14.129
Spring, 2025
Lecture 2

Blockchain as a Database

A Unified View of Distributed Ledgers and Financial Accounts as a Databases, Distinct Views of Money, the Larger Community Perspective

Robert M. Townsend

Elizabeth & James Killian Professor of Economics, MIT

Outline of the Lecture

- Blockchain: Special form of database
- Financial accounts are also special forms of database
- Blockchain and a broader view
- Tensions between individualized versus community perspectives
- A technical limitation of blockchains
- Current difficulties
- Progress in mapping economies and next steps

Blockchain: Special Form of Database

- Creation of bitcoin
- The incorrect association of blockchain with money
- Peer to peer exchange of certificates
- Central bank reactions: money and ledgers

Blockchain: Special Form of Database

- Any data structure used to store information can be considered a database
- Blockchain technology, at its core, is no more than a ledger to store information about transactions
- To that point, blockchains can be considered databases
- The data is stored as signed blocks, which link to each other, creating a chain of immutable interconnected data entries

Source: Blockchain Database MongoDB.com

Bitcoin

Each transaction in Bitcoin is an encoded message with paired private and public keys broadcast to the entire network, or at least to those listening among the community of users. The keys ensure no one can transact on someone else's ID, impersonating a node. Because the message or transaction can only be created with the key combination, there is commitment to the transaction, so it cannot be undone or reneged upon later. The transactions are transfers of coin from one account to another. All transactions are recorded on ledgers, in groups or blocks, subject to validation.

- Each node tries to bundle a set of incoming transactions since the last committed block to form a new block
- These new blocks consist of a timestamp (when the block is created), a nonce (used for verifying in POW), a reference to the previous block (a hash of it), and a list of transactions
- Diagram of *f*(nonce, prev block hash) → new block hash
- Can be thought of as a state machine, but can only be formally verified to be accurate if you start from the genesis block and perform every state update and check validity

Creation of Bitcoin

- The domain name bitcoin.org was registered on 18 August 2008. On 31 October 2008, a link to a white paper authored by Satoshi Nakamoto titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was posted. Open-source code released in January 2009.
- Nakamoto's identity remains unknown
- On 3 January 2009, the bitcoin network was created when Nakamoto mined the starting block of the chain, known as the *genesis block*
- Nine days later, Hal Finney received the first bitcoin transaction: Ten bitcoins from Nakamoto
- On May 22, 2010, the first known commercial transaction using bitcoin occurred when programmer Laszlo Hanyecz bought two Papa John's pizzas for ₿10,000, in what would later be celebrated as "Bitcoin Pizza Day
- According to computer scientist Arvind Narayanan, all individual components of bitcoin originated in earlier academic literature. Nakamoto's innovation was their complex interplay resulting in the first decentralized, Sybil resistant, Byzantine fault tolerant digital cash system, that would eventually be referred to as the first blockchain.

Source: Wikipedia (2024) "Bitcoin"

A Peer-to-Peer Example: Exchange of Certificates

- Krugman (1998) “Baby-Sitting the Economy” Slate.com
- A baby-sitting co-op, early 1970s -- Capitol Hill co-op
- A group of people (in this case about 150 young couples with congressional connections) agrees to baby-sit for one another, obviating the need for cash payments to adolescents. Parents sit for one another.
- It’s a mutually beneficial arrangement
- A couple that already has children around may find that watching another couple’s kids for an evening is not that much of an additional burden, certainly compared with the benefit of receiving the same service some other evening.
- But there must be a system for making sure each couple does its fair share.
- It issued scrip—pieces of paper equivalent to one hour of baby-sitting time. Baby sitters would receive the appropriate number of coupons directly from the baby sittees. This made the system self-enforcing.
- For complicated reasons involving the collection and use of dues (paid in scrip), the number of coupons in circulation became quite low. As a result, most couples were anxious to add to their reserves by baby-sitting, reluctant to run them down by going out. But one couple’s decision to go out was another’s chance to baby-sit; so it became difficult to earn coupons. A recession in the baby-sitting market followed.
- Eventually more scrip was issued, and then a different problem akin to inflation, money and monetary theory. An intriguing subject. Krugman writes this story changed his life.

Central Bank Reactions to Bitcoin and Blockchain Evolve

- Hyun Shin (2018) "BIS Annual Economic Report: Chapter V. Cryptocurrencies: looking beyond the hype" BIS.org
  - "Cryptocurrencies cannot scale with transaction demand, are prone to congestion and greatly fluctuate in value. Overall, the decentralised technology of cryptocurrencies, however sophisticated, is a poor substitute for the solid institutional backing of money."
- Now more than 80% of Central Banks are exploring digital currency, CBDC
  - But the case for why CBs are doing this is sometimes ambiguous and varies across countries
- Then next steps
- BIS, Augustín Carstens (2023) "The future monetary system: from vision to reality"
  - "..financial systems have evolved in separate silos and in a piecemeal way through minor tweaks of existing systems and processes. Legacy systems and outdated products abound."
  - "Even today, money and assets reside at the edges of communication networks in separate proprietary databases or ledgers. These databases are patched together via third-party messaging systems, so that messages have to be sent back and forth in a complex web of bilateral links, all following a separate path from the one corresponding to money or other financial assets."
  - "Cross-border transactions are even worse, as systems need to be connected through international messaging networks on top of domestic ones, involving a raft of different legal and governance frameworks."
  - "The best way to knit together transactions and operations among markets and financial services is to bring them onto shared programmable platforms. This is what we have labelled a unified ledger."
- Still, the view remains that Central Bank money is special, the singleness of money
- But see the earlier proposal for a single ledger and its view of money
- Adrian et al. "A Multi Currency Exchange and Contracting Platform" (2022) IMF.org

Financial Accounts Are Also Special Forms of Database

Corporate Financial Accounts, From Transactions

- Corporate balance sheet
- Income and cash flow statements
- The ledger interpretation of money

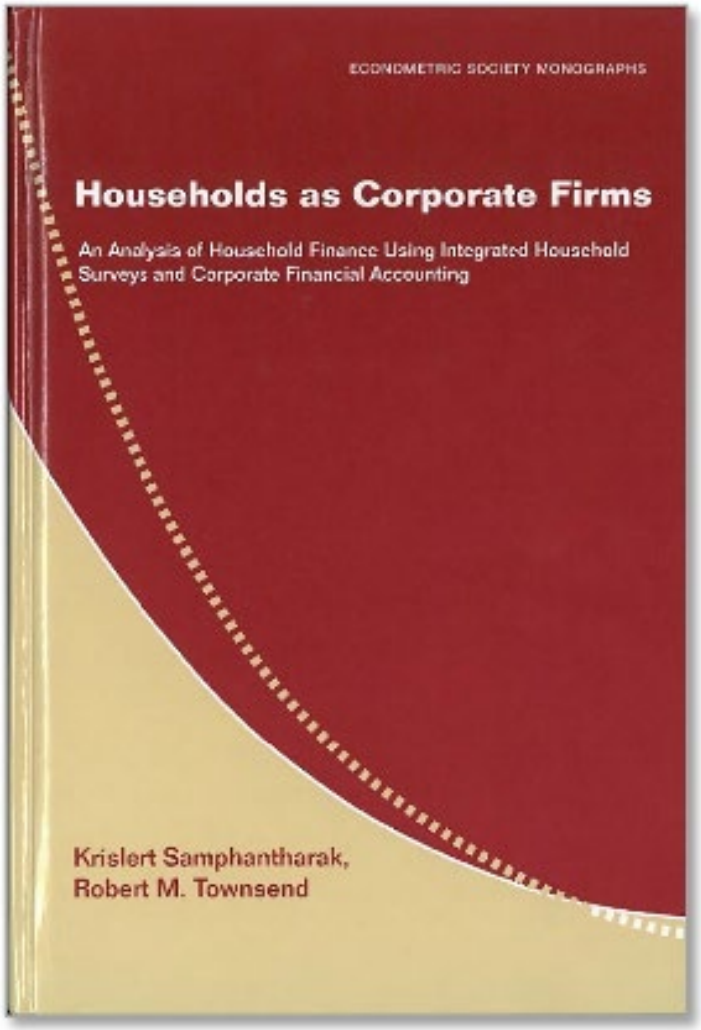


Table 4.1. *Examples of Transactions and Their Records*

Transaction	Example of Corresponding Survey Questions	Balance Sheet	Income Statement	Statement of Cash Flows	Remarks
Receive wage income in cash	**JM4D** What is the total amount of cash payments that you received since the last interview for doing this job? Include the value of any cash tips, bonuses or overtime payments. If no cash payments were received, record 0.	Increase in cash; Increase in cumulative savings	Revenue from labor	Net income (Cash inflow)	
Use cash to pay telephone bill	**XM1A [6]** Since the last interview, have you or members of your household made any cash purchases of [telephone and telecommunication services]? If yes, what is the total amount that you and members of your household have spent on [telephone and telecommunication services] since the last interview?	Decrease in cash; Decrease in cumulative savings	Consumption	Consumption (Cash outflow)	
Deposit cash with the production credit group	**SM3B** How much have you deposited to [the production credit group] in total since the last interview?	Decrease in cash; Increase in deposits at financial institutions		Increase in deposits at financial institutions (Cash outflow)	

(*continued*)

69 70

Table 4.1. (*continued*)

Transaction	Example of Corresponding Survey Questions	Balance Sheet	Income Statement	Statement of Cash Flows	Remarks
Sell calves for cash	**IM7C** What is the value of [the baby cows] you got rid of in this transaction? **IM7E** What kind of transaction was this? (1 = sell live animal for cash or credit) **IM7F** How much cash did you receive in total for this livestock? (If no cash was received, record 0)	Increase in cash, decrease in livestock assets; Increase in cumulative savings	Capital gain from livestock	Net income (Cash inflow); Decrease in livestock assets (Cash inflow)	1. We consider milk cows as livestock assets similar to fixed assets. 2. Increase in cumulative savings = Capital gain from livestock 3. Total cash inflows = Total cash revenue
Lose value of mature milk cows due to their depreciation (from getting older)	*See last column of this row*	Decrease in livestock assets; Decrease in cumulative savings	Livestock depreciation	(Negative) net income (Cash outflow); Depreciation (Cash inflow)	1. We assume a constant depreciation rate, computed from the fact that a regular mature milk cow lives for about 8 years 2. No net change in cash holding

The Ledger Interpretation of Money/ Cash

Table A.3. *Statement of Cash Flows of Household A*

Month	5	6	7	8	9	10	11	12	13	14	15	16
Net Income (+)	−22,684	−12,889	−2,945	16,125	20,597	17,290	22,960	24,627	65,891	25,475	21,494	10,383
Adjustments:												
Depreciation (+)	6,075	6,046	6,040	5,996	5,952	5,909	5,866	5,883	5,841	6,098	6,053	6,008
Change in Account Receivable (−)	−147,488	−116,288	−147,100	−107,023	−67,391	−80,302	−62,360	−50,838	−52,757	−49,851	−50,145	−51,000
Change in Account Payable (+)	149,960	149,960	147,195	147,195	147,195	147,195	147,195	147,195	147,195	147,195	135,450	152,050
Change in Inventory (−)	−126,465	−106,205	−148,866	−128,883	−158,624	−157,334	−142,232	−153,825	−147,472	−157,975	−151,519	−150,782
Change in Other Current Assets (−)	1,781	3,263	3,230	3,198	3,166	3,134	−2,897	3,132	−26,899	3,370	3,336	3,303
Consumption of Household-Produced Outputs (−)	−350	−314	−383	−373	−440	−590	−323	−396	−336	−348	−373	−205
Cash Flow from Production	−139,171	−76,427	−142,830	−63,765	−49,545	−64,697	−31,792	−24,221	−8,537	−26,036	−35,704	−30,243
Consumption Expenditure (−)	−8,685	−9,048	−7,762	−10,476	−8,126	−15,596	−9,340	−1,076	−2,669	−5,984	−2,772	−8,900
Capital Expenditure (−)	−3,281	−12,463	−3,230	−3,198	−3,166	−3,134	−3,103	−3,132	−3,101	−3,370	−3,336	−3,302
Cash Flow from Consumption and Investment	−11,966	−21,511	−10,992	−13,674	−11,292	−18,730	−12,443	−4,208	−5,770	−9,354	−564	−12,202
Change in Deposit at Financial Institution (−)	−8,895	−698	−125	11,295	−675	5	−32,080	−11,645	−39,565	455	55	55
Change in ROSCA Position (−)	−4,000	−4,000	−4,000	29,500	−4,550	−4,550	−4,550	−3,300	20,700	−3,000	−6,000	−7,000
Lending (−)	0	0	0	0	0	0	0	0	0	0	0	0
Borrowing (+)	−2,000	−2,000	−2,000	−2,000	−2,000	−2,000	108,000	−3,384	−3,384	−3,384	−3,384	−3,848
Net Gifts Received (+)	−710	618	−311	38	−1,257	940	−598	53	406	−226	665	2,137
Cash Flow from Financing	−15,605	−6,080	−6,436	38,833	−8,482	−5,605	70,772	−18,276	−21,843	−6,155	−8,664	−8,656
Change in Cash Holding (from Statement of Cash Flows)	−166,742	−104,019	−160,258	−38,606	−69,319	−89,032	26,537	−46,705	−36,149	−41,545	−44,932	−51,101
Change in Cash Holding (from Balance Sheet)	−166,742	−104,019	−160,258	−38,606	−69,319	−89,032	26,537	−46,705	−36,149	−41,545	−44,932	−51,101

Remark: The unit of currency is THB. Month 5 is corresponding to January 1999.

Samphantharak and Townsend (2009)

A Typical Labor Household in Lopburi

Table 1 – Statement of income and retained earnings of household A

Uses		Sources	
Expenses from production		Revenues from production	
Cultivation	0	Cultivation	0
Livestock	181	Livestock	340
Fish and shrimp	0	Fish and shrimp	0
Business	0	Business	0
Labor	0	Labor	91,150
Other	730	Other	260
Interest expense	10,000	Interest revenue	0
Depreciation	3,435	Capital gains	0
Insurance premium	0	Less: Capital losses	0
Property tax	0	Insurance indemnity	0
Net income before tax			
Income tax	0		
Consumption	54,076		
Savings	23,329		
Charges against total revenue	91,750	Total Revenue	91,750

Samphantharak and Townsend (2009)

Table 2 – Balance sheet of household A

Assets		Liabilities and net wealth	
Current assets		Current liabilities	
Financial assets		Accounts payable	0
Cash	22,992	Other borrowings	37,417
Accounts receivable	0	Household's net wealth	
Other lendings	0	Contributed capital	118,192
Deposits	5,560	Current retained earnings	50,779
ROSCA (net position)	14,125	Gifts (net transfer)	–1,602
Inventories	1,777		
Prepaid insurance	0		
Livestock	1,081		
Fixed assets			
Household assets	69,251		
Agricultural assets	0		
Business assets	0		
Land and other fixed assets	90,000		
Total assets	204,786	Total liabilities and net wealth	204,786

Blockchain and a Broader View

Blockchain and a Broader View

- Single-dimensional (e.g., payments) vs. multi-dimensional (e.g., contracting)
- Payments matrices capturing heterogenous velocities
- Individual vs. common accounts
- Distributed ledger technology

Blockchain: Single vs. Multidimensional

- Multi-dimensional
  - A database on many objects
  - Can even include contracts, as we shall see
- Create payments matrices: Money simply means objects appearing frequently in exchange
- Or, velocity of any object, amount traded per unit time divided by stock outstanding (on average)
- Thus, there can be multiple monies, coexisting with other objects

Payment Matrices

- Lim and Townsend (1998) "General Equilibrium Models of Financial Systems: Theory and Measurement in Village Economies"
- Village India: Money, IOUs, Grain

TABLE III
Exchange Matrix for Aurepalle Village[a]

Goods or services out	Goods or services in (value percent)													
	Money	IOU	Grain	Other crops	Food other than crops	Clothing	Other consumptions	Labor	Livestock	Physical assets	Jewelry	Consumer durables	Inputs	Others
Money	·	8.22	2.92	4.99	0.17	1.52	3.87	0.83	2.56	2.69	0.55	2.91	2.30	3.60
IOU	10.00	0.02	0.93	0.20	0.01	0.42	0.15	0.06	0.31	·	0.37	0.24	0.05	0.04
Grain	2.34	2.90	0.04		0.00	0.00	0.03	4.52	0.02	·	·	0.01	·	0.02
Other crops	6.49	0.74	0.00	0.02	0.00	·	·	0.18	0.05	·	·	·	·	0.01
Clothing	·	0.31	·	·	·	·	0.02	0.00	·	·	·	·	·	·
Other consumptions	0.02	·	0.01	·	·	·	·	·	·	·		·	·	·
Labor	1.40	·	4.56	0.16	0.01	0.00	0.00	0.02	0.00	·	·	0.00	·	·
Livestock	3.25	0.16	0.00	0.03	·	·	0.01	0.00	0.22	·	·	·	·	·
Physical assets	6.05	0.49	0.03	·	·	·	·	·	·	·	·	·	·	·
Jewelry	1.09	0.05	·	·	·	·	0.23	·	·	·	·	·	·	·
Consumer durables	0.45	0.23	·	·	·	·	0.02	·	·	·	·	0.06	·	·
Other	10.67	0.00	0.79	0.19	1.19	0.00	0.01	0.01	·	·	·	0.01	·	0.01

[a] 0.00 denotes a positive number which is rounded to zero. The heavy dot (·) denotes true zeros.

US Economy: Stmt of Account Flows
Currency, Demand Deposits, Debit Accounts, Foreign Currency

TABLE 9
DCPC Statement of Account Flows, October 2012

	Flows Associated with Accounts							
	Currency	DDA	NFDA	Foreign Currency	LTFA	Revolving Debt	Other Debt	All
A. Production (inflows)	**388**	**5,379**	**NA**	**NA**	**NA**	**NA**	**NA**	**5,767**
B. Consumption and investment (outflows)	**−1,038**	**−4,422**	**−58**	**NA**	**—**	**−1,249**	**NA**	**−6,771**
B.1 Consumption expenditure	−1,038	−4,422	−58	NA	—	−1,249	NA	−6.771
B.2 Capital (durable goods) expenditure	NA	NA	NA	NA	—	NA	NA	NA
C. Financing	**−91**	**−536**	**−1**	**2**	**NA**	**−43**	**669**	**0**
C.1 Deposits (inflows)	**498**	**564**	**20**	**2**	**NA**	**NA**	**669**	**1,753**
From currency	—	564	*15*	2	NA	NA	*8*	589
From demand deposits	455	—	2	NA	NA	NA	*643*	1,100
From nonfinancial deposit accounts	21	NA	—	NA	NA	NA	0	21
From foreign currency	0	NA	NA	—	NA	NA	NA	0
From long-term financial assets	NA	NA	NA	NA	—	NA	NA	0
From revolving accounts	22	NA	3	NA	NA	—	*18*	43
From other debt	NA	NA	NA	NA	NA	NA	—	0
Addendum: Total deposits (inflows)	*886*	*5,943*	*20*	*2*	NA	NA	*669*	*7,520*
C.2 Withdrawals (outflows)	**−589**	**−1,100**	**−21**	**0**	**NA**	**−43**	**NA**	**−1,753**
To currency	—	−455	−21	0	NA	−22	NA	−498
To demand deposits	−564	—	NA	NA	NA	NA	NA	−564
To nonfinancial deposit accounts	*−15*	−2	—	NA	NA	−3	NA	−20
To foreign currency	−2	NA	NA	—	NA	NA	NA	−2
To long-term assets	NA	NA	NA	NA	—	NA	NA	0
To revolving accounts	NA	NA	NA	NA	NA	—	NA	0
To other debt	*−8*	−643	0	NA	NA	−18	—	−669
Addendum: Total withdrawals (outflows)	*−1,627*	*−5,522*	*−79*	NA	NA	*−1,292*	NA	*−8,524*
D. Change in account balance (from Statement of Account Flows)	**−741**	**421**	**−59**	**2**	**NA**	**−1,292**	**669**	**−1,004**
E. Change in account balance (from Balance Sheets)	**164**	**NA**	**NA**	**NA**	**−4,501**	**−673**	**9,489**	**−8,816**
F. Flow error	**905**	**NA**	**NA**	**NA**	**NA**	**−619**	**−8,820**	**7,812**
G. Error (% lagged account balance)	**135%**	**NA**	**NA**	**NA**	**NA**	**92%**	**93%**	**−89%**

Samphantharak, Schuh, and Townsend (2018)

Individual vs. Common Accounts

- Consensus financial accounts
- A transaction log operates on the Townsend Thai monthly survey data and records cash transactions that each household *i* has with any other household *j*. Transactions are the basic building block.
- As with Bitcoin, there is an initial state, who holds what coins, that is modified by a transaction to deliver a new state. A difference with paper currency, though, is that currency is held by the household as part of its balance sheet and is not public. Currency is an actual portable physical token and not an electronic entry. But the accounting concepts underlying the use of currency and the use of coins are the same.
- We can now link the statement of cash flow to the new language of distributed ledgers with only a few conceptual steps, as it is not hard to imagine how the new technology could map onto the current paper currency systems. First, one could imagine in principle that accounts could be kept on a common account or centralized common ledger.
- To establish a proof of concept, this is being done with the Townsend Thai data with Chad Qian.

Create De Facto Distributed Ledger

- This ledger could also be done in practice from observed transactions, and in real time, if transactions were out of e-wallet coins and hence recorded
- Next, the common ledger could be created
- Finally, when reconfirmed, distributed among the households so that each has access to the common account or to their own identical copy (subject to privacy, which we come back to under mechanism design below)
- We could call this new common integrated database a distributed ledger
- A key step here is whether the transactions that would be recorded on the ledger are consistent with each other. We are now rechecking the database to quantify discrepancies.
  - First, we look at checking how many of the transactions in all.csv actually occur between two households that are both being surveyed
  - Next, we see how many transactions are reported by both households

Distributed Ledger Technology

- Distributed ledger technology (DLT) is the technological infrastructure and protocols that allow simultaneous access, validation, and record updating across a networked database.
- DLT is the technology blockchains are created from, and the infrastructure allows users to view any changes and who made them, reduces the need to audit data, ensures data is reliable, and only provides access to those that need it.
- Distributed computing is not new—businesses and governments have been using the concept for several decades. In the 1990s, it became possible for multiple computers and users in different locations to solve problems and return the solutions to a central location
- Advances in data science, computing, software, hardware, and other technologies have made ledgers much more capable.
- Every device on a distributed ledger network stores a copy of the ledger. These devices are called nodes—a network can have any number of nodes. Any changes to the ledger, such as moving data from one block to another, are recorded across all nodes. Because each node has a copy of the ledger, each one publishes its version with the latest transactions.
- Every blockchain is a distributed ledger but not the reverse (referring to record keeping and validation within)

Source: Nevil (2024) "Distributed Ledger Technology (DLT): Definition and How It Works" Investopedia.com

Tensions Between Individualized Versus Community Perspectives

Tensions Between Individualized vs. Community Perspectives

- Central bank accounts and RTGS payments
- Pacioli, the father of accounts, money as a liability to the community
- Community currencies

Central Bank RTGS of Payments: Store of Value vs. Medium of Exchange

- Bech and Garratt (2003) "The intraday liquidity management game,"

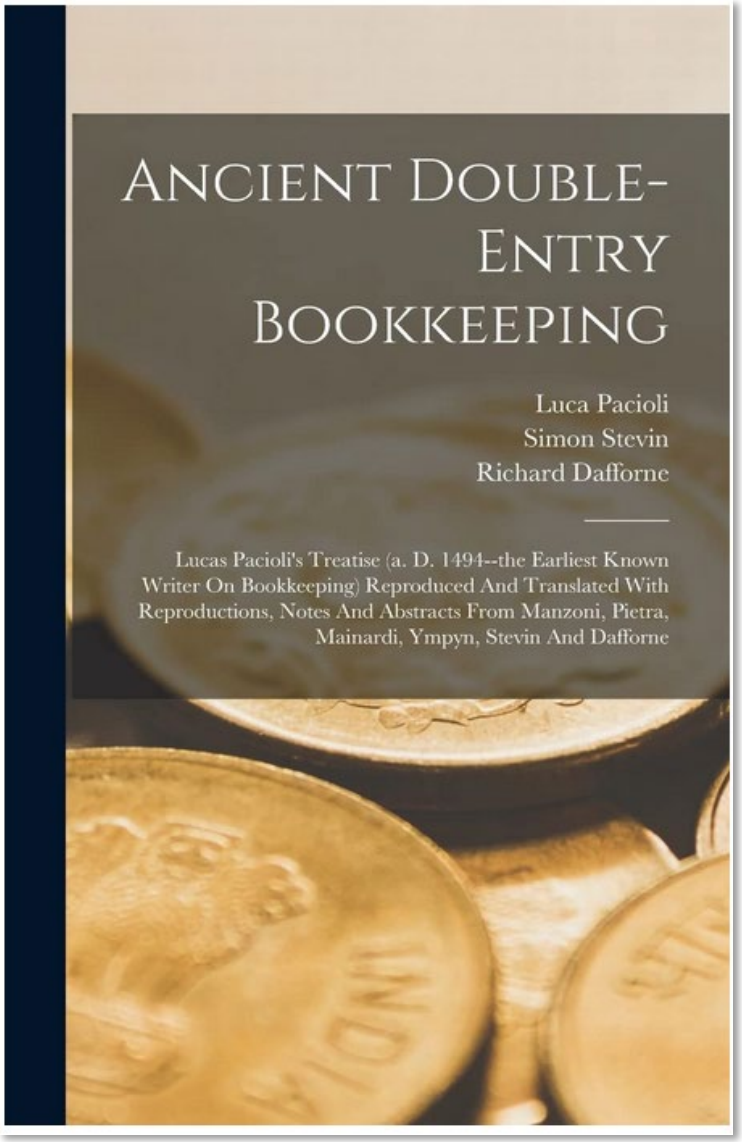
- Goldstein et al (2023) "Payments, Reserves, and Financial Fragility"

Abstract

Are payments inherently fragile, and if so, why? We propose a theory of payments that highlights a conflict between the roles of medium of exchange and store of value. We posit that payments must involve the reciprocal transfer of a scarce reserve good, which holds value for other non-payment purposes. The theory demonstrates that agents make payments only when reserves are abundant enough. Otherwise, history-dependent equilibria arise in which an agent's payment decision depends on the payment history of other agents within an equilibrium. The theory

Pacioli, the Father of Accounts, Money as a Liability to the Community

- The history
  - A problem with negative numbers
    - Until the Renaissance, negative numbers were thought of as absurd, despite Chinese, Arab deep roots in algorithms and algebra
  - What does it mean to hold negative amount of a good?
  - Yet a difference operation is standard in algebra
    - Delivers negative numbers
- Here, related, money as a liability to the community, as in "must give" back, to accomplish an objective
- The reference is not to the "owner" but obligation to the other party, owe them something



Definition of a Journal Entry

CHAPTER 11.

THE TWO EXPRESSIONS USED IN THE JOURNAL, ESPECIALLY IN VENICE, THE ONE CALLED "PER," AND THE OTHER "A," AND WHAT IS UNDERSTOOD BY THEM.

As we have said, there are two expressions (*termini*) used in the said Journal; the one is called "per," and the other is called "a," each of which has a meaning of its own. "Per" indicates the debtor (*debitore*) one or more as the case may be, and "a," creditor (*creditore*), one or more as the case may be. Never is any item entered in the Journal which also is to be entered in the Ledger, without preceding it by one of the two expressions. At the beginning of each entry, we always provide "per," because, first, the debtor must be given, and immediately after the creditor, the one separated from the other by two little slanting parallels (*virgolette*), thus, //, as the example below will show.

- Money as a liability to the community

EXAMPLE OF MAKING AN ENTRY IN THE JOURNAL.

FIRST. November 8, MCCCCLXXXXIII in Venice.

Debit 1.

Credit 2.

Line of the debit.

Per cash // A—Capital of myself so and so, etc. In cash I have at present, in gold and coin, silver and copper of different coinage as it appears in the first sheet of the Inventory in cash, etc., in total so many gold ducats and so many silver ducats. All this is our Venetian money; that is counting 24 *grossi* per ducat and 32 *picioli* per *grosso* in gold is worth: L.____ (*Lire*), S.____ (*Soldi*), G.____ (*Grossi*), P.____ (*Picioli*).

Source: Translation of Pacioli's "Ancient Double Entry Bookkeeping"

What Is the Larger Purpose of the Database? Do Not Lose Sight of the Ultimate Goal

- Jain, Townsend and Wang "Timing lumpy investments with informal bridge loans and clunky formal loans: Evidence from Thailand"
- Amberg, Jacobson, Schedvin and Townsend (2021 JPE) "Curbing Shocks to Corporate Liquidity: The Role of Trade Credit"

Community Inclusion Currencies

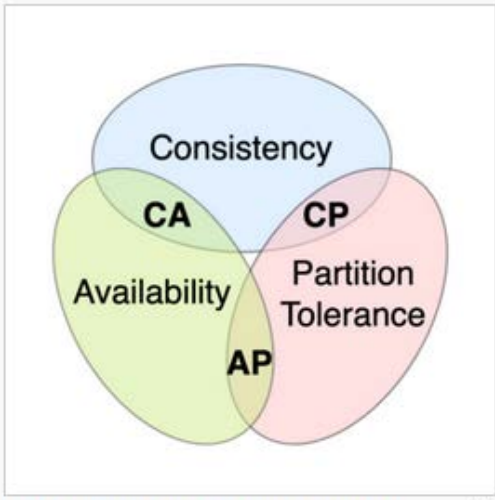
- CICs are operating as a medium of exchange that can only be used within a certain community or network. Mutual credit network is another term for CICs because their participants effectively give each other (interest free) credit. For example, sold goods but did not yet get goods in return, and instead got the community currency.
- Put differently, sold goods and got community currency with an obligation to buy the production from others.
- Others have an obligation to accept it
- Related, designed with certain incentive structures that encourage holders to spend the currency instead of hoarding it.
- CICs are used by a growing number of communities, all located in informal settlements or slum areas … more than 50 communities in Kenya and South Africa … the most well-known being Sarafu
- Essentially the voucher acts as a promissory note, a promise against future production of others. So a selected self-governing community of micro-businesses was committing their future production into a voucher and accept to trade with each other using these vouchers.
- Given it's only businesses and individuals signed up to the program that would accept the vouchers as payment, this locked the injected value into that network.
- The end result is the value circulated for longer in the targeted community, giving the businesses and the local economy a better chance to flourish.

Source: De Meijer (2023) "Sarafu: Crypto Currency for Rural Communities" treasuryXL.com

A Technical Limitation of Blockchains

- The CAP theorem
  - Impossible to have all of consistent, available, and partition tolerant
- Evolution of ecosystems
  - Coping with the CAP trilemma in practice

The Cap Theorem



CAP theorem Euler diagram

In database theory, the **CAP theorem**, also named **Brewer's theorem** after computer scientist Eric Brewer, states that any distributed data store can provide only two of the following three guarantees:[1][2][3]

Consistency

Every read receives the most recent write or an error. Note that consistency as defined in the CAP theorem is quite different from the consistency guaranteed in ACID database transactions.[4]

Availability

Every request received by a non-failing node in the system must result in a response. This is the definition of availability in CAP theorem as defined by Gilbert and Lynch.[1] Note that availability as defined in CAP theorem is different from high availability in software architecture.[5]

Partition tolerance

The system continues to operate despite an arbitrary number of messages being dropped (or delayed) by the network between nodes.

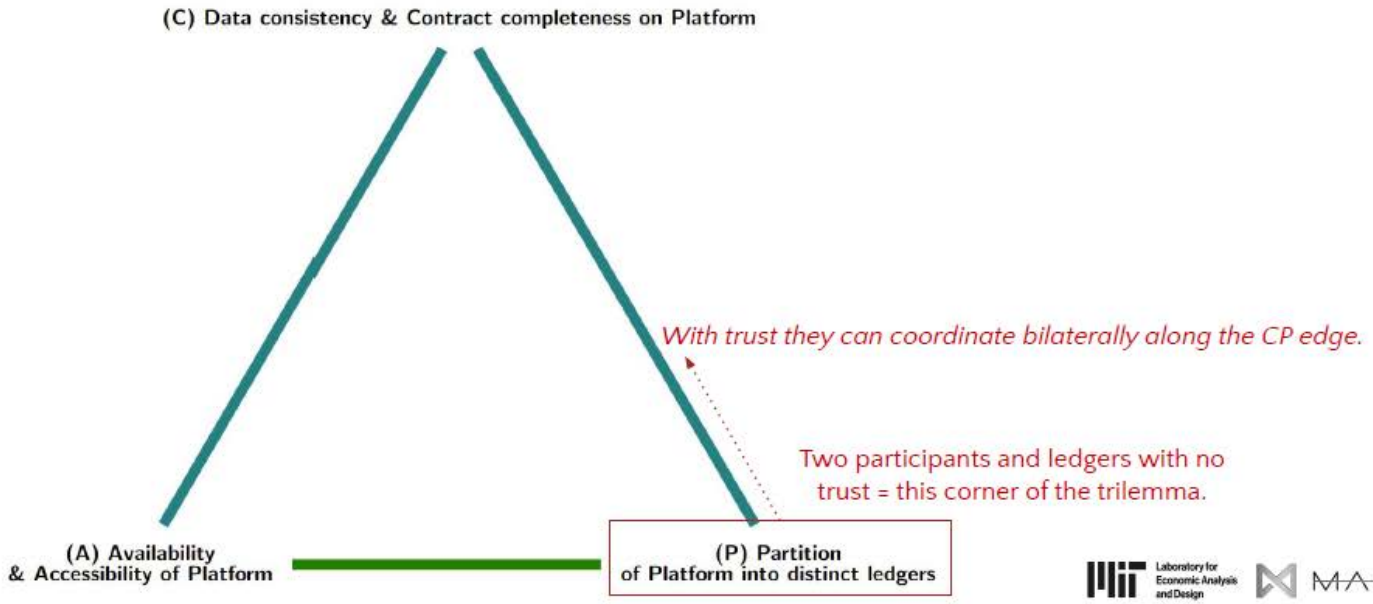
When a network partition failure happens, it must be decided whether to do one of the following:

- cancel the operation and thus decrease the availability but ensure consistency
- proceed with the operation and thus provide availability but risk inconsistency. Note this doesn't necessarily mean that system is highly available to its users.[5]

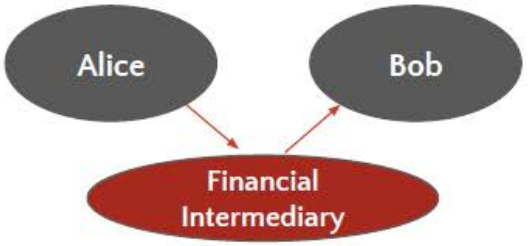
The Evolution of Ecosystems: The CAP Trilemma Extended

History started with entities not trusting each other, each one with own ledger

- Here we simplify a financial market ito just two participants and ledgers *(e.g. balance sheets on databases)*. Easily generalizable.
- **No trust** means no ways to trade. **With trust**, the two participants can try to coordinate bilaterally (*eg via nostro/vostro accounts*)



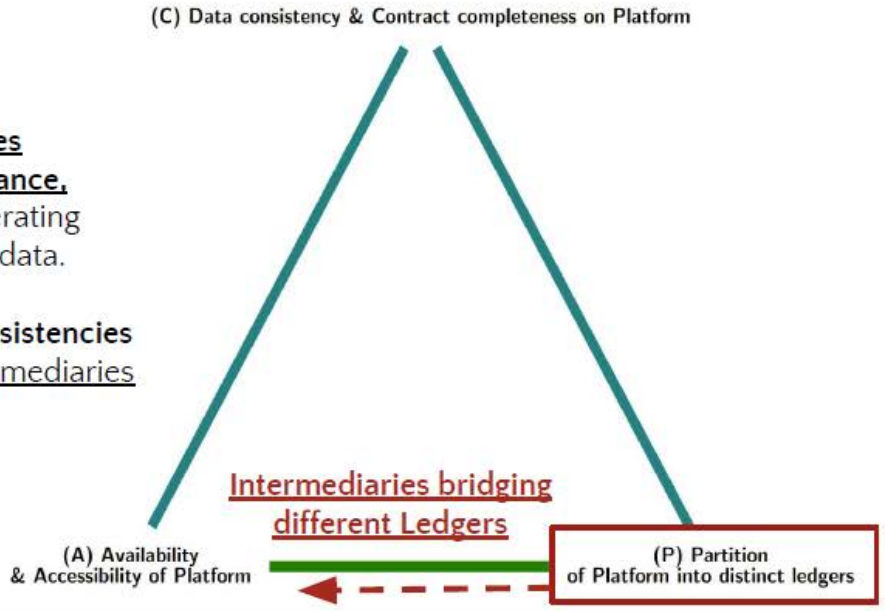
Model 1 - Common Ledger: Intermediaries bridge trust and offer services



- An intermediary *(e.g. a third bank)* can build trust amongst the two participants (via its own balance sheet to take on risks), and provide and "availability" *(see below for availability meaning)*.

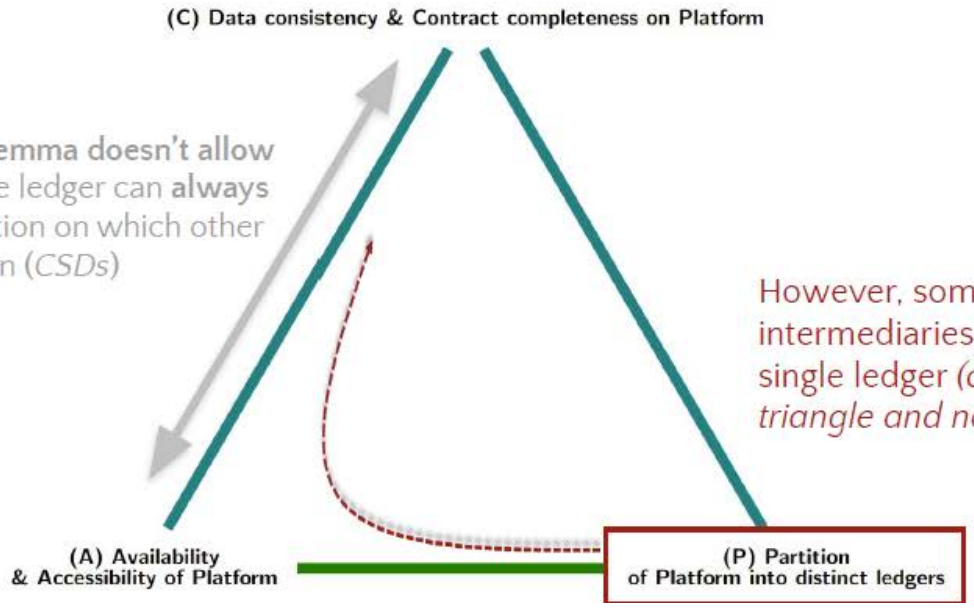
The A-P edge in the trilemma gives (A)vailability and(P)artition tolerance, allowing services to continue operating despite network splits / different data.

However, this may result in **inconsistencies across ledgers**, hence needs intermediaries for reconciliation.



Model 2 - Single Ledger: Internalizing positive externalities via a single ledger

- Functions are mutualized on one single ledger *(e.g. issuance on a CSD, novation on CCPs, reporting on Trade repositories, CB reserves on RTGS).*
- for instance, CSDs are (*imperfect*) single ledger platforms. *Imperfect as intermediaries still help for recording there* (ex: only brokers are on US CSD)



The C-A edge in the trilemma doesn't allow **partitions**, but an unique ledger can **always** give consistent information on which other Ledgers can be based on (*CSDs*)

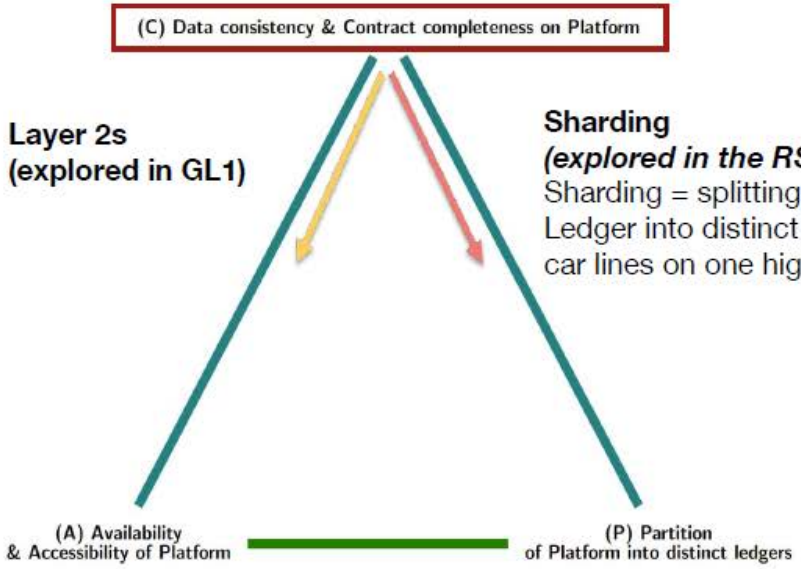
However, some *CSDs* still rely on intermediaries for data so are *imperfect* single ledger *(curved arrow inside the triangle and not on the edge)*

Model 2 - DLT-based Single Ledger Platform: a new paradigm

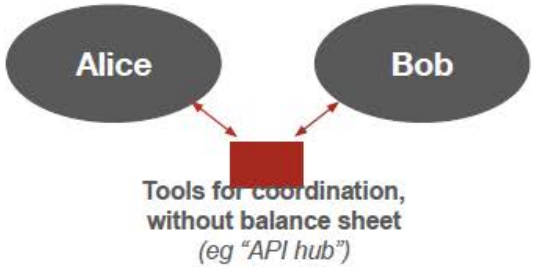
- DLT designers radically chose a single shared ledger as a starting point to reap all benefits from single ledger platforms, and thought about interoperability after

Building *on top* of a single ledger

Building *besides* a single ledger (eg Avalanche and Cosmos)



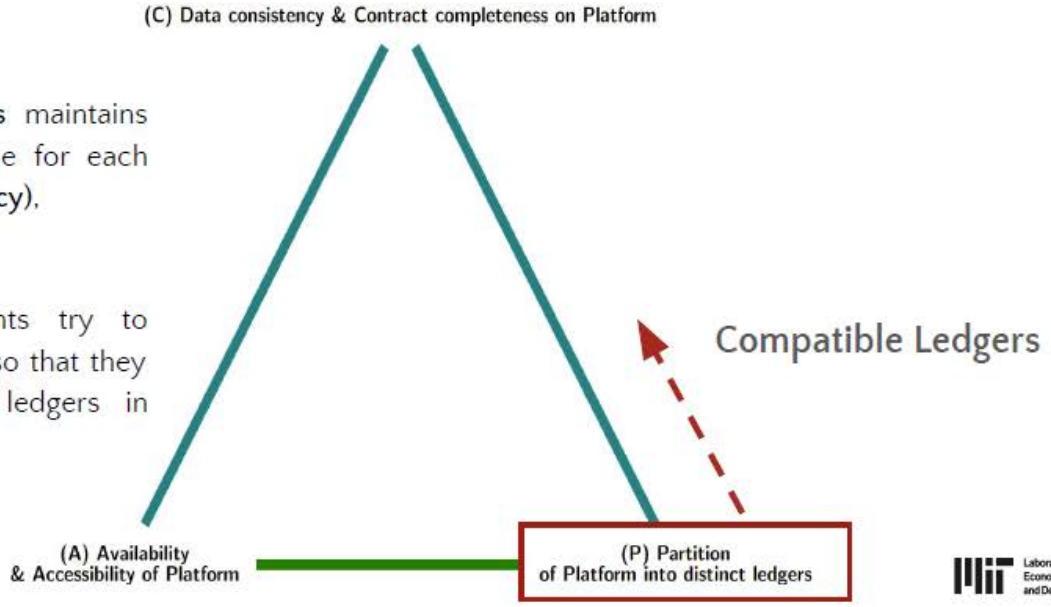
Model 3 - Compatible Ledgers: bilateral trust, with help from design



- The 2 participants trust each other and try to **coordinate only via technology or legal rulebooks**, without balance sheet intermediary *(ex Visa, SWIFT, Canton…)*
- Correspondent banks are also an example of this, coordinating via nostro/vostro, but also pre-existing systems linked together (T2 in EU, Nexus…)

The **C-P edge** or **compatible ledgers** maintains distinct ledgers or sub networks, one for each participant (so creating also more **privacy**), but this means data **inconsistencies**.

When trade is needed, participants try to coordinate actions *(via tech or legal)* so that they can each update their respective ledgers in coordinated fashion.



Current Difficulties

- Legacy technology
- Trust and fraud
- Unmeasured currency
- Data silos
- Inconsistent collection mechanisms

Legacy Technology

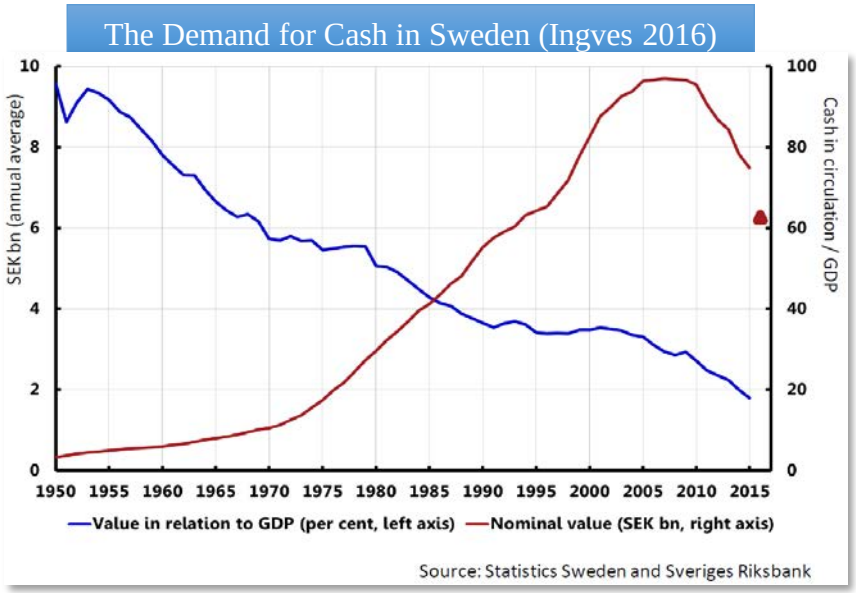
- Kansas City Federal Reserve Bank
  - Alcazar et al (2024) "The Role of Core Banking Services Providers in Facilitating Instant Payments"

Depository institutions (DIs) must make significant changes to how they manage payments to offer their customers instant payments. Some features of instant payments, including around-the-clock services and instant accessibility to funds, require real-time core and payment processing, automated connectivity to the instant payments system operators, and upgraded customer-facing solutions. To accommodate instant payments, many U.S. DIs—including banks and credit unions—may need to modernize their core banking systems and outsource some functions, requiring support from their core banking services providers (Alcazar and others 2024a). This *Payments System Research Briefing* explores the role core providers play in facilitating the implementation and broad use of instant payments and examines the implications for the U.S. payments and banking industries.

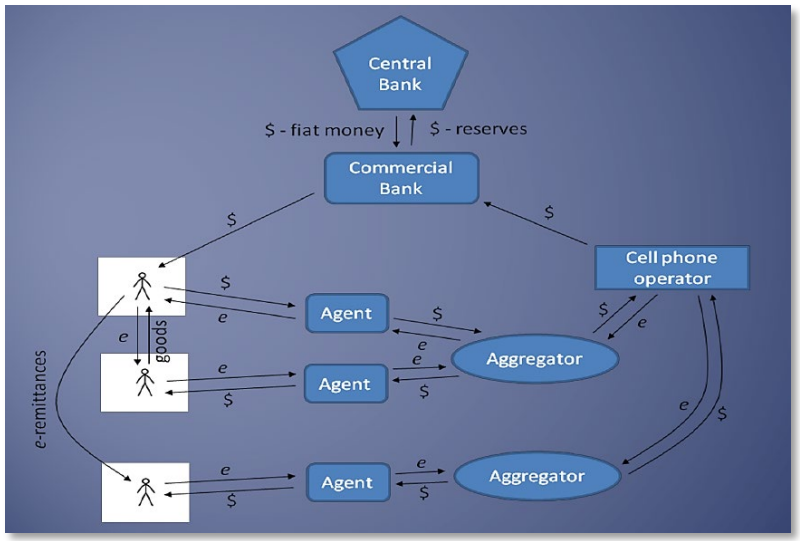
Trust and Fraud

E-Payments: Two Examples

- Sweden, almost no currency left



- Phone credits and transfers, cash in and out
- Coexistence of Payments Devices: Fiat money, Kenyan shillings
- Remittances, e-transfers of value, migrants



Limitations of Trust, Centralization and/or Decentralization Infrastructure Issues

- Trust is less obvious than it might seem
  - Taking into account the larger financial system, banks holding Safaricom accounts, and hence customer shilling accounts, subject to runs in Kenya
- Contrast: Token transfer systems rely on distributed ledgers, with immutable records and some kind of consensus validation
- Irony: Cryptocurrency exchanges are largely built as traditional systems with (trusted) brokers or centralized exchanges, in contrast to the tokens themselves- and trust broken
- FTX Diverted $200 Million of Customer Money for Two Venture Deals That Caught the SEC's Attention" (2022) NBCnewyork.com
  - "FTX … made two $100 million venture investments using customer funds through an FTX subsidiary…."

Unmeasured Currency

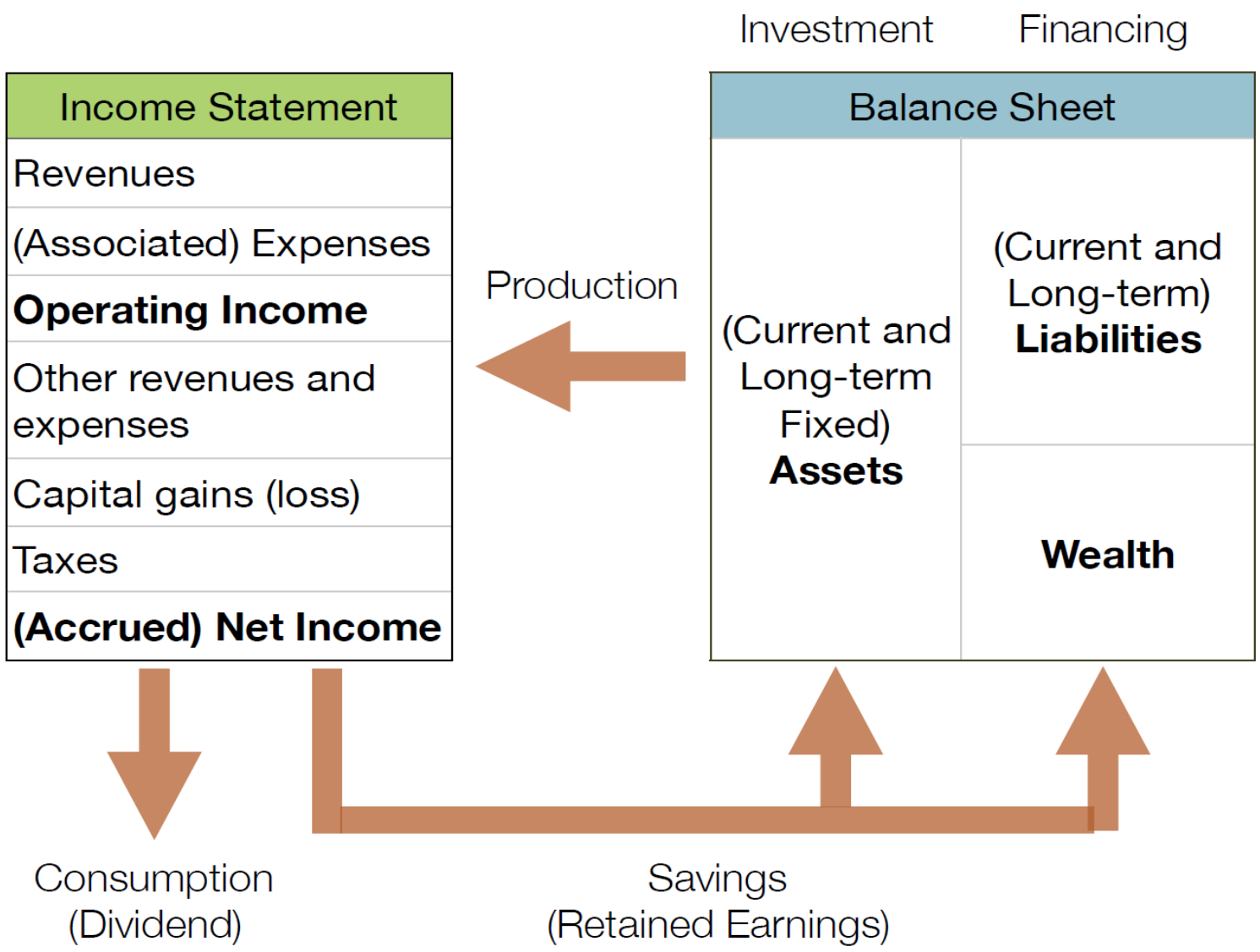
- Alvarez, Pawasutipaisit and Townsend (2023) “Currency in Village Economies: Large Welfare Losses from the Mismanagement of Petty Cash”
- FRB-Boston and MIT DCI “Project Hamilton Phase 1 Executive Summary” (2022) Bostonfed.org
  - “In light of continued innovation in money and payments, many central banks are exploring the creation of a central bank digital currency (CBDC), a new form of central bank money which supplements existing central bank reserve account balances and physical currency. CBDCs could exist in various forms depending on a central bank's objectives, including a general-purpose CBDC that can be made available to the public for retail, e-commerce, and person to person payments.”
  - “The processor's baseline requirements include time to finality of less than five seconds, throughput of greater than 100,000 transactions per second, and wide-scale geographic fault tolerance.”

Data Silos

- Product apps within digital financial service providers

Inconsistent Collection Methods

Collection Methods: How It Should Be Done



Inconsistent Micro Surveys

SST (2016): Estimates of cash flow (*indirect*)

(Cash defined as Current Assets)	PSID 2010-2012	CES 2011-2012	SCF 2010-2013	HRS 2010-2012	SIPP 2010-2011	CPC Oct-12
Net income (+)	65,350	60,971	81,856	70,082	61,431	74,756
Adjustments:						
Depreciation (+)	0	0	0	0	0	0
Change in Account Receivables (-)	0	0	0	0	0	0
Change in Account Payables (+)	0	0	0	0	0	0
Change in Inventory (-)	0	0	0	0	0	0
Change in Other (not Cash) Current Assets (-)	0	0	0	0	0	0
Consumption of Household Produced Outputs (-)	0	0	0	0	0	0
Cash flow from Production	65,350	60,971	81,856	70,082	61,431	74,756
Consumption expenditure (-)	-43,766	-49,194	-28,850	-45,073	-251	-90,284
Capital (durable goods) expenditure (-)	0	0	0	0	0	0
Cash flow from Consumption and Investment	-43,766	-49,194	-28,850	-45,073	-251	-90,284
Transfers to/from Long-Term Investments	-362	0	1,231	0	0	na
Lending (-)	0	-151	1,359	50	543	na
Borrowing (+)	4,230	-2,438	-4,556	-3,757	-2,299	0
Net Gifts Received (+)	0	0	0	0	0	na
Cash flow from Financing	3,868	-2,589	-1,966	-3,707	-1,756	na
Change in Cash Holding (from Statement of Cash Flows)	25,452	9,188	51,040	21,303	59,424	-15,528
Change in Cash Holding (from Statement of Balance Sheet)	3,091	17,770	3,843	1,678	-2,095	164
Cash flow error	22,362	-8,582	47,197	19,625	61,519	-15,692
Error (% lagged Current Assets)	25%	18%	37%	16%	51%	na

Inconsistent Macro Aggregates

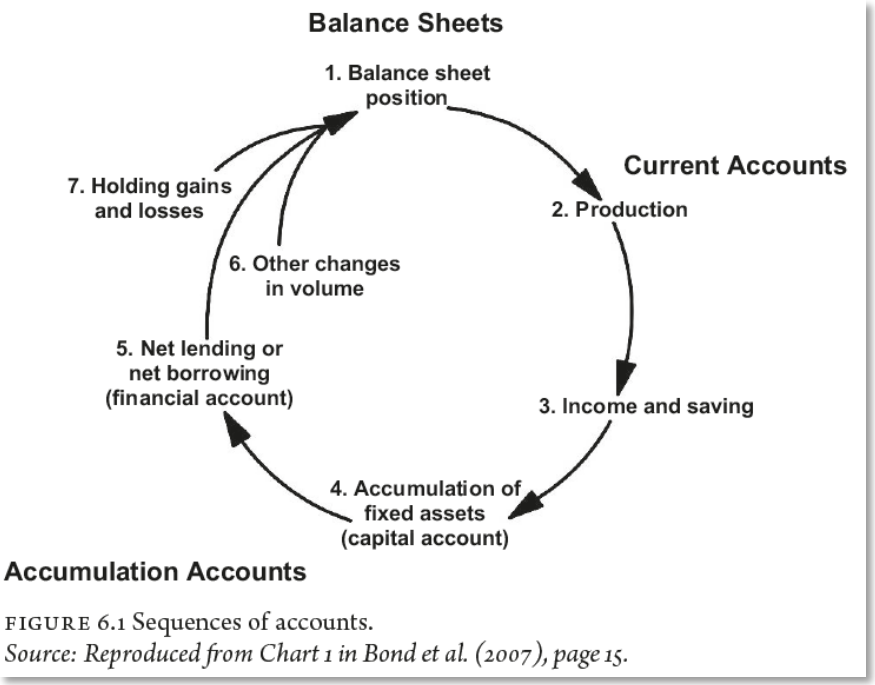


FIGURE 6.1 Sequences of accounts.
Source: Reproduced from Chart 1 in Bond et al. (2007), page 15.

TABLE 6.2. Discrepancy between the capital account measure and the financial account measure for households and nonprofit institutions serving households (in billions of dollars).

	Line	*2019*	*2020*	*2021*
Capital account	38	1,159.5	2,678.5	1,857.9
Financial account	77	1,840.0	2,996.1	1,627.9
Statistical discrepancy	82	−680.5	−317.6	230.0
% Discrepancy		−45.37%	−11.19%	13.20%

Source: Table S.3.a, Integrated Macroeconomic Accounts for the United States, Bureau of Economic Analysis; authors' calculations.

Progress in Mapping Economies and Next Steps

Progress in Mapping Economies and Next Step

- Progress in mapping
  - Creating village, regional, and national income and product accounts, NIPA, and flow of funds accounts
    - Production accounts from the income statement
    - Savings investment accounts from changes in the balance sheet
    - Aggregate up to village level
    - Balance of payments – including tracking currency
- Next steps
  - Construction of disaggregated consistent accounts for the US
    - See chapter 7 in Paweenawat and Townsend (2024) “Inequality and Globalization: Improving Measurement through Integrated Financial Accounts”
  - From the ground up, with consistent collection and links to e-accounts