Technical Assistance Consultant's Report

Project Number: 47192-001
October 2018

Regional: Development of a Global e-Government Procurement Architecture using Blockchain Technology

Prepared by

Dr. Ramanathan Somasundaram
India

S.M. Quamrul Hasan
Washington, United States of America
Solutions and Innovation in Procurement, The World Bank Group

For the Asian Development Bank

Asian Development Bank

DISCLAIMER

ABOUT THE AUTHORS

Dr. Ramanathan Somasundaram researched e-Government Procurement (e-GP) for his doctoral thesis work in Denmark and has more than 10 years of experience in Consulting, Implementation and Assessment of e-GP systems. He can be reached at ram@gugaservices.com.

S.M. Quamrul Hasan is a Senior Procurement Specialist at the 'Solutions and Innovations in Procurement' Team of the World Bank. His areas of interest include the modernization of public procurement systems through digitization and adoption of disruptive technology. Having trained in Software Engineering and Business Administration, Mr. Hasan has supported public procurement systems in the World Bank's South Asia, Africa, Europe and Central Asia regions. He can be reached at shasan@worldbank.org.

ABBREVIATIONS

ADB	–	Asian Development Bank
AoC	–	award of contract
B2B	–	Business to Business
B2C	–	Business to Consumer
BG	–	bank guarantee
BID	–	Unique ID for a Bank
DMC	–	developing member country
DPR	–	detailed project report
e-GP	–	electronic government procurement
ERP	–	Enterprise Resource Planning
GID	–	Global Blockchain ID for suppliers
ICB	–	international competitive bidding
MDB	–	multilateral development banks
NIT	–	Notice Inviting Tender
OCDS	–	Open Contracting Data Standard
P2P	–	Procure to Pay
PEPPOL	–	Pan European Public Procurement On-Line
PID	–	Purchasing Agency ID
PIU	–	Project Implementation Unit
PKI	–	Public Key Infrastructure
SAAS	–	Software As A Service
TTP	–	Trusted Third Party

NOTE

In this report, "$" refers to US dollars

CONTENTS

FIGURES

EXECUTIVE SUMMARY

1. e-Government Procurement systems (e-GP) have been operational for close to 2 decades now. Many countries in America, Europe and Asia Pacific have adopted e-GP and countries in the African region are now getting on-boarded. The number of e-GP installations worldwide will be in the range of 200 – 250. It is just a question of time before close to 100% of the countries will have adopted e-GP and almost all the government procurement will happen online in e-GP.

2. Though the implementation of e-GP systems has contributed to enhanced efficiency and transparency in government procurement, there is potential for further advancement of the existing systems:

(i) Data level interoperability requirements: Presently, a couple of hundred e-GP systems would be operational, all of which now function in silos. Both government and the supplier community will stand to gain immensely when the e-GP systems could be made interoperable at least at the data level.
(ii) De-duplicated supplier database: Many countries have had good success in developing a national database of suppliers. However, till date, there is not a reliable mechanism to de-duplicate and distinctly identify suppliers across all the e-GP systems world-wide.
(iii) Online repository of work experience certificates: A system has to be developed to enable bidders to submit their work experience certificates in an authenticated electronic format from any e-GP system across a region or even the world and not just within the national borders.
(iv) Real-Time View of Contracts Pending Completion: Purchasing agencies require a facility to pull in real-time a bidder's work-in-hand contract information from multiple e-GP systems.
(v) Electronic Performance Bank Guarantee Submission in a Distributed e-GP System Environment: Can a system be developed to enable banks to submit authenticated bank guarantees in electronic format across any of the e-GP systems world-wide

3. The vision for the global e-GP architecture is to inter-link and correlate relevant data from all the e-GP systems primarily for the development of:

(i) A de-duplicated global database of suppliers, and
(ii) An authenticated, global online repository of work experience certificates

4. The e-GP Blockchain network should be extended to enable Banks located anywhere in the world to seamlessly submit authenticated Electronic Performance Bank Guarantees on behalf of a supplier in any of the networked e-GP systems.

5. The key design principles underlying the global e-GP architecture are:

(i) Build on existing e-GP systems,
(ii) Incentivize *de facto* adoption of standards,
(iii) Open network with minimal entry barriers, and
(iv) Near zero transaction costs.

6. It is proposed to implement the envisaged global e-GP architecture using Blockchain technology. The e-GP Blockchain is envisaged as a public network, but it will not be as open as the Bitcoin Blockchain as explained below:

(i) Only transactions pertaining to e-GP systems will be recorded in the e-GP Blockchain
(ii) Instead of creating an open competition based system wherein Miners are remunerated, the stakeholders in the e-GP Blockchain Network would be asked to volunteer as Miners
(iii) Anyone can volunteer to run a full node and contribute towards building consensus in the Blockchain

7. It is proposed to build the e-GP Blockchain network on top of the existing couple of hundred e-GP systems located worldwide. The identity of e-GP systems has to be verified and then a unique Blockchain network ID will be issued. Thus, e-GP systems will get registered in the Blockchain network. Each system in the e-GP Blockchain network will be issued a private-public key pair generated from a central Public Key Infrastructure (PKI) server established specifically for the Blockchain network.

8. The number of registered suppliers in all the e-GP systems world-wide will be in millions and it will continuously grow in the years to come. The task at hand, which is essentially the single most complex problem to solve for building the global e-GP Blockchain network, is creation of a de-duplicated supplier database across all the e-GP systems. When a supplier is uniquely identified by a Global Blockchain ID (GID), it will be possible to correlate supplier activities across e-GP systems worldwide on boarded in the e-GP Blockchain network as given below:

(i) Authentic records about the contracts awarded to a supplier in e-GP systems,
(ii) The status of contracts under execution by a supplier in e-GP systems, and
(iii) Whether a supplier is blacklisted or not can be verified.

9. It is proposed to on-board suppliers onto the e-GP Blockchain network based on inputs received from e-GP systems registered in the network. An e-GP system on-boarded in the Blockchain network will act as a Trusted Third Party (TTP) and provide inputs required to create GID for suppliers. A central e-GP Blockchain server will create a unique GID in response to each request received from e-GP systems already registered in the Blockchain network. Just as it is with the user ID creation for e-GP systems, a private-public key pair will be generated from a central e-GP Blockchain PKI server for each GID.

10. As the e-GP Blockchain server does not undertake any verification of user identity, a user with multiple user IDs in the source e-GP system will get a GID for each user ID it has in the e-GP system. It is argued that the suppliers would seed one single GID in all the e-GP systems when the following 2 conditions are implemented:

(i) The e-GP systems mandate suppliers to submit the following information as Blockchain records during online bid submission: award of contract (AoC), available spare capacity and work experience certificate. The Suppliers will be required to submit Blockchain records at least from those e-GP systems already on the e-GP Blockchain network.
(ii) A Supplier will need to record its GID as a pre-requisite for submitting Blockchain record of its work experience in an e-GP system. If a supplier's GID is not already seeded, the e-GP system will disallow the supplier from submitting Blockchain record of its work experiences. A Blockchain record of supplier's work experience cannot be created unless it has GID of the supplier recorded in it. If GID of a supplier seeded in the e-GP system does not match with the GID specified in the

e-GP Blockchain record imported by the Supplier, the e-GP system will reject the upload. Consequently, the supplier will either need to update its GID in the Blockchain record or in the e-GP system and thus de-duplicate and synchronize its GID across all e-GP systems.

11. The implementation of these 2 conditions consistently across all the e-GP systems is an essential requirement for development of a de-duplicated global supplier database. By design, there will be duplicate GIDs in the e-GP Blockchain during the initial years. The extent of duplicate GIDs in the e-GP Blockchain will gradually reduce, as more e-GP systems get on-boarded onto the e-GP Blockchain network and the 2 conditions explained above get implemented.

12. If a supplier could be identified by one single GID across all e-GP systems, it will require standard software development work to develop a global online repository of work experiences using Blockchain technology. The different work experiences that can be recorded and retrieved from the e-GP Blockchain are:

(i) contract award information,
(ii) work in progress, and
(iii) work experience certificates.

13. The online repository of work experiences will initially be limited to the experiences recorded in e-GP systems on boarded in the e-GP Blockchain network. Subsequently, the e-GP Blockchain network could be expanded to cover e-Procurement systems used by the private sector as well. Then, suppliers' work experiences from both government and the private sector can be pulled from the Blockchain network.

14. In all e-GP systems, a bid or a contract is uniquely identified and the unique ID reference is known to the bidders. Given which, if the following actors can be uniquely identified, it will be possible to issue authenticated bank guarantees across national borders:

(i) bank,
(ii) supplier, and
(iii) e-GP system.

15. Of the 3, supplier and e-GP system will be uniquely identified in the e-GP Blockchain network. If identity of a Bank is not confirmedly known, it will be impossible to evaluate and confirm authenticity of a Bank Guarantee. Hence, it is essential to issue a unique identity to Banks either as a user type in the e-GP Blockchain network or in the bank Blockchain network. The process for creating user ID for banks and e-GP systems will be just the same.

16. A set of 3 variants of the electronic bank guarantee are identified, depending on the extent to which the bank guarantee message published by the bank is confidential or encrypted. In the fully open variant, the entire message is published as plain text which any interested party can view in the e-GP Blockchain. Except for identity of the e-GP system, all other key details are encrypted in the partially confidential bank guarantee. In the most confidential version, all key details including the intended recipient (i.e. e-GP system) is encrypted. The procedure to be followed to process the messages varies depending on the extent to which a message is encrypted. Also, the consensus rules can be verified by the larger public only to the extent the messages are published as plain text.

17. The software required for building and managing the e-GP Blockchain network will need to be developed and maintained by a central nodal agency. The policies governing the e-GP Blockchain network will need to be framed at first based on which the functional and technical requirements of the software will need to be prepared. The key functional components of the envisaged software are:

(i) Identity management module
(ii) Central messaging system
(iii) Central Public Key Infrastructure (PKI) server
(iv) Mining client
(v) Full nodes

18. As extensive ground work has already happened in development of the Open Contracting Data Standard (OCDS), it is strongly recommended that OCDS standards are evolved and converged with the e-GP Blockchain initiative. Then, e-GP system owners need not comply with the OCDS for the sake of desired outcomes such as transparency. Instead, the compliance to OCDS will become a necessity because the Suppliers will demand purchasing agencies to logically complete the procurement activity in the e-GP system and publish the contracting data in the e-GP Blockchain as per OCDS standards, so they can cite the Blockchain records while they bid for tenders in e-GP systems.

19. The envisaged e-GP Blockchain network would be more open and extensible as compared to the Pan European Public Procurement On-Line (PEPPOL) initiative by the European Union. However, PEPPOL and e-GP Blockchain are similar in some aspects.

20. The following benefits can be realized when the envisaged e-GP Blockchain network is fully implemented and widely adopted:

(i) performance rating
(ii) simplified external IT system integration
(iii) expedited procurement and reduced transaction costs

21. The following key activities have to be finalized to operationalize the e-GP Blockchain network:

(i) governance mechanism
(ii) funding
(iii) pilot

I. BACKGROUND

22. The adoption of e-government procurement (e-GP) is now widespread across the globe. Most countries have adopted e-GP and it can be said that e-GP as an innovation has reached the late majority phase in the diffusion of innovations model. Refer to Figure 1 for a pictorial view on the adoption status of e-GP as on August 2018.

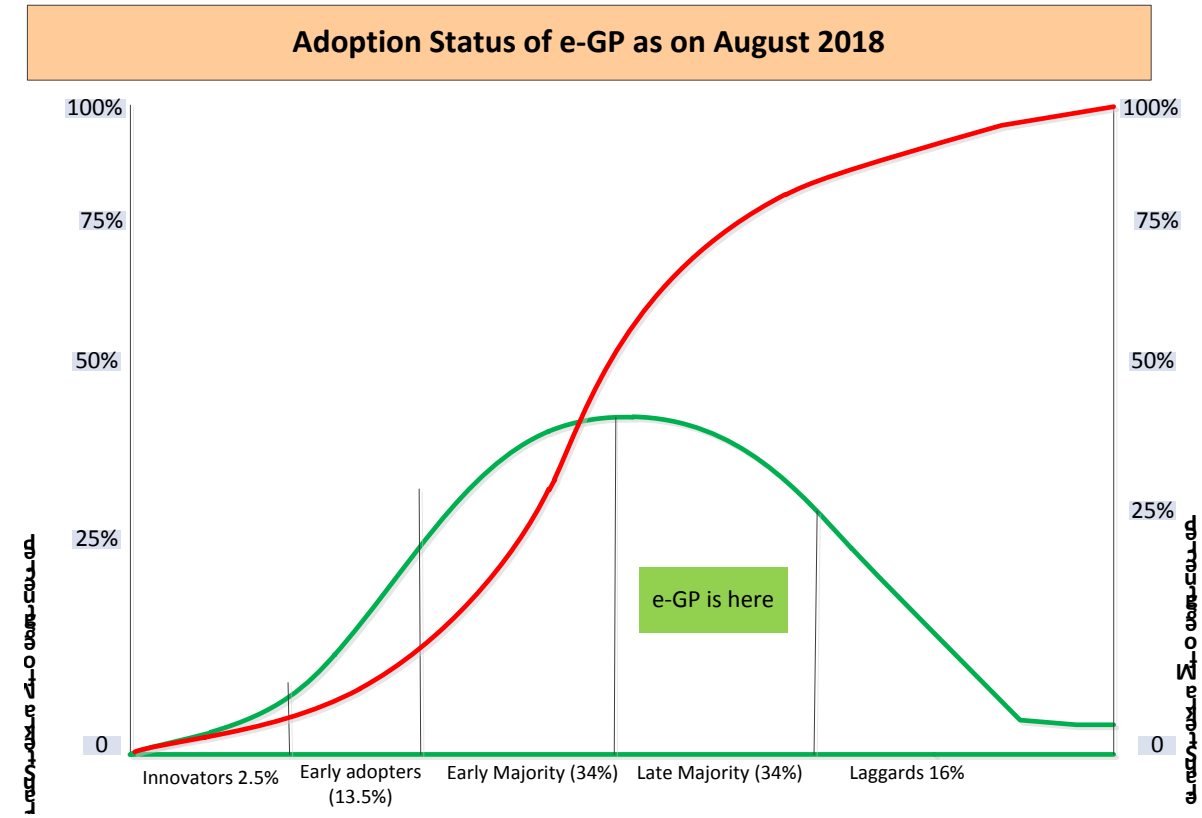

Figure 1: Adoption Status of e-GP as on August 2018 (not precisely fit to scale)

23. The Asian Development Bank (ADB) conducted survey of its developing member countries (DMC) in the Asia Pacific region to learn about the status of e-GP adoption in 2011, 2014 and 2017. As on 2017, 22 out of the 37 surveyed countries had adopted e-GP. Refer to Figure 2 for an overview of the adoption timelines. Few countries in the region such as South Korea and Singapore which were not included in the survey adopted e-GP quite early. It is close to 2 decades since the initial e-GP systems were adopted in the Asia Pacific region. Many countries in America and Europe adopted e-GP within the last 2 decades just as countries in the Asia Pacific region. A few countries in the African region have started e-GP adoption in the recent years and the pace of adoption in the region is now increasing. Given the availability of e-GP on Software As A Service (SAAS) model, even countries with small population can use e-GP for handling their government procurement online. Hence, it is just a question of time before close to 100% of the countries will have adopted e-GP.

Timeline Depicting the Start of e-GP Implementation in 22 Countries (2017 Survey)

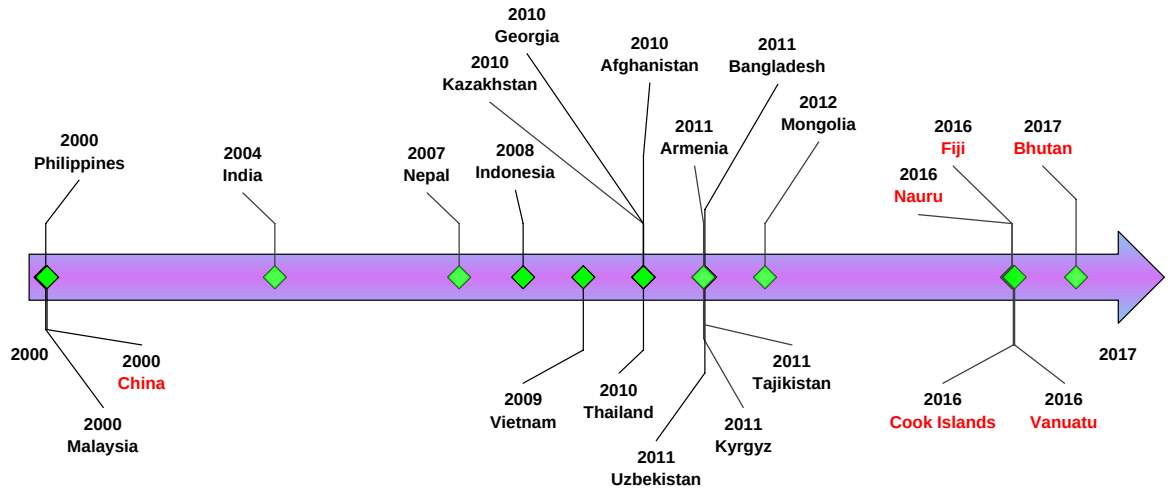

Figure 2: Timeline depicting the start of e-GP Implementation in 22 Countries[1]

[1] Source: A report by ADB "Regional: Consolidated View and Analysis of Survey Responses on e-Government Procurement System (2017)"

II. PROBLEM STATEMENT

24. Though the implementation of e-GP systems has contributed to enhanced efficiency and transparency in government procurement, there is potential for further advancement of the existing systems.

25. Data Level Inter-Operability Requirements: Few countries such as Kyrgyz Republic, Bangladesh, Philippines and Chile have had success in implementing a unified e-GP platform (i.e. one single platform used as a shared infrastructure by all government agencies in the Country). Large economies such as the USA, China, Australia and India have multiple e-GP systems in operation. India for example has more than 50 e-GP installations. Large public sector enterprises seek to implement an organization specific end-to-end Enterprise Resource Planning (ERP) type of IT systems covering all business functions including procurement and contract management. Hence, for political and technological reasons, most countries have more than one e-GP system. Unless the many e-GP systems are made inter-operable, Governments and the supplier community will not be able to realize the full benefits of e-GP. Hence, a mechanism is required to enable at least data level if not process level inter-operability among the multiple e-GP systems.

26. The key data level inter-operability requirements are:

(i) A de-duplicated supplier database with each supplier distinctly identified across all the e-GP systems, and
(ii) Authenticated work experience certificates consolidated directly from multiple e-GP systems using Open Contracting Data Standard (OCDS).[2]

27. Of the 2 requirements listed above, the establishment of a de-duplicated supplier database is the most critical and also the most difficult to implement. When a supplier can be distinctly identified across e-GP systems, it will be relatively easier to consolidate authenticated work experience data of suppliers from multiple e-GP systems.

28. De-duplicated Supplier Database: In many e-GP systems, a user can get registered as a supplier by filling an online form with email address and a few more data fields. As there is not any identity validation, a user can have duplicate identities in such e-GP systems. In some e-GP systems, users are required to authenticate their identity vis-à-vis a pre-existing national ID database (e.g.) social security number or tax ID. Such verification however can be done only for users having an identity in the referenced database. As on date, there is not any reliable mechanism to verify user identity across national borders during supplier registration.

29. Online Repository of Work Experience Certificates: Though e-GP refers to the entire Procure-to-Pay (P2P) cycle, most of the existing implementations only handle the tendering or bidding function online. Government agencies have in the recent years increasingly focused on external IT system integration to pull directly from 3rd party systems (e.g. tax clearance certificate and company registration certificate) as many of the documentary evidences required from bidders as possible. In systems where award of contract and contract management functions are executed online, it is possible for the bidders to cite their work experience certificates generated from within the same e-GP system. However, if a bidder had executed work in a contract it had obtained in a different e-GP system, the bidder will need to get the work experience certificate in physical form, scan and upload the same as part of its bid. Indeed, the scanned copy of work

2 https://en.wikipedia.org/wiki/Open_Contracting_Data_Standard

experience certificates will not be as authentic as that of an electronic certificate generated directly from the source IT system where the work was awarded or contract execution was managed. In a large country such as India which has more than 50 e-GP installations, it is practically not possible to directly interlink the 50+ e-GP systems with one another. In this globalized world with the emergence of regional blocks such as the European Union (EU) and Eurasian Customs Union, a system has to be developed to enable bidders to submit their work experience certificates in authenticated electronic format from any e-GP system across a region or even the world and not just within the national borders.

30. Real-Time View of Contracts Pending Completion: Often, a bidder which is already overloaded with contracts pending completion is awarded additional contracts primarily due to lack of knowledge about the pending work-in-hand. This challenge can be addressed only when purchasing agencies have the facility to pull in real-time the bidder's work-in-hand contract information from multiple e-GP systems. To obtain this data, the bidder has to be identified by a unique reference across all the e-GP systems. Further, a mechanism needs to be set-up to pull award of contract and current work execution status data from multiple e-GP systems on demand.

31. Electronic Performance Bank Guarantee Submission in a Distributed e-GP System Environment: An e-GP system should under ideal circumstances handle the Procure to Pay (P2P) cycle entirely electronically. In practice though, few documents are submitted in manual format due to lack of readiness of the eco-system. For example, in many e-GP systems, bidders are required to submit a scanned copy of the bank guarantee during bid submission towards bid security. Besides uploading the scanned copy, bidders are required to submit original copy of the bank guarantee in the location specified in the bidding document before the submission deadline. Bidders need to physically visit the government office or arrange to submit the original by surface mail to comply with this requirement. Hence, when a part of the process is handled manually, the full benefits of e-GP are not realized. Also, there are instances where a procuring entity learns when it seeks to liquidate that a bank guarantee submitted in manual format is not genuine or the supplier's bank refuses to honour the Guarantee. Few Governments such as Mongolia and South Korea have empanelled a set of National Banks for submission of bank guarantee in electronic format. A designated bank representative logs into the e-GP system, digitally signs as required and submits bank guarantee on behalf of suppliers (i.e. bank's customers) specifically with reference to an online bid before expiry of the bid submission deadline. All stakeholders would be aware that the bank guarantee thus submitted is authentic as it is directly submitted by the banks. This model is found to work well in countries with a unified e-GP platform and for national competitive bidding (NCB) tenders, wherein bank guarantee is compulsorily issued by the national banks.

32. In international competitive bidding (ICB) tenders, bidders can participate from anywhere in the world. As it is not possible for e-GP system owners to empanel banks from all over the world, it is unviable to extend this model of online bank guarantee submission for ICB tenders. Further, implementation of this empanelment model is inefficient in countries with multiple e-GP systems due to the reasons forthwith. Take for example the case of India which has more than 50 e-GP systems: If each e-GP system were to empanel more than a hundred banks in India, a total of 5,000 contracts ought to be signed. Further, authorized bank representatives from each of the 100+ banks ought to be provided with login credentials to each of the 50+ e-GP systems. Refer to Figure 3 for a pictorial view of exponential connections resulting from integration of multiple e-GP systems with multiple banks.

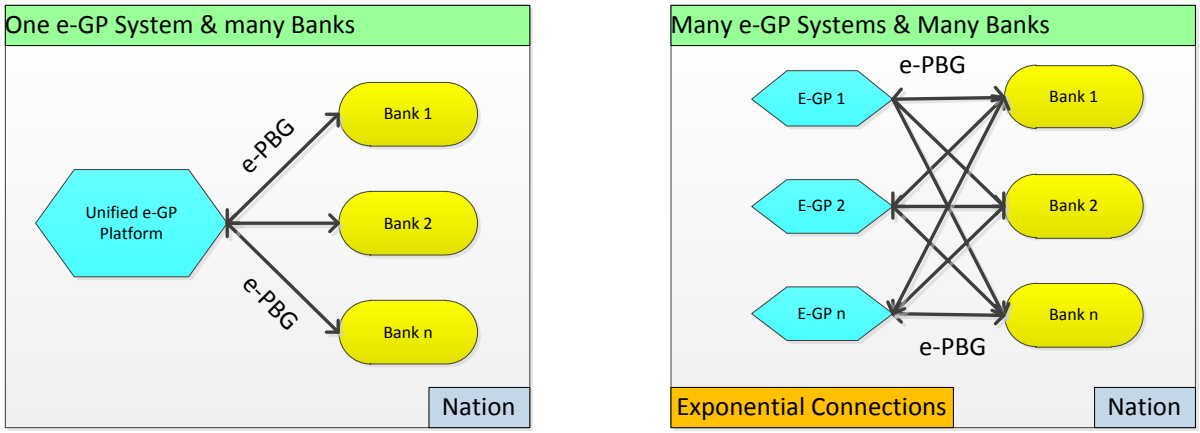

Figure 3: Bank to e-GP Connection Requirements

33. Need for e-Catalogue Standards: The adoption of government e-marketplace is now becoming increasingly common, wherein small value procurement is processed online. Each marketplace will have thousands of e-catalogues published in it, which the suppliers shall prepare as per e-marketplace specific standards. If all e-marketplaces could confirm to a global standard of e-catalogues, suppliers will find it easier to upload the same e-catalogue across all the marketplaces. It is less common for a country to have multiple e-marketplaces as compared to e-bidding systems.

34. Online Submission of e-Invoices Directly from Supplier IT Systems: Of the many countries that have embarked on implementation of e-GP, only few developed economies have adopted e-invoicing. The post award of contract processes is handled manually in most of the e-GP systems. Where contract management is implemented, bidders log into the concerned e-GP system and submit their invoices online. Except for few large enterprises and that too in the context of few developed nations, the need for automated exchange of e-Invoices directly from the supplier's IT system onto the e-GP platform is quite minimal. In a few years from now, more suppliers would demand standards-based system for automated submission of e-invoice directly from their IT systems to any of the e-GP systems not just within a nation but internationally.

III. VISION FOR A GLOBAL E-GP ARCHITECTURE

35. In a decade or so, it is expected that in excess of 80% of government procurement transactions will be processed online in a couple of hundred e-GP systems spread across the world. The vision for global e-GP architecture is to inter-link and correlate relevant data from all the e-GP systems for development of:

(i) A de-duplicated global database of suppliers. Refer to Figure 4 for a pictorial overview, and
(ii) An authenticated, global online repository of work experience certificates.

36. Further, the e-GP Blockchain network should be extended to enable banks located anywhere in the world to seamlessly submit authenticated electronic performance bank guarantees on behalf of a supplier in any of the networked e-GP systems.

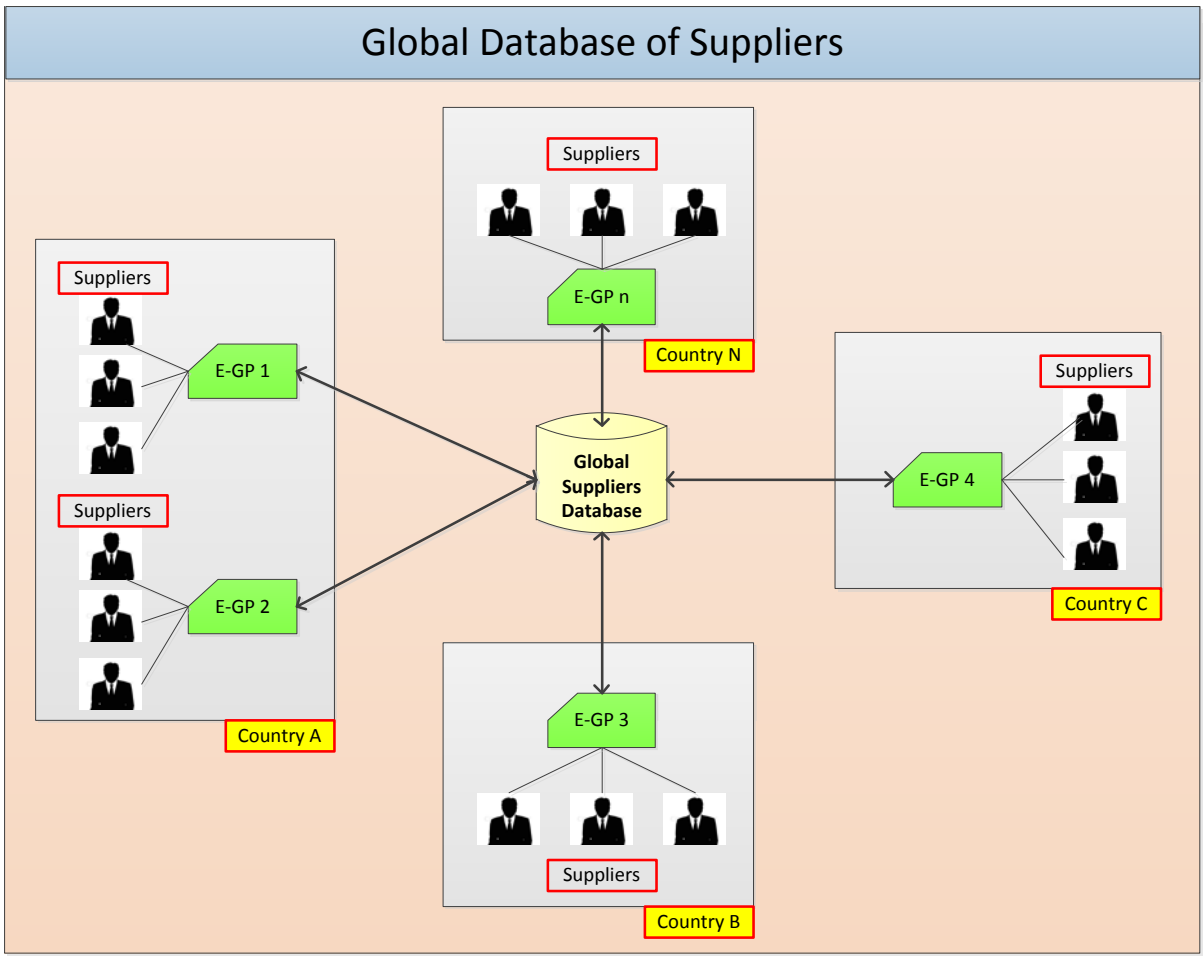

Figure 4: Global Database of Suppliers

IV. DESIGN PRINCIPLES

37. The key design principles (refer to Figure 5) underlying the global e-GP architecture is explained herein:

38. Build on Existing e-GP Systems: It takes many years (e.g. 5 – 10 years) of sustained effort to build an e-GP system and on-board suppliers and government users in it. An initiative to develop a global database of suppliers should build upon the existing e-GP systems. Indeed, it could happen that a supplier has duplicate identities within an e-GP system. Also, due to lack of standardization, it will be impossible to uniquely identify a supplier globally across all the e-GP systems only based on data correlation. Despite these known deficiencies, supplier records in the existing e-GP systems shall be the foundation because the suppliers submit bids online and conduct other online transactions in these systems. The suppliers would presumably use the same identity to conduct transactions repeatedly in the e-GP system. Hence, the e-GP system in which the supplier transacted online is the most well-suited to validate identity of a supplier.

39. Incentivize *de facto* Adoption of Standards: The e-GP system owners spread across the world are authorities in themselves. It is impossible for any agency to forcefully ensure compliance to certain laid down standards by a couple of hundred e-GP system owners. Given this limitation, the key stakeholders should be incentivized to adopt the standards prescribed for building the global e-GP architecture.

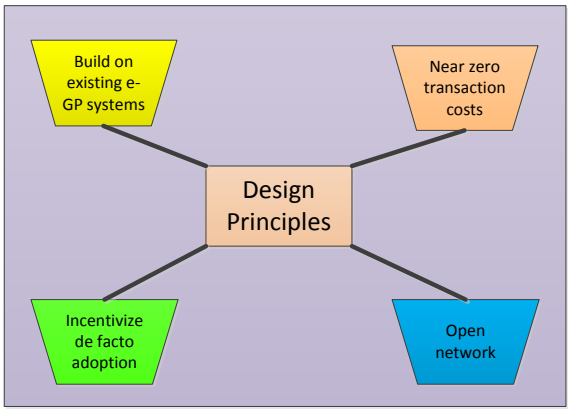

Figure 5: Design principles

40. Open Network with Minimal Entry Barriers: There are a variety of business models in which e-GP systems operate such as:

(i) Built and maintained by the government,
(ii) Development and maintenance of e-GP system is outsourced to a service provider, and
(iii) A cloud e-GP installation offered on a services model to a large number of government agencies.

41. While a government agency might be more willing to invest in complying with a standard, a cloud e-GP installation owner or an outsourced e-GP service provider would make investments only if it is absolutely necessary. If all e-GP system owners regardless of the implementation model are to come on-board, it should take minimal effort for them to comply with the standards. It should be easy to adopt and open for any interested party across the world.

42. Near Zero Transaction Costs: End users would resist complying with a standard if there is a transaction charge associated with the continued compliance. Hence, there should be minimal or non-existent transaction charges.

V. KEY BLOCK-CHAIN CONCEPTS EXPLAINED IN E-GP CONTEXT

43. It is proposed to implement the envisaged global e-GP architecture using Blockchain technology. Key blockchain concepts are explained in this section, contextualized in e-GP context, to enable the readers better understand the approach proposed in subsequent sections of this report.

44. Transaction: Refer below for examples of transactions in e-GP system of *"Country A"*:

(i) Procuring entity <<ABC>> awarded a contract worth <<USD 10,000>> for execution of contract <<Construction of Road>> to supplier <<XYZ Limited>> on <<DD-MM-YYYY>>
(ii) Procuring entity <<ABC>> blacklisted supplier <<DEF Limited>> from <<DD-MM-YYYY>> until <<DD-MM-YYYY>>

45. Transactions such as those in the list above are public records by definition in most countries. This information is typically published in a web-site for public consumption. However, full utility of the transaction data can be realized only when it is published online in compliance to global standards and there exists a mechanism to consume this data in an automated manner.

46. Only certain type of transactions in an e-GP system is eligible for public consumption. For example, online bid submission by supplier <<DEF Limited>> against tender ID <<1234>> on <<DD-MM-YYYY>> is a confidential record and it shall not be published at least until expiry of the scheduled bid submission deadline. Thus, transactions in e-GP system have to be segregated as under *"Public"* and *"Confidential"*. Only the *"Public"* transactions are amenable for publication in shared or distributed ledger.

47. Shared Ledger or Distributed Ledger: The records of both public and confidential transactions processed online are now generated and stored in the concerned e-GP system. Certain "*Public"* records such as Notice Inviting Tender (NIT) and award of contract (AoC) are published online for free view in most e-GP systems but in a proprietary format. There is demand for the public records generated in e-GP system. For example, suppliers do submit AoC information as part of their bids seeking to win new business and procuring entities seek to know the contracts pending completion while evaluating available spare capacity with the suppliers.

48. A shared or distributed ledger of e-GP transactions gets developed when e-GP systems publish transaction data in a standardized format confirming to prescribed protocols, which is verified and then added as authentic record in the shared ledger based on a de-centralized consensus mechanism. A transaction will be permanently added to the e-GP shared ledger only if it complies with certain eligibility conditions defined for the e-GP Blockchain. For example, the following transaction will be added to the e-GP shared ledger only if it satisfies the verification checks listed below:

(i) Transaction: The value of contract number <<C123>> issued in <<e-GP System A24>> to supplier <<DEF Limited>> changed from <<USD 12345>> to <<USD 23456>> on <<DD-MM-YYYY>>.
(ii) Verification check:
   a. <<e-GP System A24>> issued contract <<C123>> to supplier <<DEF Limited>> &
   b. The original value of contract <<C123>> is <<USD 12345>>

49. The verification check will be executed based on data already existing in the shared ledger. For example, *"Procuring entity <<ABC>> awarded a contract worth <<USD 12,345>> for execution of contract <<C123>> to supplier <<DEF Limited>> on <<DD-MM-YYYY>>"* ought to have been recorded as a verified transaction in the shared ledger before-hand as pre-requisite to verify and confirm whether the following newly added transaction is valid: *"The value of contract number <<C123>> issued in <<e-GP System A24>> to supplier <<DEF Limited>> changed from <<USD 12345>> to <<USD 23456>> on <<DD-MM-YYYY>>."* Indeed, such verification can happen only if someone or a group of interested agencies keep a full copy of the shared ledger (i.e. with all transaction details present in it).

50. Hash: An important concept in cryptography, a hash function converts an input message to a fixed size alphanumeric string. Hash is a one-way function in that it is not possible to generate the input message based on the Hash value. The output string resulting from Hash is of the same length regardless of the size of the input message. Even smallest of the changes to the input message will cause the Hash to differ completely. Refer to Figure 6, adding a period punctuation mark to the Hello World text changed the Hash output completely:

S.no.	Message	Hash using SHA-256 Algorithm
1	Hello World	A591A6D40BF420404A011733CFB7B190D62C65BF0BCDA32B57B277D9AD9F146E
2	Hello World.	F4BB1975BF1F81F76CE824F7536C1E101A8060A632A52289D530A6F600D52C92
3	Here is an illustration to show that Hash length remains the same regardless of the message size.	E3AD51DB684AC679ED803574EDAD875CD5CF0CF99727225DF326A1105E16AB12

Figure 6: Illustration of Cryptographic Hash

51. Block: It is a file where e-GP transaction data will be permanently recorded. A Block in the Bitcoin Blockchain for example is generated once every 10 minutes (i.e. 144 Blocks a day) and it carries transaction data amounting to 1 MB on an average. The size of a Block can vary depending on the Blockchain rules. A Bitcoin Block can contain about 4000 transactions. As of August 2018, in excess of 500,000 Blocks have been created in the Bitcoin Blockchain since the 1st Primordial Block was created on the 3rd of January 2009. A Block Header is 80 Byte long string comprising of:

(i) Bitcoin version number (4 bytes)
(ii) Previous Block hash (32 bytes)
(iii) Merkle root (32 bytes); hash of all the transactions in a Block generated in a certain pyramid like hierarchy
(iv) Timestamp of the block (4 bytes)
(v) Difficulty target of the block (4 bytes); Miners seek to create a hash value of the Block Header that is lower than the difficulty target (i.e. Proof of Work) &
(vi) Nonce (4 bytes); a key input discovered by the Miners in iteration until Proof of Work for the Block is generated. Discovery of Nonce is the mathematical puzzle the Miners solve to generate the Proof of Work.

52. Miners: e-GP system owners will continuously publish new transactions to be added on to the e-GP Blockchain. These transactions which are yet to be added on to the Blockchain will be added to *memory pool* or the *transaction pool*. A Miner will gather transactions from the

transaction pool (i.e. list of transactions yet to be published in the Block chain) to create a Candidate Block and seek to add its block in the Blockchain. At a point in time, many Miners will compete to add their respective blocks in the Blockchain. The Miner which produces first a Hash value lower than the specified difficulty target broadcasts its Proof of Work for the Block to all Nodes in the Block-chain Network. A Node downloads the Block, verifies whether the Block was created as per *consensus rules* governing the Blockchain network and then relays the Block to other Nodes if it complies with the consensus rules. These Nodes independently verify the Block and relay it further and so on. The Miners will take hash value of the latest Block as input for generation of the next Block, thus a chain of Blocks referred to as Blockchain is created. A copy of the Blockchain thus created is saved by the nodes in a distributed manner. The transactions recorded in a block are increasingly immutable as the number of blocks appended to the Blockchain increases. A Miner is remunerated typically with Bitcoin for the effort invested in adding a Block in the Blockchain network.

53. Public Key Cryptography: A user is provided with 2 keys which work in pair namely private and public keys. The private key by definition is private to the user for which it is assigned and its corresponding public key is made publicly available to any interested party. The use of these keys in a certain prescribed manner provides the following key usage benefits:

(i) Confidentiality: A user “John” can send a private message to “Peter” by encrypting the message using Peter’s public key. This encrypted message can be decrypted only using the private key held by “Peter” and in no other way.

(ii) Authenticated messaging and Non-repudiation: John encrypts a hash of his message to Peter using his Private Key, thus digitally signing the message. Upon receipt of the message, Peter will decrypt the signature to generate the hash (i.e. message digest). Firstly, if Peter can successfully decrypt the hash, it is confirmed that the hash was signed by John. Secondly, Peter can regenerate hash of the message to compare it with the decrypted hash. If both the hash values matched, it can be concluded that the message digitally signed by John has not been tampered with. In other words, if the hash values matched, John cannot deny (i.e. repudiate) that he digitally signed and sent the message.

VI. E-GP BLOCKCHAIN NETWORK

A. Design Overview

54. Bitcoin Blockchain is a public Blockchain network, open for anyone to join and participate in the network. It is widely distributed with about 30,000 full nodes. In the Bitcoin Blockchain network, any user can:

(i) Buy or sell Bitcoins and seek to record these transactions in the Bitcoin Blockchain,
(ii) Act as a Miner and seek to solve the mathematical puzzle for adding a block in the Blockchain, and
(iii) Volunteer to run a full node and contribute towards building consensus in the Blockchain.

55. The e-GP Blockchain is envisaged as a public network, but it will not be as open as the Bitcoin Blockchain as explained below:

(i) Only transactions pertaining to e-GP systems will be recorded in the e-GP Blockchain
(ii) Instead of creating an open competition based system wherein Miners are remunerated, the stakeholders in the e-GP Blockchain Network would be asked to volunteer as Miners
(iii) Anyone can volunteer to run a full node and contribute towards building consensus in the Blockchain

56. A comparative view of the key design criteria underlying the public Bitcoin Blockchain network vis-à-vis the envisaged e-GP Blockchain network is provided in Figure 7:

S.no.	Design Criteria	Bitcoin	e-GP Blockchain
1	What transactions will be recorded	Bitcoin related transaction reported by any users	Only transactions pertaining to e-GP systems
2	Who will undertaking Mining	Any interested party	Key stakeholders will be asked to volunteer as Miners
3	Building consensus	Any volunteer	Any volunteer
4	Network type	Decentralized peer-to-peer	Decentralized peer-to-peer
5	Immutability	Increasingly immutable as the Blockchain grows	Increasingly immutable as the Blockchain grows

Figure 7: Comparative view of Bitcoin vis-à-vis e-GP Blockchain network

B. On-boarding e-GP Systems in e-GP Blockchain Network

1. Building upon Existing e-GP Systems

57. It is proposed to build the e-GP Blockchain network on top of the existing couple of hundred e-GP systems located worldwide. The identity of e-GP systems has to be verified and then a unique Blockchain network ID will be issued. Thus, e-GP systems will get registered in the Blockchain network. A user designated as the <<e-GP Admin>> (i.e. root user) of the network will

create user credentials for e-GP systems in the Blockchain network. Each system in the e-GP Blockchain network will be issued a private-public key pair generated from a central Public Key Infrastructure (PKI) server established specifically for the Blockchain network. Further, e-GP systems registered in the Blockchain network can submit various online service requests pertaining to the Blockchain network such as:

(i) Publishing new transactions in the transaction pool, and
(ii) Requesting Blockchain ID for suppliers already registered in their respective e-GP systems.

58. In the figure below, <<e-GP A>> and <<e-GP B>> are uniquely identified in the e-GP Blockchain network by ID references <<e-GP system A24>> and <<e-GP System A19>> respectively. The remaining 2 e-GP systems <<e-GP C>> and <<e-GP X>> are yet to be on-boarded in the e-GP Blockchain network. The vision is to establish a single global e-GP Blockchain network, wherein all the e-GP systems are uniquely identified.

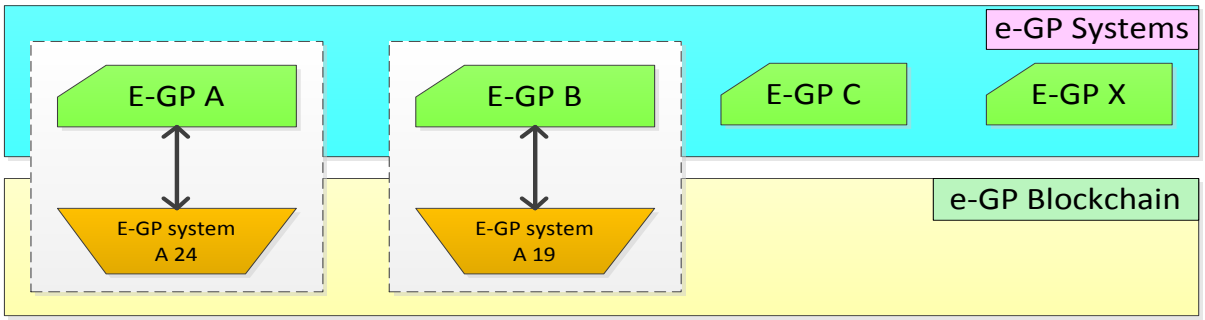

Figure 8: Issuance of Unique Blockchain Network ID to e-GP Systems

2. User ID Creation in the Blockchain Network

59. An e-GP system needs to submit a request for User ID creation in writing to the agency governing the e-GP Blockchain network, providing the following specific details:

(i) e-GP system name,
(ii) Preferred User name in e-GP Blockchain network, and
(iii) Contact information about the authorized user (i.e. designation, phone number, address and email address).

60. In response, the governing agency will verify the request and then a designated user <<e-GP Admin>> will create user credentials for the e-GP system. The password to access the e-GP Blockchain server and the link for creation of the private-public key pair will be mailed to the authorized user in the specified email address. The authorized user will log into the central PKI server to self-generate the public-private key pair. Subsequently, the <<e-GP Admin>> will broadcast creation of an e-GP system user in the Blockchain Transaction Pool as given below: *"<<e-GP Admin>> has assigned user ID <<e-GP System A24>> for the e-GP system <<e-GP A>> on <<DD-MM-YYYY>>. Public key of <<e-GP System A24 >> is <<MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAerdCTrgFelvZkX9Yh/rZK4SCIedZ0ThUth6ATNh+6Pw8Vt3PGH0g1oaHk+dbCw10uWEEYF9wSsBP2hwMRWuU7QIDAQAB>>"* [3] . This transaction data will get recorded in a Block, which will be added to the e-GP Blockchain as per

[3] A 512 bit key is used for illustration purpose.

the rules governing the Blockchain network. This transaction data will become an immutable public record and can be viewed by any interested user. Refer to Figure 9 for a pictorial representation of the user ID creation process.

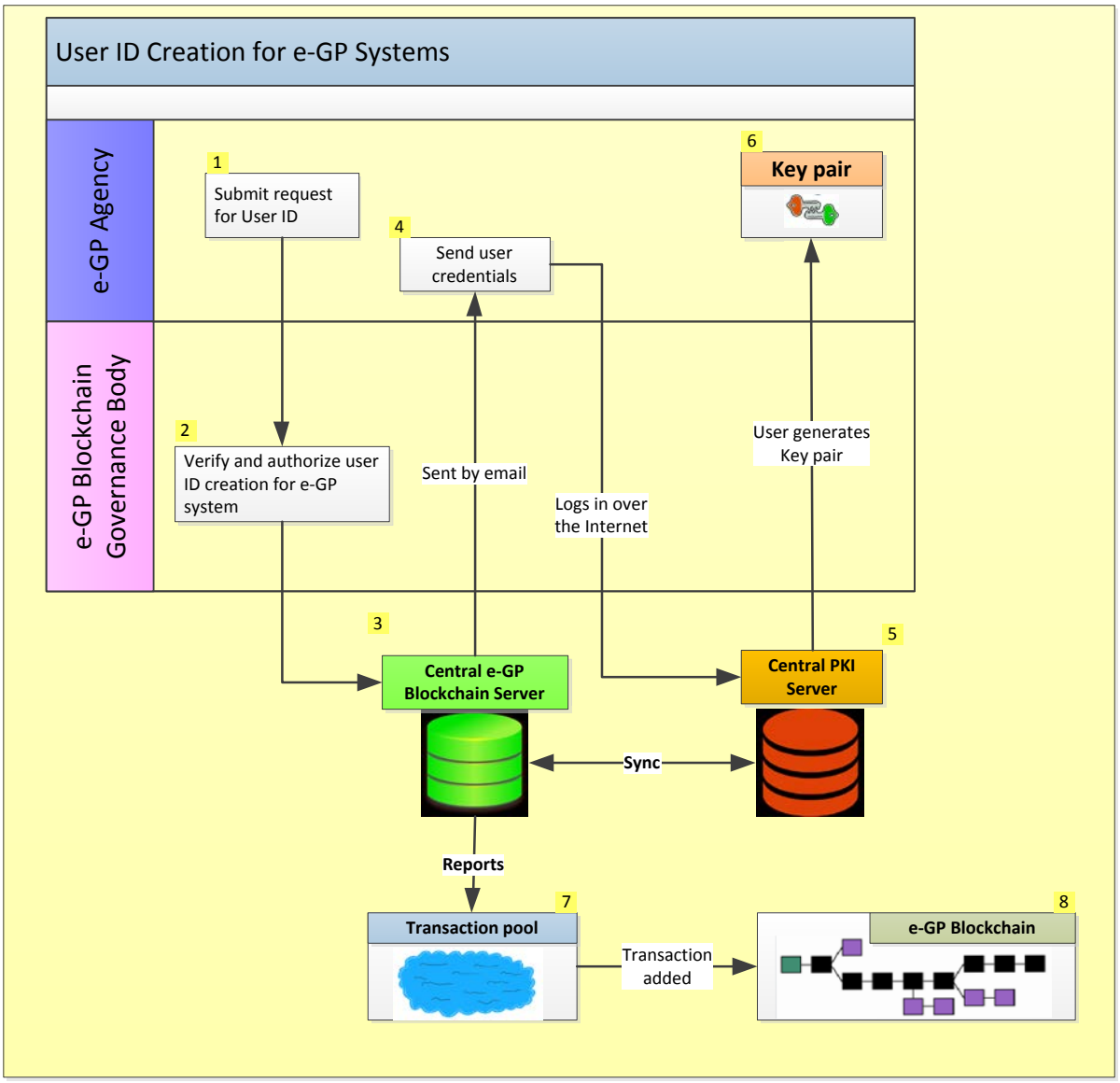

Figure 9: User ID creation for e-GP systems

Consensus rules to be verified by the Miners and Nodes to confirm this transaction (sample)
(i) A transaction reported in the transaction pool complies with the pre-defined message formats (ii) The content is digitally signed by <<e-GP Admin>> (iii) A user which reported a transaction is authorized to report such a transaction. For example, a different user other than <<e-GP Admin>> shall not report creation of User ID for an e-GP system

3. Modification of User Credentials

61. To modify user credentials in the Blockchain network, the authorized user of an e-GP system will need to authenticate its identity in the e-GP Blockchain server and then make the requisite change. If private key of the authorized user gets lost or compromised, the user will need to authenticate its identity and seek to generate a new private-public key pair as explained below:

(i) Authenticate its identity in the e-GP Blockchain server and then initiate the request for creation of a new key pair by the central e-GP Blockchain PKI server. The request message format would be as follows: <<e-GP System A24>> seeks to create a new key pair and replace the public key <<MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAerdCTrgFelvZkX9Yh/rZK4SCIe dZ0ThUth6ATNh+6Pw8Vt3PGH0g1oaHk+dbCw10uWEEYF9wSsBP2hwMRWu U7QIDAQAB>>. The email address associated with <<e-GP System A24>> is <<xyz@mail.com>>"

(ii) The PKI server will send an email with a link for the user <<xyz@mail.com>> to self-generate the private-public key pair and download the private key. A copy of the public key will be published as a transaction in the e-GP Blockchain as follows: *"The public key <<MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAerdCTrgFelvZkX9Yh/rZK4SCIe dZ0ThUth6ATNh+6Pw8Vt3PGH0g1oaHk+dbCw10uWEEYF9wSsBP2hwMRWu U7QIDAQAB>> for <<e-GP System A24>> has been replaced with <<MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAIZC49YwbjfL1leFyWrqi1SSv O3sxpK37NoY3HZGImZl+TluJLPOqLagQW+AI1dEvtLLcWrOE9UfT1Vk46Qxo1 0CAwEAAQ==>> on DD-MM-YYYY based on request received from <<e-GP System A24>> and <<xyz@mail.com>>.*

62. If name of the e-GP system attached to a User ID or public key attached to an e-GP system is changed, <<e-GP Admin>> will broadcast this in the Blockchain network by publishing the following messages in the Transaction pool:

(i) *"<<e-GP Admin>> has modified user ID of the e-GP system <<e-GP A>> from <<e-GP System A22>> to <<e-GP System A23>> on <<DD-MM-YYYY>>."*

(ii) "*<<e-GP Admin>> has modified the public key of <<e-GP System A24>> to <<MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAIZC49YwbjfL1leFyWrqi1SSv O3sxpK37NoY3HZGImZl+TluJLPOqLagQW+AI1dEvtLLcWrOE9UfT1Vk46Qxo1 0CAwEAAQ==>>*"

Consensus rules to be verified by the Miners and Nodes to confirm this transaction (sample)
(i) A transaction reported in the transaction pool complies with the pre-defined message formats
(ii) The content is digitally signed by <<e-GP Admin>>
(iii) The system <<e-GP A>> was earlier assigned the user ID <<e-GP System A22>>, as per pre-existing Block-chain records &
(iv) The User ID <<e-GP System A24>> already existed and the public key *<<MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAerdCTrgFelvZkX9Yh/rZK4SCIedZ 0ThUth6ATNh+6Pw8Vt3PGH0g1oaHk+dbCw10uWEEYF9wSsBP2hwMRWuU7QI DAQAB>>* was associated with it.

63. Thus, history of key changes in evolution of the e-GP Blockchain network will be recorded.

C. De-duplicated Global Supplier Database

4. Problem Statement

64. The number of registered suppliers in all the e-GP systems world-wide will be in millions and it will continuously grow in the years to come. The task at hand, which is essentially the single most complex problem to solve for building the global e-GP Blockchain network, is creation of a de-duplicated supplier database across all the e-GP systems. When a supplier is uniquely identified by a global Blockchain ID (GID), it will be possible to correlate supplier activities across e-GP systems worldwide as given below:

(i) Authentic records about the contracts awarded to a supplier,
(ii) The status of contracts under execution by a supplier, and
(iii) Whether a supplier is black-listed or not can be verified.

65. The various e-GP systems do not follow a standardized process to register suppliers. Some e-GP systems validate supplier identity against national databases and then register. In many systems, suppliers can register using their email address by filling out an online form. There is not any reliable mechanism as on date to de-duplicate supplier identity across national borders. It is not uncommon for large business enterprises to have multiple identities in the same e-GP system. In Figure 10, supplier <<XYZ Limited>> has multiple user ID's in <<e-GP System A24>> and <<e-GP System A19>>. The problem will be resolved if XYZ Limited could be identified by one single global ID (GID) across all the e-GP systems.

XYZ Limited having multiple ID's in the AS IS Scenario				
S.no.	**Supplier Name**	**e-GP Name**	**Supplier ID in e-GP System**	**Global ID**
1	XYZ Limited	e-GP System A24	1213	?
2	XYZ Limited	e-GP System A24	1214	?
3	XYZ Limited	e-GP System A19	7979	?

Figure 10: Supplier having multiple IDs in the AS IS Scenario

66. Often, a user in the e-GP system would not know that another user from the enterprise is already registered in the same system. Most large business enterprises would not have kept track of the user ID's created by them in various e-GP systems. As the data structures of e-GP systems would vary and since manually inputted data is prone to data entry errors, it is impossible to correlate and match user records from multiple different e-GP systems. An approach designed to build a global supplier database has to take cognizance of these challenges.

5. Blockchain ID Creation for Suppliers

67. It is proposed to on-board suppliers onto the e-GP Blockchain network based on inputs received from e-GP systems registered in the network. An e-GP system on-boarded in the Blockchain network will act as a Trusted Third Party (TTP) and provide inputs required to create GID for suppliers. A central e-GP Blockchain server will create a unique GID in response to each request received from e-GP systems already registered in the Blockchain network. Just as it is with user ID creation for e-GP systems, a private-public key pair will be generated from a central e-GP Blockchain PKI server for each GID as explained below:

(i) The e-GP system will authenticate its identity in the Central e-GP server and initiate the request for creation of a new key pair by the central e-GP Blockchain PKI server. The request message format would be as follows: The request message format would be as follows: *<<e-GP System A24>> seeks to create a new key pair for GID <<54321>> and e-GP system ID <<1212>>. The email address associated with GID <<54321>> is <<abc@mail.com>>"*

(ii) The PKI server will send an email with a link for the user <<abc@mail.com>> to self-generate the private-public key pair and download the private key.

68. The <<e-GP Admin>> will publish GID creation details in the transaction pool to be recorded in the Blockchain, as given below:

(i) "*<<e-GP Admin>> assigned GID <<54321>> to supplier <<DEF Limited>> with e-GP system ID <<1212>> on <<DD-MM-YYYY>> based on inputs received from <<e-GP System A24>>"*.

(ii) *"Public key of GID <<54321>> is <<MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAcOxYWdooDffIK8HbnAHTK1p5r4oTNmNKGC+1Frma/cyLm+cwAHpBD7muUq4TdkEafu20a6/R3d5iLsAv5QARvwIDAQAB>>"*.

Consensus rules to be verified by the Miners and Nodes to confirm this transaction (sample)
(i) A transaction reported in the Transaction pool complies with the pre-defined message formats
(ii) The content is digitally signed by <<e-GP Admin>>

69. The <<e-GP system A24>> can choose to pull the data from the Blockchain and update its records or a request-response mechanism can be established between <<e-GP system A24>> and the e-GP Blockchain server that generated <<GID 54321>>. Such implementation decisions have to be finalized while the e-GP Blockchain software is designed.

70. It is recommended that <<e-GP system A24>> submits GID creation requests only for suppliers satisfying certain *trigger events* such as the following: Suppliers with at least one award of contract issued online in the e-GP system. The e-GP Blockchain network will get overloaded if an e-GP system seeks to create GID for all its suppliers. Nevertheless, these are policy decisions to be taken while designing the finer aspects of the e-GP Blockchain network. Refer to Figure 11 and Figure 12 for a view of the database in e-GP system pre and post creation of GIDs.

e-GP System A24 before GID creation				
S.no.	**Supplier Name**	**Supplier ID**	**GID**	**GID Create Date**
1	ABC Limited	1211		
2	DEF Limited	1212		
3	XYZ Limited	1213		
4	XYZ Limited	1214		

Figure 11: e-GP System A24 before GID creation

e-GP System A24 after GID creation				
S.no.	**Supplier Name**	**Supplier ID**	**GID**	**GID Create Date**
1	ABC Limited	1211		
2	DEF Limited	1212	54321	24-Aug-18

3	XYZ Limited	1213	55256	04-Dec-17
4	XYZ Limited	1214	55924	04-Sep-18

Figure 12: e-GP System A24 after GID creation

71. In Figure 12, <<ABC Limited>> does not have a GID because <<e-GP System A24>> did not submit the GID creation request to the e-GP Blockchain server possibly because *ABC Limited* did not satisfy the trigger event. In the proposed approach, the number of suppliers with GID will increase as the number of e-GP systems on-boarded in the Blockchain network increases. Refer Figure 13 for a pictorial view of the GID generation process.

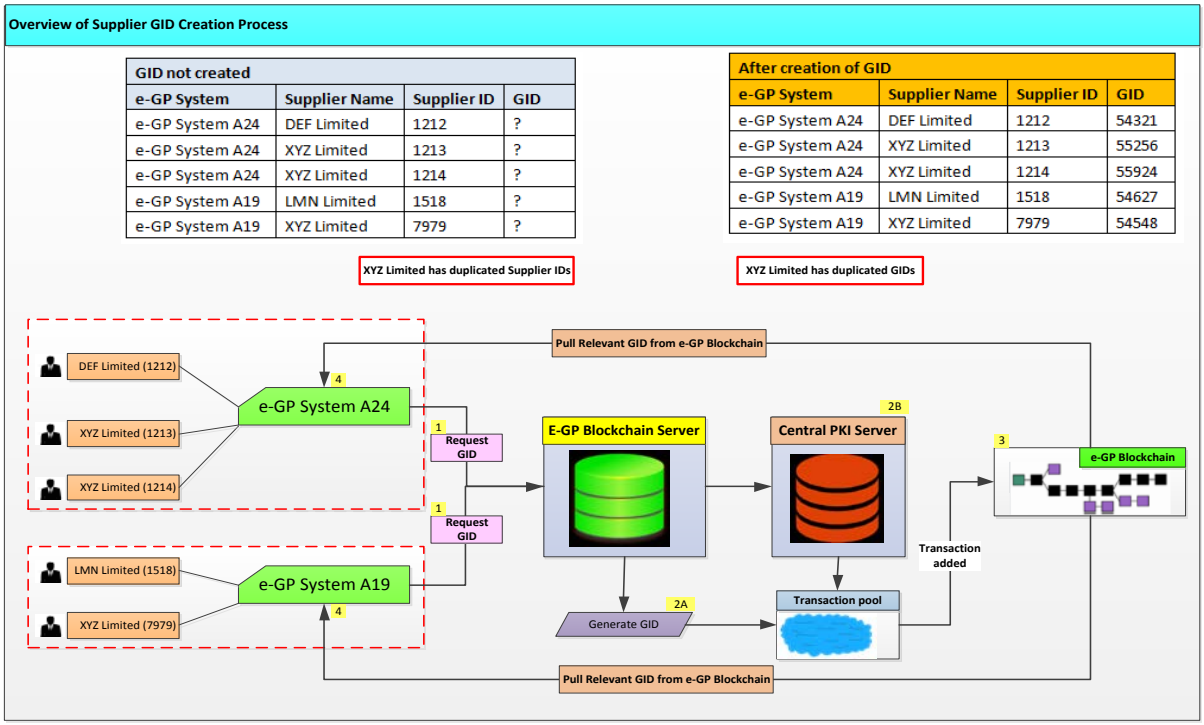

Figure 13: Overview of GID generation process

6. De-duplication of Supplier's Global Blockchain ID (GID)

72. As the e-GP Blockchain server does not undertake any verification of user identity, a user with multiple user IDs in the source e-GP system will get a GID for each user ID it has in the e-GP system. The supplier <<XYZ Limited>> in the table above has obtained 2 GID's (i.e. 55256 and 55924). Indeed, it is possible for the supplier <<XYZ Limited>> to be registered in another e-GP system (e.g. <<e-GP System A19>>) besides <<e-GP System A24>>. In which case, the <<e-GP System A19>> would have submitted a request for GID and obtained one more GID for <<XYZ Limited>>. Refer to Figure 16 for a list of GIDs <<XYZ Limited>> would have when GID is generated for all its 3 identities.

GIDs of XYZ Limited – Before Deduplication				
S.no.	**e-GP System**	**Supplier ID**	**GID**	**GID Create Date**
1	e-GP System A24	1213	55256	04-Dec-17
2	e-GP System A24	1214	55924	04-Sep-18
3	e-GP System A19	7979	54627	12-Oct-17

Figure 14: GIDs of XYZ Limited – Before Deduplication

73. It is indeed possible that <<XYZ Limited>> did not realize that it has 3 different GIDs. Given which, de-duplication is possible only when <<XYZ Limited>> is adequately incentivized to take the initiative to locate all its GIDs and consciously decide to adopt one single GID as its identity reference in all the e-GP systems.

74. It is argued that the suppliers would seed one single GID in all the e-GP systems when the following 2 conditions are implemented:

(i) The e-GP systems mandate suppliers to submit the following information as Blockchain records during online bid submission: AoC, available spare capacity and work experience certificate. The suppliers will be required to submit Blockchain records at least from those e-GP systems already on the e-GP Blockchain network.

(ii) A supplier will need to record its GID as a pre-requisite for submitting Blockchain record of its work experience in an e-GP system. If a supplier's GID is not already seeded, the e-GP system will disallow the supplier from submitting Blockchain record of its work experiences. A Blockchain record of supplier's work experience cannot be created unless it has GID of the supplier recorded in it. If GID of a supplier seeded in the e-GP system does not match with the GID specified in the Blockchain record uploaded by the supplier, the e-GP system will reject the upload. Consequently, the supplier will either need to update its GID in the Blockchain record or in the e-GP system and thus de-duplicate and synchronize its GID across all e-GP systems. For example, if the supplier <<XYZ Limited>> with <<GID 55924>> seeks to cite a Blockchain record (e.g. work experience or award of contract or available spare capacity) with <<GID 54627>> or <<GID 55924>> (both belong to XYZ Limited), the <<e-GP system A15>> will reject those records. Refer to Figure 15 for a pictorial overview of the pre-de-duplication scenario explained herein.

75. The implementation of these 2 conditions consistently across all the e-GP systems is an essential requirement for the development of a de-duplicated global supplier database. By design, there will be duplicate GIDs in the e-GP Blockchain during the initial years. The extent of duplicate GIDs in the e-GP Blockchain will gradually reduce, as more e-GP systems get on-boarded onto the e-GP Blockchain network and the 2 conditions explained above get implemented. A global de-duplicated supplier database it is argued can be developed only based on *de facto* compliance to standards by all the stakeholders.

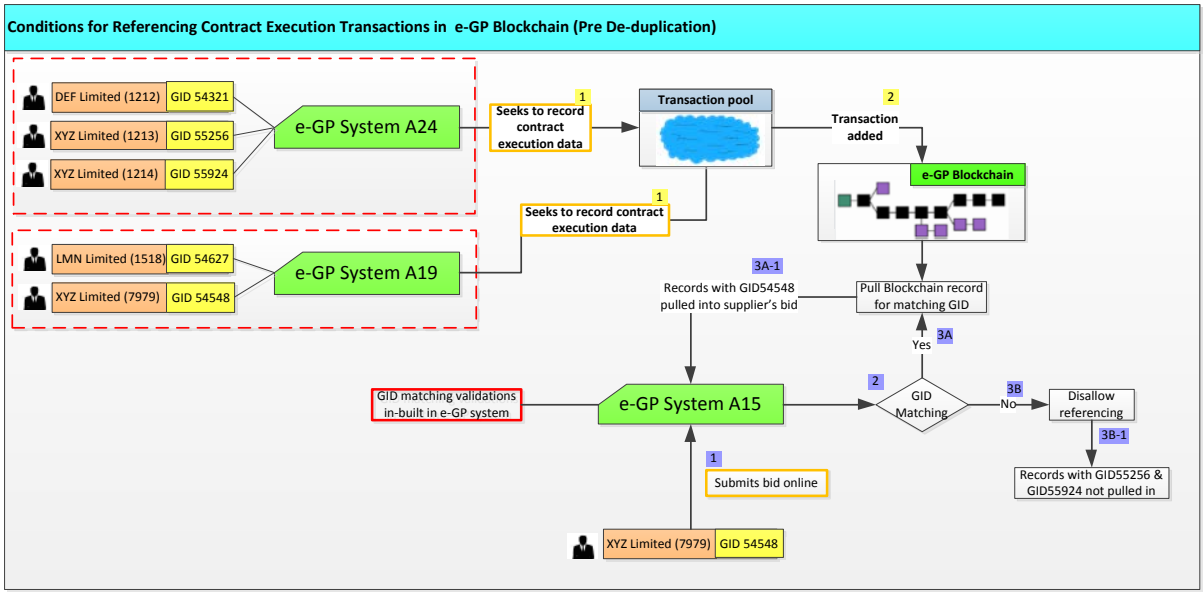

Figure 15: Referencing contract execution transaction in e-GP Blockchain (pre de-duplication)

76. The supplier <<XYZ Limited>> has to necessarily initiate the request for modification of its GID reference from the concerned e-GP system where the change is to be updated. For example, supplier has to initiate the request to change <<GID 55924>> necessarily from <<e-GP System A24>> and not from <<e-GP System A19>>. The <<e-GP system A24>> will at first verify and confirm the following before submitting the request to the e-GP Blockchain server:

(i) Authenticate identity of <<XYZ Limited>>
(ii) Verify and confirm whether <<GID 55924>> belongs to the supplier <<XYZ Limited>> &
(iii) Verify and confirm whether <<GID 55256>> belongs to the supplier <<XYZ Limited>> as explained below:
   a. <<e-GP System A24>> will encrypt randomly generated dummy plain text (A) using public key of GID 55256
   b. <<GID 55256>> will be asked to decrypt this value and input the decrypted value (B) in the e-GP system for verification
   c. If the system generated dummy plain text (A) matched with the decrypted value (B) inputted by the supplier, it is confirmed that <<XYZ Limited>> has the private key for <<GID 55256>>. Thus it can be concluded that <<XYZ Limited>> is the rightful owner of <<GID 55256>>.

77. The actions detailed in Figure 16 will take place subsequent to the confirmation:

Step	Actions
One	After confirming that <<GID 55256>> belongs to <<XYZ Limited>>, the e-GP System will submit the following request to the e-GP Blockchain server: *<<e-GP System A24>> seeks modification of GID for supplier <<XYZ Limited>> with e-GP system ID <<1214>> from <<GID 55924>> to <<GID 55256>>*.
Two	The e-GP Blockchain server will validate and confirm whether <<GID 55924>> was originally assigned to supplier <<XYZ Limited>> with e-GP System <<1214>> in response to a request generated by <<e-GP System A24>>.

Step	Actions
Three	The change effected in the Global Blockchain server will be reported as a transaction in e-GP Blockchain as given below: "*<<e-GP Admin>> modified GID of supplier <<XYZ Limited>> with e-GP ID <<1214>> in <<e-GP System A24>> from <<GID 55924>> to <<GID 55256>> on <<DD-MM-YYYY>>.*
Four	The <<e-GP system A24>> will update the modified GID in its database subsequent to receipt of confirmation from the e-GP Blockchain server.

Figure 16: Steps involved in updating GID of Supplier in e-GP System

78. Refer to Figure 17 for a pictorial view of the process for modification of supplier's GID in an e-GP System.

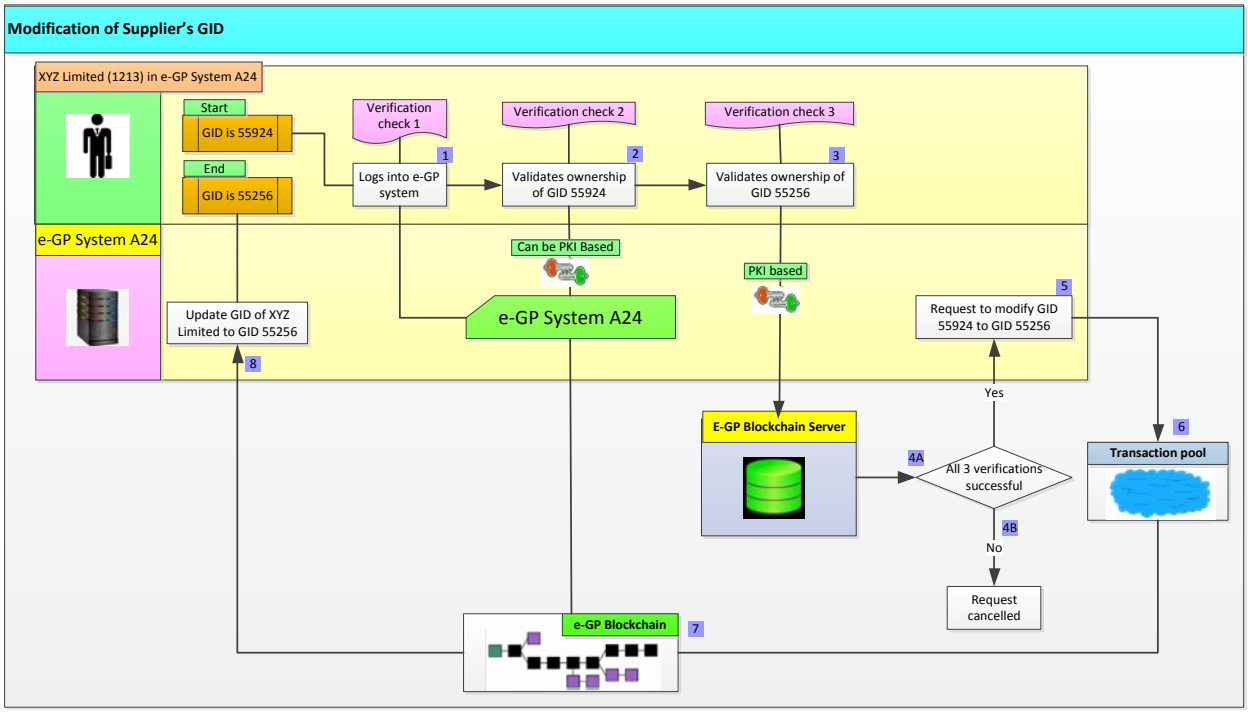

Figure 17: Modification of Supplier's GID in an e-GP System

79. Post the de-duplication, the GID of supplier <<XYZ Limited>> will be updated in <<e-GP System A24>> and <<e-GP System A19>> as displayed in Figure 18:

GIDs of XYZ Limited – Post Deduplication					
S.no.	**e-GP System**	**Supplier ID**	**GID**	**GID Update Date**	**GID Create Date**
1	e-GP System A24	1213	55256		04-Dec-17
2	e-GP System A24	1214	55256	14-Sep-18	04-Sep-18
3	e-GP System A19	7979	55256	14-Sep-18	12-Oct-17

Figure 18: GIDs of XYZ Limited - Post Deduplication

80. A pictorial view of the process followed by suppliers for referencing contract execution transactions in e-GP Blockchain post de-duplication is provided in Figure 19.

81. If private key of a user associated with a GID gets lost or compromised, the user will need to authenticate its identity and seek to generate a new private-public key pair as explained below:

(i) Authenticate its identity vis-à-vis the e-GP system credentials where the GID is seeded and then authorize the e-GP system to initiate the request for creation of a new key pair by the central e-GP Blockchain PKI server. The request message format would be as follows: *<<e-GP System A24>> seeks to create a new key pair and replace the public key << MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAcOxYWdooDffIK8HbnAHTK1p5r4 oTNmNKGC+1Frma/cyLm+cwAHpBD7muUq4TdkEafu20a6/R3d5iLsAv5QARvwI DAQAB>> for GID <<54321>> and e-GP system ID <<1212>>. The email address associated with GID <<54321>> is <<abc@mail.com>>"*

(ii) The PKI server would send an email with a link for the user <<abc@mail.com>> to self-generate the private-public key pair and download the private key. A copy of the public key will be published as a transaction in the e-GP Blockchain as follows: "*The public key << MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAcOxYWdooDffIK8HbnAHTK1p5r4 oTNmNKGC+1Frma/cyLm+cwAHpBD7muUq4TdkEafu20a6/R3d5iLsAv5QARvwI DAQAB>> for GID <<54321>> has been replaced with* "MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAdXHb60YQaOYb5WJFzys237pc VXTUxt+eeaB4hg/zX8qMc89382oIofzXX5jaF+dDvzOHxTGVI+uS4njk2ld0QQID AQAB" *on DD-MM-YYYY based on request received from <<e-GP System A24>> on behalf of e-GP system ID <<1212>> and <<abc@mail.com>>.*

82. Besides publishing the transaction in e-GP Blockchain, the e-GP Blockchain server will specifically intimate the e-GP systems associated with GID <<54321>> about replacement of the public key.

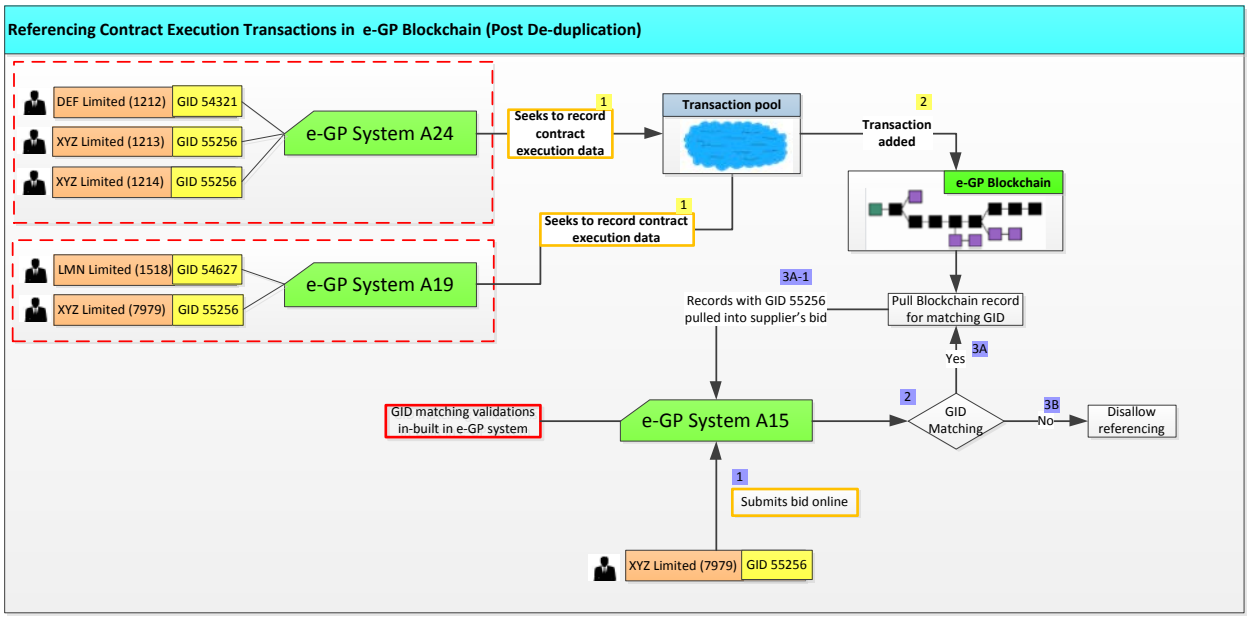

Figure 19: Referencing Contract Execution Transactions in e-GP Blockchain (Post de-duplication)

Consensus rules to be verified by the Miners and Nodes to confirm this transaction (sample)
(i) A transaction reported in the Transaction pool complied with the pre-defined message formats (ii) The content is digitally signed by <<e-GP Admin>> (iii) <<e-GP System A24>> has a supplier seeded with <<GID 54321>>

Consensus rules to be verified by the Miners and Nodes to confirm this transaction (sample)
(iv) The supplier with <<GID 54321>> has a public key attached to it

7. User ID Creation for Purchasing Agencies

83. A purchasing agency often has multiple User IDs within an e-GP system and there are instances where a single purchasing agency has multiple User IDs in more than one e-GP system. Hence, just as suppliers, purchasing agencies will need to be identified by a unique ID, herein referred to as purchasing agency ID (PID). The process for PID creation and PID de-duplication will remain the exact same as that of supplier GID creation and GID de-duplication. Hence, it is not elaborated herein. Refer to below table for a sample AoC transaction reported by a purchasing agency in the e-GP Blockchain network: *Purchasing agency <<Roads Department>> with PID <<1297>> in <<e-GP System A24>> awarded contract <<C123>> valued at <<USD 195,000,000>> with title <<Construction of Road from Destination A to Destination B>> to supplier <<XYZ Limited>> with <<GID 55256>> on <<DD-MM-YYYY>>.*

Consensus rules to be verified by the Miners and Nodes to confirm this transaction (sample)
(i) A transaction reported in the Transaction pool complied with the pre-defined message formats
(ii) The content is digitally signed by <<PID 1297>>
(iii) <<e-GP System A24>> has a Purchasing Agency seeded with <<PID 1297>>
(iv) The Purchaser with <<PID 1297>> has a public key attached to it

8. Online Repository of Contract Award, Work-in-Progress and Work Experiences

84. If a supplier could be identified by one single GID across all e-GP systems, it will require standard software development work to develop a global online repository of work experiences using Blockchain technology. The different work experiences that can be recorded and retrieved from the e-GP Blockchain are explained below:

85. Contract Award Information: Most e-GP systems are already publishing AoC online. With few modifications to the existing e-GP systems, AoC can be published online in the Blockchain. Further, software systems have to be developed to extract AoC information out of the transactions reported in e-GP Blockchain and make available each AoC as a public record that can be referenced using a web-link. The suppliers will refer this web-link during online bid submission in e-GP systems. As more e-GP systems get on-boarded into the e-GP Blockchain network and as time passes by, the government procurement AoC information available in the e-GP Blockchain will be near complete. Thus, it will be possible and even convenient for suppliers to submit all their government AoC information as authenticated web links.

86. Work-in-Progress: The adoption of contract management module is now increasingly common. If the status of physical and financial progress in a contract could be published in e-GP Blockchain as and when a payment is made against a contract, purchasing officials can extract the work pending to be executed by a supplier across all the e-GP systems registered in the e-GP Blockchain network. Thus, the actual spare capacity available with a supplier will be known. Such knowledge will enable the government to distribute contracts to larger number of suppliers

as compared to awarding contracts to few over-loaded suppliers. These few suppliers would in most cases get the work executed by sub-contracting it to smaller suppliers.

87. Work Experience Certificates: The purchasing officials should publish work experience certificates in the e-GP Blockchain upon completion of a contract. Just as it is with AoC, suppliers will cite their work experiences as a web-link reference derived out of transactions recorded in the e-GP Blockchain. A rating mechanism has to be developed to evaluate, broadcast and consolidate supplier's performance in a contract.

88. The online repository of work experiences will initially be limited to the experiences recorded in e-GP systems on boarded in the e-GP Blockchain network. Subsequently, the e-GP Blockchain network could be expanded to cover e-procurement systems used by the private sector as well. Then, suppliers' work experiences from both government and the private sector can be pulled from the Blockchain network.

D. Role of Key Stakeholders in Reporting Transactions in Blockchain

89. This section seeks to provide an overview of the roles and responsibilities of key stakeholders in reporting transactions in the e-GP Blockchain network. The user identity transactions are handled in the e-GP Blockchain server and reported in the Blockchain by <<e-GP Admin>>. All procurement transactions executed in e-GP systems will be reported in the Blockchain directly by the concerned <<e-GP system>> based on trigger events. The central Blockchain infrastructure comprising of e-GP Blockchain server and central PKI server needs to be developed. Refer to Figure 20 for details.

S.no.	Activity	Initiated by	Reported by	Software
1	Creation of e-GP system user credentials	e-GP system	e-GP Admin	Central Blockchain infrastructure
2	Modification of e-GP system user credentials	e-GP system	e-GP Admin	Central Blockchain infrastructure
3	Creation of GID for suppliers	e-GP system initiates based on trigger event	e-GP Admin	Central Blockchain infrastructure
4	Modification of GID for suppliers	Supplier initiates in the e-GP system	e-GP Admin	Central Blockchain infrastructure
5	Publishing Award of Contract	Supplier initiates in the e-GP system	e-GP system	e-GP system
6	Publishing Work in Progress	Supplier initiates in the e-GP system	e-GP system	e-GP system
7	Publishing Work experience certificate	Supplier initiates in the e-GP system	e-GP system	e-GP system

Figure 20: Role of Key Stakeholders in Reporting Transactions in Blockchain

VII. SUBMISSION OF ELECTRONIC BANK GUARANTEE ACROSS NATIONAL BORDERS

90. In government procurement context, a Bank issues guarantee on behalf of a supplier specifically with reference to a bid (i.e. bid security) or with reference to a contract processed online in an e-GP system. Especially in international competitive bidding (ICB) tenders, the suppliers obtain a guarantee from their bank in printed form and manually submit a copy of the same to the procuring entity. If a bank is to announce issuance of a bank guarantee to a supplier in e-GP Blockchain, the message would appear as follows: *<<Bank 2815>> agrees to stand guarantee for supplier <<ABC Limited>> with reference to bid reference number <<9821>> in <<e-GP System A24>>.*

91. In all e-GP systems, a bid or a contract is uniquely identified and the unique ID reference is known to the bidders. Given which, if the following actors can be uniquely identified, it will be possible to issue authenticated bank guarantees across national borders:

(i) Bank,
(ii) Supplier, and
(iii) e-GP system.

92. Of the 3, suppliers and e-GP systems will be uniquely identified in the e-GP Blockchain network. If identity of a bank is not confirmedly known, it will be impossible to evaluate and confirm authenticity of the bank guarantee. Hence, it is essential to issue a unique identity to Banks either as a user type in the e-GP Blockchain network or in the bank Blockchain network. For now, it is assumed that banks will be created as users in the e-GP Blockchain network.

A. User ID Creation for the Banks

93. The process of User ID creation for the banks will be quite similar to that of the process followed for creation of User ID for the e-GP systems. In summary, the banks will submit an offline application with the following details, seeking to register in the e-GP Blockchain network:

(i) Name of the bank,
(ii) Preferred User name in e-GP Blockchain network, and
(iii) Contact information about the authorized user (i.e. designation, phone number, address and email address).

94. The process for creating user ID for Banks and e-GP systems will be just the same. It is envisaged that Banks will get registered in the Blockchain network directly by the <<e-GP Admin>> user just the way in which e-GP systems get registered. Refer Sections 6.2.2 and 6.2.3 of this report for a detailed explanation of the process followed for creation of user ID for e-GP systems. At end of the process:

(i) A bank will be identified in the e-GP Blockchain network by a unique User ID (BID), and
(ii) An authorized representative of the bank will self-initiate and download a public-private key from the e-GP Blockchain PKI server.

95. The BID creation for a Bank and issuance of private-public key pair to the bank will be recorded as transactions in the e-GP Blockchain as given below: *"<<e-GP Admin>> has assigned user ID <<BID 987>> for the bank << Bank of Country1>> on <<DD-MM-YYYY>>. Public key of*

<<BID 987>> is <<MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAIJVHC/d3W1C/qgmTdf5sCnzNrN/a2/2r2kJg9Xu8IhhLoU7en55rP96rOK7jSxRgdyFeqVHuXz4Kg8difeoxlsCAwEAAQ==>>”. Refer to Figure 21 for an overview of the process for creation of user ID creation for banks.

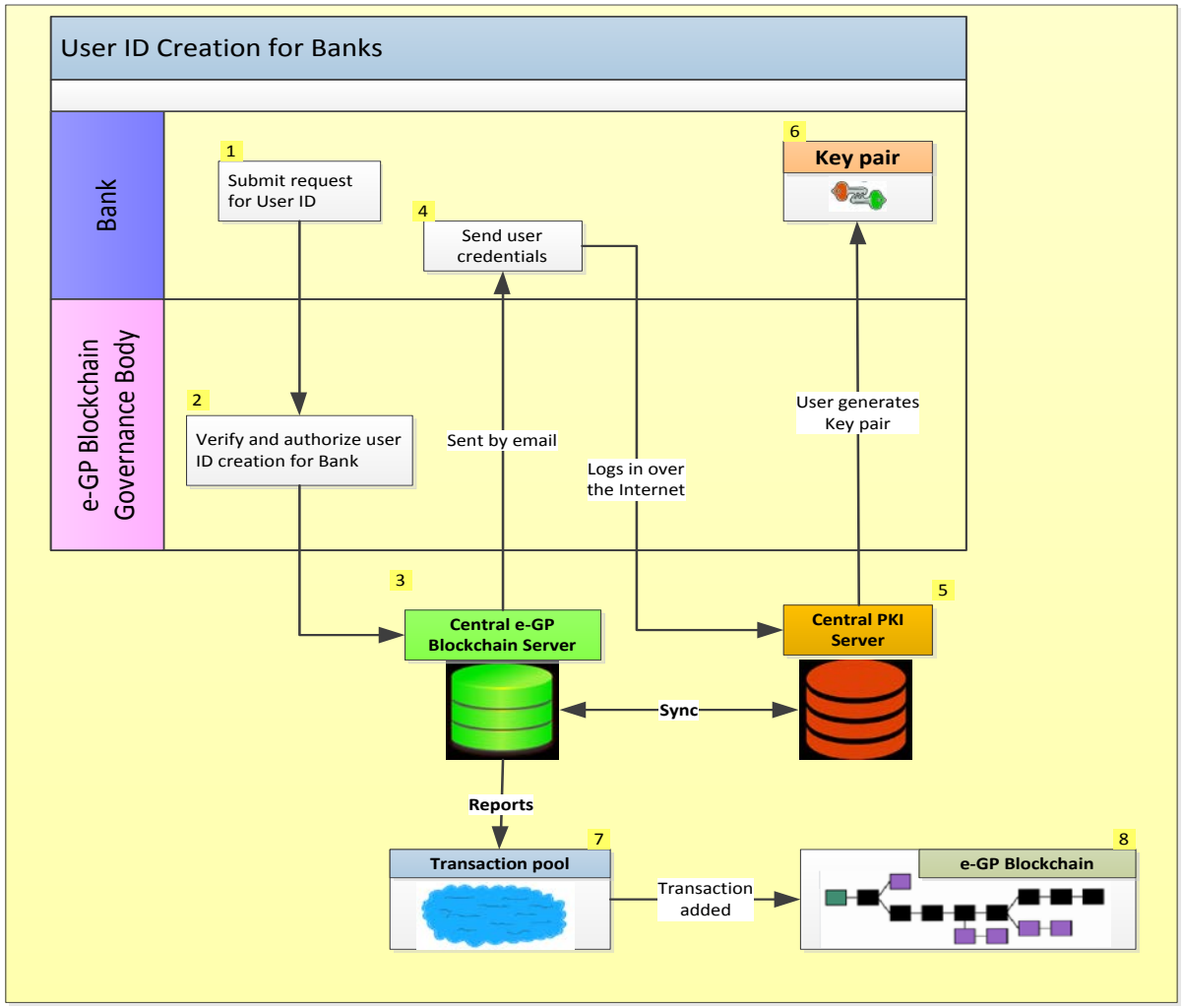

Figure 21: User ID creation for Banks

96. The process for modifying user credentials for BID users will be exactly as explained in section 6.2.3 of this report. The replacement of public key for a BID will be published as a transaction in the e-GP Blockchain as follows: *“The public key <<MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAIJVHC/d3W1C/qgmTdf5sCnzNrN/a2/2r2kJg9Xu8IhhLoU7en55rP96rOK7jSxRgdyFeqVHuXz4Kg8difeoxlsCAwEAAQ==>> for <<BID 987>> has been replaced with <<MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAcL7NVsswOpZfT1QuAvArz52nWVPlKxjfr2AlAnKujTP3ToE6HjNXHxlJuLNOn4SxbRwGfYnLuCif8/J7/aNpXwIDAQAB>> on DD-MM-YYYY based on request received from <<Bid 987>> and <<def@mail.com>>.*

B. Online Submission of Electronic Bank Guarantee

97. Firstly, a need or purpose for an e-payment should be created in the e-GP system (e.g.) a bid created by a supplier or a contract awarded to a supplier. It is standard practice for an e-GP

system to uniquely identify a bid or a contract. A supplier seeking to make e-Payment with electronic bank guarantee using the e-GP Blockchain network will provide the following key details to its bank for issuance of the guarantee:

(i) Transaction reference or purpose for which the guarantee is being issued (e.g. bid reference number)[4]
(ii) Bank guarantee amount
(iii) Name of the purchasing agency, bank guarantee validity date and so on
(iv) A format provided by the purchasing agency, in which the supplier is required to provide the guarantee
(v) e-GP system in which the transaction reference was created
  a. e-GP system reference as it is identified in the e-GP Blockchain network (e.g. e-GP System A24)
  b. Name of the e-GP system
  c. URL of the e-GP system
(vi) Supplier details
  a. GID reference issued to the supplier by the e-GP Blockchain
  b. Name of the supplier

98. Refer to Figure 22 for an overview of the process for submission of authenticated electronic bank guarantee submission in e-GP systems.

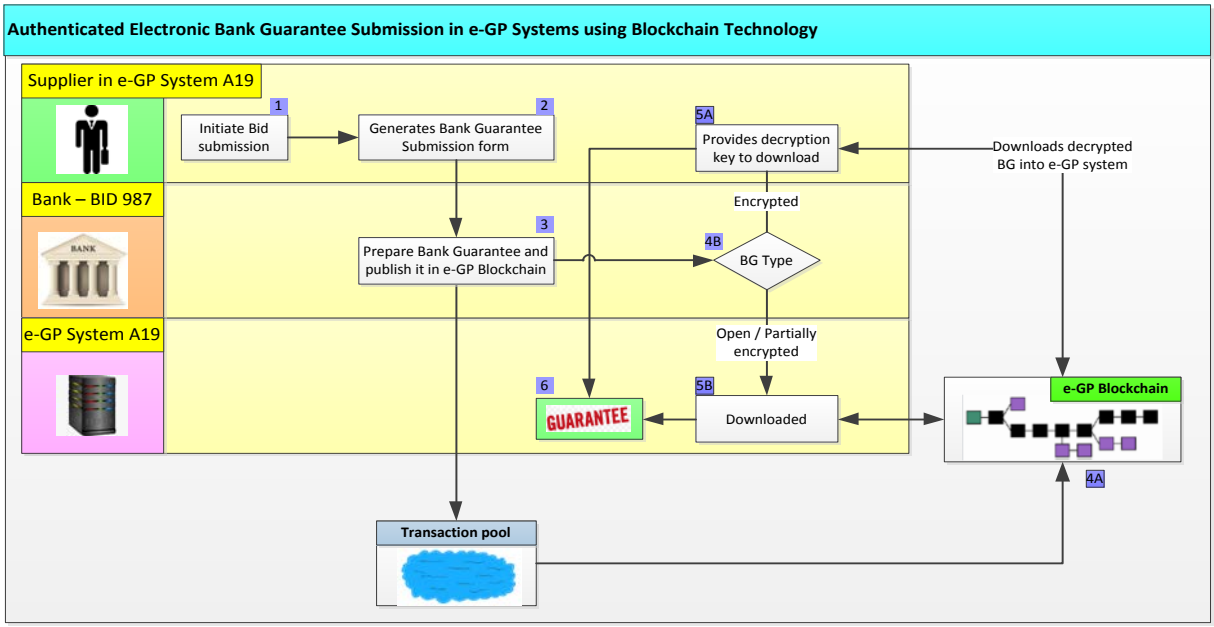

Figure 22: Submission of electronic bank guarantee in e-GP systems using Blockchain technology

99. A set of 3 variants of the electronic bank guarantee are identified, depending on the extent to which the bank guarantee message published by the bank is confidential or encrypted. In the

[4] There will be reconciliation issues when banks wrongly input the transaction reference while issuing the bank guarantee. When e-GP systems publish the bank guarantee transaction references in the e-GP Blockchain, the consensus rules would verify correctness of a transaction reference before adding the transaction onto the Blockchain. The banks could even define an interface with e-GP Blockchain to pull in the transaction reference electronically from the Blockchain against which the electronic bank guarantee would be issued. Thus, errors in issuance of the electronic bank guarantee would get minimized.

fully open variant, the entire message is published as plain text which any interested party can view in the e-GP Blockchain. Except for identity of the e-GP system, all other key details are encrypted in the partially confidential bank guarantee. In the most confidential version, all key details including the intended recipient (i.e. e-GP system) is encrypted. The procedure to be followed to process the messages varies depending on the extent to which a message is encrypted. Also, the consensus rules can be verified by the larger public only to the extent the messages are published as plain text. Refer to Figure 23 for a snapshot view of the 3 variants.

Snapshot View of Electronic Bank Guarantee Message Variants				
S.no.	**Criteria**	**Fully Open**	**Partially open**	**Fully Encrypted**
1	Supplier GID	Plain text	Encrypted	Encrypted
2	Bid reference	Plain text	Encrypted	Encrypted
3	BG amount	Plain text	Encrypted	Encrypted
4	BG document	Plain text	Encrypted	Encrypted
5	Recipient (e-GP System name)	Plain text	Plain text	Encrypted
6	Encryption key	Public key of the recipient e-GP system	Public key of the recipient e-GP system	Public key of the recipient e-GP system
7	Decryption key[5]	Private key of the recipient e-GP system	Private key of the recipient e-GP system	Private key of the recipient e-GP system
8	Informing the e-GP system	Central e-GP server informs automatically	Central e-GP server informs automatically	e-GP system pulls in the BG based on info provided by Supplier

Figure 23: Snapshot view of Electronic Bank Guarantee Message Variants

1. Fully Open Electronic Bank Guarantee

100. The bank will prepare the guarantee required by the supplier and publish it as a transaction in the e-GP Blockchain. Refer to Figure 24 for a sample message. Since the e-GP system name and bid reference is recorded as part of the transaction, the central e-GP server can be designed to automatically intimate the concerned e-GP system about a message available for processing. The e-GP system will immediately process this message and update the bank guarantee information against the supplier's bid subject to verification of the following:

(i) GID of supplier in the e-GP system matched with the GID provided in the bank guarantee message
(ii) Bid reference number specified in the message matched with the e-GP system records
(iii) BG amount specified in the message complied with the tender requirements
(iv) Verify hash value of the message

[5] If banks encrypt the messages with only one public key of the recipient and if the corresponding private key is lost or corrupted, the bank guarantees which are yet to be processed by the recipient e-GP system cannot be decrypted. There will be operational difficulties for all the involved stakeholders in this scenario. The occurrence of such a scenario can be minimized by associating 2 different public keys to an e-GP system. In which case, the Bank should encrypt the same bank guarantee message in duplicate with the 2 different keys. So, when the primary key is lost or corrupted, the e-GP system could still get the messages decrypted using the secondary key.

(v) Decrypt the hash value using public key of the bank (e.g. BID 987) to confirm that the message was actually signed by the concerned Bank and no one else

S.no.	Title	Content
1	Transaction reference	TR12345
2	Transaction Date	09-Sep-2018
3	Bank ID	BID 987
4	Bank Name	Bank of Country1
5	GID of Supplier	54321
6	e-GP system	e-GP System A24
7	Bid reference	ABC123
8	Bank Guarantee Amount	10,000 USD
9	Content Hash (MD5) of 1 – 8	302f1454f9b45367677d6e3a4d6b641a
10	BG document	www.xyz.com/TR12345
11	Hash of BG document (10)	409520C58E9AADBE78F84C57478BAA65
12	Public key of BID 987	*MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAcL7NVsswOpZfT1QuAvArz52nWVPlKxjfr2AlAnKujTP3ToE6HjNXHxlJuLNOn4SxbRwGfYnLuCif8/J7/aNpXwIDAQAB*
13	Encrypted hash of (9)	U2FsdGVkX18V9xX6D44wRj0GWmildzPmiB12+/jotTvSjqLSbsC01L/okXKOf9IpuwGKfRlNRjk=

Figure 24: Fully Open Electronic Bank Guarantee

2. Partially Encrypted Electronic Bank Guarantee

101. When an electronic bank guarantee is published in the Blockchain as provided in Figure 24, the following confidential information will be available as a public record: Supplier <<54321>> participated in a tender in <<e-GP system A24>> for which bank guarantee (BG) of USD 10,000 is to be paid. Based on this information, one can infer the actual tender against which the supplier participated. It is expected that e-GP systems and the suppliers as well would object to publication of a fully open electronic bank guarantee. To make it partially open, the bank will encrypt the following data fields using the public key of the e-GP system owner and publish only an encrypted message:

(i) GID of supplier,
(ii) Bid reference,
(iii) BG amount, and
(iv) BG document.

102. Refer to Figure 25 for a sample partially encrypted electronic bank guarantee message published in the e-GP Blockchain. Just as in the fully open electronic bank guarantee, the e-GP Blockchain server will intimate <<e-GP System A24>> about a message available for processing. The e-GP system will decrypt the message using its private key and do the same validations as in the fully open electronic bank guarantee. An external party monitoring the e-GP Blockchain can still find out that the bank <<BID 987>> issued a BG for <<e-GP System A24>> on 09-Sep-2018. The partially encrypted electronic bank guarantee would be quite safe, especially when large number of bank guarantees is published in the e-GP Blockchain network.

S.no.	Title	Content
1	Transaction reference	TR12345
2	Transaction Date	09-Sep-2018
3	Bank ID	BID 987
4	Bank Name	Bank of Country1
5	GID of Supplier - Encrypted	U2FsdGVkX1+iCktqaH8XxD0QEMZerdpP
6	e-GP system	e-GP System A24
7	Bid reference - Encrypted	U2FsdGVkX1/nuys8PO5wgKwKhaacg5ha
8	BG Amount - Encrypted	U2FsdGVkX1/HdJsfPkK3m2EvGS4JGoqykAbYs6oDwK8=
9	Content Hash (MD5) of 1 – 8	302f1454f9b45367677d6e3a4d6b641a
10	BG document - Encrypted	www.xyz.com/TR12345
11	Hash of BG document (10)	409520C58E9AADBE78F84C57478BAA65
12	Public key of BID 987	*MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAcL7NVsswOpZfT1QuAvArz52nWVPlKxjfr2AlAnKujTP3ToE6HjNXHxlJuLNOn4SxbRwGfYnLuCif8/J7/aNpXwIDAQAB*
13	Encrypted hash of (9)	U2FsdGVkX18V9xX6D44wRj0GWmildzPmiB12+/jotTvSjqLSbsC01L/okXKOf9IpuwGKfRlNRjk=

Figure 25: Partially Open Electronic Bank Guarantee

3. Fully Encrypted Electronic Bank Guarantee

103. Herein, the e-GP system name would also get encrypted in addition to the data encrypted in the partially encrypted electronic bank guarantee. All the data fields would be encrypted with public key of the e-GP system owner. Any party, including the <<e-GP system A24>> and the central e-GP server, monitoring the e-GP Blockchain cannot understand the contents of the Blockchain record. Hence, the central e-GP server will be unable to intimate <<e-GP System A24>> that a message is available for processing. The responsibility will then be on the supplier to intimate the e-GP system about the bank guarantee message. The following actions will be performed in sequence to associate the bank guarantee record to the concerned bid in <<e-GP system A24>>:

(i) Bank with <<BID 987>> will inform supplier with GID <<54321>> that a bank guarantee with transaction reference <<TR12345>> is published in the e-GP Blockchain
(ii) Supplier will log into the <<e-GP system A24>>, retrieve its bid and submit the Blockchain transaction reference <<TR12345>> against its bid
(iii) The <<e-GP system A24>> will retrieve the record from the e-GP Blockchain and apply its private key to decrypt the content
(iv) The <<e-GP system A24>> will verify whether decrypted content complied with the validation requirements. Upon successful verification, the e-GP system will update the bank guarantee status of the supplier with GID <<54321>>.

104. Refer to Figure 26 for a sample of fully encrypted electronic bank guarantee.

S.no.	Title	Content
1	Transaction reference	TR12345

S.no.	Title	Content
2	Transaction Date	09-Sep-2018
3	Bank ID	BID 987
4	Bank Name	Bank of Country1
5	GID of Supplier - Encrypted	U2FsdGVkX1+iCktqaH8XxD0QEMZerdpP
6	e-GP system	U2FsdGVkX1/5ddkKQl0HEK19RC8XaP/pHMJEQyKGfqw=
7	Bid reference - Encrypted	U2FsdGVkX1/nuys8PO5wgKwKhaacg5ha
8	BG Amount - Encrypted	U2FsdGVkX1/HdJsfPkK3m2EvGS4JGoqykAbYs6oDwK8=
9	Content Hash (MD5) of 1 – 8	302f1454f9b45367677d6e3a4d6b641a
10	BG document - Encrypted	www.xyz.com/TR12345
11	Hash of BG document (10)	409520C58E9AADBE78F84C57478BAA65
12	Public key of BID 987	*MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAcL7NVsswOpZfT1QuAvArz52nWVPlKxjfr2AlAnKujTP3ToE6HjNXHxlJuLNOn4SxbRwGfYnLuCif8/J7/aNpXwIDAQAB*
13	Encrypted hash of (9)	U2FsdGVkX18V9xX6D44wRj0GWmildzPmiB12+/jotTvSjqLSbsC01L/okXKOf9IpuwGKfRlNRjk=

Figure 26: Fully Encrypted Electronic Bank Guarantee

VIII. SOFTWARE REQUIREMENTS

105. The software required for building and managing the e-GP Blockchain network will need to be developed and maintained by a central Nodal Agency. If the entire solution is built on open source stack, extending it to a global audience will be somewhat easier to implement as the software license charges will not become an impediment in rolling out the software. Once the network reaches a certain level of maturity, a decision could be taken on whether to evolve the software in an open source model.

106. The policies governing the e-GP Blockchain network will need to be framed at first based on which the functional and technical requirements of the software will need to be prepared. A professional software development agency will need to be engaged for building the envisaged software and maintaining it for a certain specified period of time. An overview of the key functional modules in the e-GP Blockchain software is provided in Figure 27.

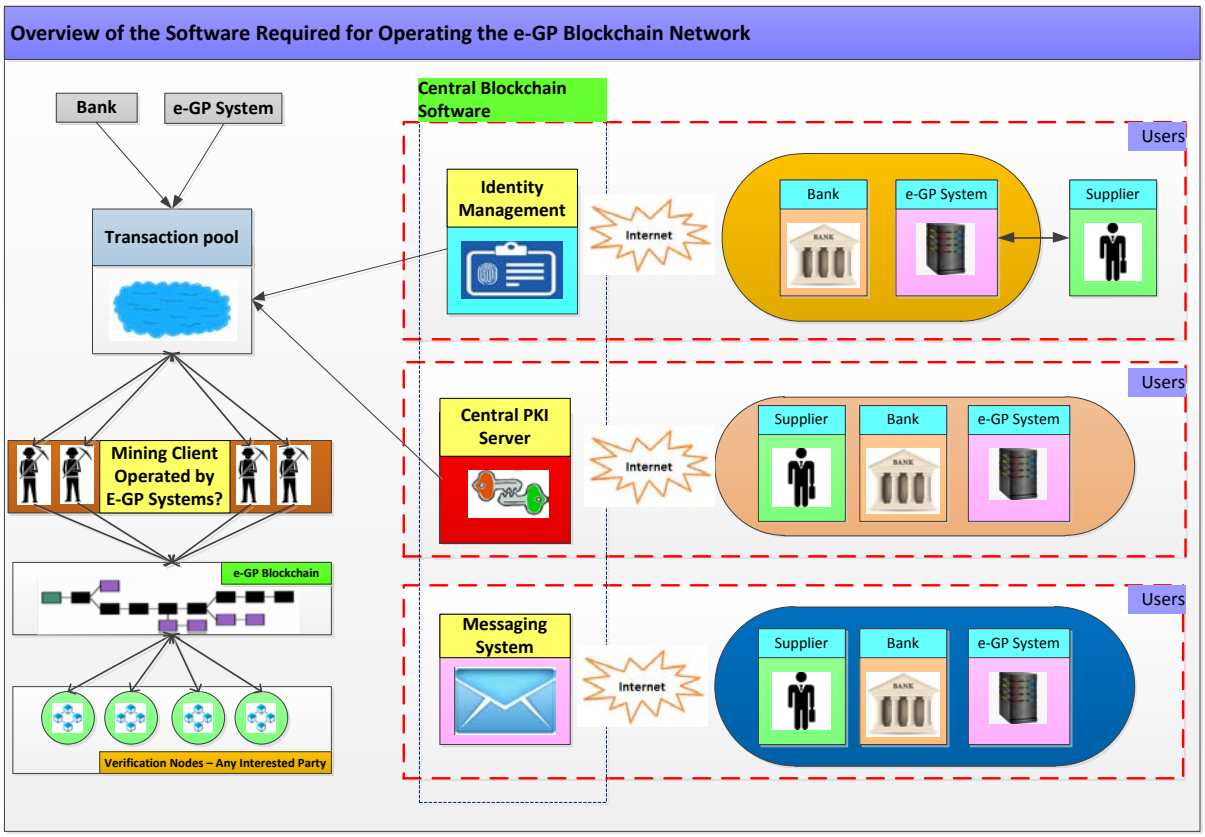

Figure 27: Overview of the Software Required for Operating the e-GP Blockchain Network

A. Identity Management Module

107. This component will be the core infrastructure underlying the e-GP Blockchain network. Its primary focus is user identity management. This software will mostly handle automated transaction requests received from a couple of hundred e-GP systems and a couple of thousand banks. As real-time response is not required for most transaction types handled by this system, it will be designed to process the requests in batch-mode. Though the supplier identities are created and modified in this module, such creation will be done based on requests received only from the

e-GP systems. Hence, the concurrent connects on this module will not be very high. The identities of tens of millions of suppliers can be managed with relatively minimal server infrastructure.

B. Central Messaging System

108. A logic layer is required to interconnect various users of the e-GP Blockchain network and enable them to work together as a unit. This module will continuously monitor the transactions in the e-GP Blockchain and send targeted intimations to specific users of the e-GP Blockchain network as and when messages relevant to them are published in the e-GP Blockchain.

C. Central Public Key Infrastructure (PKI) Server

109. A public-private key pair needs to be generated and assigned to a user in the e-GP Blockchain network for functional reasons such as:

(i) There is a need to validate and confirm whether a supplier is the rightful owner of a GID before the supplier is authorized to act upon on the GID, and
(ii) To authenticate whether a transaction reported in the Blockchain was executed by an authorized user.

110. The legally binding transactions such as submission of online bids and issuance of award of contract to a supplier will be executed in the concerned e-GP systems. The public-private key pair issued using the PKI server would not be relevant for those legally binding online transactions. The approach adopted for online authentication and encryption differs from one country to another. Few e-GP systems have adopted legally valid digital signatures and many have used password based electronic signatures to authenticate user identity. The existing authentication framework in-built in e-GP implementations will not be impacted and they will co-exist with the public-private key pair generated by the central PKI server of the e-GP Blockchain network. Hence, there is no need to correlate, map and legally acknowledge equivalence of the key pairs generated from the e-GP Blockchain PKI server with that of the existing national authentication frameworks.

111. Just as it is with the user credentials, the suppliers directly cannot submit request for generation of the public-private key pair. Instead, the suppliers will need to route the requests for generation of the key pair through an e-GP system in which it is already registered. The actual generation of the key-pair however will need to be done directly by the suppliers and other users of the Blockchain network.

112. The PKI server will need to be kept in a highly secured environment because the entire Blockchain network will get compromised if the private keys get compromised in whichever method. This module will need to be accessible over the Internet because the suppliers and authorized users of the e-GP systems will need to generate and download their private-public key pair online.

D. Mining Client

113. A Mining Client has to be developed specifically to suit the e-GP Blockchain Network. The principles of Mining, it is envisaged, will remain the same just as in the Bitcoin Blockchain Network. The rules governing the consensus will need to be built into the client and there will be multiple versions of the client as the rules will keep evolving with time. Unlike the Bitcoin Blockchain

network, the provision of financial incentives to the Miners is not envisaged. The mathematical puzzle will be kept quite simple. Hence, the Miners will not need to invest in heavy computing power. The Mining will be a procedural function which needs to be complied with so the transactions can get recorded and verified in the Blockchain. It is proposed to limit the Mining function to owners of e-GP systems, a few of which can compete to add records from the transaction pool into the Blockchain.

E. Full Nodes

114. The data reported in the e-GP Blockchain is essentially a public record. Hence, the entire e-GP Blockchain will be freely made available to the public. Any interested party can contribute towards building consensus in the Blockchain network. Further, it can parse the Blockchain records and make some meaning out of it as well. Indeed, the agency managing the e-GP Blockchain network should encourage volunteers to run full nodes and play an active role in enriching the network.

IX. SYNERGY BETWEEN THE OPEN CONTRACTING INITIATIVE & E-GP BLOCKCHAIN

115. The Open Contracting initiative seeks to enable government agencies world-wide to publish Government procurement data in compliance with Open Contracting Data Standards (OCDS). The OCDS is a non-proprietary standard, the first version of which was released in 2014 and it is continuously being evolved with newer releases. It is reported that OCDS is adopted by 30 countries[6], the prominent of which are Chile, Ukraine and Zambia.

116. The OCDS standard conceptualizes the contracting process, from an open data perspective, into 5 phases:

(i) Planning
(ii) Tender
(iii) Awards
(iv) Contracts
(v) Implementation

117. The tender related standards are now being widely used. As the adoption of e-GP system goes beyond the e-Tendering module, it is expected that e-GP systems will comply with the data standard requirements of the remaining 4 phases as well.

118. Open Contracting Partnership, the agency managing OCDS, provides detailed documentation about the standards and also provides help desk services to those interested in adoption of the standard. Government agencies can publish data taken out of the e-GP systems in compliance with OCDS with minimal effort.

119. The adoption of e-GP system is limited to e-tendering functionality in most e-GP systems. Where e-tendering is adopted, the procurement process handled online covers tender publication, bid submission and bid evaluation. Subsequent to completion of bid evaluation, procuring entities do not logically complete the process online in the e-GP system. Instead, the AoC is issued in manual format due to which there is lack of AoC data in the e-GP system. Further, contract management aspects of the e-GP system are handled using the manual system.

120. The implementation of e-GP Blockchain as it has been thought through in this paper will cause suppliers to push the government agencies and purchasing officials to:

(i) Expand adoption of e-GP system functionalities covered under awards, contracts and implementation phases of OCDS standard
(ii) Publish at least the AoC and contract management related transaction records in e-GP Blockchain, so the suppliers can refer their work experiences online while they submit bids in e-GP systems

[6] https://tinyurl.com/ybxu98mr

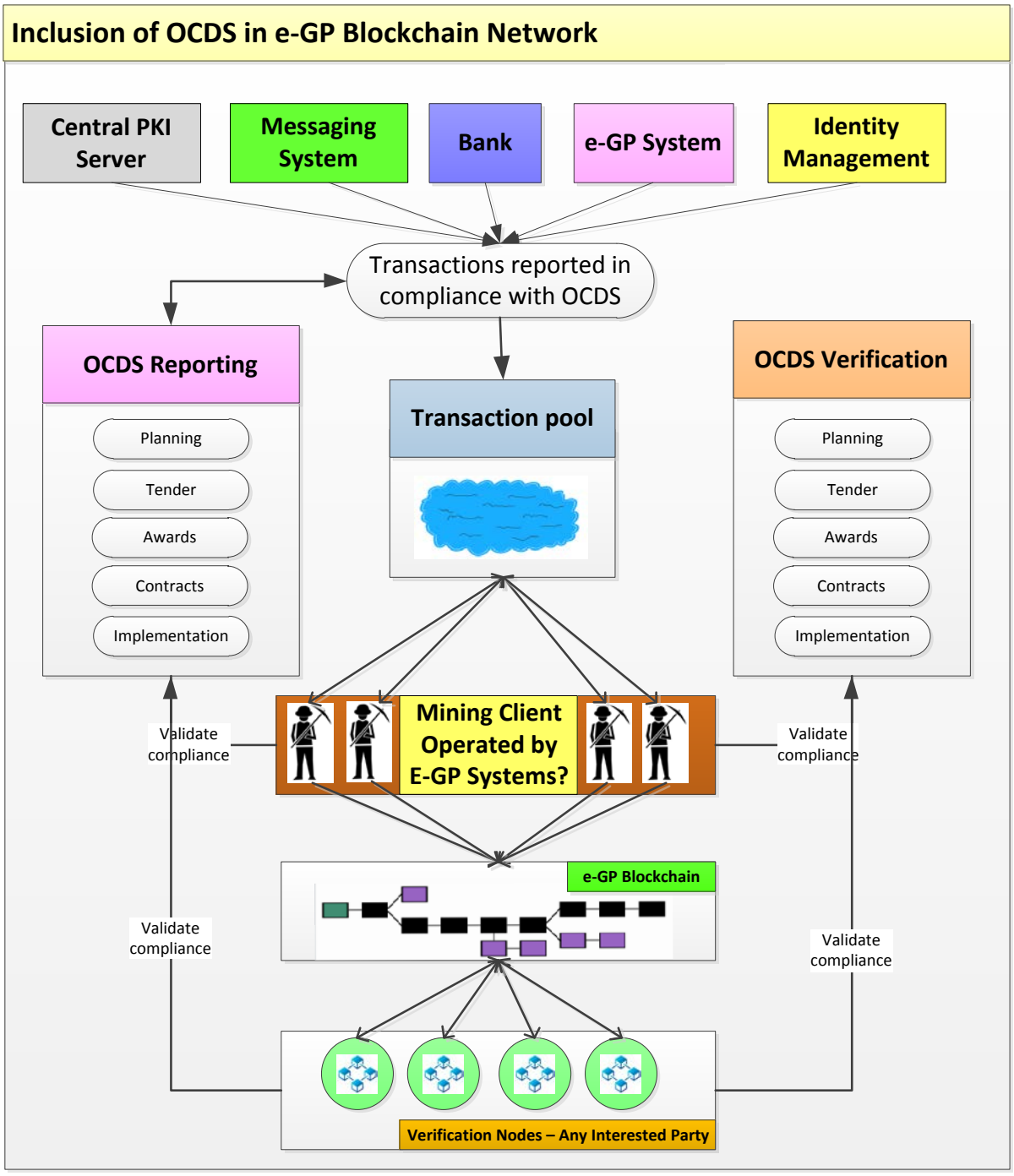

Figure 28: Inclusion of OCDS in e-GP Blockchain Network

121. If all the key policy makers could come together and mandate submission of work experience certificates in e-GP systems as Blockchain records, the government agencies will have the necessity to expand adoption of e-GP system functionality. The e-GP Blockchain software will require its users to strictly comply with standards laid down for publishing a transaction in e-GP Blockchain. Only those transactions found in compliance with the standards will get published as a public record. Such compliance verification will be done in a decentralized manner as per clearly laid down consensus rules. As extensive ground work has already happened in development of OCDS, it is strongly recommended that OCDS standards are

evolved and converged with the e-GP Blockchain initiative. Then, e-GP system owners need not comply with the OCDS for the sake of desired outcomes such as transparency. Instead, the compliance to OCDS will become a necessity because the suppliers will demand purchasing agencies to logically complete the procurement activity in the e-GP system and publish the contracting data in the e-GP Blockchain as per OCDS standards, so they can cite the Blockchain records while they bid for tenders in e-GP systems. Refer to Figure 28 for a snapshot view on the inclusion of OCDS in e-GP Blockchain network.

122. Indeed, the most fundamental requirement for this concept to work is identifying each Supplier uniquely across all e-GP systems registered in the global e-GP Blockchain network. Refer to Section 6.3 of this report for a detailed explanation of the process proposed for development of a de-duplicated global database of suppliers.

X. OVERVIEW OF ALL KEY COMPONENTS THE E-GP BLOCKCHAIN NETWORK

123. An overview of all key components of the e-GP Blockchain network is provided in Figure 29.

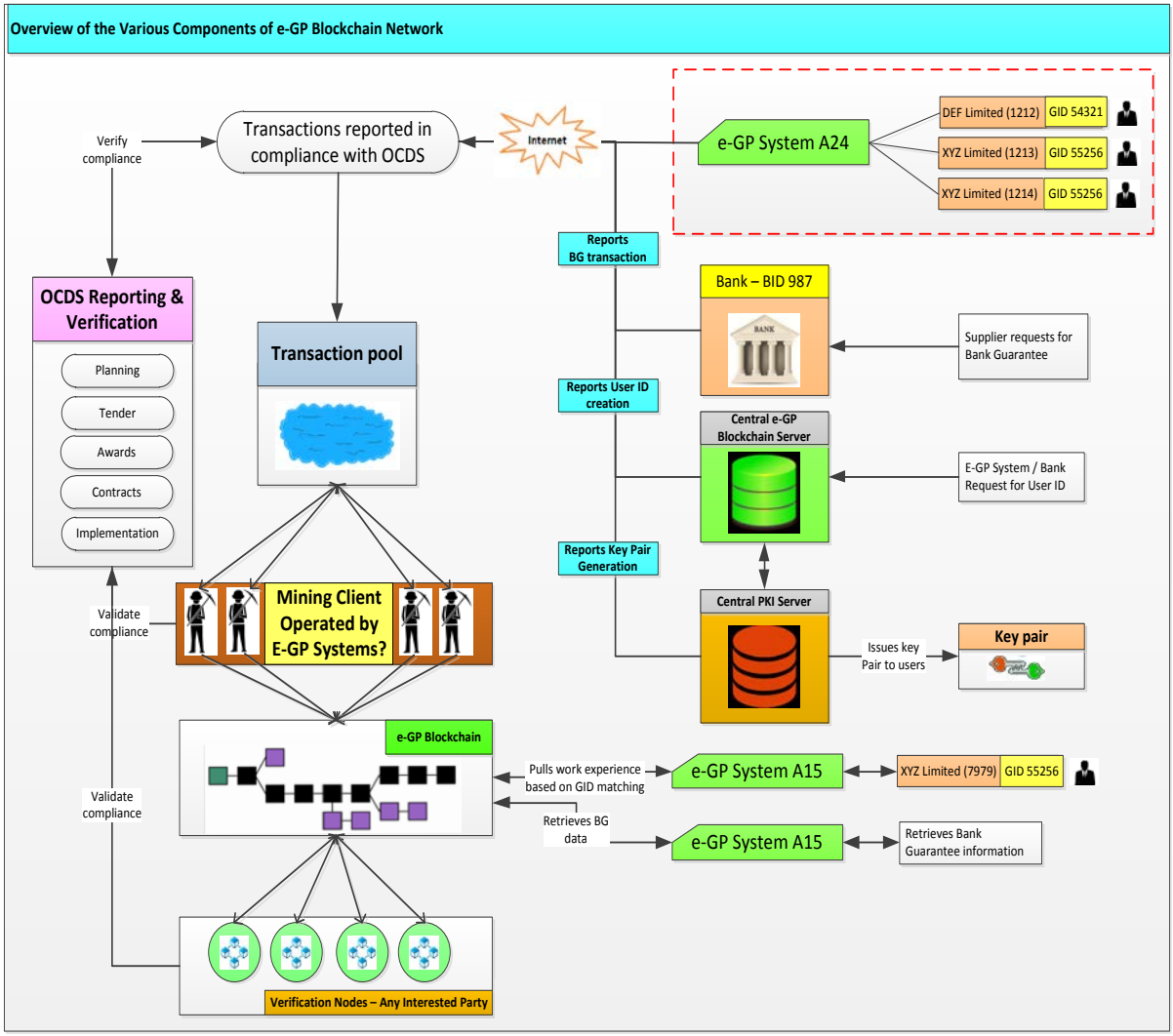

Figure 29: Overview of the various components of the e-GP Blockchain Network

XI. INCENTIVIZING STAKEHOLDERS TO ADOPT THE E-GP BLOCKCHAIN NETWORK

124. The technology (i.e. Blockchain and cryptography techniques) proposed herein to build the e-GP Blockchain network is tried and tested. With a bit of effort, the e-GP Blockchain network can be made operational. However, significant change management effort would be required to encourage key stakeholders to adopt this network as detailed below:

(i) On-board key stakeholders in the governance mechanism established to manage the e-GP Blockchain network
(ii) Obtain investments or equity contributions from key stakeholders for development of the e-GP Blockchain network. This will provide the much required ownership.
(iii) Develop technology tools such that it is easier for e-GP systems to adopt the standard (i.e.) join the e-GP Blockchain network with minimal effort with near zero investments and transaction costs
(iv) Expedite implementation of e-GP Blockchain network, so there is first mover advantage. Take efforts to attain critical mass among the targeted user community.
(v) Undertake capacity building and change management initiatives to on-board users onto the e-GP Blockchain network

125. A mechanism is most definitely required for standards based exchange of data across e-GP systems. The emergence of multiple e-GP Blockchain networks is not a desirable outcome and efforts should be taken to strictly avoid the same.

XII. KEY BENEFITS OF THE E-GP BLOCKCHAIN NETWORK

126. The following benefits can be realized when the envisaged e-GP Blockchain network is fully implemented and widely adopted:

127. Performance Rating: The proposed e-GP Blockchain concept could be extended to uniquely identify purchasing agencies across the network, just as the suppliers are identified by a GID. The purchasing agency and suppliers involved in execution of a contract can be individually required to compulsorily report their feedback on performance of the other party during the contract execution. As this feedback would be recorded in a standardized format, it will be possible to accumulate performance of a purchasing agency or a supplier. A sense of competition could be brought in amongst the purchasing agencies and the supplier community to improve their rating, so the quality of government contracting as a whole improves. Few purchasing agencies can set high benchmarks which the rest of them can strive to achieve over a period of time. The purchasing agencies with a high performance rating will presumably attract better quality competition and the suppliers with high rating will be in demand. There is immense potential to be unearthed in this regard.

128. Simplified External IT System Integration: The integration of e-GP with the banking system for electronic bank guarantee submission is just one example of how seamlessly e-GP systems could be interlinked with 3rd party IT systems. The same integration concepts (i.e. fully open, partially open and fully encrypted) can be extended to enable pulling data from a whole range of external IT systems with minimal effort. For example, the tax authority can publish tax clearance certificate of a supplier as a fully encrypted transaction in Blockchain, which a supplier can pull into its "My profile" [7] section in multiple e-GP systems. If the reporting format could be standardized by OCDS, e-GP systems can pull the suppliers data from external ID systems world-wide with one single interface.

129. Expedited Procurement and Reduced Transaction Costs: Purchasing agencies will find it easier to evaluate suppliers and to some extent they could even automate bid evaluation when the data required for evaluation a supplier's expertise can be pulled in a standardized format from authenticated sources. Suppliers can pull in all their work experiences and other capability information onto their "My profile" section of an e-GP system, after which bid submission can be done with minimal effort. When the network is adequately robust, purchasing agencies could automatically qualify suppliers when performance rating of the suppliers exceeds certain minimum threshold value. The time taken for bid evaluation will reduce substantially with the introduction of such automation. Consequently, the supplier community would find working with the government much easier and this, it is hypothesized, would reflect in higher competition for government tenders.

[7] If external IT system data about a supplier is to be encrypted and published in the Blockchain, the external IT system shall encrypt the data using the supplier's public key. The supplier will then decrypt its relevant Blockchain record using its private key and push the decrypted record onto a specific e-GP system.

XIII. GOVERNANCE MECHANISM

130. All the e-GP systems worldwide should be on-boarded in the e-GP Blockchain network for it to reach its full potential. When the e-GP systems are on-boarded in the network, the suppliers registered in these systems would follow suit automatically. Given the global nature of this network, an international team well connected with government agencies in Asia, Africa, Australia, Europe and America should be on-boarded in a steering committee to govern and manage expansion of the network. In addition to the steering committee, a core technical advisory committee has to be constituted to finalize and continuously improve the e-GP Blockchain standards and associated software.

131. A central project implementation unit (PIU) has to be set-up to manage development and maintenance of the Blockchain related software. The operations management associated with the network will be decentralized to regional hubs located closer to end users of the Blockchain network. Refer to Figure 30 for a pictorial overview of the governance structure envisaged for e-GP Blockchain network.

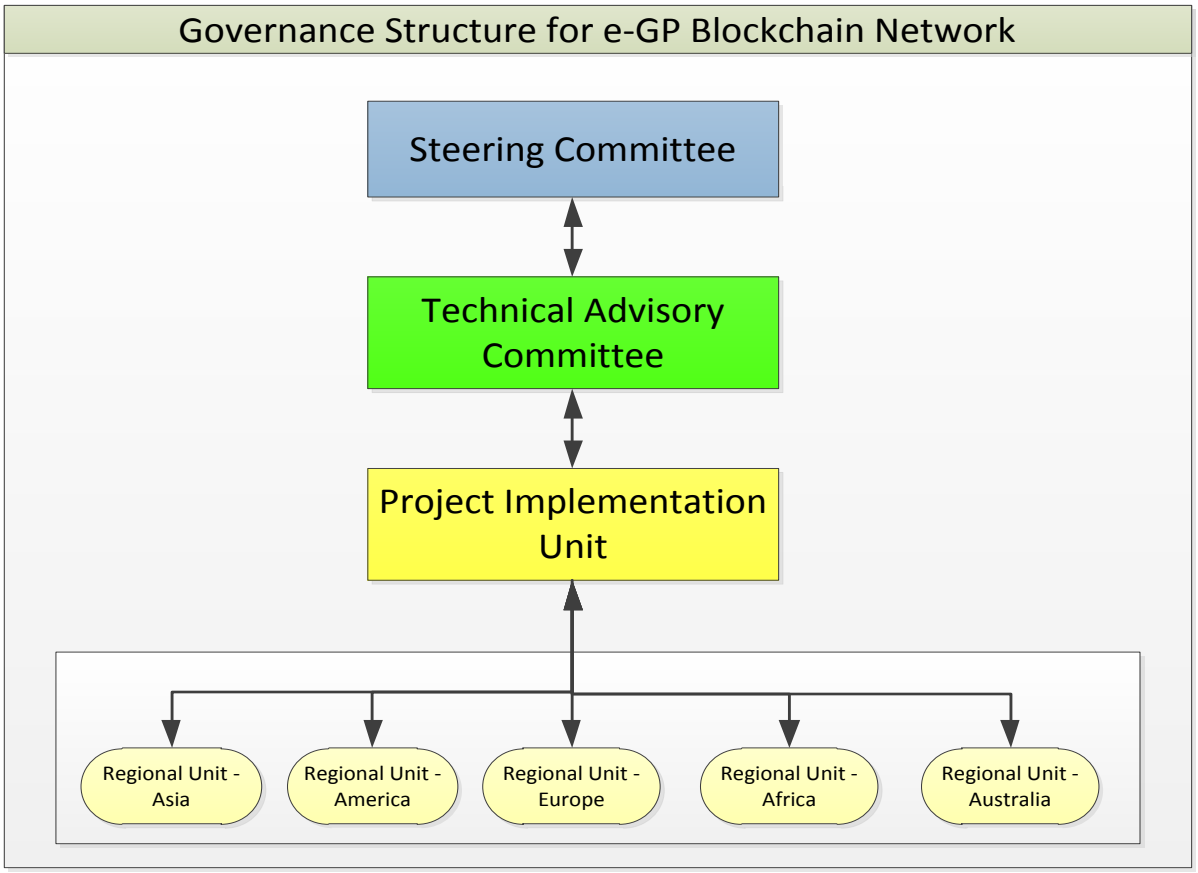

Figure 30: Governance Structure for e-GP Blockchain Network

XIV. EXTENDING THE E-GP BLOCKCHAIN NETWORK TO THE PRIVATE SECTOR

132. As government procurement accounts for about 15% of a nation's GDP, a significant percentage of the supplier community would participate in Government business. Most of these suppliers would work with the private sector as well engaging in Business-to-Business (B2B) and Business-to-Consumer (B2C) trade. When a significant percentage of the e-GP systems are on-boarded, the e-GP Blockchain network would have a very large de-duplicated Supplier database. With minimal effort, the e-GP Blockchain network could be extended to include B2B e-procurement systems. The suppliers already present in the e-GP Blockchain network can refer their work experiences and submit authenticated electronic bank guarantees in their B2B transactions as well.

133. The focus initially ought to be on building a network of e-GP systems. Once this network achieves a certain critical mass, it can be extended to include B2B e-procurement systems as well. Such an extension would require minimal software changes:

(i) New types of transaction messages would have to be considered. The mining software and associated consensus rules would need to be modified as well.

(ii) The private sector transactions may have to be encrypted and recorded in the Blockchain, quite similar to the fully encrypted electronic bank guarantee. When the intended recipient of a work experience certificate is not known, the agency issuing the certificate will need to encrypt the document using the supplier's public key. The supplier will decrypt the record and share details of the record to the concerned buyer in the B2B e-procurement systems.

XV. PEPPOL AND E-GP BLOCKCHAIN NETWORK

134. There are similarities between the PEPPOL initiative taken by the European Commission and the e-GP Blockchain network proposed herein, in that both:

(i) Seek to enable suppliers to participate in government procurement across national borders
(ii) Build on top of existing e-GP systems
(iii) Enable standards based exchange of documents
(iv) Have similar functional coverage focus (i.e. tendering, award of contract and contract management)

135. PEPPOL is designed as a European wide network, in advanced stage of adoption, with active users in many countries and a functioning eco-system. It has been close to a decade since PEPPOL was conceptualized.

136. The e-GP Blockchain network proposed in this report is a truly open network functioning entirely on standards and with no intermediaries whatsoever. As the e-GP Blockchain network is fully open, it is possible to extend the network and enable targeted communication with individual members of the network with minimal effort. This is illustrated in Section 7.2 of this report, wherein the process for electronic bank guarantee submission by the banks in e-GP system is explained. With the use of cryptography techniques, sensitive data can be published as a public record in Blockchain and yet kept confidential. Refer to Sections 7.2.2 and 7.2.3 for further details. Inherently, the envisaged e-GP Blockchain network would be more open and extensible as compared to the PEPPOL initiative by the European Union.

137. The objective of this section is to acknowledge PEPPOL as an initiative similar to that of e-GP Blockchain concept explained herein. Ideally, the e-GP Blockchain concept should build on top of the experiences of the European Union in implementing the PEPPOL project. A detailed study of PEPPOL is warranted to identify if some of the PEPPOL concepts can be incorporated while building the e-GP Blockchain network.

XVI. NEXT STEPS

138. The following key activities have to be finalized to operationalize the e-GP Blockchain network:

139. Governance Mechanism: Firstly, governance mechanism for managing the implementation of this network needs to be thought through. One of the multilateral development banks (MDB) could decide to incubate this network and then hive it off as a separate entity once it achieves critical mass. It is important for all the key stakeholders to work together as a unit and adopt one single global standard for e-GP Blockchain. A lot more detailing on this report needs to be done to get this concept implemented in practice. A core technical committee has to be established to finalize and approve Blockchain related technology standards. The core Blockchain related software will need to be developed as well.

140. Funding: A detailed project report (DPR) has to be prepared to define funding requirements for this project and identify funding sources to sustain and continuously evolve the e-GP Blockchain network. It needs to be evaluated if the network can be sustained from the revenue earned from providing value added services.

141. Pilot: A set of at least 3 neighbouring countries with active international bidder participation among them should be selected to pilot this initiative. It is proposed to limit the Pilot to 3 agencies at the beginning. As the system stabilizes, more e-GP systems can be on-boarded into the network in a phased manner.