A Regime to Enhance the Next Generation EU Fund

Chao Liu[1], Xiaoshuai Zhang[2], Francesca Medda[1]
[1]Institute of Finance and Technology, University College of London, London, WC1E 6BT, United Kingdom
[2]School of Electronic Engineering and Computer Science, Queen Mary University of London, London, E1 4NS, United Kingdom
E-mail: {chao.liu, f.medda}@ucl.ac.uk, xiaoshuai.zhang@qmul.ac.uk.

***Abstract*—The Covid-19 pandemic has accelerated the digitalisation of the global economy and industry. However, the Next Generation EU (NG-EU) plan, which aims to provide a strong economic recovery for EU member states, has been criticised for its allocation delay and increased risk of hysteresis, that is, the dependence of the state of a system on its history. Under these circumstances, this paper proposes a blockchain-based two-layer system, Next Generation Digital Currency (NGDC), to assist an accountable and transparent fund allocation process for NG-EU funds. A consortium network in layer one is designed for all EU national central banks and the European Central Bank (ECB) to maintain a trustable and verifiable fund tracking ledger. A Prime-Coordinator PBFT (PC-PBFT) consensus mechanism-based agreement protocol is proposed to resolve discrepancies in the transaction validation process. The simulation results show that PC-PBFT can support at least 30 transactions per second (tps) with transaction processing time less than 1 second on average.**

***Index Terms*—NG-EU, consortium blockchain, consensus protocol, financial stability.**

I. Introduction

A fund totalling Euro 750 billion was approved in July 2020 by the European Council under the Next Generation EU (NG-EU) plan in response to the Covid-19 crisis, comprising the Recovery and Resilience Fund (RRF) [1]. The objective of the NG-EU fund is to ensure a sustainable, resilient, and inclusive recovery for all member states [2]. The largest part of the NG-EU fund is offered to member states for investments and reforms in relation to the green and digital transitions, and to enhance the national economic resilience. On 10 December 2020, European Union leaders agreed on the long-term budget of the Next Generation EU recovery package. By April 2021, EU countries had presented their national plans for investment. A special task force established in August 2020, called RECOVER (Recovery and Resilience Task Force), coordinates and monitors the national plans, investments, and their progress operations [3].

The RECOVER activity, and in particular the allocation of fund mechanisms, is following well-established practices in large international organisations such as The World Bank and United Nations; nonetheless, these mechanisms may be exposed to possible failures and delays due for instance to a long decision tree process, lack of preparedness by local authorities, complex bureaucratic procedures, regional differences in pandemic effects, macroeconomic imbalances, and different national fiscal capacities [4]. Indeed, the NG-EU fund offers a decisive contribution to overcoming the economic depression-induced in the EU by the pandemic shock, but only if the management of NG-EU resource application and allocation is well-recognised and coordinated within the horizontal surveillance.

The Covid-19 crisis has not only accelerated the digitalisation of the economy, but it also highlights the chronic difficulties, in terms of time and complex procedures, in the supply of capital for example to the industrial sector, as well as to European citizens through the conventional financial service industry [5].

Against this background, blockchain technology has been recognised as a valuable tool to overcome some of the aforementioned limitations in the finance of the NG-EU, where an accountable and reliable system to facilitate and monitor the delivery of NG-EU fund is vital in order to achieve overall European economic goals [6]. The distributed ledger system is capable of recording and storing all transactions in a decentralised, secure, transparent, and immutable environment. The characteristics of blockchain technology have shown to be useful in core banking and financial markets and can potentially also be applied in the NG-EU fund delivery process [7]. As examined in the project STELLA by the Bank of Japan and ECB [8], through a comprehensive examination on different DLT platforms, the advantages of the DLT system include real-time implementation, accountability of the financial decision through the transparency inherent in the system, and security and resilience mechanisms that can shelter Euro stability and prevent possible failures. Furthermore, the consortium blockchain infrastructure ensures the coordination and autonomy of each member in the consortium.

Additionally, in the design of blockchain technology, it is possible to use a consensus mechanism within the network to enable an open-source and transparent community to support decision making and system running [9, 10, 11]. By designing and deploying a suitable consensus mechanism, a blockchain-enabled system could leverage the level of decentralisation and autonomy to enhance the fund delivery process.

Our objective is to define a mechanism to enhance the NG-EU fund delivery process; in so doing we propose an experimental regime of the DLT. Specifically, we test the implementation of the Recovery Resilience Fund (RRF) on a consortium blockchain we call "Next Generation Digital Currency" (NGDC). This is not a traditional central bank digital currency, but rather a pseudo-currency only for the implementation of the RRF. The contributions of the present work are as follows:

1) This paper proposes an NGDC system on a consortium blockchain that delivers and operationalizes, using a swift and accountable process, NG-EU funds across the EU.
2) A Prime-Coordinator (PBFT) consensus mechanism is proposed in the agreement protocol to reduce the communication cost for reaching consensus in the consortium network; this mechanism has proven to achieve increased scalability and throughput in the simulation results.
3) A test of the technology and solution that provides insights from political and economic points of view about which steps to take upon completion of the experimental phase.

The paper is organised as follows. Section II discusses the architecture of the two-layer NGDC system. In Section III, the details of the proposed agreement protocol and consortia chain process are described. Thereafter, the system simulation for the novel consensus protocol and performance evaluation are presented in Section IV, and conclusions round out the paper in Section V.

II. Architecture of NGDC

The NGDC system adopts a two-layer operation system to manage the funding allocation and management. Figure 1 depicts the proposed architecture of the NGDC system with various stakeholders, including ECB, national central banks, commercial banks, and funding projects/beneficiaries.

In layer 1 we observe that it is the consortium blockchain maintained by the ECB and EU national central banks which ensures that each EU member state has access and can monitor the allocation of NGEU resources. Each node in the layer 1 consortium network has an equal right to submit and verify transactions; this ensures autonomy within the NGDC system. The consortium network records the funding information provided by each central bank and updates the funding progress, where information flow in the P2P network is depicted as a solid line in Figure 1. By providing a transparent and auditable platform for each consortium member, it can accelerate the translation of a strategy into concrete projects and their swift implementation.

An interface is provided in layer 2 for the commercial banks to submit funding proposals, and each commercial bank is responsible for verifying and auditing funding proposals in accordance with NRRP guidelines. We observe that layer 2 is still a hierarchical structure in the transaction reporting process where blockchain is not necessary. The information flow is captured using dashed lines in this zone comprising various stakeholders in the fund application process. Besides commercial banks, each central bank is also capable of submitting national economic recovery plans to fulfil a systematic effort to define and deliver a strategic resource allocation. In this way, the existing financial infrastructure is also used to improve the efficiency and quality of the access to NG-EU resources. In order to meet the design features as described above, we first introduce the Project Account (PA) address, transaction format, and consortium chain data structure.

A. PA address

Every commercial bank should validate funding proposals from companies or institutions upon submission. After approval, a proposal initiated by a central bank i is assigned with a private key ($PrK(i)$) to uniquely identify the funding information. At the same time, PA's public key ($PuK_{usotx}(i)$) and address are generated according to the PA's $PrK(i)$. $ustox$ stands for unspent output transaction, which is a balance transaction that has remained in the PA. Each PA transaction history can be traced back with one or more $ustox$. Each commercial bank keeps a record of the public key of funding projects, and its corresponding central bank maintains its private key on the consortium blockchain. With $PuK_{usotx}(i)$, we can obtain the project transaction address using a series of encryption algorithms provided by the blockchain protocol, such as ECDSA [12]. Thereafter, the PA wallet address can be inferred from the transaction address. In this way, the consortium blockchain can produce the public/private key and wallet address using the PA identification number.

NGDC combines the wallet address with the account feature to manage all funding information. When submitting funding updates to the consortium blockchain, the value in the transaction is subtracted from the corresponding project ID and recorded by the PA wallet address. PA is used to preserve the project account balance, while the wallet address is used to lock the transaction value to ensure both the transparency of transactions and to prevent the double-spending attack, if only using UTXO protocol in Bitcoin blockchain [13].

B. Transaction format

Transactions (TX) are the building units of the consortium blockchain. We use a single-type transaction to record the project funding flow from the beginning of proposal submission until the end of the project. Each transaction is generated when the consortium network receives funding information, including funding proposal and progress updates (cash flow involved), related keys, parameters, and the unique identification number. The concrete structure of a transaction Tx is shown as below:

$$\begin{aligned} TX =& UI_i||St||num||\{PuK_{usotx}||PrK\}_i \\ & ||\{PuK_{new}||num_{usot}\}_j||Sig_i, \end{aligned} \tag{1}$$

where UI_i is the unique identification number of the transaction initiated by the central bank i, St is the status indicator represented as:

$$St = \begin{cases} 0, inactive \\ 1, active, \end{cases} \tag{2}$$

where $St = 1$ indicates the project is in progress and vice versa. num is the balance of the corresponding account address, and num_{usot} is the number of balance updates submitted to the consortium blockchain. $\{PuK_{usotx}||PrK\}$ is the ith unspent output transaction address and its corresponding private key. Note that any on-chain updates require the private key to access and modify. The mod result of $\{PuK_{new}||num_{usot}\}$ is the new address and the amount of fund moving in/out of the account address. The latest balance

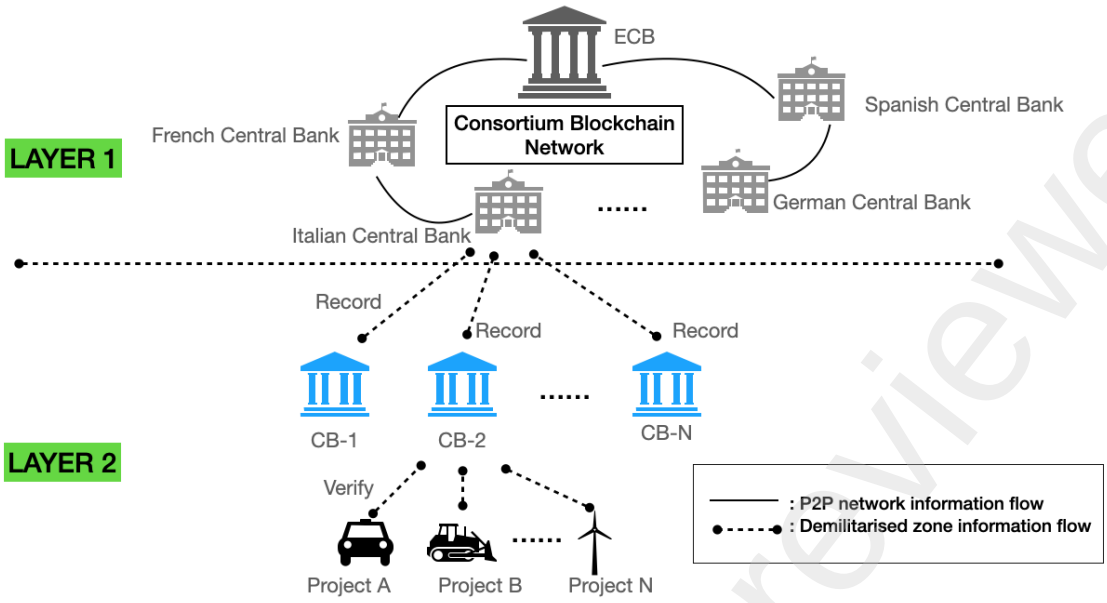

Fig. 1. NGDC system architecture.

of the account address will be $\sum num_j$. Sig_i is the signature of the initiator of TX, which should be its corresponding EU national central bank. Note that Equation (1) only lists key information fields in a transaction, where some standard data fields, such as timestamp, are omitted.

C. NGDC block data structure

Each NGDC block can generally be divided into two parts. The first part is the transactions collected from the consortium network, where each EU national central bank node is able to submit the funding information in the transaction format as defined above. Before TX is encapsulated, the transaction needs to be encrypted to prevent a breach of data. The second part of the block is the sequence number for each truncated transaction in the block. The transaction data can be retrieved with the Merkle tree data structure, where the sequence number could also reduce computation time for searching the neighbour information [14].

The proposed PA address, transaction format, and block structure together provide an innovative and secure platform for the consortium network, which supports a system to trace and retrieve transactions efficiently. In short, the design of NGDC architecture in the consortium blockchain enables a regulatable system for a national level digital currency to enhance the NG-EU resource allocation.

III. Agreement Protocol Description

The core of a blockchain-based system in the financial system, especially for a national level digital currency, is the ability to regulate and manage the decentralised system. Henceforth, the ability to achieve consistency among different consortium nodes is the most important factor in the system design. In a permissioned distributed system such as NGDC, all participant nodes are trusted entities who have been through the Know Your Customer (KYC) process, where we can assume that no node will send error messages in normal circumstances. So, the traditional PBFT algorithm will not be efficient in this way because the communication process will be at least $O(n^2)$. We next propose a simplified agreement protocol for the NGDC consortium network for layer 1 design in the NGDC system with some fair assumptions to solve the problem of Byzantine fault tolerance, which is to reach the consensus on the monetary flow on the funding project account PA.

A. Prime-Coordinator PBFT protocol

Considering the unique features of the NG-EU fund and participants of the consortium network in layer 1, we can make the following assumptions in order to propose the PrimeCoordinator PBFT (PC-PBFT) protocol:

1) All nodes comprised of ECB and 27 EU national central banks are compatible with system requirements, and each participating node will behave normally unless some nodes are being hacked by malicious attacks.
2) Each funding proposal for the NG-EU from its corresponding central bank has been checked against national and EU strategies, where the final approval of the resource allocation is carried out by the European Commission and other European institutions [4].

With the above reasonable assumptions, we can assign two identities for the node in the consensus process: prime nodes working as the coordinator, and general nodes. The PC-PBFT protocol contains one prime node that controls the consensus process and generates new blocks from the transaction pools. One complete consensus coordination process consists of four steps:

- Selecting a prime node among all NGDC nodes. The prime node p selection formula is p = Nonce mod $N(nodes)$, where Nonce is a random number generated from the previous block hash value; and $N(nodes)$ is the number of nodes (28) in the NGDC network. Note that Nonce will be the same for all participating nodes, as the previous block has been agreed by all peers; and each node has an equal chance for accessing and generating a block in the system.
- The prime node, which works as the coordinator, collects all transactions from each node. Also, all nodes will broadcast transactions that they receive from their neighbour nodes or the transaction pool.
- The coordinator checks whether all transactions from the network are consistent, where the main consistency check criteria is the project status recorded by each node. If there are some inconsistent transactions, the system will enter the transaction selection process. For those transactions where St is active, it requires the consensus process carried out by the prime node until it is confirmed by the network. The PC-PBFT transaction selection process is shown in Figure 2.

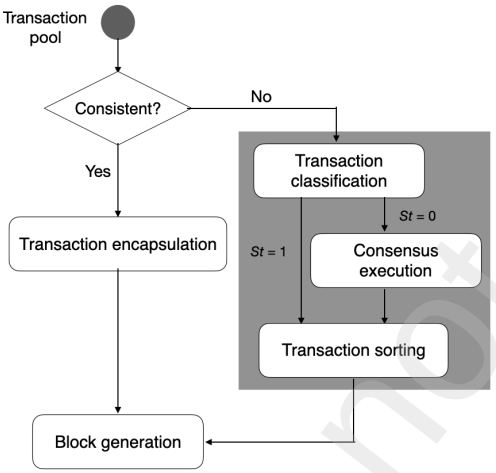

Fig. 2. Prime coordinator PBFT transaction selection process.

- The coordinator merges consistent and confirmed transactions, where the sorted transactions are then encapsulated into a block to be executed and confirmed by the whole network.

Instead of being confirmed by the public miners, NGDC transactions can be verified by consortium members using the prime-coordinator selection mechanism. By eliminating the mining process, it saves computation power and communication cost for generating a new block and also reserves transaction confidentiality. In this way, the system ensures local autonomy while reserving the right for the ECB and EU national central banks to roll back in emergency situations.

B. Consortium chain process

In the NGDC system, each node represented by the institution determines the control power over the system with the agreed control protocol in the consensus process. A regulatable NGDC model includes three main steps: system initialisation, PC-PBFT protocol consensus execution, and block generation

1) System initialisation: The first stage of the consortium chain process is to initialise the system with security parameter settings. With the input of the system security parameter λ_1 and the elliptic curve key generation parameter λ_2, each node can generate a key pair (PK_b, SK_b) for signing and verifying. And an encryption key SK_b can be obtained by the elliptic curve cryptographic algorithm to encrypt transactions [15]. The PrK should be kept secretly by each node. Meanwhile, the public key $PubK_b$ is broadcast to the network to generate the identity authentication signature Sig_i, which is then exchanged between nodes for checking the transaction authenticity. In this way, the message is encrypted in the network to prevent information leakage in the network channel. Transactions can then be sent to the network and be checked against the system agreement protocol.

2) PC-PBFT protocol consensus execution: PC-PBFT consensus execution is the core phase to coordinate the consistency of the system state. Once the prime node/coordinator receives transactions from the transaction pool, it will check if all transactions are consistent. If there is an inconsistent transaction found, all active transactions will be entered into the PC-PBFT consensus process to maintain network consistency according to Algorithm 1.

Algorithm 1 PC-PBFT consensus protocol

Inputs: TX_{ini} = $\{TX, \forall TX[St] = 1\}$
Outputs: $List_{agreed}(TX)$
Initialize: $List_{tx} \leftarrow \{TX_{ini}, \forall TX[St] = 1\}$,
$List_{tmp} \leftarrow \{\}$, $List_{agreed} \leftarrow \{\}$.

for $(i = 0, i < N(nodes), i++)$ ***do***
  for $(j = 0, j \leq N(TX_{ini} \in List_{tx}), j++)$ ***do***
    if $TX_{ini}[\{PuK_{usotx}||PrK\}_i] == Adr_{PC}$ &&
      $TX_{ini}[Sig_i] == Sig(hash_{Merkel})$ ***then***
      $List_{tmp} \leftarrow List_{tr}[j]$
    end if
  end for
end for
request $Node_{prime}$ to execute ($List_{tmp}\{\}$)
return $List_{agreed}\{\} \leftarrow List_{tmp}\{\}$

For each active transaction TX_{ini}, it is stacked into the $List_{tx}$ which stores all available transactions. In the consensus execution step, it enters the loop to check all transactions from all nodes $N(nodes)$, 28 in this case. First, it checks if the account address of the PA generated by $\{PuK_{usotx}||PrK\}_i$ points to prime coordinators' wallet address Adr_{PC}. Then it verifies the validity of the transaction by checking if the signature of the transaction is equal to the previous Merkel Tree hash value using the public key $PuKey_{usotx}$. All transactions that satisfy both requirements are then stacked in the temporary list $List_{tmp}$. The prime node is then requested to perform the PBFT-based consensus algorithm to communicate over the network for validation. Importantly, any PBFT-based consensus algorithm can be applied with an approximate

communication overhead of $O(n^2)$ [16]. Finally, a list of agreed transactions $List_{agreed}\{\}$ will be returned for block generation.

3) Block generation: The last step in the PC-PBFT protocol is to generate a new block to add to the previous block. The prime node encapsulates all transactions that are agreed by network peers into a block and append it to the longest chain of the NGDC. Then the prime node broadcasts the information to the consortium network and requests all nodes to append the new block into their previous block's hashes.

**Transaction tracing and retrieval:* : The system realises the supervision and regulation functionality by tracing and retrieving the node identity and transaction details. Similar to other blockchain systems, the results of transaction traceability do not affect the blockchain system. However, in the NGDC system, there might be malicious attacks, even with all trusted nodes. In PC-PBFT consensus protocol, we can add an additional secret sharing information $Share_i$ issued by the prime node to request a review process in an emergency situation; in this case, the consortium network is able to retrieve the transaction if needed.

IV. System analysis

In this section, we implement the prototype of our proposed PC-PBFT protocol to evaluate the costs for computation and communication. Specifically, this section is divided into three parts. First, the key parameters to design TX are illustrated to estimate the capacity of a block. In the second part, we measure the time consumption of processing TX. We present in part three the computational cost and communication overhead for transactions in the NGDC system.

In the evaluation, we use one conventional computer (with Intel i5-4200H processor running at 3.30GHz) as a client, and three small workstations (with Intel i7-8700 processors running at 4.20GHz) as three central bank nodes to build up the experimental platform. The prototype of PC-PBFT is tested using Hyperledger Fabric version 1.4 and Blockbench platform [17]. We have also considered Corda and Quorum to test the proposed consortium network; however, the conceptually designed protocol requirements are not well fitted in the aforementioned platforms due to SegWit, privacy control, etc. In addition, we use 256-bit ECDSA for signature, 128bit AES for symmetric encryption, and SHA-256 for hash operations to ensure our prototype can meet 128-bit security [18] in our experiments.

A. Capacity of block

Based on our proposed block structures Eq. (1) and Eq. (2), we need to regulate the length of the block header and body to determine the capacity of the block. In the block header, the lengths of Prehash, Index and Merkle root are all set as 256 bits. Meanwhile, the lengths of Time (GMT) and Nonce are defined as 32 bits. Whereas, in the block body, the lengths of Hash, ID and Signature are set as 256 bits since we use SHA256 and 256-bit ECDSA in our experiments. The length setting of the key parameters in the block is summarised in Table I.

Regarding the design Eq. (1) of TX, the length of a transaction TX is 357 Bytes. Because the block size, which means the number of transactions involved in a block, can affect the transaction latency, we evaluate the average transaction latency (over 100 transactions for each block size) under different block size with TX length 357 Bytes in Blockbench. The results shown in Figure 3 imply that setting block size as 50 can reach the lowest latency for our TX length. Therefore, a block length is 17.43 Kbytes.

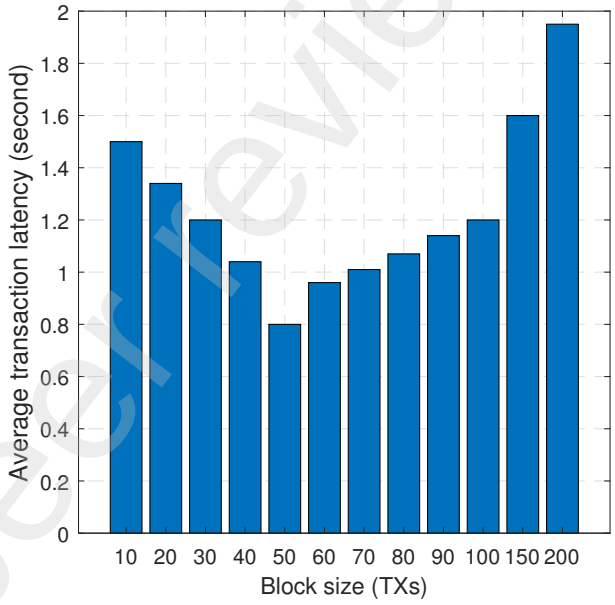

Fig. 3. The average transaction latency under different block size.

To determine a suitable time interval for block generation, the failure probability of PC-PBFT is evaluated in Blockbench in terms of transaction throughput, i.e., tps. In the experiment, the tps varies from 20 to 200, with step 20 to obtain the results shown in Figure 4. When tps is less than 60, the failure probability is less than 10% that can be tolerated. Here, the tps cap of the PC-PBFT protocol is recommended at 30 to balance the tps and failure probability.

TABLE I
The length (bits) of the parameters in each block

	Parameter	Size
Header	Prehash	256
	Index	256
	Root	256
	Time	32
Body	UI	256
	St	1
	num	256
	PuK	256
	PrK	256
	Sign	256
	Hash	256

B. Processing time of transactions

To measure the processing time of transactions, we consider the time consumption of local computation in central bank

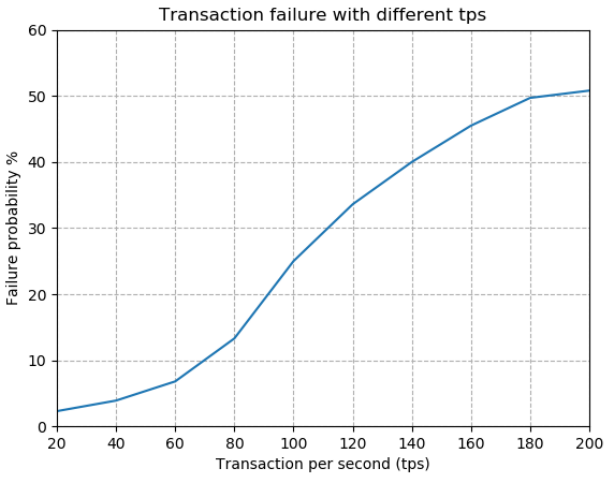

Fig. 4. The failure probability of PC-PBFT in terms of transaction per second.

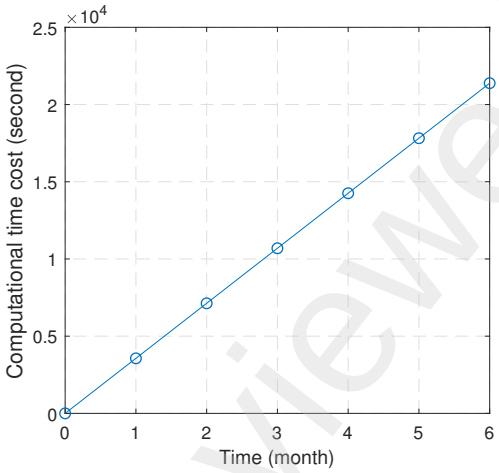

Fig. 5. The computational time cost for generating transactions (TX) with using PC-PBFT protocol.

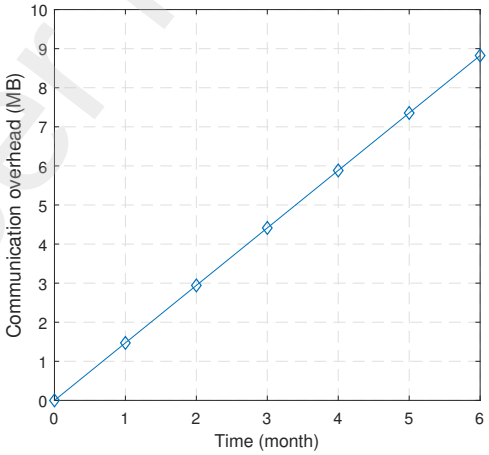

Fig. 6. The communication overhead for transmitting transactions (TX) between the client and central bank nodes.

nodes and communications between the client and central bank nodes. Results are shown in Table. II. Note that all the time results are the average of observing 1,000 transactions in the experiment. The average total time consumption of processing a TX is 0.83 second, and it is clear that the computation of executing PC-PBFT protocol requires half of the total time cost to process a transaction.

TABLE II
THE AVERAGE TIME COST OF PROCESSING A TRANSACTION.

Operation	Time cost (ms)
Receive TX	165
Check TX	5
PC-PBFT computation	466
Insert into database	28
Send feedback	161
Total	825

C. Computational cost and communication overhead

Next, we demonstrate the computational cost and the communication overhead for the blocks generated by PC-PBFT protocol in the NGDC system. Since project funding management does not require frequent transactions when compared with people who make payments more frequently in real life, we assume that a TX is generated every 10 minutes. Our estimated results are shown in Figure 5 and Figure 6.

It is clear that both the computational cost and the communication overhead present the linear trend of increase as the usage time of NGDC grows. As depicted in Figure 5, the time cost for computing transactions is 21,384 seconds when the running time reaches six months. Meanwhile, the communication overhead shown in Figure 6 for transmitting transactions between the client and central bank nodes is 8.82MB when the running time reaches six months.

V. CONCLUSIONS AND FUTURE RESEARCH

In this paper, we have proposed an NGDC system based on consortium blockchain to assist the implementation of NG-EU fund. The novel consensus mechanism PC-PBFT can support NG-EU funding management to handle project funding transactions of at least 30 tps with transaction processing time less than 1 second on average.

We propose that the pilot regime, and thus only a part of the NG-EU fund, will be allocated through this DLT mechanism. This regime will allow us to better understand the political impacts and consequences of the introduction of Euro central bank digital currency (CBDC). In particular, it will be possible to test if such a DLT system will foster a more inclusive recovery, sustainable growth, and acceptability for and by the European citizens. Achieving such an objective is necessary in order to provide greater education and understanding of digital finance across the EU.

In future research, the NGDC system could act as a blueprint for extending the digital Euro beyond the specific NextGeneration Facility, and thus to launch a CBDC such as the digital Euro. A more flexible simulation platform for testing the robustness and functionalities would also be essential for simulating the efficiency and safety of CBDC.

REFERENCES

[1] C. Alcidi and D. Gros, "Next generation eu: A large common response to the covid-19 crisis," *Intereconomics*, vol. 55, no. 4, pp. 202–203, 2020.

[2] C. Fuest, "The ngeu economic recovery fund," in *CESifo Forum*, vol. 22, no. 01. ifo Institute-Leibniz Institute for Economic Research at the University of Munich, 2021, pp. 03–08.

[3] C. de la Porte and M. D. Jensen, "The next generation eu: An analysis of the dimensions of conflict behind the deal," *Social Policy & Administration*, 2021.

[4] M. Buti and M. Messori, "Next generation–eu: An interpretative guide," 2020.

[5] N. R. Moşteanu, A. Faccia, and L. P. L. Cavaliere, "Disaster management, digitalization and financial resources: key factors to keep the organization ongoing," in *Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing*, 2020, pp. 118–122.

[6] J. R. Varma, "Blockchain in finance," *Vikalpa*, vol. 44, no. 1, pp. 1–11, 2019.

[7] J. Chod, N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber, "On the financing benefits of supply chain transparency and blockchain adoption," *Management Science*, vol. 66, no. 10, pp. 4378–4396, 2020.

[8] M. Casey, J. Crane, G. Gensler, S. Johnson, and N. Narula, "The impact of blockchain technology on finance: A catalyst for change," 2018.

[9] M. Kishi, "Project stella and the impacts of fintech on financial infrastructures in japan," 2019.

[10] P. Csóka and P. Jean-Jacques Herings, "Decentralized clearing in financial networks," *Management Science*, vol. 64, no. 10, pp. 4681–4699, 2018.

[11] I. Roşu and F. Saleh, "Evolution of shares in a proof-of-stake cryptocurrency," *Management Science*, vol. 67, no. 2, pp. 661–672, 2021.

[12] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[13] C. Pérez-Solà, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Double-spending prevention for bitcoin zero-confirmation transactions," *International Journal of Information Security*, vol. 18, no. 4, pp. 451–463, 2019.

[14] Y. Jiang and S. Ding, "A high performance consensus algorithm for consortium blockchain," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*. IEEE, 2018, pp. 2379–2386.

[15] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, and T.-Y. Ni, "A multi-dimensional adversary analysis of rsa and ecc in blockchain encryption," in *Future of Information and Communication Conference*. Springer, 2019, pp. 988–1003.

[16] Y. Li, Z. Wang, J. Fan, Y. Zheng, Y. Luo, C. Deng, and J. Ding, "An extensible consensus algorithm based on pbft," in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE, 2019, pp. 17–23.

[17] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, pp. 1085–1100.

[18] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management part 1: General (revision 3)," *NIST special publication*, vol. 800, no. 57, pp. 1–147, 2012.