



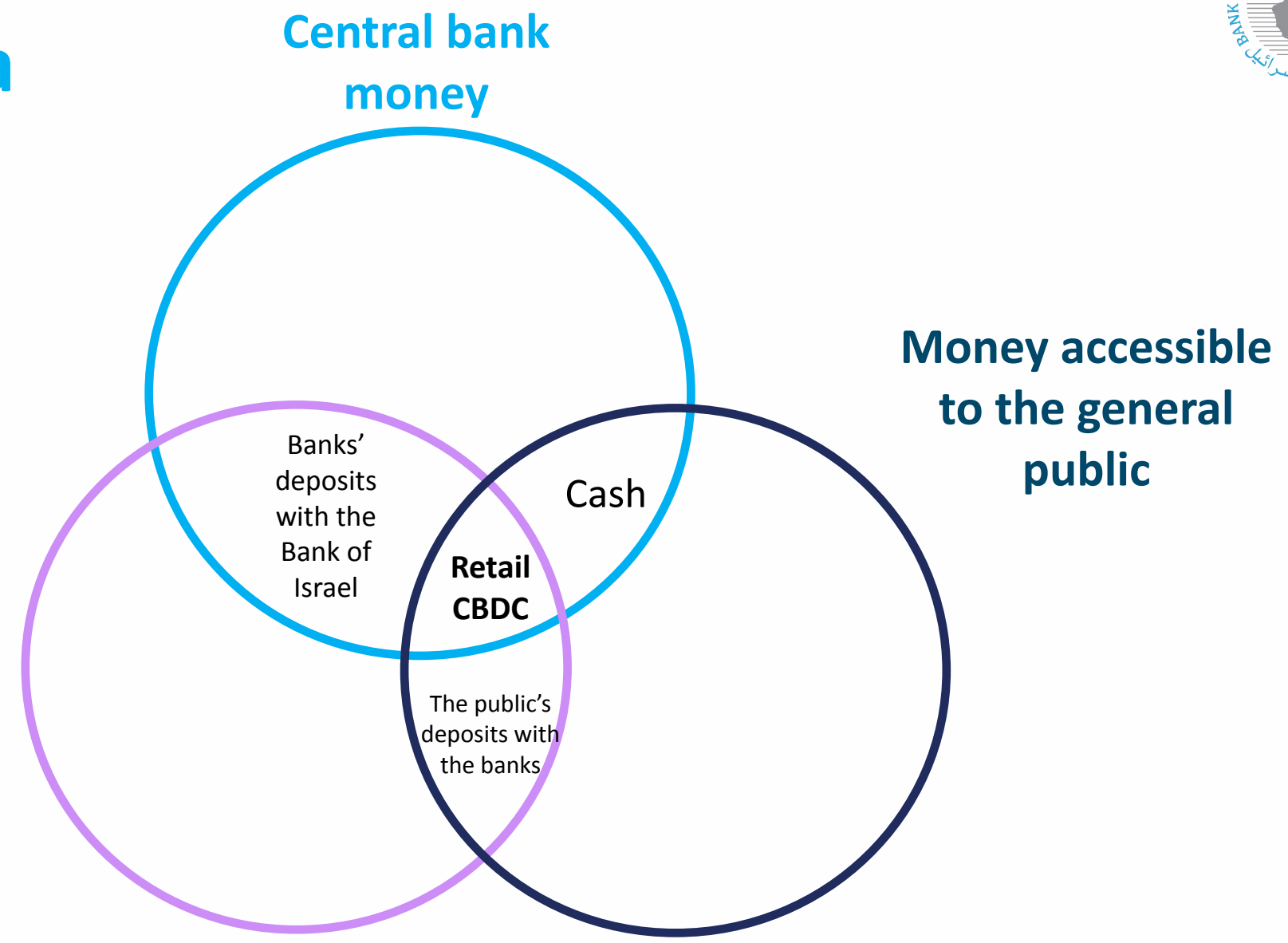
Privacy in CBDC – what are the needs and what can ?technology offer

Yoav Soffer, Digital Shekel Project Manager

5th ZKProof Workshop

Tel Aviv, Nov. 16 2022

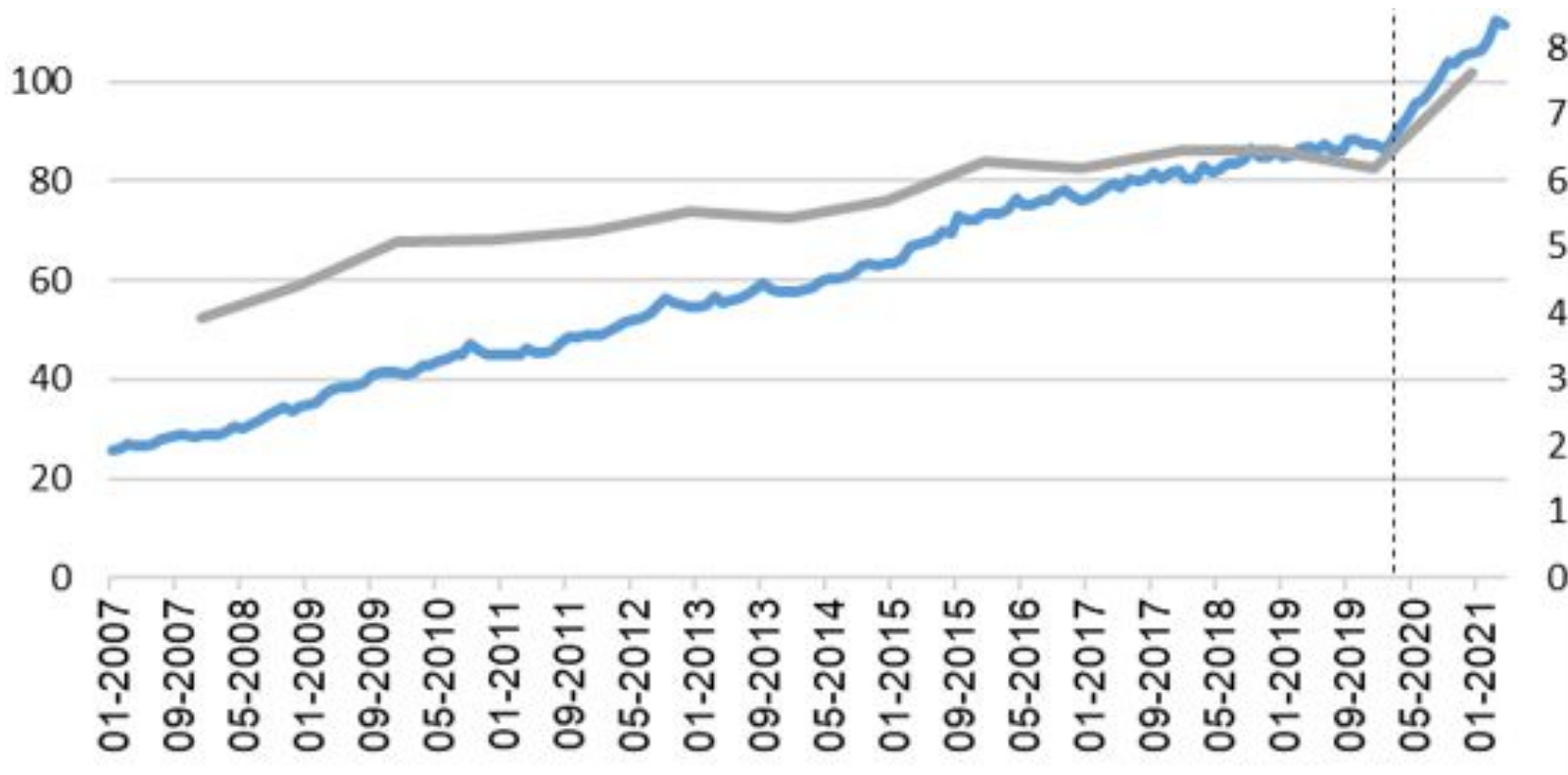
What is a ?CBDC

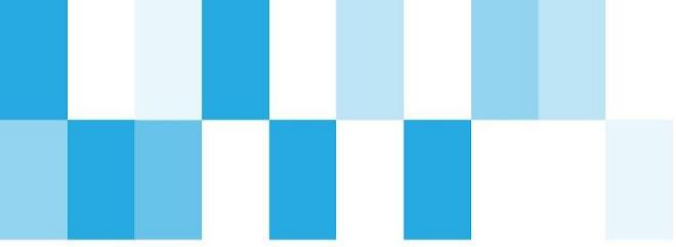


Cash is not disappearing in Israel



Stock of cash in NIS billion (left, blue) and as share of GDP (right, gray)

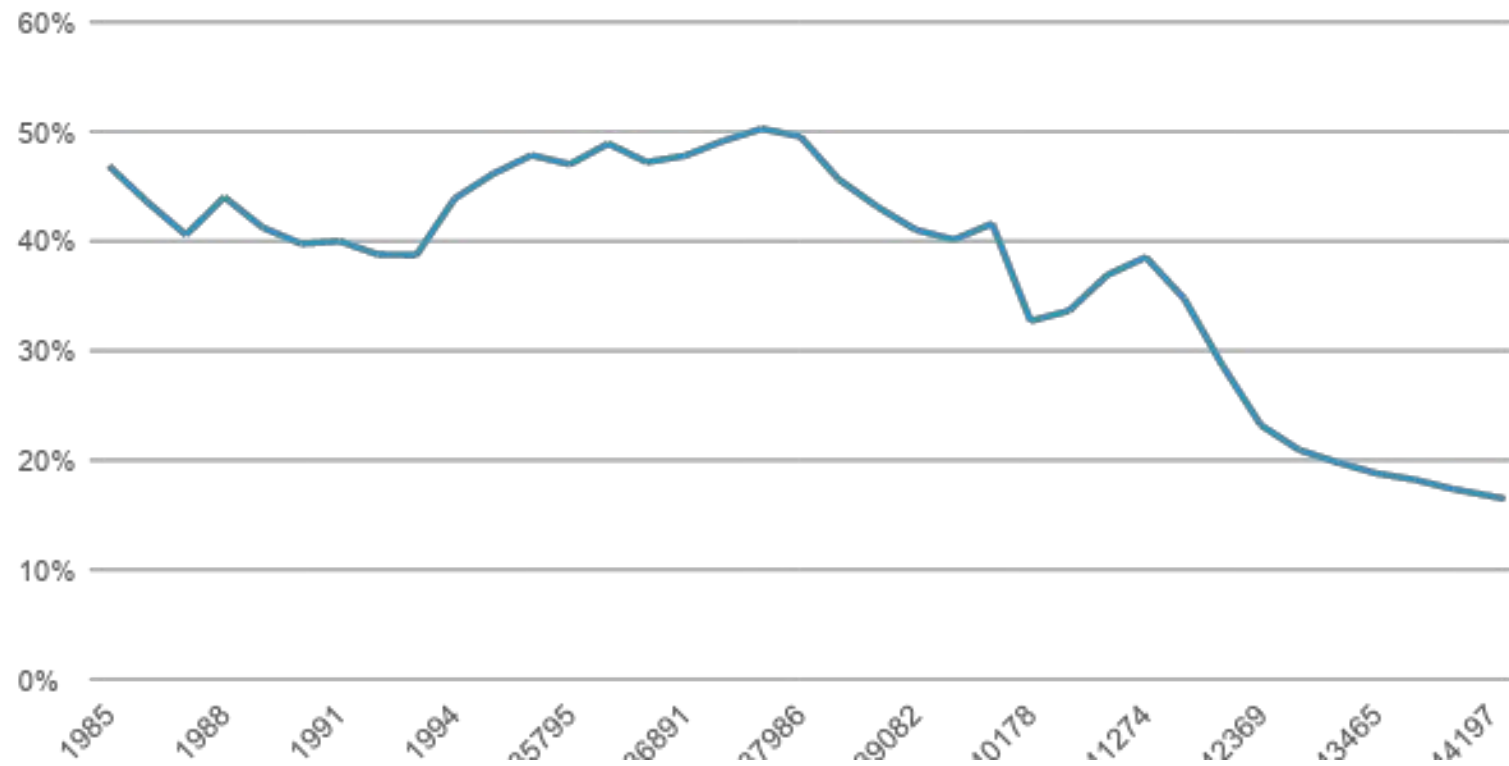




But is loosing its share as a means of payment



Share of Cash in M1



Possible Motivations for a Digital Shekel



Competitive alternative to the existing and new means of payment in the digital era



Innovation and adaptation of the payment system to the needs of the digital economy



Redundancy of the payment system in view of emergencies or breakdowns



Efficient and inexpensive infrastructure for cross-border payments



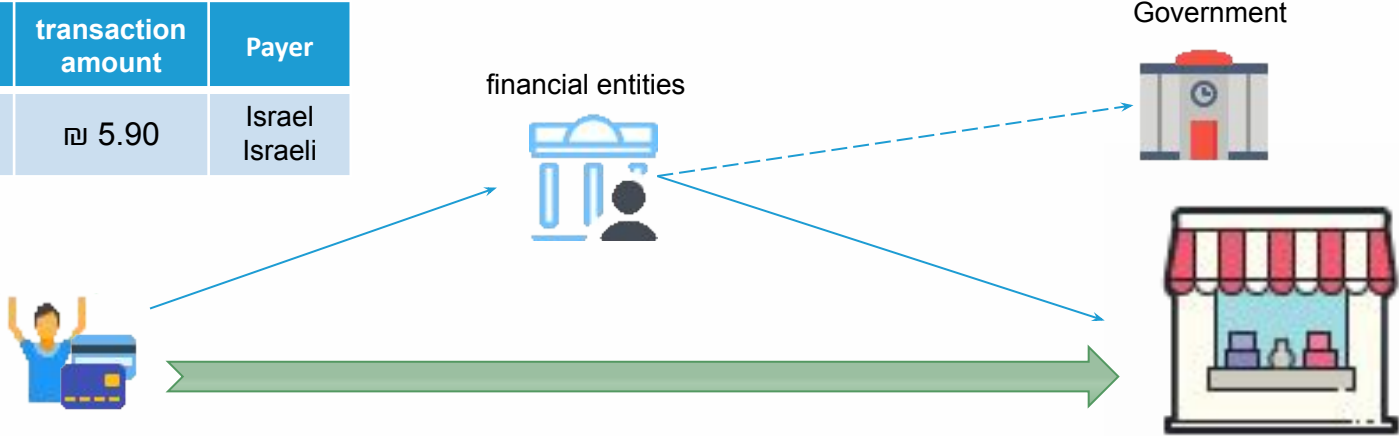
Paying digitally while maintaining a certain level of privacy



Support government's policy to reduce the use of cash and the struggle the "underground economy"

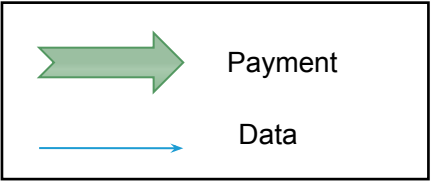
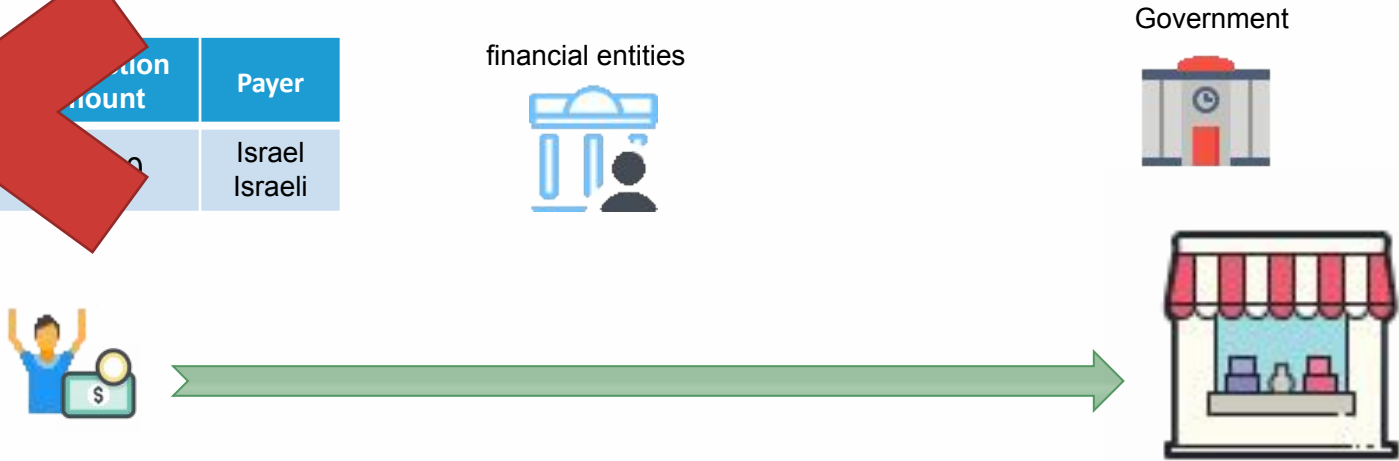
Paying with a digital means of payment

time	payee	transaction amount	Payer
11:14	Cohen's Supermarket	₪ 5.90	Israel Israeli



Paying with cash

time	payee	transaction amount	Payer
11:14	Cohen's Supermarket	₪ 5.90	Israel Israeli



Privacy

Privacy in the use of means of payment in general, and a digital shekel, should one be launched, in particular, is an issue that requires an in-depth discussion. The extent of privacy that will be enabled when using a digital shekel will in the final analysis reflect a societal decision.

- ① The digital shekel will be designed in keeping with AML-CFT rules, in a way that will not hamper the government's tax collection efforts. As such, and contrary to cash, it will not be possible to enable absolute anonymity for the payer or the payee.
- ② It will be possible to decide in the future on the extent of privacy for users vis-à-vis providers of payment services and on the commercial use that suppliers will be allowed to make of users' information.

5. Maintaining the public's option of using digital means of payment, while maintaining a certain level of privacy



1

Another feature of cash is that using it does not leave any “digital signature”. The use of cash is completely anonymous.

2

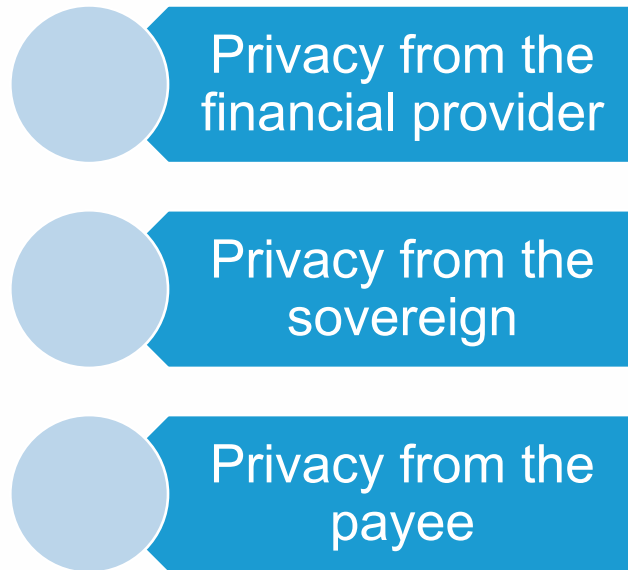
*The information that financial participants collect may be of value to the citizen. Based on this information, they can offer the citizen various products and are consistent with her preferences, offer credit, and more. **However**, the citizen has the right to purchase products without commercial entities using information about her purchases and payments.*

3

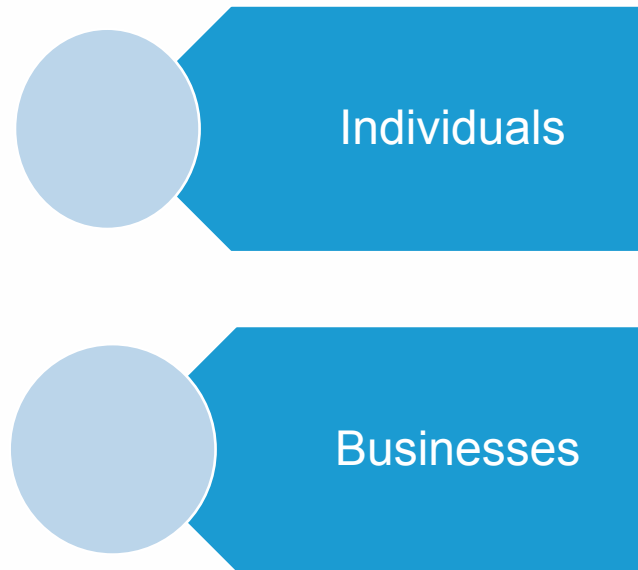
A central bank digital currency can maintain some of the features of cash in the context of maintaining the payer's privacy, while at the same time meeting the AML-CFT rules set by the state authorities.



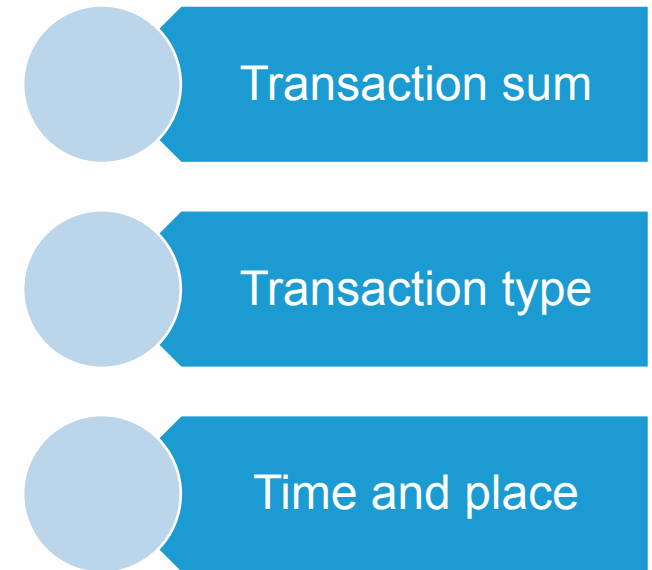
Privacy from whom



Privacy for who



Privacy on what

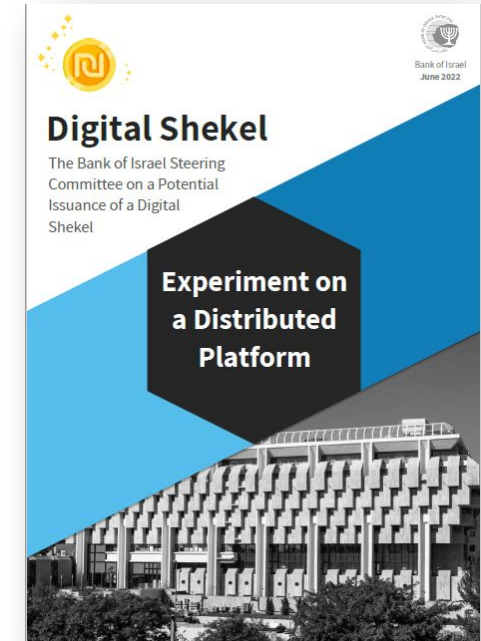


?Can there be several models or intermediary models

New technologies create new opportunities – Bol and VMware POC



- ❖ Motivation – to explore whether technology may allow policy makers a wider menu of policy alternatives as compared to those that exist today.
- ❖ The experiment examined an innovative technology that enables policy makers to set a periodic threshold for digital payments that can be made anonymously, beyond which payments are documented in the system.
- ❖ Each wallet can hold “ordinary” digital shekels, the transfer of which is recorded in the ledger, and “private” digital shekels, the transfer details of which are not recorded openly, so both sides to the transaction enjoy complete anonymity as with cash payments.



EN



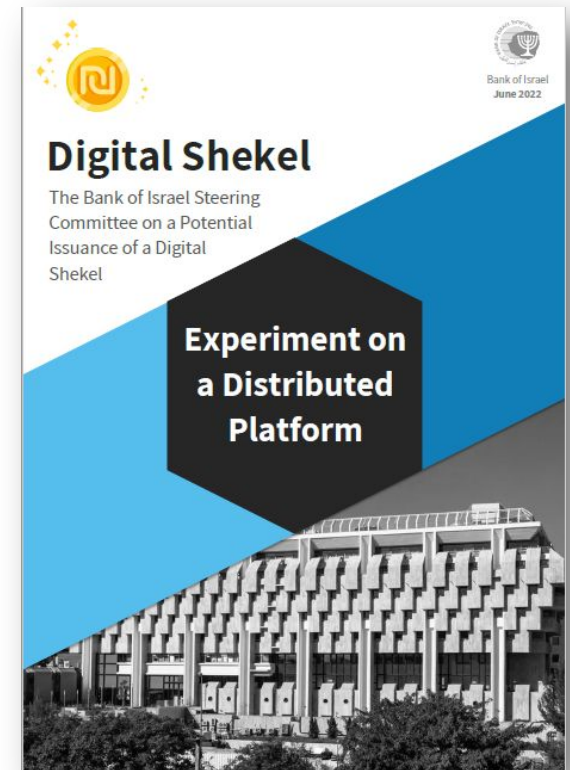
HE



Policy questions



1. What is the threshold to allow private payments?
2. Should there be a different threshold for different types of wallets (Business, individual, adult/child, etc).
3. Should there be types of transactions or types of payees to which private payments should not be allowed?
4. Could this create economic incentives for the misuse of “private” shekels?
5. Can the technology support other privacy modalities other than a periodical privacy budget?





תודה THANK YOU شکرا جزيلا

