Central Bank Digital Currency Cross-Border Payment Model Based on Blockchain Technology

Mao Hanyu

Abstract Since the turn of the twenty-first century, the growth of the globalized economy and trade has accelerated, and the cross-border payment system, which is an essential component of the international financial infrastructure, has played a significant role in the global economy and trade. However, traditional cross-border payments present risks and challenges, such as expensive processing fees, limited payment efficiency, information asymmetry in the trade process, and reliance on a highly centralized cross-border payment system. This chapter is based on consortium blockchain technology and utilizes Polkadot's Parachain, Relay chain, and cross-chain technologies as references; a scalable, high-efficiency, high-security, and privacy-protecting central bank digital currency cross-border payment model is designed. Analyzed the usage of hash digest technology and CoinJoin technology to avoid the tracing of transactions in order to protect privacy. The issuance of multi-country central bank digital currency or stablecoin anchored to a basket of fiat currencies is discussed as the currency in circulation in the model. Finally, the central bank digital currency cross-border payment development trend is summarized and forecasted.

Keywords Payment model · Cross-border · Blockchain technology · CBDC

1 Introduction

Since 2020, the global digital transformation has been developing rapidly, and the era of central bank digital currency (CBDC) is accelerating, with China's digital currency—e-CNY leading the world. The launch of the e-CNY not only promotes the healthy development of China's digital economy but also benefits the RMB internationalization plan and speeds up the pace of RMB internationalization. At the same time, CBDC has especially significant advantages in cross-border payments,

M. Hanyu (✉)
School of Mathematics, Renmin University of China, Beijing, China
e-mail: 2020103607@ruc.edu.cn

Z. Zheng (ed.), *Proceedings of the Second International Forum on Financial Mathematics and Financial Technology*, Financial Mathematics and Fintech,
https://doi.org/10.1007/978-981-99-2366-3_10

which can effectively solve the problems of extended time, high cost, low efficiency, and low transparency faced by current cross-border payments. In addition, building a cross-border payment network system based on CBDC will also be a pivotal key to unlocking the opportunity to break the monopoly position of the US dollar and reshape the global cross-border payment system. Therefore, CBDC cross-border payments will inject new vitality into the rapid growth of our economy and will also play a pivotal role in establishing a fair and equitable international monetary settlement system.

With the rapid development of CBDC, CBDC cross-border payments are becoming a research hotspot in the central bank's digital currency research area. According to a survey by BIS, more than 50% of central banks consider cross-border payments as one of the crucial reasons for accelerating the development of CBDC. Traditional cross-border payments suffer from high fees, low efficiency, information asymmetry in the cross-border trade process, and the potential financial risk of a highly centralized cross-border payment system. The CBDC cross-border payment system, with the characteristics of high payment efficiency, low cost, and high transparency, is not only conducive to solving the current existence of cross-border trade friction and breaking the centralized cross-border payment system, but also conducive to eliminating the use of competitive currency devaluation, currency war, and other vicious behaviors between countries, promoting the peaceful development of financial markets, and laying a moderately centralized cross-border payment system with a healthy market foundation for international trade (Yang, 2020). Therefore, a large number of central banks and international organizations have started to try to explore the application of CBDC in cross-border payments. On February 26, 2022, the United States, together with the European Union, the United Kingdom, and Canada, issued a joint statement announcing that Russia is banned from using the Society for Worldwide Interbank Financial Telecommunications (SWIFT) international settlement system. It undoubtedly accelerated the research of countries investigating the idea of bypassing SWIFT for cross-border transactions.

Currently, the research on cross-border payment of central bank digital currency is still in the initial stage. There is a lack of in-depth research for a scalable and high-efficiency cross-border payment model, which leads to a lack of necessary theoretical research and essential technical support for its development. Therefore, it is significant to design a scalable, high-efficiency, CBDC cross-border payment model based on blockchain.

CBDC cross-border payments issued by central banks have become a significant trend. In this chapter, we use Polkadot's Parachain, Relay Chain, and cross-chain technologies as references for the CBDC cross-border payment model, and we commit to designing a scalable, high-efficiency, highly secure, and privacy-preserving CBDC cross-border payment model based on consortium chain.

2 CBDC Cross-Border Payment Development Current Situation

CBDC cross-border payments can be made in two ways: first, retail central bank digital currencies (CBDCs) in a given jurisdiction are available to people both inside and outside the jurisdiction, with no coordination between central banks; and second, central banks work together to establish access and settlement arrangements between different retail or wholesale CBDCs (Wan & Wu, 2022). CBDC cross-border payments can be divided into four quadrants: "same system and same currency", "same system and different currency", "same currency and different currency", "same currency and different system", and "different currency and different system". Among them, "same system and different currency" and "different currency and different system" are the most typical scenarios for cross-border payments and will be a key research focus in the future.

At this stage, for CBDC cross-border payments research, the following three models are used to achieve cross-border and cross-currency interoperability, enhancing compatibility of CBDCs systems; linking multiple CBDC systems; integrating multiple CBDCs in a single multi-CBDC (mCBDC) system (Auer et al., 2021). Models linking multiple CBDC systems include the Stella project of the European Central Bank and the Bank of Japan (2019); and the Jasper-Ubin project of the Bank of Canada (BOC) and the Monetary Authority of Singapore (MAS) (2019). Jura project for cross-border payment between Banque de France and Swiss National Bank. Integrating multiple CBDCs in a single mCBDC system mainly contains the Aber project of the UAE and the Central Bank of Saudi Arabia (2020); Dunbar, a joint project of the Monetary Authority of Singapore and the BIS (2022); and the Inthanon-LionRock project of the Bank of Thailand and the Hong Kong Monetary Authority (2020). In 2021, with the addition of the Digital Currency Institute of the People's Bank of China and the United Arab Emirates Bank, the project evolved into its third phase. It was renamed the mCBDC Bridge (mBridge) Project (Inthanon-LionRock to mBridge-Building a multi CBDC platform for international payments, 2021).

Recently, the CBDC projects Jasper, Ubin, and Stella have completed their experiments. All these projects continue the line "from wholesale payments to voucher payments to cross-border payments" (Yao, 2021). Thus, enabling cross-border payments is the ultimate goal and an essential part of the CBDC research route. Moreover, the experimental results of these representative wholesale CBDC projects show that current technology and design solutions can support Real-Time Gross Settlement (RTGS) in terms of efficiency and can also realize Liquidity Saving Mechanism (LSM) in terms of functionality (Huang, 2022). Also, these projects show that cross-chain technology is a crucial issue for CBDC cross-border payments. Although CBDC cross-border payments have become a research hotspot both at home and abroad, most existing research scholars focus on the two fields of economics and law for CBDC cross-border payments, and the proposed CBDC cross-border payment model has not been sufficiently investigated on a technical level.

At the technical level, most research by central banks or international organizations has focused on linking multiple CBDC systems and integrating multiple CBDCs in a single mCBDC system. However, most projects are still at the experimental stage with the participation of only a few countries and lack a certain degree of scalability in practice. At the same time, the cross-chain technology used to link multiple CBDC systems, hash time-locked contract (HTLC), is limited in its application scenarios, where the two sides of a transaction need to establish N^2 magnitude of transaction channels between them, and the number of transaction channels grows in power as N increases. Therefore, the scalability of hash time-locked contract (HTLC) is deficient and may not be suitable for application to large-scale economies. While integrating multiple CBDCs in a single mCBDC system can avoid complex hash time-lock contract (HTLC) and improve payment efficiency, the establishment of privacy groups inevitably introduces multi-ledger-style behaviors and constraints that hinder the realization of transaction atomicity. Therefore, research on cross-chain technology and the introduction of effective privacy protection mechanisms to achieve transaction atomicity and improve transaction efficiency while ensuring transaction privacy are the focus of future research.

3 Polkadot Technology Overview

Polkadot is a scalable heterogeneous multi-chain technology that provides a more general cross-chain protocol. Any blockchain system compatible with Polkadot's cross-chain protocol will be able to complete cross-chain interconnection (Polkadot, 2016). Polkadot is envisioned as a new form of blockchain "blockchain network" and one of the critical infrastructures of the future web 3.0. As shown in Fig. 1, Polkadot is completed with Parachain, relay chain, and bridge. It uses various Parachain technologies to satisfy the needs of different applications. It uses Relay chain technology to unify the management of consensus security and data interaction, which can solve the scalability and isolability problems of current blockchain technology.

3.1 Relay Chain and Parachain Technology

The Parachain is a member blockchain of Polkadot that collects and processes transactions and transmits them to a Relay chain. Each participating Parachain has a high degree of autonomy and flexibility. Each Parachain can be designed and focused on a specific scenario as long as it follows the protocols set by Polkadot. The Relay chain is the core of the Polkadot network, responsible for maintaining the whole network's security, coordinating consensus among different Parachains, and forwarding cross-chain transactions between each Parachain. The consensus mechanism of the Relay chain uses an asynchronous Byzantine fault-tolerant algorithm to reach consensus.

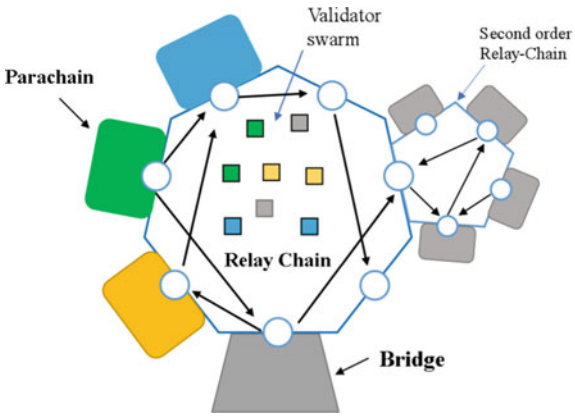

Fig. 1 Polkadot architecture schematic

In order to maintain the relay chain, the Polkadot network establishes four roles: Nominator, Validator, Collator, and Fisherman. Nominators are a group of token (DOT) holders who have the authority to vote for the Validator. Validator nodes have the highest authority in the network, having the ability to create blocks for the whole network. They are elected by Nominator vote and can validate blocks and pack blocks after a sufficient deposit (TOKEN) is mortgaged in the system. If the validators perform their duties, they are rewarded for generating blocks. If the validators don't perform their duties, they are punished by having some or all of their deposit deducted. The collators are a group of nodes that collect information from the Parachain and package it for submission to the validators. They submit candidate blocks to the validators and assist them in creating valid blocks, which are rewarded with a fee. Collators will go and collect as much information as possible in order to get more fees. Fisherman is a relatively independent node in the system. It is only responsible for monitoring the system's illegal activities and reporting their detection. Then it will receive a substantial one-time reward. Moreover, a deposit is required to become a Fisherman, mainly used to prevent Sybil Attack by witches that waste the verifier's computing time and resources.

3.2 Polkadot Cross-Chain Technology

Cross-chain communication is the most critical part of Polkadot, as shown in Fig. 2. Because of the relay chain's security guarantee for the whole system, transactions conducted on one Parachain can be transferred to another Parachain through the relay chain. As a result, cross-chain transactions on Polkadot are simpler and more efficient than other cross-chain methods. Specifically, each Parachain maintains an egress and an ingress transaction queue. The queue uses Merkle trees to ensure data authenticity. When a Parachain (A) initiates a cross-chain transaction to another Parachain (B), the transaction is pushed to Parachain A's egress queue. Then the

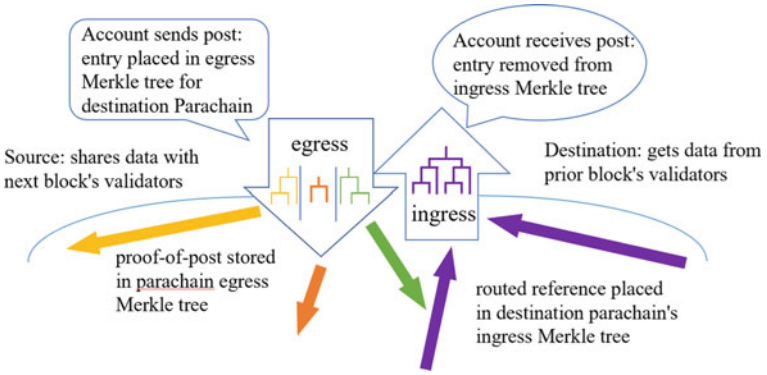

Fig. 2 Schematic diagram of cross-chain transactions on Polkadot This figure from Polkadot White Paper Polkadot (2016)

relay chain transfers the transactions in Parachain A's egress queue to Parachain B's ingress queue, which then processes the transactions in its ingress queue itself (Yuan & Wang, 2019).

4 CBDC Cross-Border Payment Model

This section will introduce a CBDC cross-border payment model based on consortium blockchain technology, referencing Polkadot's Parachain, Relay Chain, and cross-chain technologies. Figure 3 depicts a scalable, high-efficiency, high-security, and privacy-protecting CBDC cross-border payment model.

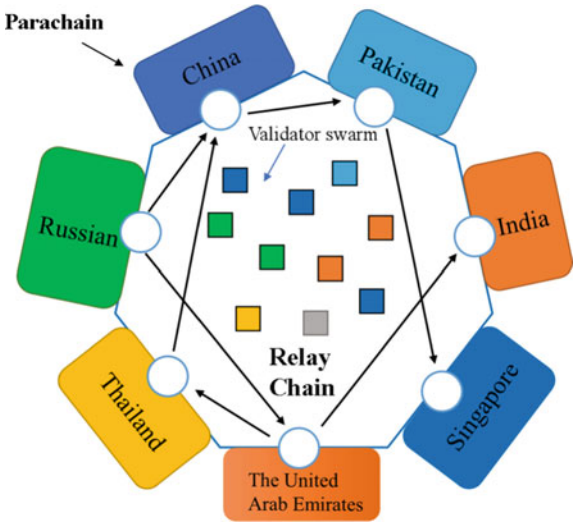

Fig. 3 CBDC cross-border payments model schematic

4.1 Design of Parachain

Every country is a Parachain in this model, and each Parachain is a consortium blockchain. The consortium blockchain is a permissioned blockchain, meaning only the internal designation of several nodes can upload, record, and read data. These nodes act as bookkeeper nodes, and they collectively decide to generate blocks. Using consortium blockchain can significantly improve the blockchain's operational efficiency and reduce network latency, all while ensuring the privacy of each transaction's data. Therefore, Parachain in each country can be adopted in the form of consortium blockchains, which can achieve the purpose of improving efficiency and protecting privacy.

Since Parachain has a high degree of autonomy and flexibility, each country's Parachain can be designed independently according to its own country's conditions. Therefore, the consensus mechanism of each country's Parachain can be chosen according to the country's reality, such as the mainstream consensus mechanisms applied to the consortium blockchain: Raft, PBFT, etc. The Parachain of each country can be divided into several nodes with different authorities according to the actual situation of cross-border payment in the country, including the central bank, trusted financial payment institutions, and regulatory agencies. As a result, three roles are established in the network of this model: Validators, Collators, and Supervisors.

The work of Collators is to collect information on the Parachain, submit candidate blocks to the Validators, and assist the group of validators in creating valid blocks. They also have the authority to vote for the Validators. Consequently, the Collators can be commercial banks and trusted financial payment institutions in every country. Validators are the nodes with the authority to generate blocks and have the highest authority in the system. The Validators nodes are elected by vote of the Collators and are responsible for validating the blocks and packaging them. Each country's central bank or specialized agency can fill this critical role. Supervisors are the nodes that need to be responsible for regulating illegal activities in the system. Thus, it can be held by the regulator of each country.

Taking China as an example, the nodes of Collators can be served by six state-owned commercial banks, including Industrial and Commercial Bank of China (ICBC), Agricultural Bank of China (ABC), Bank of China(BOC), China Construction Bank (CCB), Bank of Communications (BCM), and Postal Savings Bank of China (PSBC), and trusted commercial banks and third-party payment institutions can be added in the future. Validators are the central bank of China, the People's Bank of China, and its affiliated institutions. Supervisors are mainly served by the Ministry of Commerce, the China Banking and Insurance Regulatory Commission, the National Audit Office, and other regulatory authorities.

4.2 Design of Relay chain

In this model, the Relay chain is the same as the consortium blockchain, which contains the protocols of all Parachains, can recognize the transaction format of each country's Parachain, and can be responsible for coordinating consensus and forwarding cross-chain transactions between different Parachains. The Validator nodes, which the Collators vote on in each country, are also added to the relay chain and are responsible for packaging transactions and generating blocks.

Specifically, the Collators in each country's Parachain first elect the Validators in charge of their Parachain, and the Validators are added to the Relay chain. After that, the Collators on each country's Parachain will collect the transactions into the blocks with a Noninteractive Zero-Knowledge Proof, which is used to prove that the father block of this child block is valid, and hand them over to the Validators in charge of their country's Parachain. The Validators from each country involved in this cross-border transaction form a team of Validators to validate the blocks in the order in which the Collators send them and then consensus out the Parachain blocks for that height. When the Validators of each country's Parachain involved in cross-border payments confirm that their country's Parachain has confirmed the transaction, the Validators group then routes the message to the Relay chain and generates the Relay chain blocks. In the next round, the Collators in each country's Parachain vote again to elect new validators and round this cycle.

4.3 Cross-Chain Transaction

The cross-chain transactions of the model are approximately the same as those of Polkadot. Each country's Parachain contains an egress transaction queue and an ingress transaction queue (there can be multiple exports and ingresses if the transaction volume is large). The Relay chain transfers transactions from the egress transaction queue at the source Parachain to the ingress transaction queue at the destination Parachain.

The egress transaction queue contains a list of grids with routing information, each with a concatenated structure of exit submissions. Merkle tree proofs can be provided between verifiers of Parachains so that blocks of one Parachain can be proven to correspond to the egress transaction queue of another Parachain, guaranteeing data authenticity. If the ingress transaction queue of a Parachain exceeds the block processing threshold, it is marked as complete on the relay chain, and no new messages are received until the queue is emptied. The Merkle tree is used to prove that the collector's operations in the Parachain blocks are trustworthy.

For example, the flow of a cross-border transaction between China and Russia is as follows. When a Chinese Parachain launches a cross-chain transaction to a Russian Parachain, this transaction will first be pushed to the Chinese Parachain's egress transaction queue. Then the Relay chain will transfer this transaction from

the Chinese egress transaction queue to the Russian ingress transaction queue. Then the Russian Parachain will process the transaction in the ingress queue. This design can effectively guarantee the security of cross-chain transactions and significantly improve the efficiency of cross-chain transactions.

4.4 Privacy Protection

In Parachain, the blockchain ledger takes advantage of the irreversible nature of the hash algorithm and uses hash digests instead of transaction-sensitive information. At the same time, CoinJoin technology is used to obfuscate transactions and sever the relationship between the input and output addresses of transactions so that the origin and destination of transactions cannot be traced for privacy protection.

In Relay chain, if other countries are not involved, the block can be generated by only the countries involved in cross-border transactions confirming the transactions. The relevant detailed information does not need to be authenticated by the nodes of other countries, which can prevent other countries from knowing the details of the transactions and can effectively protect the privacy of cross-border transaction information for each country.

5 CBDC Cross-Border Payment Model Architecture

The whole cross-border model is divided into four layers, as shown in Fig. 4. They are application layer, architecture layer, blockchain layer, and digital currency issuance layer.

Application layer: This layer mainly faces users and can provide user identity authentication services, system access services, etc. The authentication technology verifies the user's identity through the authentication center to ensure the validity of the trader's identity. Users can access the system if they pass authentication.

Architecture layer: This layer is composed of Parachain, which is designed by each country, and Relay chain, which is responsible for forwarding cross-chain transactions, as shown in Fig. 3. Parachain and Relay chain are consortium blockchains that are ideal for practical applications. Three trusted roles are established in the network of the model: Validators, Collators, and Supervisors, to help the whole system work more effectively.

Blockchain layer: This layer consists of the core technical aspects of blockchain, such as Peer-to-Peer networks, Smart Contracts, Time stamps, and Consensus mechanisms. Distributed ledger technology resolves the problem of storing, transferring, and querying transaction information in cross-border payments. The consensus mechanism solves the agreement between validators on transactions and ledgers (Zhu, 2021). Resolving the problem of double payment through Digital signature and Time Stamp, Smart Contract technology can realize automatic accounting rec-

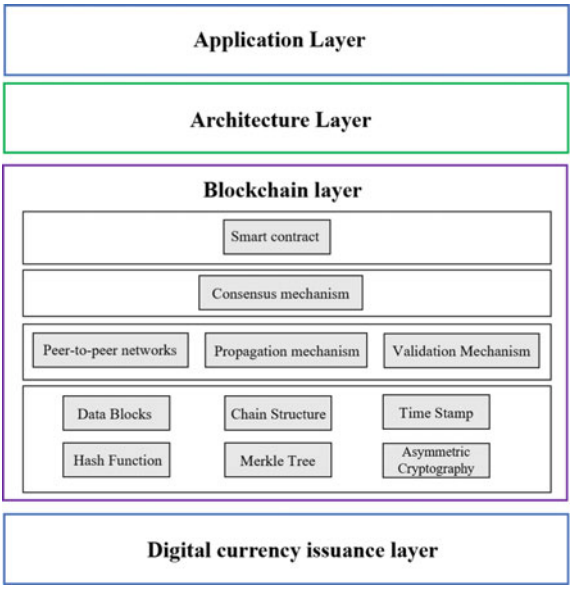

Fig. 4 CBDC cross-border payment model architecture diagram

onciliation and error handling in cross-border payments, ensuring that transactions are trusted and reliable. The smart contract automatically identifies and executes the actual conditions and matches the situations that arise to the relevant processing rules. This way, all information is recorded between the parties synchronously and cannot be tampered with by either party. It can also effectively prevent the loss of information due to technical failures (Huang & Luo, 2021).

Digital currency issuance layer: It mainly corresponds to the issuance and redemption of the digital currency used in this model, as well as the management and maintenance of this digital currency. Since the essence of building a cross-border payment system based on CBDC is to establish a regional economic association, regional economic cooperation is a prerequisite for CBDC to be recognized in cross-border payments. Therefore, a multi-country CBDC anchored to a basket of legal currencies is considered to be issued as the circulating currency in the model; or a stable currency anchored to a basket of legal currencies is issued as the circulating currency. This digital currency should only be used for cross-border payment clearing between Parachains of individual countries. It cannot be freely exchanged or used outside this cross-border payment model between financial institutions on the parallel circulation chain. The intrinsic value and purchasing power of this digital currency can be determined by each party's central basket of traded goods based on historical transaction volumes (or other forms). In this way, it can bypass the US dollar settlement and circumvent the constraints of countries' foreign exchange reserves anchored by the US dollar without challenging the monetary sovereignty of national central banks (Huang & Luo, 2021).

6 Summary and Prospect

This chapter utilizes Polkadot's Parachain, Relay chain, and cross-chain technologies as references and is based on consortium blockchain technology; a scalable, high-efficiency, high-security, and privacy-protecting CBDC cross-border payment model is designed. The purpose of privacy protection is investigated by using hash digest technology and CoinJoin technology to obfuscate the input address and output address of transactions. The construction of a free-floating legal digital currency system bypassing U.S. dollar settlement is discussed so that multi-country CBDCs anchored to a basket of legal currencies can be issued, or stablecoins anchored to a basket of legal currencies can be issued as the circulating currencies in the model in order to contribute to the study of CBDC cross-border payments.

With the increasing perfection of CBDC cross-border payment technology and the more mature development of cross-chain technology, the future is expected to form a regional-centric polycentric pattern. A new pattern of economic development in which "different currencies in the same system" are used within a region and "different currencies in different systems" are used between areas in the future. Nowadays, CBDC cross-border payment has become an international research hotspot. Although some countries are already experimenting with CBDC cross-border payment, the security and scalability of its cross-chain still need time to be proven. Follow-up research can focus on the following two levels: Technically, the focus and difficulty of CBDC cross-border payments lie in cross-chain technology, so the research of more secure and efficient cross-chain technology is a hotspot for future research. At the same time, the research of new consensus algorithms that can be applied to blockchain cross-chain will also greatly improve the efficiency of CBDC cross-border payments. In terms of regulation, it is necessary to strengthen the supervision of CBDC cross-border payments; it is not only essential to identify the regulatory authority of CBDC cross-border payment but also to improve the legal study of CBDC cross-border payment. In addition, we can also learn from the regulatory sandbox model and introduce a new model of the "Chinese regulatory sandbox" to balance risk and innovation.

References

Auer, R., Haene, P., & Holden, H. (2021). Multi-CBDC arrangements and the future of cross-border payments.

Bank of Canada & Monetary Authority of Singapore. (2019). Jasper-Ubin design chapter-enabling cross-border high value transfer using distributed ledger technologies.

Bank of Thailand, Hong Kong Monetary Authority. (2020). Inthanon-LionRock Cleveraging distributed ledger technology to increase efficiency in cross border payments.

BIS. (2022). CPMI, innovation hub, project Dunbar, international settlements using multi-CBDCs.

European Central Bank & the Bank of Japan. (2019). Project Stella-Sync-Hronised cross-border payments.

Huang, G. P. (2022). Cross-border payments of digital currency. *The Chinese Banker, 2022*(4) (in Chinese).
Huang, H. T., & Luo, C. (2021). Constructing the cross-border trade trust mechanism supported by blockchain: A prospective analysis on the trade between China and the Five Central Asian States. *Nankai Journal (Philosophy, Literature and Social Science Edition),2021*(02), 98–110 (in Chinese).
Inthanon-LionRock to mBridge-Building a multi CBDC platform for international payments. (2021).
Polkadot, W. G. (2016). Vision for a heterogeneous multi-chain framework: Draft 1.
Qian, Y. (2021). Some insights and reflections on global central bank digital currency experiments. *Tsinghua Financial Review, 2021*(03), 16–19 (in Chinese).
Saudi Central Bank & Central Bank of The U.A.E. (2020). Project Aber: Saudi Central Bank and Central Bank of The U.A.E. Joint Digital Currency and Distributed Ledger Project. Saudi Central Bank and Central Bank of The U.A.E.
Wan, J. R., & Wu, Y. (2022). Research on the cross-border payment of central bank digital currency. *New Finance, 2022*(01), 58–64 (in Chinese).
Yang, D. (2020). Develop cross-border payment vigorously to enhance international competitiveness. *Economy, 2020*(06), 112–113 (in Chinese).
Yuan, Y., & Wang, F. Y. (2019). Blockchain theory and method (Vol. 2019, p. 97). Tsinghua University Press.
Zhu, L. X. (2021). Challenges and prospects of blockchain for cross-border payment and clearing industry. *Finance Theory and Teaching, 2021*(06), 4–10+17 (in Chinese).