Bank of Israel
June 2022

Digital Shekel

The Bank of Israel Steering Committee on a Potential Issuance of a Digital Shekel

Experiment on a Distributed Platform

Bank of Israel - The Bank of Israel Steering Committee on the Potential of a Digital Shekel Issuance

June 2022

The experiments described in this paper are part of the work of the digital shekel project's technology team.

Participants in the experiemnt work:

Eyal Zafrani, Tomer Mizrahi, Nawras Dahleh, Avia Hollander, Ilan Matityahoo, Daniel Skorikov, and Gil Polak – Bank of Israel Information Technology Department

Paper written by: Eyal Zafrani, Tomer Mizrahi – Bank of Israel Information Technology Department, Yoav Soffer – Digital Shekel Project Manager

Table of Contents

04

Background

07

Structure of the System

10

Connecting end-customers to the system and executing a payment

13

Potential smart contract applications in the digital shekel system

18

Limited privacy in digital payments

22

Conclusion

24

References

1. Background

The Bank of Israel's Steering Committee on the Potential Issuance of a Digital Shekel is building an action plan so that if future conditions indicate that, in the Bank of Israel's estimation, the benefits of issuing a digital shekel outweigh the potential costs and risks, the Bank of Israel will be prepared to put such a plan into action. As part of the project, the Bank of Israel is studying technological alternatives, and the opportunities and risks that may be inherent in the various technologies for implementing a digital shekel system. This studying is being done through both theoretical analysis and practical experiments that examine various technologies.

Many central banks around the world are conducting a variety of technological experiments of varying scopes — some under laboratory conditions only (sometimes referred to as Proof of Concept—PoC) and some using "real" money and "real" participants, such as financial entities, businesses, and consumers (these experiments are sometimes referred to as Pilots). However, no advanced country has yet decided to issue a central bank digital currency (CBDC), or has even decided on what technology such a currency would be based, which makes the study of technological alternatives more challenging. Research through experiments makes it possible to tackel technological issues while also examining business aspects and policy issues.

This document outlines the first technological experiment conducted by the Bank of Israel as part of the digital shekel project's work plan. The experiment was conducted under laboratory conditions (PoC), and included the establishment of distributed ledger technology (DLT) on the cloud in a test environment, over which a system based on Ethereum was put in place. It should be emphasized that the choice of this

environment for the experiment does not indicate any intention on the part of the Bank of Israel to issue a digital shekel – if the Bank will decide to do that - using a DLT environment in general or Ethereum technology in particular. Furthermore, it does not indicate that this technology is preferable to others. Experiments conducted by other central banks examined this technology[1] alongside other distributed technologies[2], and also examined non-distributed technologies.[3] The Bank of Israel chose to conduct this experiment in this technological environment in order to enable its teams to experiment with distributed technologies in general and with Ethereum technologies in particular, since this technology is an open code platform that enables the development of a variety of applications. Examining some of these applications can support an analysis of the digital shekel's ability to realize some of the potential motivations that were described in the report published by the Steering Committee (2021). The intention is that the platform that was established for the experiment will serve as a rolling master template, over which it will be possible to further examine various technological issues while changing the format as needed.

The first stage of the experiment included the establishment of the platform and an examination of the ability to make basic transactions over it, such as issuing a digital shekel and transferring it from one wallet to another (making a payment). In addition, it examined the ability to impose quantitative restrictions on payment transactions, and to make use of "smart contracts" in order to execute delivery vs. payment. This ability may be one of the elements of the digital shekel's potential to create an innovative infrastructure that will ensure the adaptation of the payments system to the needs of a future digital economy — one of the motivations outlined by the Steering Committee.

[1] See, for instance, Bank of Thailand (2021); Reserve Bank of Australia (2021)
[2] For instance, Sveriges Riksbank (2022); Federal Reserve Bank of Boston (2022)
[3] For instance, Bank of Japan (2022)

Another motivation listed by the Steering Committee is maintaining the public's ability to use digital payments with some level of privacy, provided that the rules set out by the State authorities concerning the prohibition of money laundering and terrorism financing (AML/CFT), as well as the required disclosure to the tax authorities, are maintained. In this context, the second stage of the experiment examined an innovative technology by developed by researchers at VMware[4], which makes it possible for policy makers to define a periodic benchmark of digital payments that can be made anonymously.

The Bank of Israel is continuing to study the possibilities inherent in innovative technologies that have been developed in recent years, and the possible applicability of these technologies in realizing the motivations for a potential issuance of a digital shekel. The Bank will update the public from time to time regarding its findings.

[4] Tomescu, et al. (2022)

2. Structure of the system

In order to conduct the experiment, we established a DLT infrastructure on the Microsoft Azure cloud using Azure Blockchain Services, which enables the realization of an Ethereum-based Quorum blockchain. According to the draft model published by the Steering Committee, the digital shekel experiment system was developed in a two-tier model (Figure 1). While the digital shekel constitutes a central bank liability toward holders of the currency, the public does not directly approach the bank to receive, redeem, or pay digital shekels. The public's access is enabled through "payment service provider" — which may be banks, other financial institutions (such as credit card companies in Israel), fintech firms, and more. The experiment environment included the establishment of a private network, in which four nodes were set up on the blockchain, simulating a situation in which the digital shekel includes three payment service providers in addition to the central bank. Each payment service provider is created in a separate node, and the network is fully distributed. The Bank of Israel is the network administrator and defines the payment service providers as validators. In addition, the Bank of Israel is the party realizing the smart contract that defines the digital currency, and is the party solely authorized to mint or burn coins. The payment service providers provide end customers with digital wallet infrastructure and service, through which the customers access the digital shekel network, and are the ones that transfer payment orders between end customers. It should be emphasized that the providers do not hold the end-customers digital shekels. They only provide customers with technological access to the blockchain network, and transfer payment orders on their behalf.

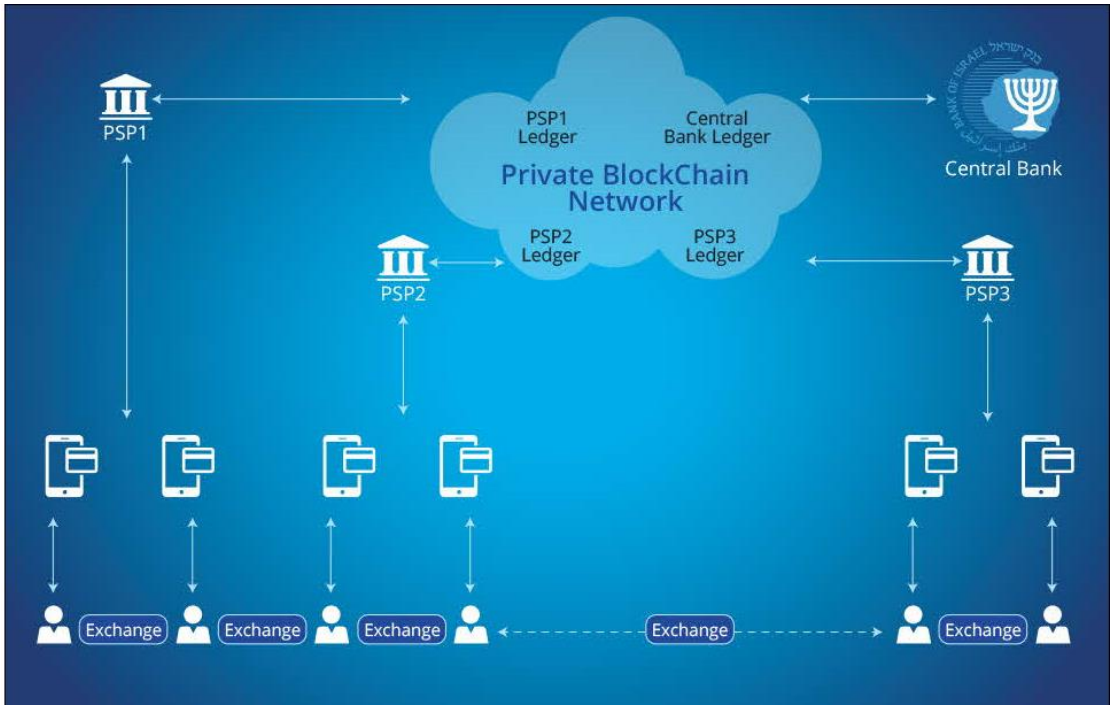
The transaction approval mechanism (consensus mechanism) selected for the experiment was Proof of Authority (PoA). On completely distributed blockchain networks that can be accessed by any user (permissionless blockchain), there is no trust between the network's participants, and the networks are based on consensus mechanisms such as Proof of Work (PoW) — an expensive and complex mechanism that consumes large quantities of energy. In the CBDC system, trust is based on the central bank's reputation, and the fact that the bank is the party that decides who can serve as a validator essentially devolves the trust on the central bank to those validators, while maintaining the distributed nature of the system (and te energy consumption is significantly lower – similar to that of standard payment systems).

There were thirty "end customers" in the experiment. In practice, these were Bank of Israel employees who are members of the digital shekel work teams, who simulated customers in the experiment, and who were randomly distributed among the three payment service providers. The following three parameters were created for all participants in the network (Bank of Israel, payment service providers, and end users):

i. Public address on the blockchain network (Address):
ii. Private Key
iii. Central Digital Identity

The payment service providers hold the Private Key and the KYC data of the end customers.

Figure 1: System structure in a two-tier model

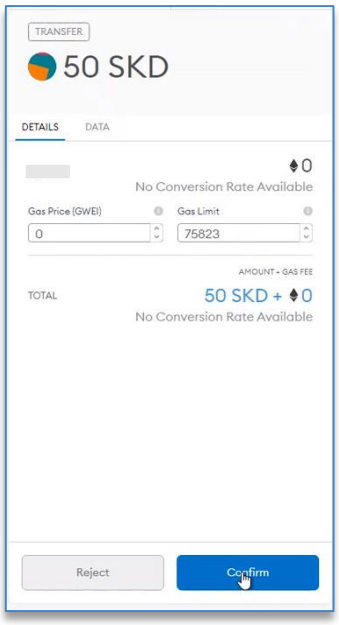


Following the establishment of the system, the Bank of Israel "issued" the "digital shekels" using the ERC20 standard. The standard includes currency issuance and payment operations by end users or payment service providers.

The use of the ERC20 standard on a standard Ethereum Quorom blockchain basically makes it possible to hold digital shekels issued in the experiment in any standard wallet available. In order to examine the system's compatibility with the standard, a MetaMask wallet[5] was connected, simulating a situation in which the end customers hold the private key in their digital wallet. The wallet identified the token representing the digital shekels in the experiment, and it was possible to make a transfer of digital shekels from one customer to another (Figure 2).

[5] Any wallet that supports the ERC20 standard could have been used.

Figure 2: Access to the blockchain network and initial transfer of digital shekels using a standard wallet



3. Connecting end-customers to the system and executing a payment

Part of the rationale for implementing a two-tier model for a central bank digital currency is based on the business sector's relative advantage over the central bank when it comes to conducting the "know your customer" (KYC) process required by the AML/CFT rules. As part of the experiment, we conducted a simple simulation of a situation in which there is a national identity system from which payment service providers can access information regarding customers' identity.[6] Following identification by the payment service provider, the customer is connected to the

[6] Since the customers in the experiment were Bank of Israel employees, they were identified using the Bank of Israel's organizational identification system.

system and obtains a blockchain address that is attached to his identity, and to which other users are permitted to transfer digital money. For simplicity, The experiment did not examine how the customer "obtained" the digital shekel — meaning the transfer of money from the bank account or cash to the digital shekel wallet was not simulated. Instead, at the start of the experiment, end customers received an initial balance of digital shekels issued by the Bank of Israel, so that they could experiment with making payments.

In order to make a payment to another customer, the customer chooses the address to which the payment should be sent, and the amount he wishes to transfer (Figure 3). The payment service provider identifies the customer and accesses his address and his private key. The provider connects to the blockchain and transfers the receiver's address and the amount of the transfer to the network. The order is received in the blockchain, and the transfer function is executed from the smart contract in the ERC20 standard. This action verifies that the payer's address has a sufficient balance, and if that is the case, the amount is transferred to the receiving address. The consensus mechanism verifies that the new status is synchronized in the ledger at all the other nodes.

Figure 3: Display of the customer's wallet to the payment service provider. The wallet shows the balance and the transfer request by the amount and the receiver's name

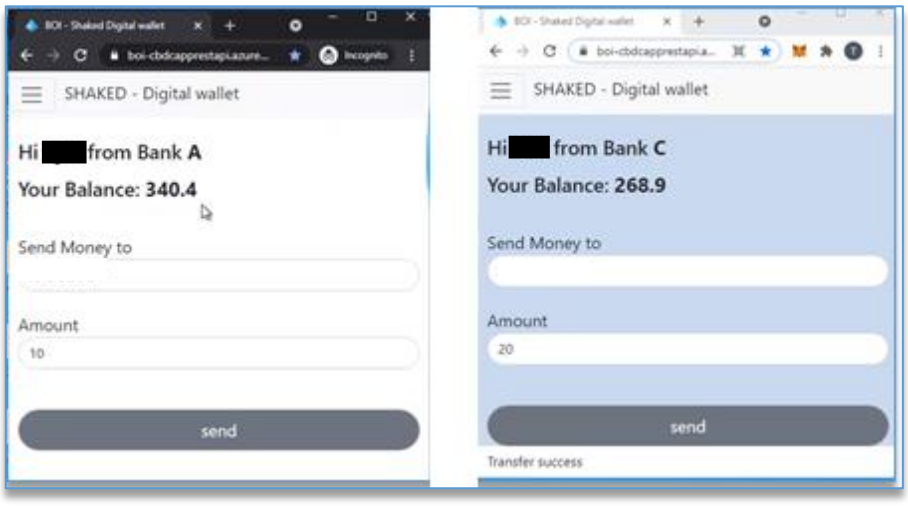


Figure 4: Description of the transactions fed into the system

Transfer From	Transfer To	Amount
0xcad739f1d9db299464f8685b4bd6d6d6b8835c148	0xebb4c6e6abb89ddec9c28265d02e89784342984	10
0xcad739f1d9db299464f8685b4bd6d6d6b8835c148	0xe2aa67e6127f7d94cf7765f6417e301a098c4b	50
0xe2aa67e6127f7d94cf7765f6417e301a098c4b	0xcad739f1d9db299464f8685b4bd6d6d6b8835c148	2000

One of the risks inherent in implementing a CBDC is the risk of bank disintermediation — a situation in which customers withdraw a large portion of their bank accounts and convert the money to digital shekels. In this context, different countries are examining the need to restrict the use of CBDC in order to prevent a sharp impact to the banking system.[7] The experiment examined the ability to restrict the amount of an individual transfer and of the overall number of transfers in a single day, by writing the restrictions into the smart contract.[8] A customer attempting to transfer an amount greater than the defined amount or to make a number of transfers that exceeds the daily limit, received an error message. It should be emphasized that this was not an examination of the business feasibility or of the economic impact of such restrictions, but only of the ability to implement such restrictions using the standard token.

[7] The central bank digital currency in the Bahamas—the sand dollar—has two levels of wallet. The higher level allows the user to hold up to 8,000 dollars, and has a payment limit of 10,000 dollars, and the wallet is linked to the customer's bank account such that any amount beyond the balance will automatically be transferred to the bank account. In Europe, the ECB noted a limit of 3,000 euros as a potential ceiling beyond which it would not be possible to hold digital euros.

[8] For the purpose of moderating the impact on the banking system it would have been more appropriate to limit the balance that can be held in the wallet and not the individual transfer. However, this would require connecting the wallet to a bank account which could absorb any excess balance. It was not possible to test that in this experiment.

4. Potential smart contract applications in the digital shekel system

One of the motivations that the Steering Committee outlined for a potential issuance of a digital shekel is the creation of a payment infrastructure that would support the adoption of innovation and the adaptation of the payment system to the needs of a digital economy. The development of distributed ledger technologies (DLT) and the concept of digital tokenization of money led to new ideas for development of advanced payment applications based on the use of smart contracts. For instance, a digital currency can support the use of "delivery versus payment" (DvP) use-cases, which would simplify many payment processes and provide security and certainty to both parties of a payment transaction. According to the draft model that the Steering Committee published, the Bank of Israel should provide the infrastructure to support payment service providers' ability to offer advanced payment applications.

The manner in which the digital shekel is technologically realized in the experiment, as a token on a DLT platform that supports smart contracts, basically enables any party connected to the blockchain — in our case, the payment service providers — to write programs that will set rules on how to transfer money using a smart contract that uses a token naturally, without that party needing to write a dedicated program on its core systems (exposure of dedicated API).

As a test case, the experiment examined a situation in which a vehicle is sold[9] in exchange for digital shekels. In the current reality, ownership is transferred from the seller to the buyer at the Licensing Authority (for instance at a post office counter), and the money is transferred from the purchaser to the seller (for instance through a transfer in the RTGS system), while the two actions are not synchronized with each other, and the first party to take action is exposed to the risk that the other party will not complete his part of the transaction. The experiment executed a process in which the car's ownership was transferred simultaneously with the transfer of the payment. For that purpose, a nonfungible token (NFT) was issued with the ERC 721 standard, showing the sold vehicle, and a smart contract was written that activates three basic actions:

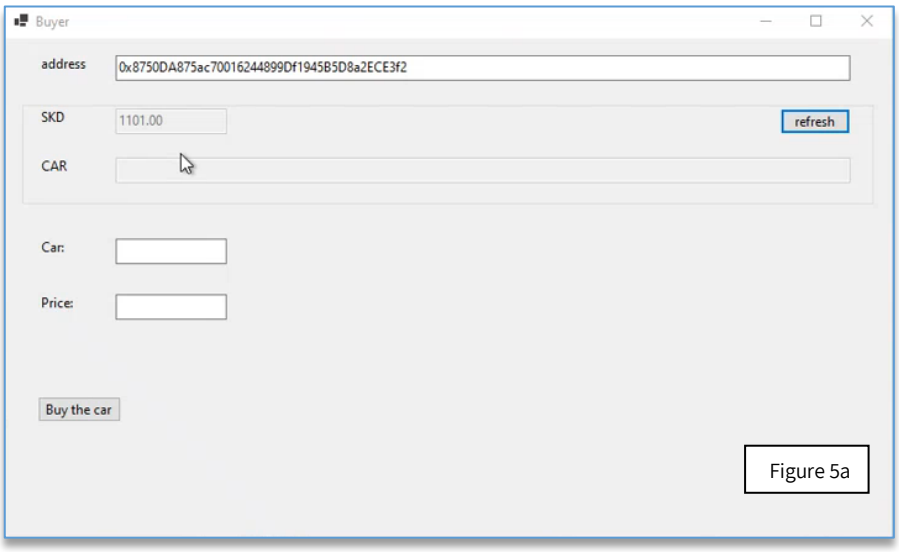
1. Offering the vehicle for sale: The seller, who owns the NFT showing ownership of the vehicle, offers the vehicle for sale in exchange for some amount. The NFT moves from the seller's wallet to the smart contract's wallet.
2. Purchase of the vehicle: The buyer, who holds digital shekels, agrees to purchase the vehicle for the amount proposed by the seller.
3. Cancellation: The seller cancels the sale if the conditions for upholding the transaction are not met (for instance, the buyer offers a lower amount than demanded by the seller), and the NFT showing the vehicle's ownership leaves the smart wallet, returning the situation to the beginning.

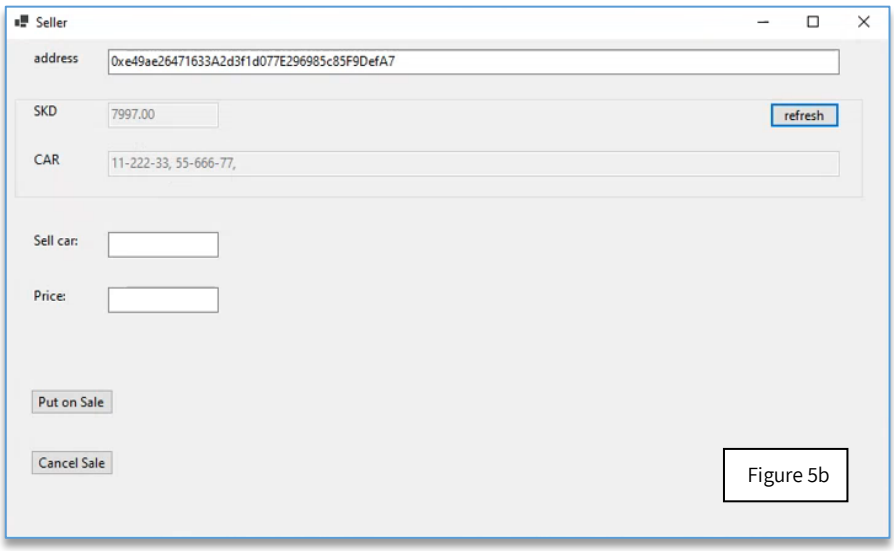
If the buyer enters the amount demanded by the seller in the smart contract, the transaction is completed. The digital shekels are transferred from the smart contract to the seller, and the NFT showing the vehicle's ownership is transferred from the smart contract to the buyer. In the experiment, two simple applications were written for interaction with the smart contract — one for the seller and one for the buyer.

[9] The example of selling a car is easy to understand and well-known to most readers. The example is relevant for any asset that can have a digital representation, from a real estate deed to a ticket to a show or movie.

Figure 5 shows the status as seen by the buyer (figute 5a) and the seller (figure 5b) before the transaction is made. There are 1,101 digital shekels in the buyer's wallet, and 7,997 digital shekels in the seller's wallet. It also shows that the seller owns two vehicles, which are shown by their license numbers.

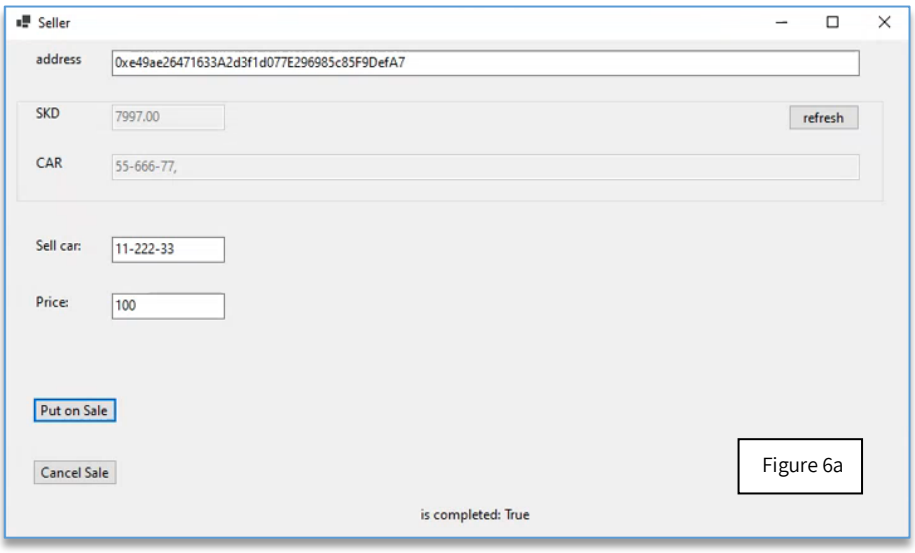
Figure 5: The situation before the DvP transaction is made:





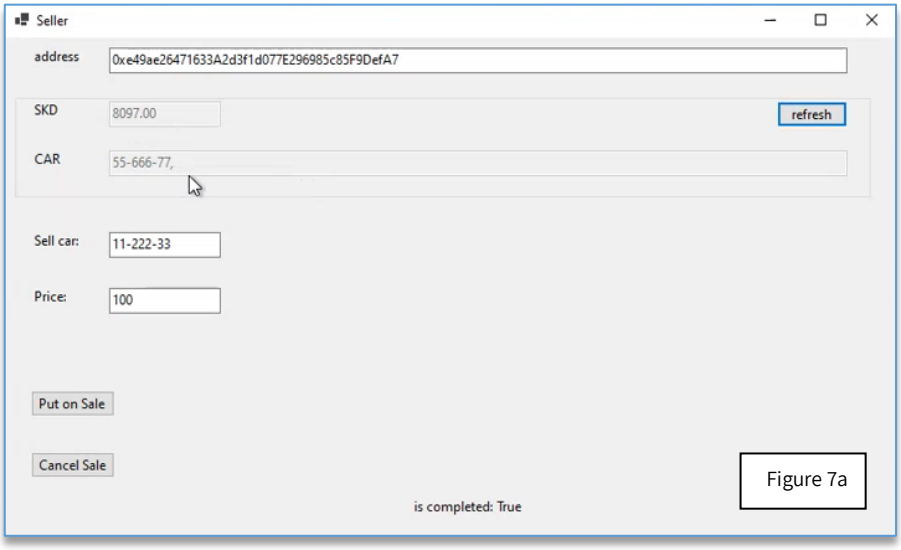
The seller offers one of the vehicles for sale in exchange for 100 shekels. Figure 6 shows that the NFT that represents the vehicle is temporarily deducted from the seller's balance of digital assets and moves to the smart contract.

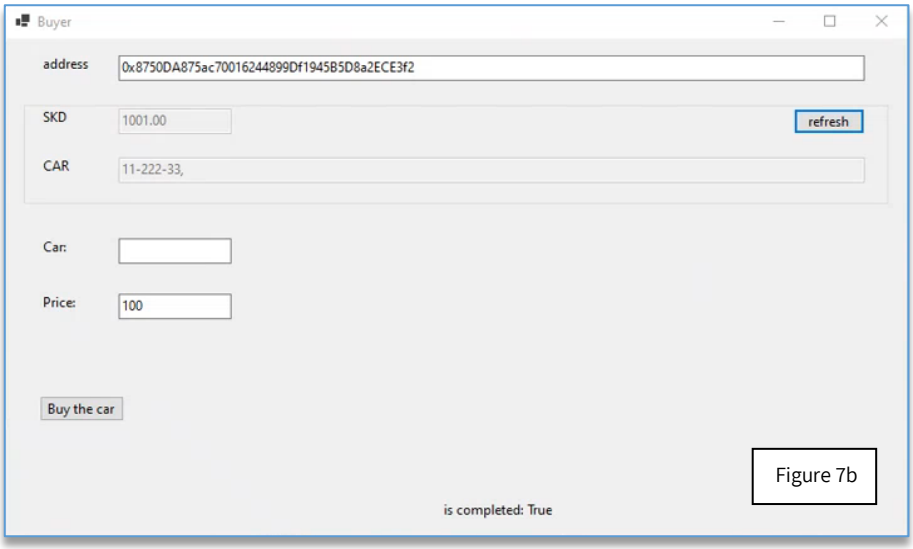
Figure 6: Ownership of the digital asset offered for sale through a smart contract



After the buyer offers the amount demanded by the seller into the smart contract, the transaction is made immediately. Figure 7a shows that seller's balance of digital shekels increased by 100 shekels (figure , and the vehicle is deleted from his ownership, while the buyer's balance of digital shekels declined by 100 shekels (figure 7b), and the ownership of the vehicle is not shown in his digital wallet.

Figure 7: The situation at the end of the DvP transaction





If the smart contract was written by a trustworthy entity and functions correctly, no side will be exposed to risk during the period between the transfer of ownership and the completion of payment, since both actions are interdependent, and if one is not completed, the other is cancelled. An important question in this context is who writes the smart contract. In the experiment, the contract was basically written by

the network's administration — the Bank of Israel. In the digital shekel system, it is not likely that the Bank of Israel would write applications for specific payments. However, it is difficult to assume that the Bank would enable just any party to write a smart contract on the blockchain itself, since it may pose a significant risk to the entire system as a result of bugs in the smart contract's code, if the code is written improperly in a way that would overload the system, or if a malicious coder writes an untrustworthy smart contract that leads to customers' loss of money. One possible solution is for the payment service providers to be authorized to write smart contracts, but then there is a question of the extent to which supervision would be required on the type of contract, reliability of the contract's code, and so forth[10].

5. Limited privacy in digital payments

5.1 Background

In the current payments system, there are two contrary situations regarding the maintenance of privacy when making a payment. Cash is completely anonymous. A cash payment contains no information regarding the identity of the payer, the amount of the payment, the date and location of the payment, or the identity of the receiver. In contrast, when a payment is made using any digital means of payment — payment card, bank transfer, payment app, and so forth — the financial entities operating the means of payment gain full information regarding all these details. Each of these options has advantages and disadvantages. Individuals have a basic

[10] Researchers at the Bank of Canada discussed the advantages and risks of how to use smart contracts in a CBDC system (Usher et al., 2021). The Bank of England analyzed the various options regarding how to implement smart contracts and programmed money in CBDC: at the network core, as a separate module, or as a function that will be provided by the payment service provider (Bank of England, 2020).

right to privacy, and as long as the payment and the transaction are legal, there is no reason to encroach on this privacy. However, the complete anonymity involved in cash payments has broad policy implications, since it enables tax avoidance, money laundering, and terrorism financing. The information held by the financial entities has value from the standpoint of the consumer, in that it enables the financial entities to tailor various value offers to the consumer, assess his ability to repay credit and offer credit accordingly, and so forth. However, the information may also be exploited to the consumer's disadvantage.

Either way, the consumer is faced with two contrary options, and in practice, the ability to pay while maintaining privacy exists only when making a physical payment. Remote payments, which are becoming more common as the economy becomes more digital, can only be made using means of payment operated by the financial entities, which gather the information contained in each payment.

Maintaining the public's ability to use digital means of payment with some level of privacy is one of the motivations identified by the Steering Committee on the Potential Issuance of a Digital Shekel. There is broad discussion around the world regarding the potential of a CBDC to enable payments with some degree of privacy. For instance, at a public consultation held by the European Central Bank regarding the potential issuance of a digital euro, privacy was identified as the most important characteristic of a digital euro in the view of the respondents (ECB, 2021).

The second stage of the technological experiment conducted by the Bank of Israel examined a model which was recently published by researchers from VMware that enables payment with limited privacy using a digital shekel. The idea behind the model is that each wallet can hold "ordinary" digital shekels, the transfer of which is recorded in the ledger as outlined in Figure 4, and "private" digital shekels, the transfer details of which are not recorded openly, and where both sides to the transaction enjoy complete privacy as with cash payments. The policy maker can set

out a periodic "budget" for payment using private shekels. For instance, it can be determined that from each wallet it will be possible to pay up to 1000 shekels per month privately, and beyond that each payment transaction will be recorded in the ledger.

5.2 Description of the model

For the purpose of the second stage in the experiment, a VMware blockchain infrastructure was set up in an AWS cloud that supports zero knowledge proof technologies for limited privacy. Here too, the system was built using a two-tier model, with a Byzantine Agreement system based on VMware Blockchain and a VMware Decentralized Cash Infrastructure payment engine. Four nodes were established to manage the central bank's blockchain in a distributed format, and three payment service providers were set up to communicate directly with the central bank's blockchain and intermediate between users' wallets and the bank's blockchain. The digital wallets provided by the payment service providers to the end customers include "ordinary" digital shekels, "private" digital shekels, and a private budget.

The transaction approval mechanism (the consensus mechanism) in the experiment is a Permissioned Byzantine Agreement[11] that enables the network to deal with the "Byzantine" behavior of one of the nodes — a failure of the node (electricity, faulty disc, or other kinds of usual failures), or a malicious take-over of the node that results in the node trying to write errors to the blockchain. In general, the number of intersections, n, must be in line with the formula: n=3f+1, where f is the number of intersection failures (or their Byzantine behavior) that the system can absorb. For instance, a blockchain system with 10 intersections can be protected from an enemy attack on three of them. The system ensures liveness, safety, and security as long as

[11] Gueta, et al. 2019

the enemy takes control of no more than f intersections. The limited privacy mechanism in the experiment was based on an expansion of eCash[12] technology while using zero knowledge proof tools in order to ensure the limitation of privacy in a way that maintains full privacy for payments within the periodic privacy budget[13] .

The experiment simulated ten end customers. After establishing the system, the Bank of Israel "issued" ordinary digital shekels, private digital shekels, and a privacy budget.

In order to test the system, the following actions were examined:

1. Privacy-protected payments using private digital shekels from the privacy budget, which maintain full privacy and are not openly recorded on the blockchain.
2. Payment using ordinary digital shekels that are recorded openly on the blockchain.
3. Conversion from ordinary digital shekels to private digital shekels and back (Such an action does not change the size of the privacy budget. It does, for instance, enable conversion of private shekels to ordinary shekels if the periodic privacy budget is exhausted).
4. The resilience of the system when one of the blockchain's nodes fails and loses all of the information. The system continues to operate as usual, and when the node returns it is synchronized with the other parts of the system so that it returns in full.
5. The resilience of the system when a payment service provider failes and loses all of the information. When an alternative payment service provider comes online, it restores all the wallets (including the distribution between private and ordinary digital shekels and the periodic privacy budget).

[12] Chaum, 1983.
[13] Tomescu, et al. 2022

Conclusion

The experiment described in this document is the first technological experiment carried out by the Bank of Israel's work teams as part of the digital shekel project. Many central banks are examining the use of distributed technologies as a potential platform for the issuance of a CBDC, despite the fact that such a currency, by its very nature, will be issued by a central authority. Certain aspects of distributed technology in general, and of the blockchain technology in particular, may pose an advantage in the issuance of a CBDC, and some of those were examined in the experiment conducted by the Bank of Israel. The selection of this technology for the experiment should not be construed as a statement that the technology is appropriate for a future issuance of a digital shekel, should a decision be made to issue one. The experiment also touched on two of the motivations identified by the Steering Committee for the Potential Issuance of a Digital Shekel — creating an innovative infrastructure that will ensure the adaptation of the payments system to the needs of a future digital economy, and providing the public with the ability to use digital means of payment while maintaining some level of privacy.

In the first stage of the experiment, an experimental infrastructure was established on an Ethereum blockchain. The use of this technology on a cloud platform and the application of a standard token enabled a relatively simple experiment with technology without needing to set up dedicated serves or write code from a basic level. In addition, the technology enabled an examination of the ability to use smart contracts and create an infrastructure for DvP transactions where, in addition to the token that represents the money, a nonfungible token represents ownership of an asset that changes hands in exchange for money.

Despite the fact that the use of standard technology made the digital shekel accessible to "customers" through a standard wallet, the experiment simulated a

dedicated wallet developed by programmers using a two-tier model, while providing a solution in an experimental environment for conducting a KYC process relaying on a central identity database. This simulation brought into sharper focus the need to create a convenient and efficient infrastructure for identification so that intermediaries will be able to make digital shekel services accessible to customers while meeting the requirements of the law.

The second stage of the experiment examined the ability to enable digital shekel payments while maintaining limited privacy in accordance with the rules that policy makers will set. The attempt to create a solution for this issue in the experimental environment showed that it is difficult to use encryption keys in a distributed architecture, and that it is therefore necessary to work with other mechanisms involving zero knowledge proof technologies. An examination of an innovative development of this technology showed that it is possible to implement a policy whereby a periodic budget of "private" digital shekels can be allocated to each customer on the digital shekel network, which the customer can use to pay without any documentation of the payment being kept. The experiment and the discussions held following it brought into sharper focus the fact that despite proof of the technological feasibility, there are many policy questions that still need to be examined and discussed. For instance, what is the "correct" private budget, and is it proper to allocate the same amount to each type of wallet (private, business, and so forth), could this create economic incentives for the misuse of "private" shekels, and so forth.

The Bank of Israel can use the infrastructure that was set up for the experiment in order to examine other applications and policy issues in the future as necessary. The Bank of Israel will continue examining various technological issues involved in the potential issuance of a digital shekel.

References

1. Bank of England, (2020): Central Bank Digital Currency: Opportunities, Challenges and Design
2. Bank of Israel, (2021). "A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine"
3. Bank of Japan, (2022): Central Bank Digital Currency - Results and Findings from "Proof of Concept Phase 1"
4. Bank of Thailand, (2021): Central Bank digital Currency: The Future of Payments for Corporates
5. Chaum, D. (1983): eCash, Blind Signatures for Untraceable Payments
6. ECB, (2021): Results of the Public Consultation on the Digital Euro
7. Federal Reserve Bank of Boston, (2022): Project Hamilton Phase 1
8. Gueta, G, et al. (2019): SBFT: a Scalable and Decentralized Trust Infrastructure
9. Sveriges Riksbank, (2022): E-krona pilot, phase 2
10. Tomescu, A, et al. (2022): UTT: Decentralized Ecash with Accountable Privacy
11. Usher, A., E. Reshidi, F. Rivadenyera, and S. Hendry. (2021): The positive case for a CBDC. Bank of Canada Staff Discussion Paper, 2021-11.