

Digital Bank Guarantee

Section 1: Summary

Use Case Summary			
Use Case ID:	FIN-003	Use Case Type:	Vertical
Submission Date:	December 5, 2018	Is Use Case supporting SDGs	Yes
Use Case Title:	Digital Bank Guarantee	Domain:	List 6 Appendix 2
Status of Case	Pilot	Sub-Domain	Financial
Contact information of person submitting/managing the use-case	<p>Full Name: Dergachev Ivan Job Title: project manager E-mail address: ivan.dergachev@fintechru.org Telephone number: +7 926 773 77 74</p> <p>Full Name: Alexander Chuburkov Job Title: Expert GOST R * Russian TC 26 Cryptography and security mechanisms * ISO TC 307 Blockchain & DLT * Fintech Association (RUS) * FOCUS GROUP DLT ITU-T E-mail address: chuburkovalex@gmail.com Telephone number: +7 965 336 62 92</p>		
Proposing Organization	<p>FinTech Association Address: 4 Shlyuzovaya Embankment, Moscow, 115114, Russia http://fintechru.org/</p>		
Short Description	<p>Development and implementation of a software package for the organization of work with Digital Bank guarantees (DBG) based on the distributed ledger platform (blockchain platform "Masterchain").</p>		
Long description	<p>The market is ready to move from paper bank guarantees to digital ones, and it has already come to the realization that the digitization of paper documents and further work with digital copies of paper documents is a non-optimal approach and it is necessary to move to a system where the digital document will be primary;</p> <p>The potential availability of CBG solutions currently being developed by individual Banks is limited to the clients of the respective Bank, which reduces the possible effect of their implementation (the Buyer and the Seller, as residents of the Russian Federation, are not always clients of the same Bank). The System (solution, set of services) developed in the project is an interbank platform that is not tied to one Bank and, therefore, is devoid of the mentioned restriction.</p> <p>Project goals:</p>		

	<ul style="list-style-type: none">• Creation and implementation of the System• Improvement of legal regulation of CBG <p>Project objective:</p> <ul style="list-style-type: none">• Generation of requirements and hypothesis to test• Development of a prototype System and test the hypothesis• System pilot development and integration with "external" systems• System implementation/Start-up of pilot <p>Key assumption:</p> <ul style="list-style-type: none">• the technological platform for the project implementation is the infrastructure of the distributed Masterchain network, which includes the functionality for its administration and support of the role model of the system participants,• technological implementation of the system involves two stages: 1) creation of a prototype System and 2) creation of a pilot System,• openID Connect 1.0 is proposed as a technology for authorization of users of the developed system (user ID is signed by the authorization center, and can also be signed by the client in the browser through the EDS plug-in),• to store scans of documents (accompanying release, entry into force, change of conditions, termination of the warranty, etc.), it is planned to use a local document Storage integrated with the node of the distributed Masterchain network. <p>Beyond the scope of the project</p> <ul style="list-style-type: none">• Approval by the Principal and the Bank of the conditions for issuing a Bank guarantee,• Verification of the conditions for the entry into force of the Bank guarantee (except for the agreed date),• Check the conditions of termination of the Bank guarantee (except for the expiry of the guarantee),• Payment by the Principal of the Commission to the Bank for the issuance of a Bank guarantee,• Transfer of funds to the Beneficiary of the Bank guarantee when paying for it,• Integration with government agencies for the exchange of information on transactions with Bank guarantees.				
	SDG in Focus (when applicable)				
	Value Transfer:	Stage 1: no value transfer; Stage 2: payments in DLT allowed (CBDC)	<table><tr><td>Number of Users:</td><td>10</td></tr></table>	Number of Users:	10
	Number of Users:	10			
	Types of Users:	Principal, Guarantor bank, Beneficiary.			
Stakeholders	Principal, Beneficiary, Bank. Central Bank as observer				

Data:	Electronic documents, such as BG and contract, accounts in DLT
Identification:	Full identification of participants required
Predicted Outcomes:	<ul style="list-style-type: none"> • Reduction of terms and reduction of costs to ensure document flow under Bank guarantees (According to Bain&Company, 2016, more than 50% of operating costs of banks to conduct transactions of Bank guarantees goes to the implementation of paper document flow). • Reducing the cost of storage and risks of loss of information on paper (Distributed ledger guarantees the technical safety of information on the documents). • Increasing the availability/reducing the time for obtaining information on the Bank guarantee and its status for all stakeholders through the use of a single information environment, in the future integrated with national electronic trading platforms.

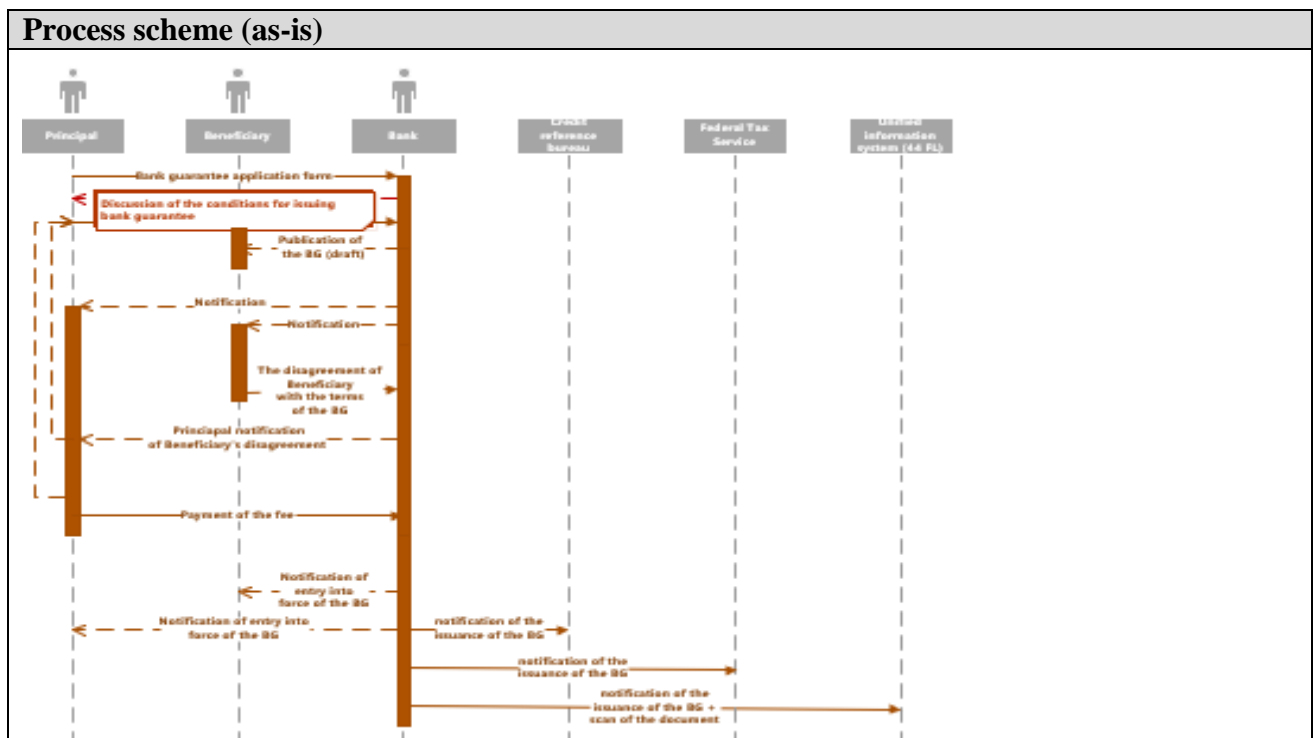
Overview of the Business Problem or Opportunity
<p>The objectives of the project:</p> <ul style="list-style-type: none"> • Switching from paper documents to digital form • Protection of confidential data by limiting the visibility of the issued document <p>For all participants of the business process it means a significant reduction of time (1-2 days). Process reduces the risk of falsification of the document, for economy that means increase of origin BG market. For banks, it means a reduction of operating costs by 10-15%. For Beneficiary, there is no reason to waste time on letters to Bank to verify authenticity of the issued bank guarantees. The process of document verification is simplified for the Regulator.</p>
Why Distributed Ledger Technology?
<p>The Blockchain and smart-contracts make this interaction trustworthy, transparent and understandable for each one of them. The implementation of DLT solution, which allows tracking paid bank guarantees, can eliminate paperwork and shorten the time of transaction.</p>

Section 2: Current process

Current Solutions
Documents exist in paper form; funds are transferred by corresponding bank; procedure of verification of the BG is manual, confidential data of issued BG is not protected.

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Principal contacts bank for a BG issuance	n/a

Existing Flow (as-is)		
Step	User Actions	System Actions
2.	Beneficiary receives BG and checks that it matches with the contract	n/a
3.	BG has expired	n/a

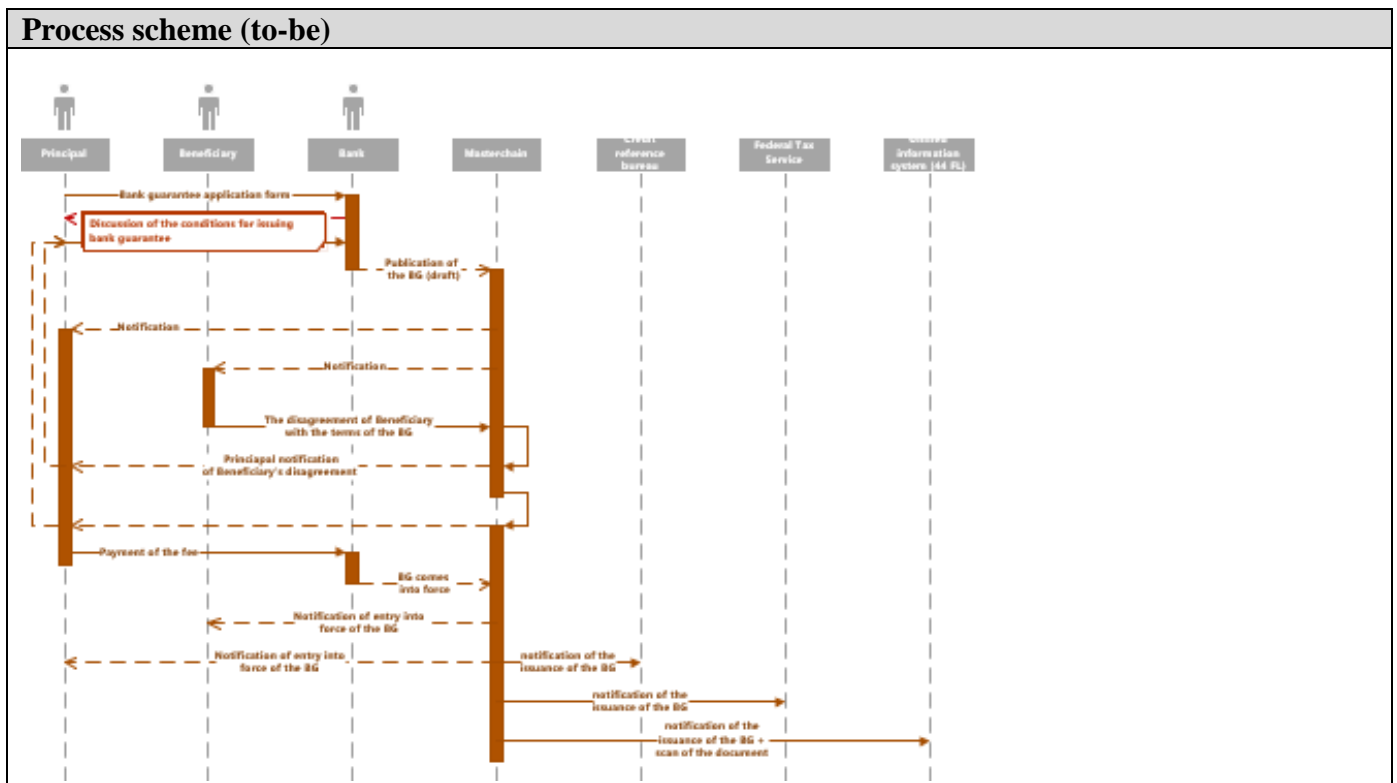


Data and information (as-is)		
Data	Type	Description
1	Documents	Contract, bank guarantee, agreements
2	Payment transactions	Payment of the fee for issue of bank guarantee

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Principal	Principal of bank guarantee
2	Beneficiary	Beneficiary of bank guarantee
3	Bank	Bank that issues the bank guarantee

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Bank writes BG`s data to the blockchain and the distributed storage	System writes smart contract to the blockchain and save the contract to the distributed storage
2.	Beneficiary validates BG`s data from the blockchain and the distributed storage	System marks the smart contract and the contract from the distributed storage as validated by the Beneficiary
3	BG comes into force	System marks the smart contract as active
4	The extension of the BG	System marks the smart contract as active. System saves hash of the documents to the blockchain and the consignment to the distributed storage
5	Changing conditions of the BG	System saves the data into distributed storage and blockchain
6	BG expired	System finalizes the smart contract



Participants and their roles		
Actor	Type/Role	Description
1	Bank	Bank that issues the bank guarantee
2	Principal	Principal of bank guarantee
3	Beneficiary	Beneficiary of bank guarantee

Data and information		
Data	Type	Description
1	Documents	Documents' hashes exchange in DLT-network
2	Payment transactions	Payment of the fee for issue of bank guarantee

Security and privacy		
<ol style="list-style-type: none"> 1. The bank guarantee conditions should be confidential to other blockchain network participants. 2. DLT-system should be able to provide mechanisms of BG documents and payments data integrity control; 3. BG documents and payments data and related services (System Actions) should be available in 24/7/365 mode. 		

Main Success Scenario + expected time line		
<ol style="list-style-type: none"> 1. Principal furnishes documents to Bank 2. Bank approvals loan 3. Principal accepts Bank conditions 4. Beneficiary accepts the text of BG 5. Principal pays fee 6. BG comes into force; 7. BG conditions adhered; 8. BG expired. 		

Conditions (pre- or post-)		
All parties are connected to DLT-network		
Performance needs		
<ol style="list-style-type: none"> 1. Volume of transactions > 700 Tx/day. 2. Network participants > 150 		
Legal considerations		
Switching from paper documents to digital form		
Risks		
<ol style="list-style-type: none"> 1. Legal risks; 2. Security risks; 3. Risks related to DLT immaturity. 		

Appendix 1: **Domains and subdomains for use cases categorization**

Vertical:

1. Finance
 - a. Financial management & accounting
 - b. International & interbank payments
 - c. Clearing and settlement
 - d. Reduction of Fraud
 - e. Financial messaging
 - f. Asset lifecycles and history
 - g. Trade finance
 - h. Regulatory compliance & audit
 - i. AML/KYC
 - j. Insurance
 - k. Peer-to-peer transactions
2. Healthcare
 - a. Pharma
 - b. Biotechnology
 - c. Medicine
3. Industries
 - a. Manufacturing
 - b. Energy
 - c. Chemical
 - d. Retail
 - e. Real estate
 - f. IT and telco
 - g. Supply chain management
 - h. Transportation
 - i. Agriculture
4. Government and public sector
 - a. Taxes
 - b. Government and non-profit transparency
 - c. Legislation, compliance & regulatory oversight
 - d. Voting
 - e. Taxation and customs
 - f. Intellectual property management
 - g. Land Registries

Horizontal:

1. Identity management
2. Security management
 - a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
 - a. Data Validation (includes provenance)
-