

[SQUEAKING]

[RUSTLING]

[CLICKING]

ROBERT

So this is the second lecture, although the first full presentation of a body of material rather than just a summary.

TOWNSEND:

And in particular, we're going to talk about blockchains as a database. And the underlying themes here are a unified view of distributed ledgers and financial accounts, putting them in one bin, so to speak. Distinct views of money and the larger community perspective. So this is an outline of what we're going to do.

Talk about blockchain as a database. Talk about the financial accounts. Take a broader view of the blockchain. This tension I mentioned last time between individual and community perspectives. Then some technical limitations of blockchains also reflected in current difficulties and some progress in mapping economies and next steps. So that's the overall outline of the lecture. And then we have the individual sections within.

Blockchain is a special form of the database. We'll talk about the creation of Bitcoin, an incorrect association of blockchain with money, peer-to-peer exchange certificates, and central bank reactions to money and ledgers.

OK, so here's a definition. Any data structure used to store information can be considered a database. A blockchain technology is a ledger to store information about transactions. So those are the objects in the database. And hence a blockchain can be considered to be a database and nothing more or less.

Data is stored in signed blocks. The blocks are linked to each other, creating a chain of immutable, interconnected data entries. So that is an important mechanical aspect of how the blockchain database works. In particular for Bitcoin, for example, each node is trying out a bundle of the set of incoming transactions since the last committed block in order to form a new block. And these blocks consist of a time stamp when the block is created, a nonce used for proof of work as a reference to a previous block, the hash of it, and a list of transactions.

Pause a minute. We're going to develop the material to go back and describe nonces, and hashes, and so on. But still I wanted to get the ingredients on the table here. So this is how you create new blocks from previous blocks. And this is a curious item. The blockchain for Bitcoin can be thought of as a state machine. But actually it's not giving you the current state automatically. You have to go back to the whole history of transactions since the genesis block in order to get the current state, which is a bit odd, but that's the way Bitcoin was constructed.

OK. Oh, and then there's even more detail up here. Just anticipating more material on encryption and so on. So these messages are encoded with public and private keys. The keys ensure no one else can transact on someone else's ID, impersonating a node. I guess I should add the node is like a computer account. It's not a personal identifier. So you know who the node is but not who's operating the node.

The keys ensure no one can transact on someone else's ID. There's a commitment to the transaction, so it can't be undone later. And these transactions are, again, just transfers of, quote, the coin from one account to another. And it's the transactions that are being recorded on the ledger in groups. OK? So back to the creation of Bitcoin.

It was registered August the 18th, 2008. A white paper came out by someone under the pen name of Satoshi Nakamoto. The title of the white paper is revealing. *A Peer-to-Peer Electronic Cash System*. So remember the peer-to-peer aspect. And open-source code was released in January of 2009. We still don't know who Nakamoto is or was, although there's a lot of speculation about it.

January 3, 2009, Bitcoin network was created when Nakamoto mined the first block, known as the genesis block. And nine days later, Hal Finney received the first Bitcoin transaction from Nakamoto. And five months later, in May, there was a commercial transaction where Bitcoin was used by a programmer to buy pizza, called Bitcoin pizza day, and a summary of sorts.

Arvind Narayanan, a computer scientist at Princeton, is saying that all the individual components of Bitcoin originated in earlier literature. There's really nothing original about each of the pieces. But their complex interplay resulted in this Bitcoin, the first decentralized, Sybil-resistant, Byzantine fault-tolerant digital cash system. And we'll get into, again, Byzantine fault tolerance. I'm not today getting into the verification or validation algorithm of the blocks. Just reminding us all that is part of the system.

Now, again, a peer-to-peer electronic cash system. So it sounds like money, and it sounds like it's peer to peer. So I discovered this work of Paul Krugman, the babysitting economy, where there is a peer-to-peer exchange going on. It's an exchange of certificates. So the idea is in 1970s, there was a group of staffers, young couples with congressional connections. They agreed to babysit for one another, so no need for a babysitter. The parents are doing the babysitting, and the idea is it's mutually beneficial.

The couple with children doesn't mind necessarily having a few more kids in the house. And they earn a certificate for the number of hours babysitting someone else's kids. And likewise, they're now armed with the certificate. So they on an evening out find another parent who would receive those certificates in exchange for providing the babysitting service.

So it's kind of like money, but they're certificates. They're certificates earned by providing a service and then can be used subsequently in exchange. Well, cutting the story short a bit or a lot because there's a whole book about it, for complicated reasons, involving the collection and use of dues paid in script, these coupons in circulation became quite low.

Couples were anxious to add to their reserves of the certificate. And they're reluctant to run them down by going out where they would pass them along of necessity to someone else. But one couple's decision to go out was another chance to babysit. So not going out means others aren't babysitting, so they're not earning coupons. And the whole babysitting market collapsed in a recession.

Eventually, more script were issued to compensate for this, creating a different problem, inflation. So Krugman says this story changed his career, changed his life. This is when he started thinking deeply about monetary theory and business cycles and so on. I have this here just to begin to be a bit provocative in terms of thinking about what do we mean by cash, what do we mean by money. I mean, clearly these certificates function as a kind of money but with a purpose, namely the babysitting platform. OK.

Central banks did not take kindly to the invention of Bitcoin. And I'll just editorialize. A bit later, Facebook proposed Meta, and that was like the ultimate threat. So you'll see quotes. This is 2018 from Hyun Shin. "Cryptocurrencies cannot scale with transactions demand, are prone to congestion, and greatly fluctuate in value." Part of that is an allusion to the validation algorithms we haven't gone into in detail yet.

His quote continues. "Overall, the decentralized technology of cryptocurrencies, however sophisticated, is a poor substitute for the solid institutional backing of money." However, and due to Meta and so on, about 80% of all central banks in the world are exploring their own digital currency. It's kind of maybe a preemption strategy so that they retain a central role in money issue, although the case for why central banks are doing it is sometimes less clear.

So that's 2018. By 2023, Augustin Carstens and the BIS staff issued this paper called *The Future Monetary*

System:

From Vision to Reality. So this is essentially a year and a half ago. The quotes are revealing. 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 edge of communication networks in separate proprietary databases or ledgers. These databases are patched together via third-party messaging system so that messages have to be sent back and forth in a complex web of bilateral links, all following a separate path from one corresponding to money and the other to financial assets.

Cross-border transactions are even worse. The best way to knit together transactions and operations among markets and financial services is to bring them into a shared programmable platform. This is what the paper labels as a unified ledger. But still in the paper, the view remains that central bank money is somehow special. They refer to it as the singleness of money. Well, they mean the singleness of a central bank, fiat money. And we'll revisit this idea through the lens of monetary theory.

But let me just say, if there is such thing as a singleness of money, then what do we do with all the different monies existing issued by central banks, each country one at a time? It's inherently a multiple money world. Do we need to create some super currency? And people have proposed it, that the IMF should issue, for example, a single convertible currency.

However, in theory, you don't need it in the sense that in Walrasian equilibria, where the objects being traded are the different countries' fiat monies, all you need is a unit of account. You don't need the store of value or medium of exchange role to set up a cross-border platform. And the reference here is to this IMF work.

So lots of important and interesting views and controversies in this literature. But the point of this slide mainly is that it's no longer "Bitcoin is bad." People are recognizing the platform aspect of the blockchain and even proposing that the domestic and international monetary system be based on this is technology.

OK. So let's think about the twin cousin here, financial accounts. Financial accounts are also a sort of database. In this book, we enumerate how even for households to think of households as corporate firms using standard financial account constructions of the income and cash flow statements and the corporate balance sheet. So they come in triples, basically. You've got a cash flow, income statement, and a balance sheet. Those are the standard financial accounts. And then you get the ledger interpretation of money, which is as a liability of the central bank.

So back to the transactions. In Bitcoin, we're talking about the exchange of the coins recorded in blocks and validated. Here we were running a monthly survey, and we asked the households a lot of questions. So for example, what is the total amount of cash payments you received since the last interview for doing this job? This is pertaining to wage income, including blah, blah, blah, blah.

So they got the wage. So that's an increase in cash. OK. Where does it enter? Cash is an asset, so it enters as a change in the balance sheet. It's also revenue received for supplying labor. So that enters on the income statement. The same transaction also enters on the third account count, net income from cash inflow.

Then you have cash used to pay a telephone bill, which is like outgoing decrease used for consumption. It's a cash outflow. You could deposit cash in a production credit group. That's like changing, getting rid of your cash and getting an equivalent credit in value. So you're swapping assets. No implication for the income statement. Every single transaction that they report to us has been systematically put into the financial accounts. And we have a way, you'll see, of checking to make sure we're doing it consistently.

And the rest is kind of fun. What happens when you sell little animals for cash? What happens when the mature animals die? You've got capital appreciation and depreciation and so on, but I think it's enough. The book goes on for three or four pages of tables, but you get the idea. The basic block is the transaction. Then where to put it-- in this case, the financial accounts-- as a database are three accounts. So we're organizing the transactions into those three accounts. OK.

Here's a view of the cash flow account. So what we want is cash flow from production. Now, it's a little more complicated than you might think. The basic idea is that when you use cash-- say, currency-- to buy inputs, that is an outflow of cash. And when you sell your crop, for example, for cash, you have an inflow, a cash inflow.

This starts, however, with an income statement, which is on an accrual basis. So if you sell something and get an account receivable, that counts as income, but you didn't get the cash. You got a promise to pay, that someone would pay you. So we actually have to subtract that off from income in order to get the cash implications, otherwise we're overcounting. And similarly for inventory, and here's consumption.

Consumption of household-produced outputs. They just grew the crop and ate it, you know. So there's no implications for cash, but it's still revenue. All right. So we get cash flow from production. Then you can spend cash on consumption goods or spend it on investment goods. Cash flow from consumption and investment. Then we have the financial side, change in deposits at financial institutions or other institutions, borrowing and gifts. So we have cash flow from financing.

Lots of details. This stuff turned you off very quickly because there's so much to absorb. But the main thing is we're classifying cash flows into cash flows from production, from consumption, investment, and from financing. Also, as a check, the change in cash holdings from the statement of cash flow-- this statement should also be reflected in the change in cash on the balance sheet. So that's the obvious check. Rarely done. We did it in order to make sure we hadn't missed transactions, and it's very much in the spirit of double-entry bookkeeping. But I'll come back to this-- here, the lack of discrepancy. But in other cases, the discrepancies are going to be glaring. We'll come back to that later.

So just to remind you, that household is a wage-earning household in Lopburi, Thailand. And this is the income statement of that household. Most of the revenue is coming from labor. There's a few bits and pieces of other things. The revenue is offset in part by expenses. And what's left, if it's positive, can be either used for consumption or saving.

The saving part is, of course, the increment if it's positive in assets on the balance sheet. And here's a balance sheet, which in this case a lot of it is cash currency. US accounting, you say "cash," but we actually mean by that demand deposits at commercial bank. Here, I'm just referring to the currency, the paper stuff.

Total assets on the left is equal to total liabilities and net worth on the right. So the balance sheet balances on both sides. So blockchain in the broader view as per the outline. Single-dimensional as in money for payments versus multi-dimensional as in, for example, contracting. So we're embracing for sure because that's the nature of it, the multi-dimensional aspect of the blockchain and, for that matter, of the financial accounts.

I guess I featured blockchain here and not also financial accounts only because there's so much misunderstanding in my view of what the blockchain really is. So it's not just about money. And you can see this with payment matrices that capture velocities. And then we'll cover individual versus common accounts and finally have a formal definition of a distributed ledger. Blockchains are a distributed ledger.

So multi-dimensional is a database of many objects and can include contracts. So we can create payment matrices. Money would be an object that appears frequently in exchange or, alternatively, is an object that has a high velocity. It's an object where the amount traded typically divided by the stock of it is large. In other words, there's a lot of turnover in the stock. Most of the stock changes hands from one period to the next. That's a high-velocity object. And ipso facto it's almost surely something appearing frequently in exchange.

That's the monetary theory definition of money. That's really the definition, if we had to pick one, that we should be using in our conversations, otherwise we're going to get confused if not embroiled about the controversy of whether Bitcoin is a cash, money or not, and are going to be inextricably wedded to the financial accounts point of view that one or more objects in the financial accounts are, quote, "the money."

This definition covers both blockchains and financial accounts. And there can be multiple monies, and they can coexist with things that do not appear frequently in exchange. So here's an example of Village India with my co-author, Yung Jae Lim. So there's actually quite a lot going on here. You've got goods or services going out from a household or goods and services coming into the household. So conventionally, you would think money goes out - you use money to buy something. And indeed that is typically the case. Money is used to buy grain, clothing, livestock, jewelry, and so on.

Then we have these IOUs. IOUs are a promise to pay but not the money like you're going to owe. You have an account payable. Grain. OK, so now we get to something more interesting. Grain can be used to pay labor. This, of all these row-column items, is a fairly large number. So in these villages in India, people work for compensation. The compensation comes in form of the grain as a result of growing the crop or inventory that they're carrying around. It's a dual monetary economy. You've got the real good-- some people say barter-- coexisting with the more traditional definition of money as currency.

A couple of clarifications. Labor going out and money coming in. This table is mixing up households who are purchasing stuff with producers who are selling stuff, selling labor or farmers selling grain, for example. So that's the reverse transaction. And the other thing-- it's a little confusing here-- this is an aggregated account. It's not household A or something in Thailand. It's aggregating up over all the transactions we see in a village.

This is the US. It's created by the Boston Fed in some joint work. A long story short, I came home from Thailand and collaborating across the river with the Boston Fed. They were already collecting payments data, as you will see. And so this led to the creation of analog financial accounts for US households. So this is the statement of cash flow, but let me say it's actually a statement of account flows, not just cash. It distinguishes items within cash.

So we do have production flows, flows coming from production, flows coming from consumption and investment, flows coming from financing. And we have a check here on the consistency. So those are the standard items I showed you previously in the statement of cash flow.

Here, the featured aspect of it is deposit inflows. So we're going to distinguish under, quote, deposits currency, demand deposits, debit accounts, foreign currency, other things OK? Multiple accounts for a given household, for example. And you can see from currency-- so for example, this is off the diagonal from currency into a demand deposit. That's a deposit of cash into the bank.

Deposits from non-financial accounts, from foreign currency. So again, from and to are always Xed out here because they're on the diagonal. Otherwise one payment account is being converted to another one or vice versa. And likewise, withdrawals from one account-- say the currency account-- into demand deposits. So there you're cashing out your demand deposit.

So multiple monies. Multiple account flows. Not everything is used by a given household. But on average this is what US households are doing. You could say that many of them are, in fact, directly or indirectly a liability of the Federal Reserve. Households don't have direct access to reserve accounts at the Fed. They do have access to demand deposits, which are-- and the banks in turn who are issuing the demand deposits have accounts at the Fed. So there's kind an indirect backing, but it's not necessary that everything here be linked to the US Federal Reserve.

You can see this principle would apply for households transacting in cryptocurrency.

STUDENT: A quick question. The flow errors here seem massive between the account flows and the balance sheets. That has to do with the difference in timing, that balance sheets might only be available annually in the--

ROBERT TOWNSEND: Lots of different factors. I'm glad you reminded me to emphasize this. So there was nothing automatic about creating consistent accounts. You have a database created for different purposes. This is coming from the Boston Fed's survey of consumer payments. And it wasn't created with the idea of using it for consistent financial accounts. So that shows up here. So something's big, typically missing. I have even more egregious examples.

Individual versus common accounts. So this is another thing to think about when you think about blockchain and so on. Call it consensus financial accounts. Back to the Thai villages, where we, the enumerators, were recording cash transaction and other transactions in the previous month. Save of i with j . This is similar to Bitcoin. There's an initial state in Bitcoin, who owns the coins, modified by a transaction that alters the state.

Paper currency is like that. Currency is held as a balance on the part of the household, although it is not public, obviously. It's private to the individual unless they show you. And currency is, of course, an actual portable physical token. It's not an electronic entry.

I kind of wish Bitcoin had not said it was a coin, because it's clinging to this representation that we've seen so often when we talk about monies. Bitcoin isn't really a coin at all. It's just code. It's an organized database with transactions. But anyway, currency is clearly literally a coin if it's not paper. And here it's both. And you could imagine that these transactions of individual households-- say if household i was household j -- are the transaction that ought to be recorded at the individual level but also could have been, if it had been like Bitcoin database, recorded on a common ledger to begin with.

So with a UROP with his help, Chad, looked at the Townsend Thai data. And we started to create, well, a common distributed ledger, but the data weren't collected with that purpose in mind. So this is like hindsight. So we have the observed transactions. Create a ledger. It could have been a common ledger. That would have consisted of the enumerators collecting the data each month, and then pooling the record transactions, and validating or deciding which transactions are valid, and then putting it on the common database, which would then be redistributed to the households.

Of course, we weren't doing that. In retrospect, we're just organizing individual accounts and not sharing it publicly or with other households. But we could have done it this way in principle, and we would have a common integrated database, a distributed ledger. Remember Carsten's quote about the fragmentation and so on. The alternative here is to have, quote, centralized it to begin with.

Well, now we come to both a disappointment about the Thai database but also an important lesson in terms of the functionality of blockchains. Namely, when household i reports that it bought something, we know who they bought it from. We have recorded i and j . So we go and look at household j to see if they sold it. And unfortunately, not infrequently, the transaction appears only on one person's account and not both. So those are discrepancies.

So one of the advantages of having a common but distributed ledger to begin with is to reconcile discrepancies as quickly as possible. US financial markets do not do this either. There's an end-of-day process. State Street over here will take you to last couple of hours of a working day to work with all the correspondent agents to both parties to a transaction to reconcile transactions that one party thought it had made and the other denied that it did, or the amounts could be different, or the security could have been different. It's a very long, cumbersome process. Not to mention that the prices have changed since the transaction was recorded. So there are disincentives that grow with the time lag in between the actual transactions and the reconciliation.

So I'm extolling one of the virtues of the distributed ledger. Here's a formal definition. Distributed ledger is a technological infrastructure and protocols that allow simultaneous access, validation, and record-keeping across a networked database. DLT is a technology blockchains are created from. The infrastructure that allows users to view changes and who made them up to the identity of the nodes reduces the need to audit data, ensures reliability, et cetera. It's not new really. Businesses and governments have been using this concept for several decades in the form of having multiple computers in different locations used to solve problems like decentralizing the problem to multiple computers, parallel computing, and then consolidating the answers.

Advances in data science, computing, software, hardware, et cetera have made ledgers much more capable than they used to be. The rest is a repeat of things we've talked before. This thing at the bottom-- every blockchain is a distributed ledger, but not necessarily true that a distributed ledger is a blockchain. Here the blockchain-- part of the definition of a blockchain had to do with the validation algorithm used across the different blocks. And you could have a distributed ledger as a database that is not being validated in that way. So I think that's the distinction.

Tensions between individual versus community perspectives. We'll talk about central bank accounts and real-time gross settlement about the father, so to speak, of double-entry bookkeeping and community currencies. So central bank real-time gross settlement-- quite seminal article is Bech and Garrett in 2003, which is *The Intraday Liquidity Management Game*. Oddly, in some respects, banks know what their obligations are because their customers tell them they want to make a payment. But they get to choose the timing of when to report that payment obligation to the real-time gross settlement system.

So the data are consistent with a delay in reporting. And the idea is that if you report early, that's cash or reserves out the door, and you're trying to conserve liquidity in your account. So you prefer that someone pay you first. And that results in this Nash equilibrium, where the payments tend to get bunched at the end of the day. And that could be potentially inefficient.

They're not the only one. The Goldstein here-- I met staff at the Swiss National Bank who referred me to this classic paper about payments and financial fragility. Payments are inherently fragile. Why? A theory of payments involves a conflict between the role of the medium of exchange and the store of value. Payments must involve a reciprocal transfer of the scarce reserve good, which holds value for other purposes, namely not just for transactions but as a store of value.

The theory demonstrates payments are made only when reserves are abundant enough. Otherwise, we get history-dependent equilibriums. So Rafa, this is building on global games. This is also the conflict we saw with Krugman's babysitting exposé-- holding on to the coupons as a store of value rather than using them in transactions as intended. It's an inherent conflict. It's a universal conflict.

People say, what's the role of money? Store value, medium of exchange, as this were obvious and innocuous that you are potentially serving multiple masters. There are consequences. OK. Then we come to Luca Pacioli, who, as I said, is credited with double-entry bookkeeping. And actually, I think he was just consolidating previous work and studies on this and wrote it all up. So it's certainly the first published manuscript.

But let me start with something odd, the problem of negative numbers. So even in the Renaissance, negative numbers were thought of as absurd, although Chinese and Arab scholars understood the concept. Why did it seem absurd? Because what does it mean to hold a negative amount of something? It's a physical object. It's either there or it isn't, but it can't be negative.

They were clinging to this idea. Of course, we know from algebra the basic functionality of addition, multiplication, et cetera. You have inverses. There's an obvious negative number. That's a necessary part of algebra. So here money, which, from the financial account point of view, you kind of naturally think of as an asset-- I mean, it's embedded. It's confusing if it's something else. But Luca referred to it as a liability, not as an asset.

He has in mind that the reference should not be to the, quote, owner of it but rather the obligation to the other party that you owe something to the community. So to try to substantiate this claim-- and this is from the book. But Tomaž Fleischman who I've told you about last time, is the one who had explored this in detail. Two expressions are used in the journal, especially in Venice, one called per and the other A. And what is understood by them?

These expressions, the per and the other-- per indicates a debtor, and A is a creditor. And these cash items, I hesitate to say, either appearing in transactions or in the balance sheet are denoted with per. Per means you're a debtor. It's clear that this is what he had in mind. I'll come back to that.

Today is probably everything you ever wanted to know or more about databases. I put in a reminder that actually-- and starting the next lecture, we will look at ultimate goals. So here I just gave you some citations to database being used for what and evaluating the purpose and the effectiveness. We're not doing that today.

Well, then we come to community inclusion currencies. So these CICs are a medium of exchange that can be used only within a certain network or community, like the peer-to-peer stuff, which was registered babysitting services. It's a mutual credit network. That's another term for this community inclusion currency, because the participants effectively give each other interest-free credit. Now, what does that mean?

For example, you sell your goods. And at least not right away, you don't get something that you directly value, like goods in return. You sell your goods, and you get one of these community inclusion currencies to denote the value of goods sold. Then you take that and buy goods with it. So it's sort of a credit, but that's the accounting point of view.

The Pacioli point of view is you sold goods, and you got community currency. And now you have an obligation to use it to buy the production of others. That's the purpose, and others have to accept it. In fact, there are certain incentive structures loaded in that encourage holders to spend the currency instead of hoarding it. Back to that tension again.

And these are used in informal settlements in slum areas in Nairobi, for example, also South Africa. The best known is Sarafu. So the vouchers are promissory notes as a promise against future production. What was the idea? Self-governing community of microbusinesses committing their future production into vouchers to accept trade with one another so that the value would not leave the community.

And there's this notion-- if everyone goes shop at Walmart or something, that's leakage. That's value that doesn't recirculate in the community. These guys are doing very interesting work. It's not necessarily the way we would approach. As economists, there's stuff to prove here that this stuff is really not only fulfilling the purpose for which they intended it but is actually efficient. And we could come back to that.

But the bottom line here is it's running on a blockchain. Everything that I described here is being run on Ethereum in a slum in Nairobi. Blockchains was the topic of the day. OK. At the risk of extolling the virtues, I promised you balance. So let me provide some caution in terms of the limitation of blockchains.

The first has to do with something called the CAP theorem, which is a theorem in computer science. And then there are more liberal interpretations of that to classify current payment systems. The CAP theorem, CAP, has to do with Consistency, Availability, and Partition tolerance. So, again, think blockchain, databases. Common database ideally consistent in the sense that anyone who tries to read the data will get the same answer. Availability means that at any time they can request data. And yet partition tolerance says that the system continues to operate even if you get a partition of potentially inconsistent data.

By the way, Bitcoin has this, at least for a while, because the blocks are proposed. There's multiple conflicting blocks. They're not immediately consistent with one another. The whole validation process is to try to decide at least asymptotically what's the valid block. But it's not just about Bitcoin. It's inherent with distributed ledgers.

So if you're going to allow the system to keep functioning despite network failures, you have a hard choice. You could cancel the operation, which decreases availability but ensures consistency. You're only allowing whenever a query is made, it must be the case that anyone asking will get the same answer. But then you have to shut down availability. I don't know. End of day, end of month. When are the accounts reconciled? Or you allow the partition, and you proceed. So you have availability, but then you risk this inconsistency. So this is what [? Breuer ?] is saying is a fundamental choice to be made.

So, again, extolling the virtues, you would think consistency, availability, and don't worry about partition tolerance. So now you have to think a little more carefully about the design and the trade-offs. And in particular you could use this as a dilemma. It's really a trilemma. I said that, right? You can't have all three. So that's a dilemma, trilemma. Which one are you going to drop?

So here's an interpretation. We start with two parties to a contract, classic Alice and Bob. And they don't trust each other. And they have their own financial accounts, and they're not necessarily consistent with one another. That's kind of the starting point over here in the partition vertices.

Now, that's awkward. And so you begin to see in economic history the creation of intermediaries. So the intermediary has a representation of the accounts, at least for some transactions of the individual participants. So it could still be inconsistency and partition tolerance in the sense of multiple accounts. But if third parties are dealing with the intermediary, they're getting a consistent answer. Yeah, you should be worried if you're thinking layman or something, but OK.

So those are intermediaries. Now the system evolves, and we're on this edge here. In this case, we've given up on having multiple partitions. We're on the consistency-availability axis. And in particular a unique ledger will always give consistent information across the different ledgers. A security depository, the CSDs, are like that. They're a centralized log of the ownership of financial assets, typically run by a licensed private party or even run by a government entity.

Now, if we start at the top with consistency, there is a one common, consistent, distributed ledger. Common but distributed. But people have realized with congestion and other things that sometimes you have to choose. There's something called sharding, which basically is splitting the single database into subledgers in order to facilitate processing, or the layer 1, layer 2, which, as a reminder, I showed you last time, which is you have a smart contract and participants agree that it functions the way they wanted it to.

So you're implementing a multi-agent smart contract among the parties, but the only transactions that are actually executed on the ledger are the transfer of assets, not running the code. So that's this layer 2 terminology. But in the end, it's all about trying to make something functional that can handle large numbers.

And finally, we get to so-called compatible ledgers. You might say unified ledgers. So at this point you're like, which is which? Hmm. The BIS was referring to unifying multiple ledgers. That's what they had in mind, as opposed to having one unique common ledger to begin with. So that's trying to move from these partitioned and potentially inconsistent ledgers to something more centralized. That's what Carsten was hoping for. But we do need to worry about whether or not you lose the functionality of smart contracts if they're not consistent.

By the way, I should have said all along up here under consistency, it wasn't just data consistency. It's contract completeness because on Ethereum we're running contracts as a node. So we have to worry about whether the multiple contracts that can coexist with each other are consistent with one another. So let me turn to current difficulties in addition to what we've already said-- legacy technology, trust and fraud, unmeasured currency again, data silos, and inconsistent collection mechanisms.

So legacy technology-- this is from the Kansas City Fed, part of the Federal Reserve System. So Fed Now is a fast payment system that the US has finally implemented literally for fast, almost instantaneous payments. However, commercial banks, depository institutions, must make significant changes to how they manage payments to offer customers this instant payment service. I did not know about this. I learned this when I was visiting the Bank of Canada.

Some features of instant payments include around-the-clock services, instant accessibility-- and this requires real-time core-- payment processing and automated connectivity to the instant payment systems operator. But this is not automatic. Many depository institutions-- I'm paraphrasing here-- need to and have not yet modernized their systems to be able to use the fast payment service.

So how are they getting by? Typically, they will subcontract to an aggregator payment system provider, which, as it turns out, is an incredibly concentrated industry. So we start to touch on industrial organization. And I don't know. It could be inherent in the technology. It could be sort of an economic capture. But that, anyway, is a fact for the legacy technology.

Trust and fraud. OK. This is Sweden up here, which has to do with the value of the amount of currency left in the system and sometimes divided by the nominal value of GDP. Either way, it's kind of going down. In fact, for quite a while, the Riksbank was concerned that the central bank liabilities are going to be disappearing and not used at all because commercial banks have a net clearing operation having to do with Swish, which is an odd name. But Swish is an instant payment system among Swedish households.

That concern led them to contemplate having a central-bank-issued digital currency. But I think a few months ago, they decided they're not going to do it. This is cute. This is from Stefan Ingves, who was the then Governor of the Bank of Sweden. In anthropological writings, the reserve was a big stone buried at the bottom of a lake, and people would trade claims on it. And that was the currency. So Stefan is displaying this stone being transferred on a cell phone. It's kind of cute.

This is Kenya. And here the e-money, so to speak, is basically phone credits. So they jumped the landline technology. Almost everyone has a cell phone, and they have multiple accounts on cell phones. So you can use the fiat money, Kenyan shillings, to buy an account. But then you can transfer your credits, your cell phone credits, to somebody else. And that becomes an e-money. And this is a picture of how it works. Central bank fiat money denoted with dollars, so to speak. It's Kenyan shillings. It was a British colony.

And you can see the stick figure here takes his or her dollars to an agent, a Safaricom agent from the mobile company, and gets credited with the phone credits, which then can be used to buy something. And the supplier can cash it out. Goes back to a different agent to cash out. This is like cashing in, cashing out, or send money back home from Nairobi to his wife or mother still in the village. And she would take it to a local agent and cash out. It's a dual currency system.

You have the e-money part of it, which are the phone credits, and the paper currency ultimately backed by accounts at the central bank. It actually works pretty well. But when you start to think about it, it's kind of risky. Where is the ultimate cash? It's in a Safaricom account at a commercial bank. And Kenyan banks do fail. So there's that risk. But it's not on a distributed ledger. So the record of your account resides with Safaricom and what you have shown on your cell phone.

Broadening the discussion out a little bit, you have multiple cryptocurrencies. But they are built as exchanges of one currency for another on trusted broker dealers or centralized exchanges, not blockchains. So unfortunately, this is the story of FTX that diverted customer money into other investments. So that's the trust aspect.

This is on unmeasured currency. First of all-- and I'll come back to this, hopefully at the end-- there's a paper for Thailand where paper currency was so heavily used. And we actually were able to back out huge measure the use of it and detected huge welfare losses. And then this Hamilton picture over here is what would have been the digital dollar. And DCI here on campus designed it and implemented the algorithm jointly with the Boston Fed.

However, they wanted to preserve the privacy of the transactions. So it was heavily influenced, for good or bad, by cryptographers who did not want the history of transactions to be anywhere in sight and basically destroyed. So it didn't have contract functionality. And there's a new version that does, but it wasn't their first inclination.

So then we have the problem of unmeasured currency. And we're back to earlier discussions. Do we want to just have an electronic version of the cash, or do we want more capabilities with potential trade-offs? And then a slide here on data silos. And here I was referring to Indonesia, but it could have been another payment provider where basically they develop apps for payments for credit lending and so on. And each is a separate department, and the database is separate.

There is a common identifier-- multiple, actually. It's a lot of work to unify the data in order to know the transactions belong to a common entity. So it's not like the basic unit is the business or the basic unit is the household. And then there are multiple uses. It's not designed that way. So this is another problem.

So inconsistent collection mechanisms. So this is what I was alluding to before-- again, the savings, profits not eaten or given out as dividends, or savings that should show up in the change in assets in the balance sheet. So this is how the accounts are connected in principle. But we did this with the Boston Fed for the Panel Study of Income Dynamics, which is one of the premier US microdatabases for the consumption expenditure survey, the survey of consumer finances.

And long story short, we looked at the discrepancy between cash holdings on the constructed statement of cash flows from each and every one of these data surveys with the change in cash holdings in the balance sheet. And it's typically way off. I'm not saying these are bad surveys. They're basically the bread and butter of research on many aspects in the US. But they were not constructed with this notion of consistency across financial accounts.

And likewise for new data or something, if you were starting from scratch, you probably want to have that standard as a check on the data you're proposing to enter into the database. That was a micro picture. There's a macro picture, which is very similar. These are macro aggregated accounts done by the Department of the Bureau of Census. And you get inconsistencies.

So both at the macro and micro level, unfortunately, we don't have very much consistent data in the US. But I've done it with the data we collected in Thailand, where we do have consistent accounts, and hence we can aggregate up. And we'd like to go and do this in the US somehow. And there is a project underway in West Virginia with Scott, who was at the Boston Fed, now at the University of West Virginia. And so we're creating templates.

The idea would be not to do what we did in Thailand, where we're using enumerators to have and recall one month at a time but rather to ask the households if they're willing to share with us their electronic data, whether it's commercial bank account or credit card account and so on. And then we merge that along with an enumeration of their paper currency transactions into consistent financial accounts. It is a labor of love. It's taking some time, but we're hopeful.

So I just wanted to say at the end two things. One, this lecture on distributed ledgers, payments, cash, et cetera-- there's a parallel lecture for 193. And some of you are registered actually to take that class, but it's not a requirement for this class. The lecture material will be available. And I just edited, and Deb will release lecture one in 193, and it's parallel with this. So you can read about measurement of inefficiency in cash, et cetera.

And it ends still not written down with the experience we had in Indonesia, where it's clear that it's neither a pure digital economy, despite the digitization, nor is it a pure fiat money economy. It's a dual economy. And households and businesses are really struggling with developing strategies for payments, with inflows and outflows across these multiple accounts, including the fact that there are transactions costs. And if you're using a local informal agent, there are huge markups and potentially theft and fraud.

So the first goal is documentation. And I'll just say that if anyone is-- hopefully, someone will be-- interested in doing this, it's to take a version of the material covered here, along with the details of creating consistent accounts and create a template that we can use in turn in Indonesia when we go and interview households and businesses. So it's a bit like starting from scratch in West Virginia, except we would be doing it in Indonesia.

So some of you are involved as already research assistants. And so that's a proposal if you're interested, but it's not an obligation. I will try in each lecture, if I can remember to do it, to form these links to the larger picture and potential research. And even if-- you know, otherwise, there's a whole series of papers in the syllabus, some with double stars and many others. So for your project for this class, feel free to peruse and pick potentially. See what's in there. Think about it as a write-up of a two pager or something to share with your classmates or even potentially the one longer-term research proposal.

OK. And the red hand is crossing 12:00. That's kind of amazing.