BANKING IN THE DIGITAL AGE –

WHO IS AFRAID OF PAYMENTS DISINTERMEDIATION

Benjamin GEVA

Professor of Law

Osgoode Hall Law School York University

Toronto, Canada

bgeva@osgoode.yorku.ca

EBI's Global Annual Conference on Banking Regulation in Frankfurt am Main (jointly organised by the European Banking Institute and Goethe University

February 23 -24, 2018

Banking as Intermediation

1. **FINANCIAL INTERMEDIATION**

Account Holders

Depositors /savers ⬄ Borrowers

Commercial Bank

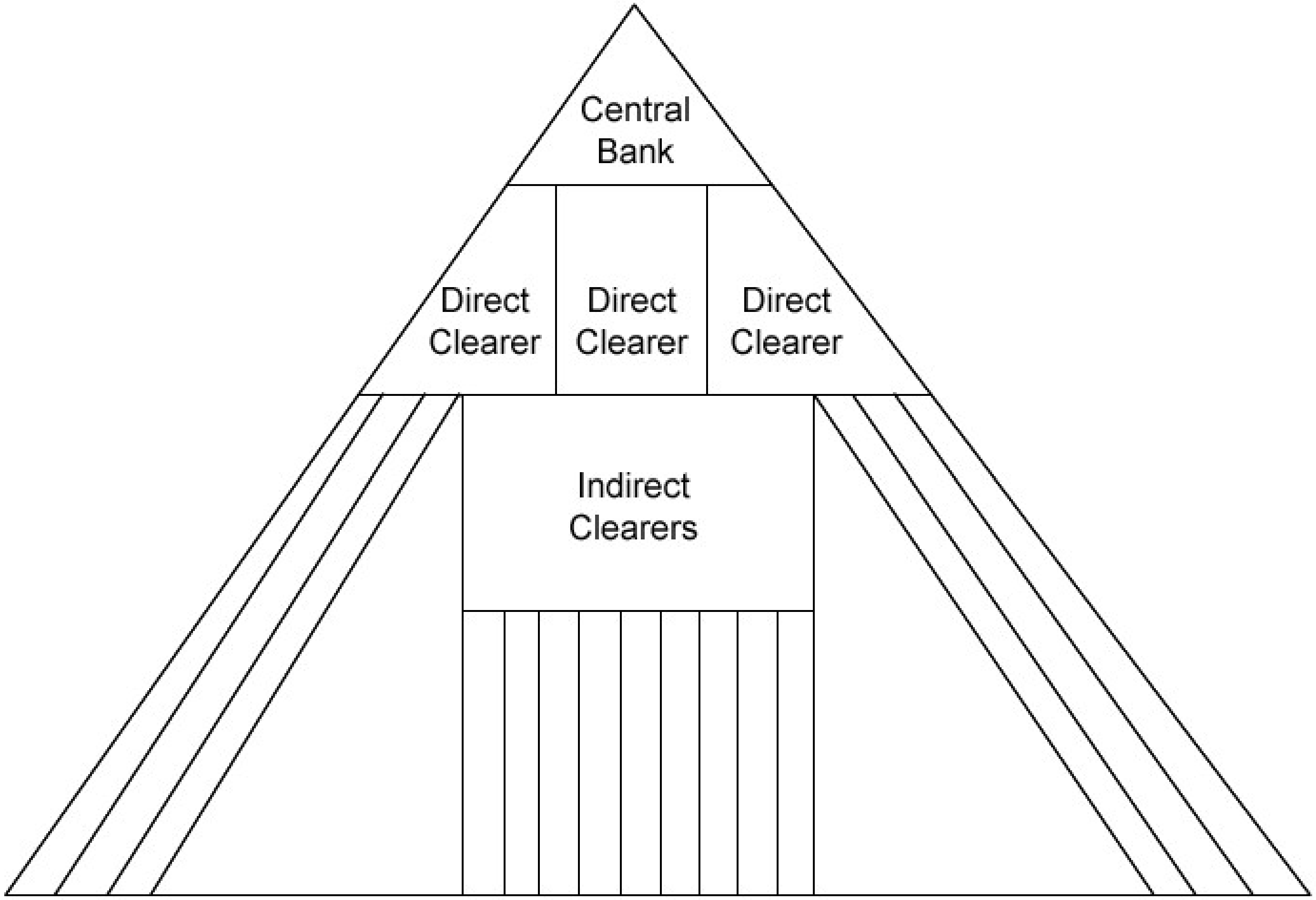
Money

(Historically: also banknotes)

2. **PAYMENT INTERMEDIATION**

Among account holders [in same or different banks]

Participants in the Domestic Payment System



Central Bank

Direct Clearer

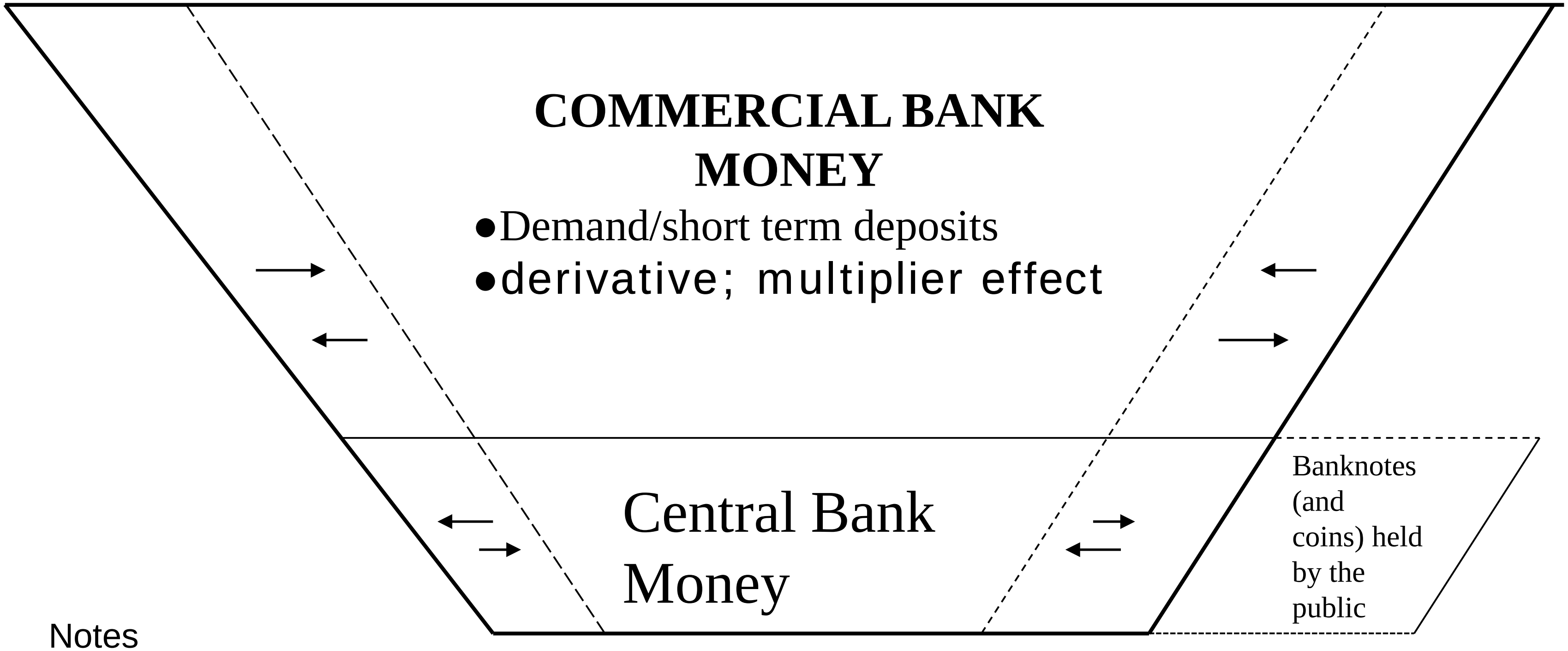
Direct Clearer

Direct Clearer

Indirect Clearers

CUSTOMERS

Regulation of Money Supply
Cash + bank Deposits)


COMMERCIAL BANK MONEY
●Demand/short term deposits
●derivative; multiplier effect
Central Bank Money
Banknotes (and coins) held by the public

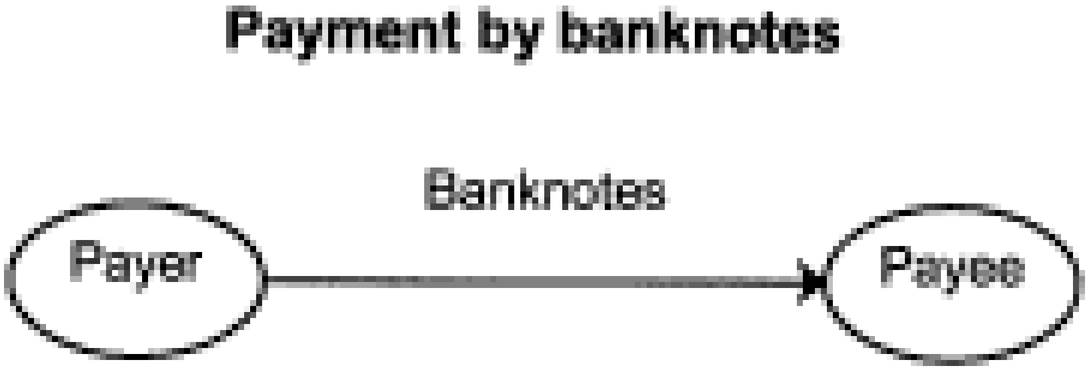
Notes

1) Amount of Commercial bank money **increases** with the **increase** in the amount of central bank money
2) Amount of commercial bank money **decreases** with the **decrease** in the amount of central bank money

Definition

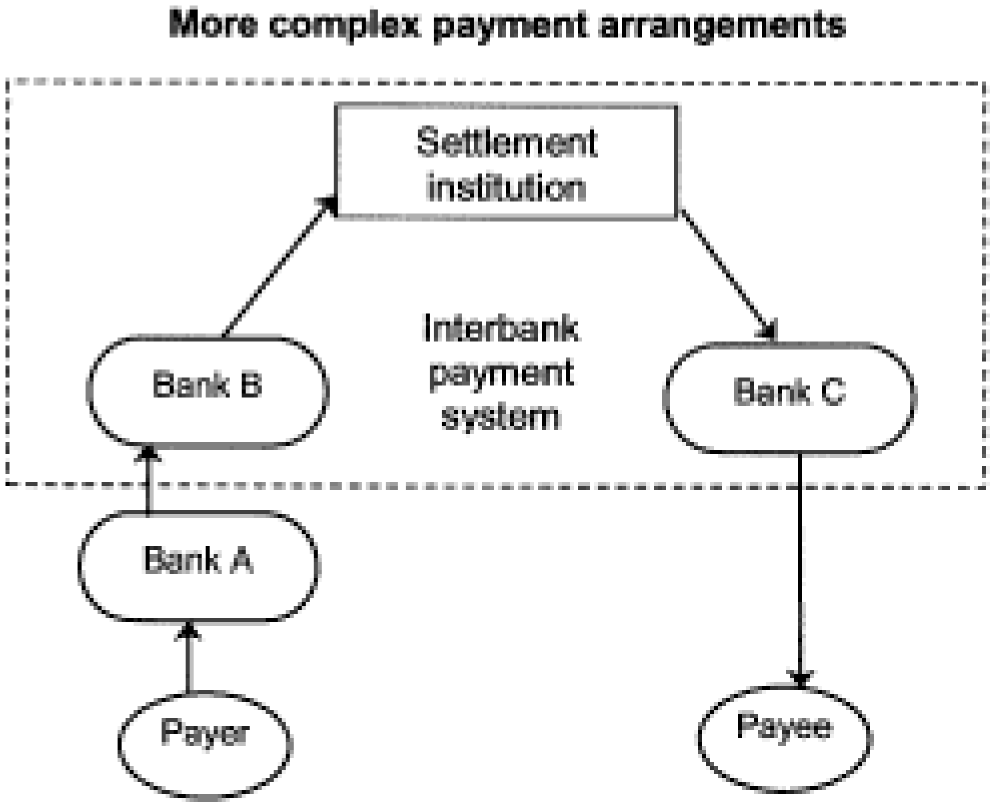
1. **Monetary base** = central bank money + banknotes (and coins) held by the public
2. **Money supply** = commercial bank money + banknotes (and coins) held by the public

Cash Payment



Source: CPSS Publications No 55 August 2003

Non-cash complex interbank Payment (in commercial bank money)



Source: CPSS Publications No 55 August 2003

The Electronic Age v. The Digital Age

<u>The Electronic Age: Communication & processing</u>

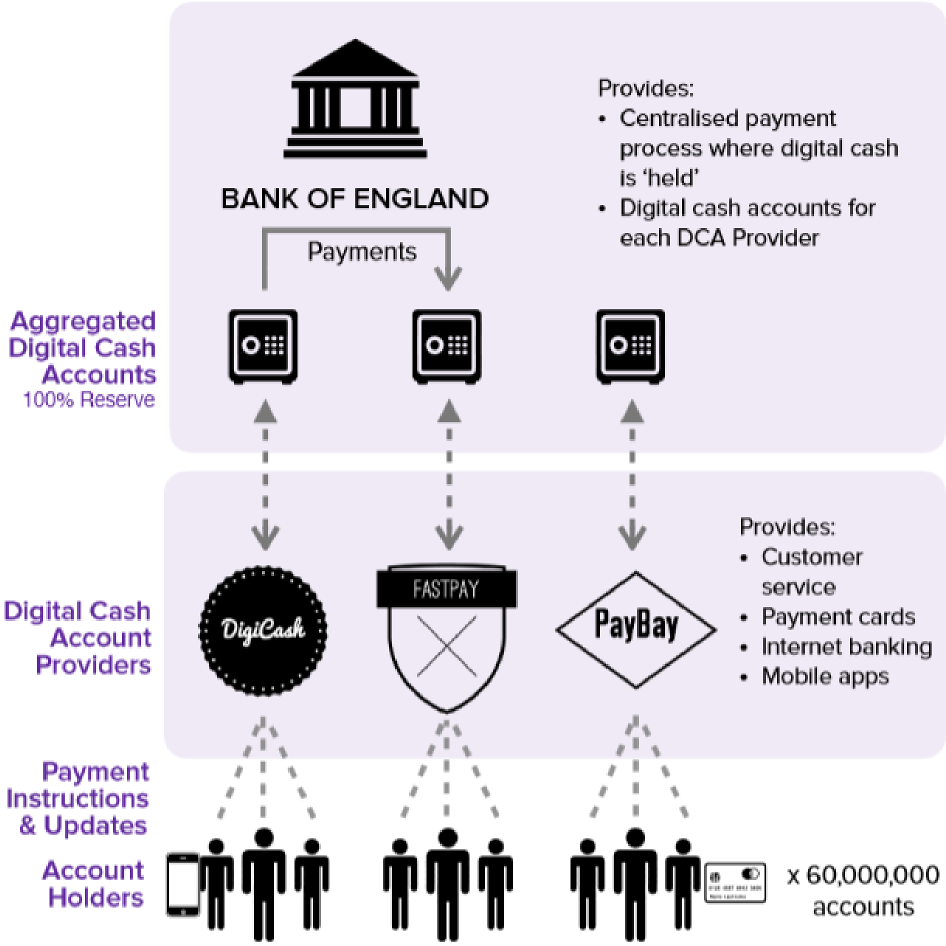
First, *electronic funds transfers (wire/telegraph; computer; mobile; Internet**//** **Second:** e-money/SVP: bank balance loaded on a card*

<u>The Digital Age: disintermediation of payments</u>

First, *the digital age is about to facilitate the availability of central bank money balances or their equivalents to the public. **Second**, cryptocurrencies and blockchains were born. **Third**, claim-check centralized digital currencies have been created*

Why Central Banks Should
Start Issuing Electronic Money
DIGITAL
CASH
Ben Dyson & Graham Hodgson ‘***FULL RESERVE BANKING’***

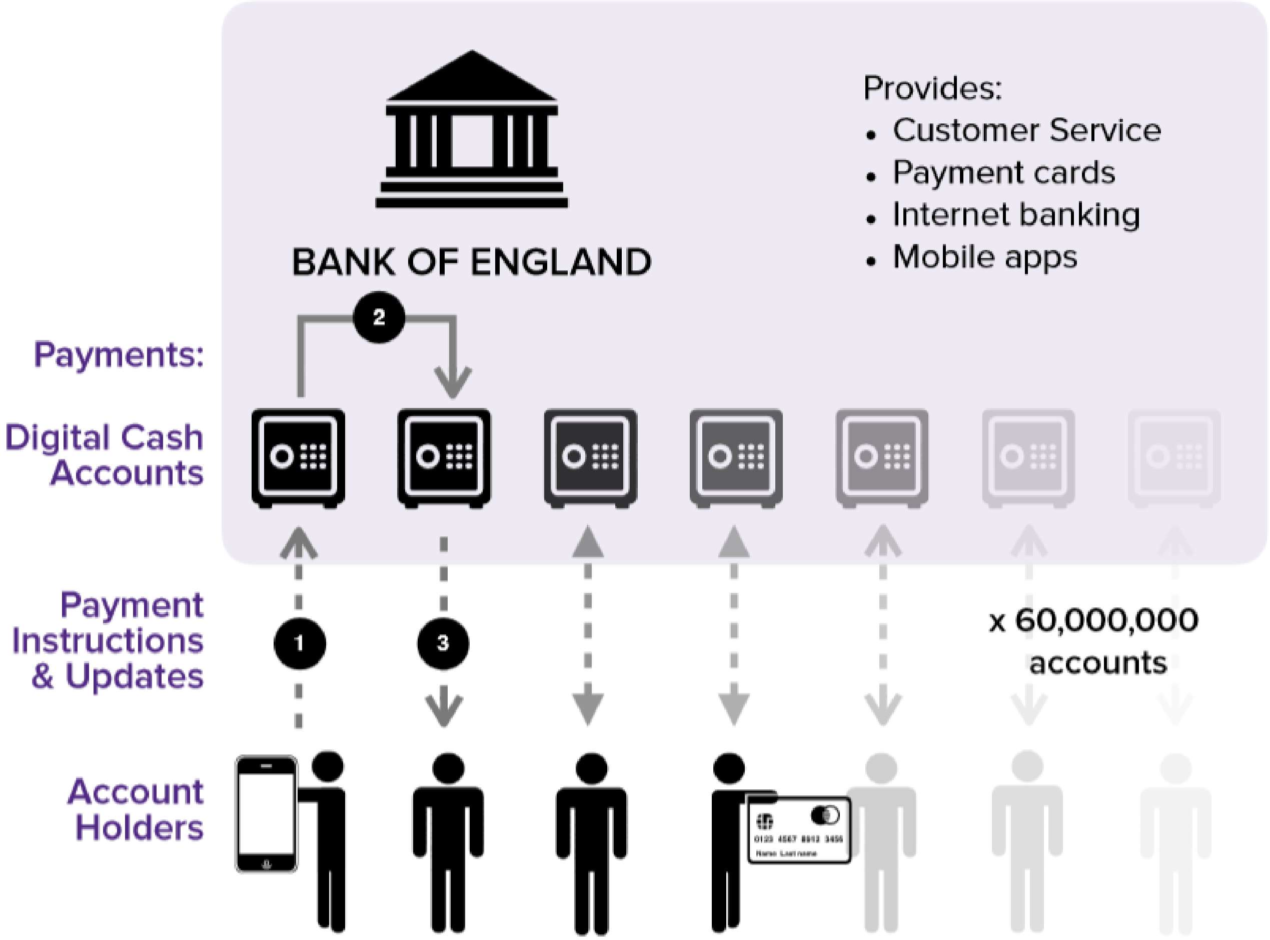
Figure 2.1.2: Indirect Access via Digital Cash Account Providers


BANK OF ENGLAND
Payments
Provides:
• Centralised payment process where digital cash is ‘held’
• Digital cash accounts for each DCA Provider
Aggregated Digital Cash Accounts
100% Reserve
Digital Cash Account Providers
DigiCash
FASTPAY
PayBay
Provides:
• Customer service
• Payment cards
• Internet banking
• Mobile apps
Payment Instructions & Updates
Account Holders
x 60,000,000 accounts

http://positivemoney.org/wp-content/uploads/2016/01/Digital_Cash_WebPrintReady_20160113.pdf

Why Central Banks Should
Start Issuing Electronic Money
DIGITAL
CASH
Ben Dyson & Graham Hodgson ‘***PLAIN SOVEREIGN MONEY’***

Figure 2.1.1: Direct Access to Accounts at the Bank of England



http://positivemoney.org/wp-content/uploads/2016/01/Digital_Cash_WebPrintReady_20160113.pdf

Digital Coin Defined

- It is “an entity that amounts to a string of bits.” The string must have a numerical value and, in order to prevent double spending, it must have a unique identity”

  Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*, (Elsevier, 2015)

  • Cryptocurrency, digital currency in which cryptography is used to control the **creation and transfer** of money

- Digital Currency can be issued either privately or a central bank
- What specific regulation and legislation are required?

Currency, Bank-money; and digital currency

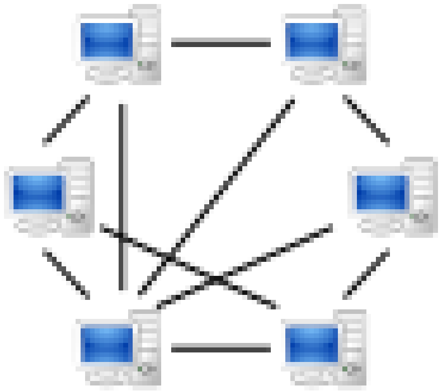
- ‘Cash’ or ‘currency’ consists of **tangible items**, each with its own identity and yet are fungible.

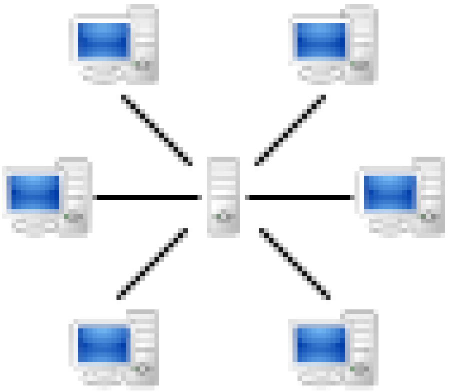
- Conversely, **‘bank money’** is ***generic value*** credited to a bank account, denominated in a unit of account and redeemable at par (though possibly subject to a transaction fee) to ‘cash’ or ‘currency’ in the same unit. At present, such value may be available on computer screens and digital devices. This, however, does not make it into digital cash or currency.

- **It is where money is digitally expressed *not only in the “generic value”,* namely, in a sum or account balance, but also where “both the face value and the *identity* of the money are carried digitally,” that we have *digital currency.***
  - Payment by digital currency does not require the surrender to the payee of the payer’s account information and may be made directly – hence more secure than an inter-account transfer
  - Digital currency security focuses on the issuer rather than on numerous bank accounts used for payment in bank money and hence, by concentrating on one or few locations, it facilitates enhanced defence, and improves the safety of the financial system.
  - Legal issues: transferability free of claims? Tracing?

Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*, (Elsevier, 2015)

Peer-to-Peer (P2P) /distributed/decentralized vs. Centralized Models





Type of Digital Currency Schemes

- A digital currency scheme in which coins are issued, transferred and redeemed under a centralized protocol is **centralized.**
- A digital currency that is issued, transferred and redeemed over a *distributed ledger,* is **decentralized**.
- A digital currency transferable over a *distributed ledger* and yet issued (& redeemed) by a centralized operator is **hybrid**.
- Payees may protect themselves against receiving digital coins that are either fake or have already paid ('double spent') by respective payers by consulting an 'oracle' as to their validity.
  - In case of a centralized system, the 'oracle' is the issuer; in a decentralized system, the 'oracle' is the *blockchain*.

Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*
(Elsevier, 2015)

Self anchored v. Claim check

Self-anchored digital currencies are mathematical creatures; **they hinge on cryptographic algorithms, not only for protection against hacking but also to control the creation of new units and facilitate payments**. Not being anchored in a specific tradeable asset, such as a commodity or a fiat currency, a self-anchored digital currency is inherently unstable, volatile, and easily amenable for speculation.

Conversely, in a *claim-check format*, a digital coin is a claim against a specified measure of a defined tradeable asset, or a cocktail thereof, such as a commodity or a fiat currency. Cryptographic protection of the value expressed by a digital coin in a claim-check format may be premised either on cryptographic algorithms or, so far as the bits string is concerned, pure randomness.

Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*, (Elsevier, 2015)

DLT/Block Chain

- A ***distributed ledger*** is an asset data-base that can be shared across a network of multiple sites, geographies or institutions.
- ***Blockchain*** is an underlying technology, or digital implementation for a distributed ledger. Being a computerized ledger on a distributed network it generates a single version of the record on each computer and in essence is
  - a type of a database that takes a number of records and puts them in a block … Each block is then chained to the next block, using ***a cryptographic signature.*** This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions.

UK Government Office for Science, *Distributed Ledger Technology: beyond the block chain* (2016), at 17

CPMI, *Distributed ledger technology in payment, clearing and settlement – an analytical framework* (BIS: February 2017), available online at: http://www.bis.org/cpmi/publ/d157.pdf

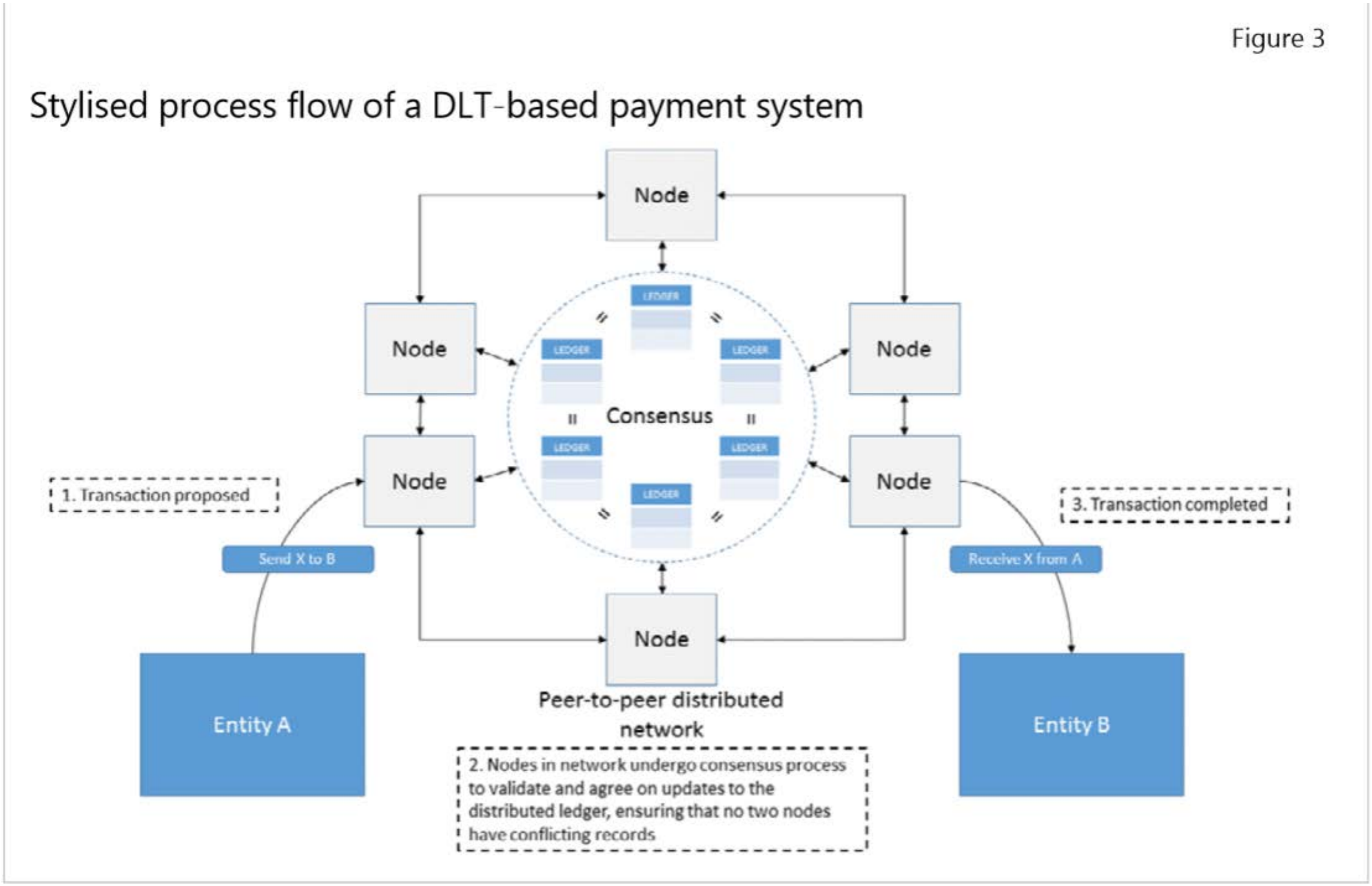


Figure 3

Stylised process flow of a DLT-based payment system

1. Transaction proposed

2. Nodes in network undergo consensus process to validate and agree on updates to the distributed ledger, ensuring that no two nodes have conflicting records

3. Transaction completed

Bitcoin

- Stuart Hoegner, “What is Bitcoin?” in Stuart Hoegner, (ed.), *The Law of Bitcoin* Bloomington IN: iUniverse, 2015)
- Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008) at 2, https://bitcoin.org/bitcoin.pdf.

- It is a virtual, self-anchored cryptocurrency and a peer-to-peer decentralized system.
- It is an “electronic coin” consisting of a “chain of digital signatures” transferable from the payer to the payee “by digitally signing a hash of the previous transaction and the public key of the next owner and adding them to the end of the coin.”

Each coin has verifiable mathematical properties. Each ‘digital coin’ is a unique solution to a mathematical problem. Both its creation and transfer are premised on ‘smart contracts’ of which terms are recorded in a computer rather than legal language.

Bitcoin Overview

- It is a cryptocurrency, because it uses cryptography to control the **creation and transfer** of money. Users send payments by broadcasting digitally signed messages to the network. Participants known as miners [acting as notaries] verify and timestamp transactions into a shared public database called the **BLOCK CHAIN**, for which they are rewarded with transaction fees and newly minted bitcoins. .
- Bitcoins can be obtained by **mining** or in exchange for products, services, or other currencies.
- Fixed supply cap (21m') and decreasing growth rate. If the mining power had remained constant since the first *Bitcoin* was mined, the last *Bitcoin* would have been mined somewhere near October 8th, *2140.*
- Through various exchanges, bitcoins are bought and sold at a variable price against the value of other currencies.

Bitcoin Block Chain

- The block chain is a public ledger of every bitcoin transaction that does provide a certain level of anonymity; it identifies transactions by Bitcoin address [public key] not individuals names. Tracking the flow of bitcoins through transactions can give clues as to who the owner is, however. And while Bitcoin uses cryptography, it does not do so to protect the identities of its users. In addition, Bitcoin intermediaries such as exchanges are required by law in many jurisdictions to collect personal customer data

How are new bitcoins ‘minted’?

- Blocks added to the block chain by ‘**miners**’ – competing to solve a ‘**proof of work**’ puzzle determined by the Bitcoin protocol
- Puzzle solving requires a significant expenditure of computational power – while verification of the correctness of the proposed solution is easy.
- Miner who solve the puzzle broadcasts the solution to other miners who start solving a new puzzle determined by a value included in the newly added block.
- Newly added block is called a “**nonce**”.

Bitcoin Downside

- Vulnerability to erosive cryptographic intractability- [‘Bitcoin operates on borrowed time’]
- Vulnerability to leadership corruption: democratic deficit; collusion by 51% of the miners..
- Infinite amount of bitcoins [21m’– production is envisaged to be exhausted by 2140]– to fight inflation: deflationary and yet not engraved in stone
- Value instability: fluctuating demand and supply; self-anchored- risk of ‘Bitcoin 2.’
- Poor scalability: blockchain low processing rate
- Risks to societal interests: hidden wealth; inability to enforce judgment.

S. Ammous, *Blockchain Technology: What is it good for?*,

- Bitcoin has a blockchain ***not because it allows for faster cheaper transactions, but because it removes the need to trust in third party intermediation***: transactions are cleared because nodes compete to verify them, yet no node needs to be trusted.
- Whether removing third party intermediation is a strong enough advantage to justify the increased inefficiency of distributed ledgers is a question that can only be answered over the coming years in the test of market acceptance of digital currencies.
- What can be clearly seen is that blockchain payment applications will have to be with the blockchain’s own decentralized currency, and not with centrally - controlled currencies.

According to S. Ammous, *Can cryptocurrencies fulfil the functions of money?* (August 2016), [summary]

- In Bitcoin, it is the high processing power which prevents both hacking and the establishment of a central control. Both achievements secure neutrality and full benefit of decentral structure at Bitcoin, and yet **at the cost of a fixed supply of growth that cannot be made to adjust to satisfy a purely market-determined demand and hence results in price instability**: **<u>High ratio of the stock to the flow //'hard money'</u>**
- At the same time, attempts in other currencies to bypass the expensive, inefficient and wasteful Proof of Work, by other settlement mechanisms such as ***Proof of Stake, consensus***, or a ***trusted notary***, compromised the neutrality of the system, enhance the control of the issuer, and/or require a third party verificator, all at the expense of the DLT premises!
- Hence he concludes, Bitcoin could be no more than a <u>*store of value*</u>– **due to strict commitment to low supply growth, credibly backed by the network 's distributed protocol and very large processing power**. Other cryptocurrencies are unlikely to fulfill any monetary feature

S. Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* [forthcoming book]

- Bitcoin may be “the best store of value humanity ever invented” so as to be capable of functioning as “a reserve currency” to be held by banks in cold storage.
- Against it they will perform payment transactions by debiting payers’ accounts and crediting those of payees. With it they will settle.
- Other than eliminating the central bank, this model will mimic the role of banks in relation to payments in fiat currencies so that in fact everyday Bitcoin transactions will be carried out 'off-chain' in effect through banks or similar deposit taking institutions.
- The system he envisages eliminates the central bank and its role as a lender of last resource as well more in general in relation to monetary policy.

CBDC Proposed Cryptocurrency Hybrid Schemes

•In the US proposals have been made for **Fedcoin**, being a central bank-issued cryptocurrency, to be available to the public at large. **Digital coins are to be centrally issued on a blockchain-style de-centralized ledger, but nevertheless with the central bank being in full control of quantity, timing, and fixed value in denominations of the national fiat currency unit of account.** Effectively, transactions will be validated by an independent notary nominated by the central bank. : <https://news.bitcoin.com/fedcoin-u-s-issue-e-currency/>

•A similar proposal was made in the UK for **RSCoin**. : <https://eprint.iacr.org/2015/502.pdf>,

•Another proposal is for a **NationCoin,** being a Regulated and Sovereign Backed Cryptocurrency (RSBC). The scheme envisages **cryptocoins, which as in Bitcoin, will be created by and transacted over a blockchain. However, upon their creation, cryptocoins will be stored, and released to the public by a Digital Asset Reserve (DAR),** as RSBC, at the fixed value of the national unit of account. Transactions are to be verified by ‘miners’ who will be paid freshly minted cryptocoins. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2888347>

BoC Jasper Project Experiment –Cad-Coin Platform--- Proof of Concept

- Not a fiat crypto (or otherwise digital) currency available to the public -- but rather a **Digital Depository Receipt** (***DDR***) used in a wholesale interbank payment system-premised on settlement over a permissioned blockchain (accessed only by BoC and the large banks)
- Each participant pledges [T1] cash collateral (fully collateralized $1 securing $1) into a special pooled account held by the BoC – and receives against the cash collateral a DDR in the same amount– transacted throughout the day over a balockchain.
- DDR is fungible and divisible – Phase I used smart contracts and ***ethereum consensus protocol**** ***Phase II switched to Corda- verification by a notary – BOC;***
- ***Jasper II:*** liquidity-saving mechanisms (LSM) in the form of a payment queue with periodic multilateral payment netting for payments designated as ‘non-urgent’.
- Participants exchange payments throughout the day over the blockchain. They can exchange assets on the Cad-Coin platform and redeem the digital currency for the T1 cash collateral, with the BoC destroying the redeemed DDR.

** More adaptable and flexible than the Bitcoin Protocol in in not being dominated by specialized hardware and allowing a more decentralized distribution of security.*

Cryptographic Algorithms

- Cryptographic algorithms are subject to ‘erosive complexity’ or ‘intractability,’ meaning “[c]ryptographic complexity that erodes with time, usually on account of (i) more effective computing machines, and (ii) deeper mathematical insight.”
- Furthermore, cryptographic algorithms may be cracked by ‘brute force’, namely, a trial and error method used by application programs to decode encrypted data through exhaustive effort, rather than employing intellectual strategies.
- Last but not least, even the cryptographic algorithm facilitating the derivation of the private key from its public counterpart is crackable.
- Developers of cryptocurrencies “simply migrated the cryptographic tools used to safeguard communication and applied them to safeguard digital currency”

Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*,
(Elsevier, 2015)

Randomized Coins

Entropic or randomized coins in which the bits string is totally pattern-less are not subject to the same or even a similar degree of risk. They are nevertheless subject to "the threat of a successful guessing of the coin bits," a risk which is substantially reduced by increasing the size of the bit string. As such, entropic or randomized coins are said to be practically unhackable

Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*, (Elsevier, 2015)

Tethering

A unique feature of digital currencies is the extensive potential for tethering. ‘Tethered money’ is defined to mean “[m]oney with built-in limitation on its use.” Tethering is an important tool for budgeting, gifting and grant giving, as it releases the payer from the heavy burden of monitoring and overseeing the actual use of the money in compliance with the terms under which it was paid. It thus eliminates both waste and corruption

Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*, (Elsevier, 2015)

Proposed Centralized CBDC/Virtual Claim Check Schemes

•*WingCash* is a multi-platform centralized system under which a claim-check to fiat currency may be issued. Each claim-check is in the form of a unique web page with an immutably assigned web address (URL), typically cryptographically signed by the issuer. It is described as a digital bearer instrument which simulates a physical banknote.

•*BitMint* is a centralized scheme for a tethered, non-speculative, and stable claim-check to a defined quantity of a specific commodity, including a fiat currency. It consists of randomized coins and is said to be identified as “the only candidate qualifying as a universal digital representation of worldwide currencies.” <http://pennwell.sds06.websds.net/2015/amsterdam/slideshows/T1S7O3-slides.pdf>,

Final Observations: Who is afraid of payment disintermediation?

•The availability to the public of central bank money, in the form of either full-reserve banking or plain sovereign money, is unlikely to affect the role of banks other than in money creation.

• Cryptocurrencies are mostly not a new form of money; blockchains do not pose a major threat to the traditional interbank settlement system; at most they spur improvements in legacy systems.

• The creation of claim-check centralized digital currencies will nevertheless allow banks to continue their role in providing payment services and even create alternative currencies fully backed by fiat ones.

• Banks will retain their role as intermediaries; Fintech does not have a payment services model which will supersede banking so that, in order to competitively provide payment services, IT firms will have to become banks.

THANK YOU!
QUESTIONS?

bgeva@osgoode.yorku.ca