Digital Currencies and Fast Payment Systems

ABFER Class

Darrell Duffie
Graduate School of Business, Stanford University

ABFER
Singapore, May, 2019
With research assistance from Hanna Tian and David Yang

Duffie is a member of boards of directors of Dimensional Funds and TNB Inc.
Class outline

1. Fintech is changing the payment landscape.
   - Token-based and bank-account-based payment systems.
   - Implications for financial inclusion.
   - Central bank digital currencies.
   - Primer on digital ledger technologies.
   - Private cryptocurrency stablecoins.
   - The money-flower classification of digital currencies.
   - Fast payment systems and open banking rules.

2. Disruption of profitable banking franchises.

3. Implications for monetary policy transmission, KYC-AML, and financial stability.

4. Summary of policy tradeoffs and predictions.
Token-based payment

Alice

$8

Bob, the baker
Swedes now rarely use cash

Bank-account-based payment

Alice

Bob

Alice's bank

Bob's bank

$8

message

payment rails

message

$8
Banks form the backbone of the payment rails
Illustrative cryptographic payment authorization flow

Figure 25 illustrates the device-centric POS wallet transaction flow used by Apple Pay, Android Pay, or Samsung Pay with NFC and EMV payment tokenization.

Figure 2. Device-Centric POS Transaction Flow

Figure 3. In-App Device-Centric Wallet Transaction Flow with Tokenization

Source: Federal Reserve Bank of Boston.
Emerging-market financial inclusion and digital payments

Data source: World Bank Global Findex Database.
CBDC account payment

A's account $8 B's account

central bank
CBDC token issuance

500 USD tokens

$500 payment

bank

$500 payment

500 USD tokens

central bank
Most central banks are now working on digital currencies

Private stablecoin issuance

500 tokens

issuer bank

authorization

$500 deposit claim

trust

bank

$500 payment
Public key cryptography

Alice has two keys: a public key known to the entire network and a private key known only to Alice.

1. Only Alice can use her private key to encrypt a “hash” of her digital message in a way that ensures to all that it has been uniquely signed by Alice.

2. The hashed message is broadcast to the network.

3. Everyone on the network has access to the encrypted digital message and knows from the public key that the message is from Alice.

4. Bob uses Alice’s public key to verify that Alice is the sender of the message and that he is intended recipient.
A blockchain is a form of distributed ledger.

3. KEY FEATURES OF DLT

Network participants each have a private key, which is used for signing digital messages and only known by the individual user, and a public key which is public knowledge and is used for validating the identity of the sender of a digital message. The public key is also used to identify the recipient. These three concepts help explain the fundamentals of DLT.

The process by which data is recorded in a blockchain-based distributed ledger is by forming an append-only chain of 'transaction blocks' in chronological order that contains hash digests of the transactions (digital messages) to be added to the ledger, a proof-of-work (or a different consensus mechanism output), and a digital signature of the hash by the sender's private key, and public keys of the sender and the intended recipient of the transaction.

This chain starts with the first-ever entry in the ledger (the 'genesis block') and each appended block contains hashed information of the previous block, setting the chronological order of the chain.

Figure 4 below depicts an example of a blockchain structure: The last block (block 5) was added to an existing blockchain (blocks 1-4, block 1 being the 'genesis block'). Each block contains a unique "proof-of-work" protocol, a reference to the previous block that determines the correct chronological ordering of blocks, a series of hashed digests of transaction information which cannot be changed, and a digital signature. In this figure, block 5 represents the newest addition to this blockchain which updates the ledger. Once a new block is added to the chain via a specified consensus mechanism, the chain cannot retroactively be changed and blocks cannot be deleted or amended without redoing the proof-of-work protocol for each block. This means that as the chain grows in length, this becomes progressively more difficult because all nodes are constantly competing for solving proof-of-work puzzles and adding new blocks to the chain. In doing this they only consider the transaction blockchain that reflects the greatest amount of computational work. Each successful addition to the chain is broadcast to the entire network and all nodes have an up-to-date copy of the entire blockchain.

Cryptocurrency transactions

- Distributed ledger technology for confirming and storing transactions cryptographically.
  1. Permissionless DLT: maintained by a trusted third party.
     - Examples: Ripple and Corda.
  2. Open DLT, also known as or “permissionless.”
     - Examples: Bitcoin and Etherium.

- Open DLT transactions are currently relatively slow, thus not suitable for heavy-throughput payment systems.

- A bank can issue its own stablecoin (e.g. JPM Coin) as a substitute or complement to its account-based payment services.

- Cryptocurrencies can be traded on exchanges for fiat currencies or other cryptocurrencies.

- Custody services can be provided by exchanges, banks, and others.
Digital petals of the money flower

Adapted from the “money flower” of Bech and Garrett (2017).
Illustrative and emergent digital money

- M-pesa
- Jasper (BoC)
- Ubin (MAS)
- eKrona\(_A\) (Riksbank)
- eKrona\(_V\) (Riksbank)
- DCEP (PBOC)
- CB tokens (wholesale)
- CB tokens (general)
- Deposited currency accounts
- Bank deposits, mobile money
- Stablecoins
- Crypto
Fast bank-based payment systems

- Key defining properties:
  1. $24 \times 7 \times 365$ availability.
  2. Near real-time access to the funds by the recipient.

- Operational approaches:
  1. Deferred net settlement of interbank obligations (DNS).
  2. Real time gross settlement (RTGS).
Examples of fast bank-based payment systems


- Bank of Mexico’s Sistema de Pagos Electrónicos Interbancarios.

- Swish, a private mobile payment system available in Sweden.

- The United Kingdom’s non-profit utility, Faster Payments.

- Singapore: Fast and Secure Transfers (FAST).

- The European Central Bank TARGET Instant Payment Settlement (TIPS), based on the SEPA Instant Credit Transfer platform.

- The US: Real-Time Payments System (private sector) and a proposed Fed RTGS fast payment system.
New open-API fast payment rails proposed by Token

- Ledger 1: A parallel form of commercial bank money, one ledger per currency.
  - Banks issue claims to customers on this ledger, analogous to conventional deposits.
  - This single high-speed ledger is shared by all member banks of a given currency.
  - Millions of transactions per second, with millisecond latency for each transaction.
  - Payments by customers are private-key transfers on this ledger, using a standard API.

- Ledger 2: Central bank money.
  - Real-time settlement of inter-bank claims by member banks.
  - Ledger claims are backed by central bank deposits held in a shared account.
  - Maintained by the central bank.
Fast payments via ledger 1 and ledger 2
Example: Alice pays Bob

Alice (who banks at Citi) instantly pays $8 to Bob (who banks at Wells).

1. Debit Alice’s Citi account on Ledger 1 by $8.

2. Debit Citi on Ledger 2 by $8.

3. Credit Wells on Ledger 2 by $8.

4. Credit Bob’s Wells account on Ledger 1 by $8.
Bank-based payment system revenues will probably be disrupted

North America: $0.40 trillion
Rest of world: $1.18 trillion

Consumer:
- Cross-border transactions: 7.9%
- Account-related liquidity: 5.0%
- Domestic transactions: 9.9%
- Commercial cards: 8.9%
- Cross-border transactions: 3.0%
- Account-related liquidity: 7.9%
- Domestic transactions: 19.8%
- Commercial cards: 37.6%

Commercial:
- Cross-border transactions: 9.1%
- Account-related liquidity: 27.6%
- Domestic transactions: 17.1%
- Commercial cards: 2.7%
- Cross-border transactions: 18.4%
- Account-related liquidity: 11.3%
- Domestic transactions: 12.5%

Technology firms entered China’s payment system

U.S. banks do not offer competitive rates for retail deposits

Data sources: U.S. Federal Reserve and Federal Deposit Insurance Corporation.
A large fraction of U.S. bank deposits earn no interest

Data source: U.S. Federal Deposit Insurance Corporation.
New open-banking rules may force banks to compete

- The EU’s Second Payment Services Directive (PSD2):
  - Third-party payment providers now have direct access the customer’s payment account information if they have the customer’s consent.
  - TPPs can use banks’ infrastructure to facilitate payment initiation and account information services.
  - Consent is also subject to General Data Protection Regulation (GDPR), introducing potential rule conflicts.
  - Similar new rules in India, China, Brazil, Australia, …

- Forbes (2018):  *With open APIs, many of the long-standing barriers to switching providers will dissipate. Big banks face the prospect that many of their customers may seek out the convenience of digital aggregators, taking their accounts, and the profit pools they represent, with them.*
Implications for monetary policy transmission and financial stability

- Increased passthrough efficiency through rate competition:
  - Entry of technology firms and digital banks.
  - Open-banking APIs and fast payment systems
  - Potential use of CBDCs or private stablecoins.

- Reduced control by central bank of its balance sheet.

- Potential financial stability concerns.
  - Easing flight from stressed banks to other banks, CBDCs, or stablecoins.
  - New operational risks.

Key policy tradeoffs

- Privacy versus anti money laundering.
- Transaction efficiencies; wholesale (settlement) and retail.
- Disruption of monetary policy implementation and financial stability.
- Disruption of banking; competition over deposit rates and payment fees.
- Financial inclusion.
A few predictions

- Instant payments of some form will dominate within, say, 10 years.

- Effective forms of instant payment are feasible now or will be within a few years:
  - instant bank-account payment systems.
  - central bank digital currencies.
  - private stablecoins.

- Large bank business franchises will be disrupted, whether by non-banks or banks.

- Most developed-market central banks will support the ranking:
  
  fast bank-account payment systems > CBDCs > non-bank stablecoins.


