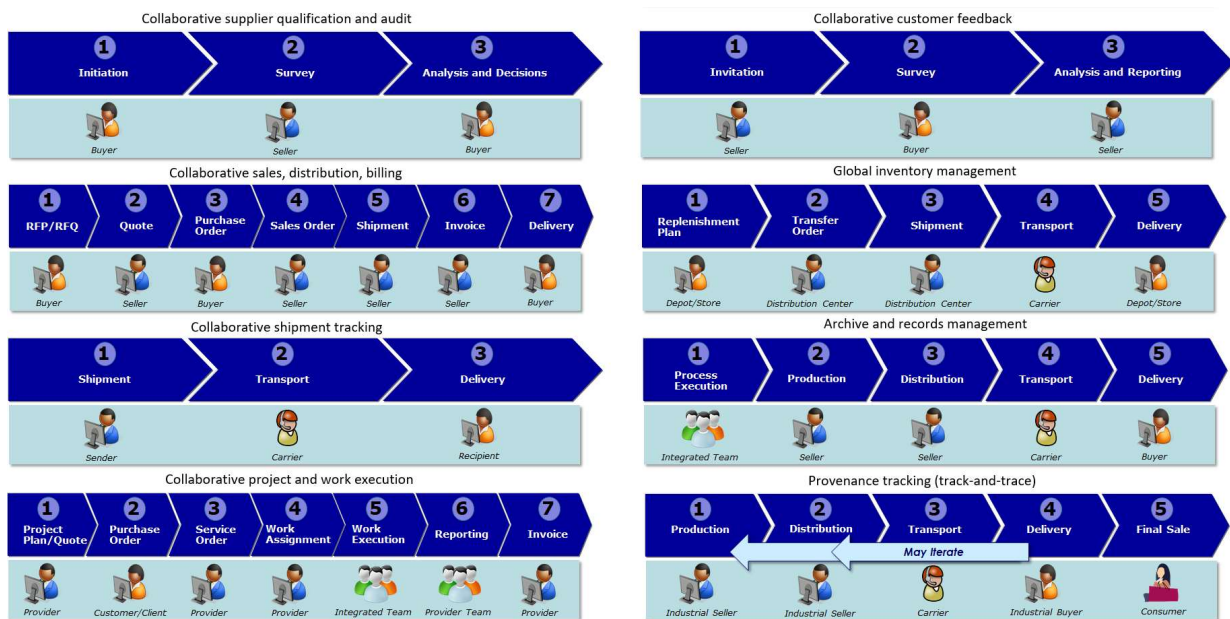


Figure 14 – End-to-End Ecosystem Resource Planning Scenarios Supported by GM-X for Blockchain

Today, by and large, those replacement systems are still in use but are by now a quarter-century old. New technologies have emerged since then including Web applications, powerful encryption and the blockchain, which those replacement—and by now, legacy—systems were never designed or engineered to utilize. The new technology greatly interests information technology professionals, but building the business case for deploying it has been a challenge.

It takes a compelling event to build a compelling business case. That compelling event is today's security breach pandemic, which is destroying corporate as well as professional reputations and wiping enterprise value away by the billions.

Faced with this new compelling event, Geoprise Technologies is certain that most enterprises will opt to replace their existing ERP systems instead of patching them, just as they did in the 1990s. As they search for replacements, they will discover that none of the enterprise-grade COTS ERP packages on the market today are collision-proof, which means that none are blockchain-ready—except GM-X ERP for Blockchain. Competitors will no doubt rise to the challenge in the future but, today, GM-X ERP for Blockchain is the only blockchain-ready replacement ERP system available for consideration.

ACRONYMS

3PL: third party logistics provider
AES: Advanced Encryption Standard
API: application programming interface
ASN: advance shipment notification
CAD: computer-aided design
CAGR: compound annual growth rate
CMZ: classified military zone
COTS: commercial off-the-shelf software
CSRF: cross-site request forgery
DMZ: demilitarized zone
D-U-N-S: Data Universal Numbering System
ECDSA: Elliptic Curve Digital Signature Algorithm
EDI: electronic data interchange
ERP: enterprise resources planning; ecosystem resource planning
ETL: extract, transform and load
GCN: global coupon number
GDTI: global document type identifier
GEPIR: Global Electronic Party Information Registry
GIAI: global individual asset identifier
GINC: global identification number for consignment
GLN: global location number
GPID: global component/part identifier
GPO: group policy object
GRAI: global returnable asset identifier
GSIN: global shipment identification number
GSRN: global service relation number
GTIN: global trade item number
HTTP: hypertext transfer protocol
HTTPS: secure hypertext transfer protocol
IP: Internet protocol
IT: information technology
JSON: JavaScript Object Notation
KYC: know your customer
LAN: local area network
PC: personal computer
PO: purchase order
POW: proof of work
RPC: remote procedure call
RDBMS: relational database management system
RFP: request for proposal
RFQ: request for quotation
RSA: Rivest-Shamir-Adleman cryptosystem
SaaS: Software-as-a-Service
SFA: sales force automation
SHA: secure hash algorithm
SQL: structured query language
SRM: supplier relationship management
SSCC: serialized shipping container code
TFA: two-factor authentication
URL: uniform resource locator
VPN: virtual private network
WAN: wide area network
XSS: cross-site scripting



www.geoprise.com

Corporate Headquarters

Geoprise Technologies Corporation

601 Carlson Parkway
Suite 1050
Minnetonka, MN 55305-5219
USA

USA, Canada and Puerto Rico

Toll-free phone: 1 888 965 8868

Toll-free fax: 1 888 965 8868

Outside the USA, Canada and Puerto Rico

Phone: +1 310 209 8973

Fax: +1 310 209 8973

Asia-Pacific Headquarters

Geoprise Technologies Co., Ltd.

3F, 72/322 Moo 8, Rattana Thibet Road
Bangkrasor, Muang, Nonthaburi 11000
THAILAND

Phone: +66 (0)2 965 8868

Fax: +66 (0)2 965 7761

Singapore

Geoprise Technologies Pte. Ltd.

(201333331K)
137 Market Street
Level 6
SINGAPORE 048943

Phone: +65 3158 0453

Fax: +65 6809 3701

ABOUT GEOPRISE TECHNOLOGIES

Geoprise Technologies was formed in 1999 by a group of software executives with over a century of previous cumulative experience building enterprise resources planning (ERP) and manufacturing operations management systems, and implementing them worldwide.

Our mission, then and now, is to create exceptional value for our customers by harnessing the power and economy of information technology to enable lean, world-class industrial operations on a global scale.

Today, Geoprise Technologies focuses exclusively on delivering top-quality expertise and technology solutions for businesses operating in Asia and the Pacific Rim, Europe and North America. We concentrate our expertise in three practice areas, strategy and operations, product lifecycle management and information technology, serving primarily the life sciences, aerospace and defense, automotive, construction, consumer products, energy, food products and machinery & equipment sectors.

We deliver value with the utmost integrity by maintaining strict independence from other professional firms and technology providers, intense commitment to business ethics and profound respect for intellectual property rights.

DISCLAIMER

The material included in this publication is intended as a general guide only, and its applicability to specific situations will depend on the circumstances involved. You should not rely upon this information as final advice. While we have made all reasonable attempts to verify the accuracy of the information contained herein as at the publication date, Geoprise Technologies accepts no responsibility for any errors or omissions it may contain, whether caused by negligence or otherwise. Neither does Geoprise Technologies accept any responsibility for any losses, however caused, sustained by any person that relies upon it.

Geoprise™, the Geoprise logo, Geoprise Technologies™, GM-X™ and the GM-X logo are trademarks of Geoprise Technologies Corporation and/or its subsidiaries in the United States of America and other countries.

Amazon®, Amazon Web Services® and AWS® are either registered trademarks or trademarks of Amazon Services LLC in the United States. D-U-N-S® is a registered trademark of Dun & Bradstreet, Inc. in the United States. Google® is a registered trademark of Google, Inc. in the United States and other countries. GS1® is a registered trademark of GS1 AISBL in Belgium, the United States and other countries. The term "Linux" is a registered trademark of Linus Torvalds, the original author of the Linux kernel. Microsoft®, Azure® and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries. Oracle®, Java®, JavaScript® and MySQL® are registered trademarks of Oracle Corporation and/or its affiliates. Python® is a registered trademark of the Python Software Foundation. Ruby on Rails® is a registered trademark of David Heinemeier Hansson. All other product names referenced herein may be the trademarks of their respective owners.

Copyright © 2018 by Geoprise Technologies Corporation, All Rights Reserved.

Designed and produced at Geoprise, Thailand. Front cover photo credit: Tiago Fioreze.