IOU

Money, Banking and Cryptocurrencies

Preliminary and Incomplete
Please do not distribute without permission from the author

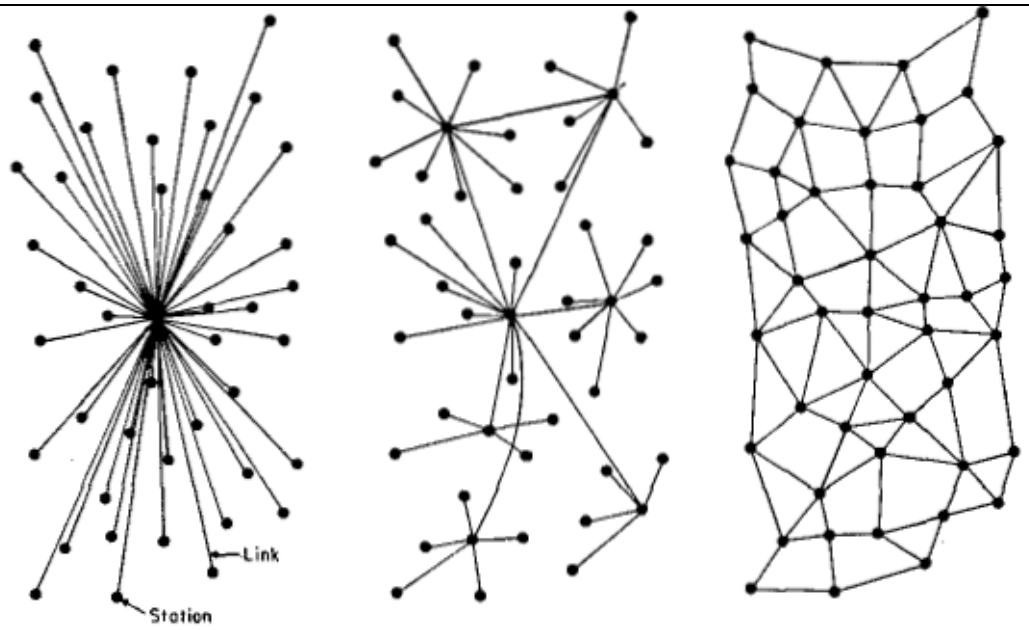
Part E

George Dotsis

Faculty of Economics and Political Sciences
Department of Economics
National and Kapodistrian University of Athens

Cryptocurrencies

Digital cryptocurrencies are transferred through a distributed computer system. In distrbited ledgers, transfer takes place without the intermediation of conventional banking payment systems and transactions are verified on-line using cryptographic methods.

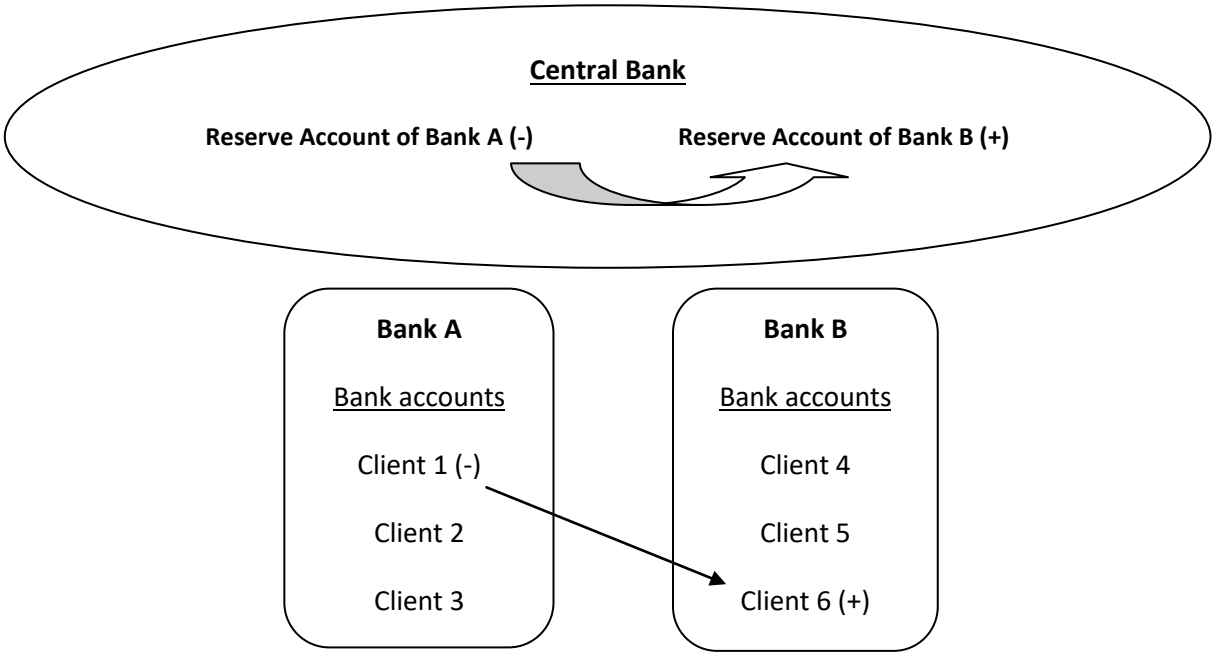


Source: Baran, 1964

Centralized systems	**Decentralized systems**	**Distributed systems**
The conventional banking system with the Central Bank as the central node.	The conventional payment system with direct interaction of users with different banks and payment providers. The Central Bank again acts a central node.	Peer-to-peer payment. Peers collectively maintain and operate the system (the database of all transactions). Users communicate with each other and settlement is automatic.

1. Bitcoin and Public Ledger

In conventional banking payment systems, money is transferred between bank accounts through the intermediation of the Central Bank that acts as the clearing house. The cash settlement of all interbank transactions is made with Central Bank money using their respective reserve accounts. Of course, in the case of banknotes, the transfer takes place physically rather than electronically. For example, as shown in the diagram below, if Bank A's client 1 orders a transfer of 100 Euros to client 6 that has a bank account with Bank B, client 1's account will be debited with 100 Euros, and the account of client 6 will be credited with 100 euros, Bank A's account with the Central Bank will be debited with 100 euros, and Bank B's account with the Central Bank will be credited with 100 euros.



In order to transfer money from one account to another, the bank first checks whether the client's account has the amount available. In case the amount is not available the transaction is not executed. Also, account credits/debits are reversible, as errors can be corrected. Banking payment systems are key infrastructures of a financial system and must be conceived as reliable and trustworthy by all counterparties for the smooth operation of the economy.

Bitcoin

Bitcoin is a digital payment system whereby digital assets - referred to as bitcoins (with a lower casem) - are transferred across a distributed, peer-to-peer, open source network. Each node (a computer) of the network is connected to other nodes. The nodes that make up the network do not necessarily all have the same

computing power. The Bitcoin payment system is completely decentralized and operates without the mediation of the banking system and central banks. In order for any payment system to be credible, it must, among other things, have mechanisms that certify that the originator of a transaction has the amount he wishes to transfer to another account. In the case of a non-banking mediated payment system, such as Bitcoin, a mutually acceptable and credible mechanism must be in place to check ownership first and ensure that the same digital currency cannot be sent to two different recipients at the same time. In the computer science literature this is known as the "double spending" problem. Transactions in the bitcoin network are recorder in a public ledger known as blockchain. The blockchain is at the heart of the distributed ledger technology. Distributed ledger technology is a decentralized database that can be used in order to record information that can vary from transaction data to real and financial asset ownership. Distributed ledge technology is a significant innovation rooted in computer science research that has the potential to change the landscape of the finance industry.

The creator of bitcoin is Satoshi Nakamoto. In his paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System, which was released on the Internet in October 2008 (https://bitcoin.org/bitcoin.pdf), he analyzes the basic architecture of the payment system. In January 2009, Nakamoto released the first software to build the peer-to-peer network and created the first units of bitcoin. The name Satoshi Nakamoto is a pseudonym and to this day no one knows the author's true identity.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin payments are recorded in a ledger which is publicly available. To make bitcoin payments requires the use of a secret code (private key), similar to the pin card, known only to the holder of the electronic wallet. The public ledger records all bitcoin payments made since the digital currency was created in 2009. The public ledger is updated using cryptographic methods that ensure its security and make it impossible to tamper with, since users can only add new transactions without having the ability to change the old ones. Verified transactions are gathered in blocks (just like pages in an accounting ledger) and the public ledger is updated approximated every 10 minutes by adding a new block to the previous chain of blocks – this process is a called mining. In contrast to traditional banking payments systems, transactions in Bitcoin are irreversible.

Public Ledger

Address	**bitcoin transaction**
13PkmTRamYQ9zVnhfG9W8ZBV6MUeaFzpd3	0.00546758 BTC
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	0.01660014 BTC
1EmSRLsXg8yaQX8xe9QLoyxz9KVuBDrcJJ	0.02320993 BTC

https://www.blockchain.com/btc/unconfirmed-transactions

Validation of payments is carried out using encryption methods based on hash functions. The hash function takes as input a string of characters of any arbitrary length and produces a fixed-size set output. The key feature of hash functions is that they are irreversible, that is, it is almost impossible to calculate the input variable when only the output variable is known. The Bitcoin payment system uses the SHA-256 function (http://www.xorbin.com/tools/sha256-hash-calculator) which produces 64-character alphanumeric series. Each individual input variable in the SHA-256 corresponds to 16 possible values: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f. The table below shows the results produced by the function when the input is the word IOU. As shown in the table, adding a single number to the word IOU produces a completely different alphanumeric result. If the output variable is known it is (almost) impossible to find what the input variable is.

Input	Output (hash value)
IOU	97a61b687155ba36ac9d280940760c9aa4705520482ab9489b3713d0029b3bf0
IOU1	48655cf7ed3183aa7f1033a810c441d020cee0a16e45a52772816f6aa9346430
IOU2	ed174a31b9e9793093cf90428dade09826b909046afad13670d484a90e6dc111
IOU3	db0ef324261dd302d15e0037475ed08cd0d832848413ff709dd91f849d85c48d
;;	01b7cc720b3af40a848cf28902ee40dc0f9a5ad9ded28da13b480ce2a8422bc9

The blockchain is considered almost immutable. If a malicious actor attempts to change previous pages (blocks) of the ledger with the aim to send bitcoins to his personal account it is highly improbable to succeed. This is because he will have to re-calculate all subsequent blocks. The computing power required to perform this task is enormous as the blockchain grows. A hacker could be able to manipulate the current block (to be validated) only if he could control more than 51% of the total mining power. This is the highest risk in this system.

The verification of bitcoin blocks is based on finding solutions of computationally intensive problems that secure the integrity of the system. This process is called “proof of work”. The proof of work is the process of generating a piece of data that is difficult to produce but it is easy for other nodes to verify. The proof of work provides a consensus mechanism among peers who share the ledger about its true state.

Using the example made earlier with hashing the word IOU, suppose that we want to produce a hash value that starts with two zeros. Using trial and error it appears that the word IOU9 produces a hash value that starts with two zeros. The number 9 is called “nonce” which is an abbreviation for the expression "number only used once". It is easy to understand that as more zeros are required for the hash value the more difficult is to find the right nonce. The mining process in bitcoin involves the continuous use of different nonces until finding a hash value with certain characteristics.

For example, the probability of producing a hash value with 9 consecutive zeros is equal to 1/16^9 =1.45519E-11. The reciprocal of the probability is equal to 68,719,476,736. So, on average, it would take about 69 billion trials to find the correct hash. The computational burden for solving the hash problem increases with the CPU power of the network. As new miners enter the network it takes more trial and errors through consecutive repetitions to find the required hash. The difficulty level (that is the number of zeros) is periodically adjusted. The system calculates the average number of blocks created over a particular short-term period and then adjusts upwards or downwards the number of zeros. The total supply of bitoins is fixed at 21 million and new bitoins are created to compensate miners for updating

the public ledger. Every time a new block is added to the blockchain miners are compensated with 12.5 newly issued bitcoins. After the first launch of Bitcoin, 50 units were emitted every 10 minutes. Then, 25 units and now this number is halved to 12.5 units. This happens approximately every four years or 2106 blocks in accordance with the predetermined supply schedule which is increasing at a decreasing rate. The smallest unit of bitoicn is satoshi which is equal to 10^(-8) bitcoins. Given the current rate of blockchain evolution the bitcoin will reach its total supply around 2140. As of the early 2020 about 87% percent of bitcoins have already been issued.

Many bitcoin enthusiastics believe that fixed supply of bitcoin renders bitcoin something equivalent to a "digital gold". However, although the total supply of bitcoin is fixed, the number of different cryptocurrencies can become arbitrarily large (currently there are thousand different cryptocurrencies) and hence the total supply of all cryptocurrencies is not predetetermined and not known in advance.

The graph below shows the total hashes per second performed in Bitcoin network for validating the Bitcoin blockchain. As of March 2020 the hash rate is about 130,000,000 trillion hashes per second. The profitability from mining bitcoins depends primarily on the cost of electricity for running the computers and on the sunk cost for buying the equipment. It is reasonable therefore to observe that most mining facilities are built in countries with low electricity cost.

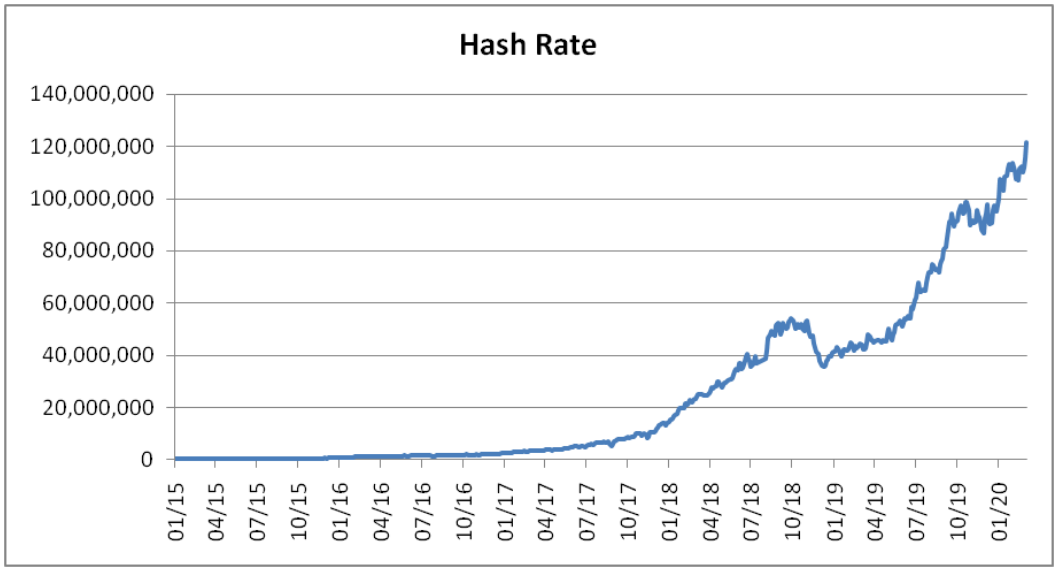


Figure xx. The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing. The data are 7-day averages.

The graph below shows the time evolution of bitcoin prices.[1] Bitcoin is quite volatile with a daily standard deviation ranging from 2% to 7%. The high volatility of bitcoin remains a serious obstacle with respect to the use of bitoin as a means of payment or as a store of value.

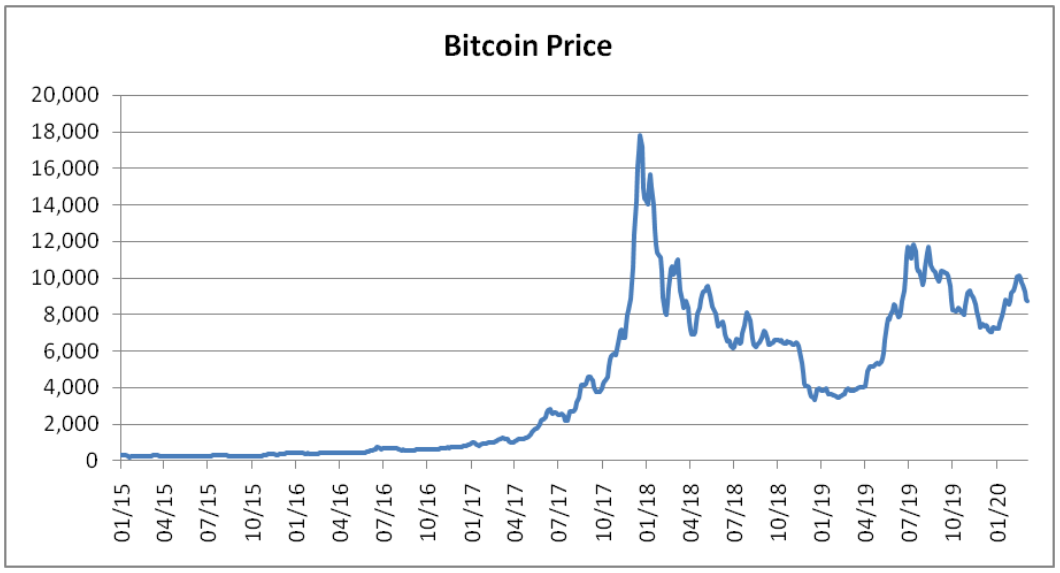


Figure xx. Time series data of bitcoin price (7-day averages).

Some economists believe that the intrinsic value of bitcoin is zero. I don't agree with that. Bitcoin is not a financial asset backed by taxes or loans but it is a digital asset that offers a convenience yield- due to transactional services- and this convenience yield is difficult to be determined and a sort of insurance which is difficult to measure. Bitocin is a borderless asset that can be transferred quickly in a decentralized network, it's not subject to bank regulation or sovereign controls and it has a predetermined fixed supply. Bitcoin is gradually gaining legitimacy after the introduction of bitcoin futures in late 2017 and there seems to be an increasing interest by institutional investors for investments in cryptocurrencies. The biggest risk of bitcoin is still legal risk. If a country like US deems bitcoin illegal the value of bitcoin will drop significantly and the whole project will most probably fail. My guess is that this is not very likely to happen. I think that gradually there will be some sort of integration between fiat money and conventional banking systems and cryptocurrencies (e.g., convertibility, use of cryptos as collaterals, cust0dy services). It has happened before with private forms of money that circulated along with state paper money back in the 18th and 19th century and it is likely to happen again.

[1] According to anecdotal evidence, back in 2010 a programmer purchased two large Papa John's pizzas for 10,000 bitcoins, worth about $30 at the time. Today (August 2020) they worth close to 100 million dollars.

Three largest Crytpocurrencies by market capitalization

Bitcoin	Bitcoin (BTC) is a consensus network that enables a new payment system and a completely digital currency. Powered by its users, it is a peer to peer payment network that requires no central authority to operate.
Ethereum	Ethereum (ETH) is a smart contract platform that enables developers to build decentralized applications. Ethereum is the pioneer for blockchain based smart contracts. When running on the blockchain a smart contract becomes like a self-operating computer program that automatically executes when specific conditions are met. On the blockchain, smart contracts allow for code to be run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. It can facilitate the exchange of money, content, property, shares, or anything of value
XRP	XRP is an independent digital asset that is native to the XRP Ledger. With governance and fast transaction confirmations, XRP is said to be the most efficient settlement option for financial institutions and liquidity providers seeking global reach, accessibility, and fast settlement finality for interbank flows.

Source: https://coinmarketcap.com/

2. Stablecoins

Another recent innovation is the emergence of “stable coins”, which are pegged to an anchor asset, usually the US dollar, at parity. The large volatility of cryptocurrenies, like bitcoin, has created the need for the introduction of digital assets with less fluctuation. As the market for cryptocurrencies evolves there is growing demand for low volatility safe liquid assets that can be stored and transferred in peer-to peer payments systems. The volatility of the stable coin is determined by the volatility of the pegged asset. In international economics, hard pegging a currency is known a “currency board arrangement”. In the currency board the liabilities of the central bank (cash and reserves of commercial banks) are in principle fully covered by liquid foreign-currency securities. Stable coins come in two flavors. They can be either decentralized or centralized.

Centralised stablecoins

Centralised stablecoins are IOUs convertible to a predetermined quantity of other assets (fully collateralized), like currencies (the US dollar, euro) or commodities (gold). They are run by limited liability companies that receive deposits and maintain the reserves in bank accounts and in exchange they issues IOUs/currencies.

Centralized Stable Coins	
Assets	**Liabilities**
Deposits in local currency Deposits in foreign currency Commodities	Stablecoins Net worth

The most popular stable coin of this type is Tether token (USDT). The graph below shows that Tether on average retains its parity to the dollar, but occasionally displays some upward and downward deviations.[2]

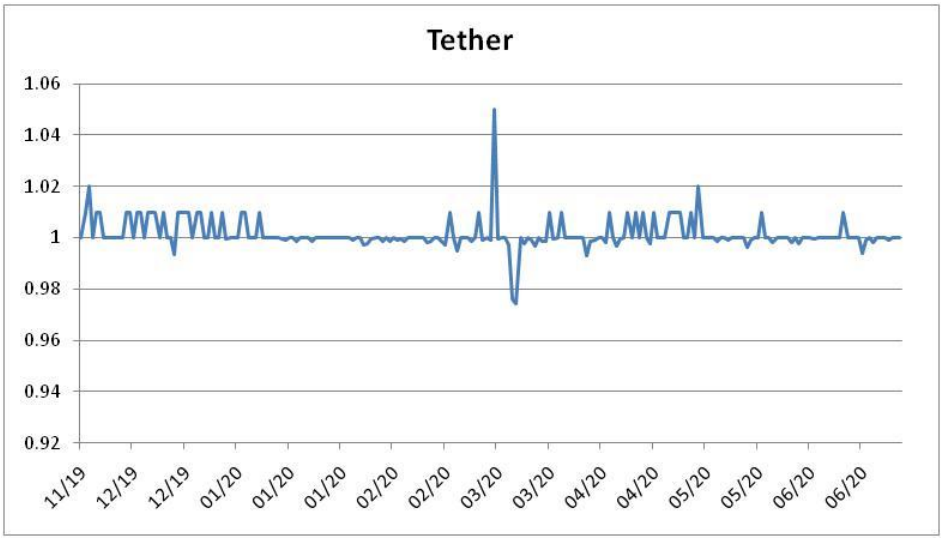


Figure xx: Time series data of Tether

In 2019 Facebook proposed a plan for the introduction of a token named Libra that facebook users will be able to use. The plan is for the Libra token to be backed by financial assets such as a basket of currencies and US Treasury Securities in an attempt to avoid volatility.

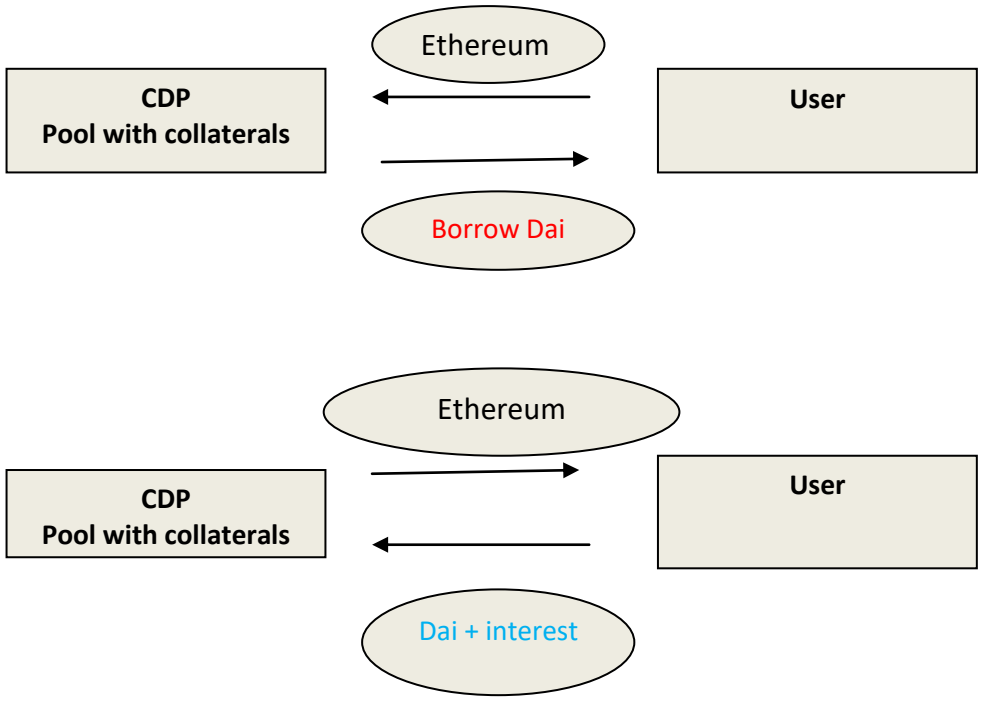
[2] There have been some allegations that the total supply of Tether is not fully backed by US dollars. Short-term deviations from parity can be explained by market frictions like transaction costs bid/ask spreads.

Facebook	
Assets	**Liabilities**
Deposits in local currency **Deposits in foreign currency** **Government bonds** Other assets	**Libra** Net worth

Given the size of Facebook's users (around 2.5 billion), the introduction of an unregulated asset that will serve as a unit of account, means of payment and store of value is a potential threat to financial stability. Because of the underlying basket of currencies Libra users will be exposed to exchange rate risk and there is a serious threat of market de-stabilization if there is a "run" on libra. Part of Libra's collateral assets will be government bonds and a run on Libra and high redemption rates may cause fire sales with negative effects on the markets and side effects on the implementation of monetary policy. The introduction of Libra will generate significant seigniorage profits for Facebook since Libra will have zero interest rate, while the collateral assets will generate positive interest income, but it's unclear what type of increase in social welfare the introduction of this type of private form of money will bring.

Decentralized stablecoins

In decentralized stablecoins the underlying collaterals are cryptocurrencies and there is no central party that keeps reserves in bank accounts. An example of a decentrilised stablecoin is Dai, which is a collateral-backed cryptocurrency soft-pegged to the US Dollar. Dai is generated through a dynamic system called Collateralized Debt Positions (CDPs). A user can deposit Ether (or any Ethereum-based asset that has been approved as collateral by MKR holders) as collateral in a personal smart vault and in exchange to borrow a specific amount of newly created Dai. The creation of new Dai generates new debt and once the Dai is returned, and after paying a fee (called stability fee), the debt is cancelled. Dai is overcollateralized with a minumum ratio of 1.5 to 1, e.g., for every Dai worth of 1 dollar the user needs to deposit as collaterals ethereum assets worth at least 1.5 dollars.



If the value of the collaterals starts to fall, some vaults will become undercollateralized (e.g., the ratio will fall below 1.5) and a liquidation process will begin in order to preserve Dai's dollar parity. In the liquidation process the Ether assets are sold using an internal market-based auction mechanism. The Dai received from the auction process cover the vault's obligation (including a liquidation penalty fee) and the total supply of Dai in circulation is contracted. If there is a surplus of collateral this is returned to the original vault owner. If the Dai received cannot cover the vault's obligations then in order to preserve Dai's solvency the system mints MKR (collateral of last resort) and sells them in exchange for Dai. MKR is the governance token and recapitalization source and MKR holders have the incentive to govern the system well to avoid dilution from an increase in MRK supply. [3] The figure below plots the price of Dai and the price of ETH. Dai displays deviations from parity but has much less volatility compared to ETH. The Dai creation process shares some similarities with securitization as in both cases overcollateralization is used in order to produce a low risk asset from an underlying pool of risky assets.

[3] The Dai white paper is available here https://makerdao.com/en/whitepaper/

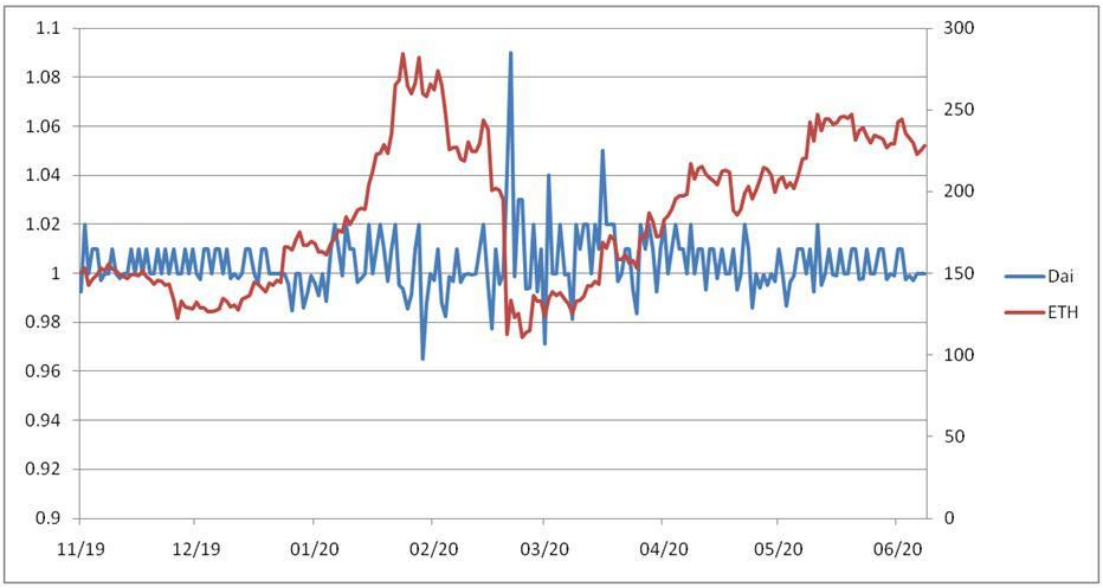


Figure xx: Time series data of Dai and ETH.

Central Banks Digital Currencies

Central Bank Digital Currencies (CBDC) are the digital equivalent of cash. In the current institutional framework, only banks and certain financial institutions are allowed to hold accounts with the central bank. CBDCs will be stored in deposit accounts of households and corporations held at the central bank and could be used for payments and as store of value.

Central Bank	
Assets	**Liabilities**
Gold FX reserves Loans to banks Securities Other assets	Corporations and households' deposit accounts (CBDC) Commercial bank reserves Banknotes Other liabilities Net worth

1. Central Banks Digital Currencies

Over the last couple of years the introduction of Central Bank digital Currencies has been the subject of intense debate and research by central banks and academics. Many central banks are currently considering the introduction of Central Bank Digital Currencies (CBDC), but there are some serious concerns that if CBDC are not properly designed their introduction may have a negative impact on financial stability and bank's solvency. Note that money is already mostly in digital form (bank deposits) hence CBDC can best be viewed as the digital equivalent of banknotes.

In modern economies the vast majority of the money supply is in the form of bank deposits (private IOUs) which in principle are fully converted to banknotes (central bank IOUs). With the gradual abolishment of cash, households will be deprived from the possibility of holding central bank/state money.

According to Swedish Rijksbank: "For a long time, the state has provided the general public with banknotes and coins to use for payments. Cash has enjoyed the confidence of the general public and facilitated trade in goods and services. Today's digital payment market means that we face a new situation in which all means of payment accessible to the general public are issued and controlled by private agents. If the state, via the central bank, does not have any payment services to offer as an alternative to the strongly concentrated private payment market, it may lead to a decline in competitiveness and a less stable payment system, as well as make it difficult for certain groups to make payments. Ultimately, it may also risk eroding basic trust in the Swedish monetary system. Some of these problems could be neutralised or mitigated by an e-krona."

CBDCs need to be carefully designed and take into considerations potential threats to financial stability and adverse effects on commercial bank's cost of financing. Central bank liabilities and bank deposits are close substitutes. However, during times of systemic crisis or market stress central bank liabilities are superior in value compared to bank deposits because, unlike a private bank, a central bank cannot go bankrupt. Unlike deposits which are usually guaranteed up to a certain amount (e.g., 100.000), CBDCs will have no credit risk and constitute a pure form of a safe asset.

In the current institutional framework only financial institutions are allowed to hold deposit accounts with the central bank. Central bank money (reserves) is the means of payments for settling all interbank transactions. There have been various proposals regarding the different types of CBDC. Here I discuss them following the CBDC typology suggested by BIS (2018). [4]

[4] Available here: https://www.bis.org/cpmi/publ/d174.htm

Taxonomy of CBDC

	Existing central bank money		Central bank digital currencies		
	Cash	Reserves and settlement balances	General purpose token	accounts	Wholesale only token
24/7 availability	✓	×	✓	(✓)	(✓)
Anonymity vis-à-vis central bank	✓	×	(✓)	×	(✓)
Peer-to-peer transfer	✓	×	(✓)	×	(✓)
Interest-bearing	×	(✓)	(✓)	(✓)	(✓)
Limits or caps	×	×	(✓)	(✓)	(✓)

✓ = existing or likely feature, (✓) = possible feature, × = not typical or possible feature.

Source: BIS (2018)

Current central bank money is in the form of cash and reserves. Cash offer 24/7 availability, transactions with cash are between counterparties and are not recorded in the central bank ledger, cash offer zero nominal return and, in principle, there are no limits or caps. Central bank reserves are available for transactions only when payment systems are open and working, transactions with reserves are recorded in the central bank ledger and settled via the central bank and reserves are interest-bearing assets.

Central bank digital currencies can be either general purpose or wholesale. General purpose means that private households and non-financial corporations can have a CBDC account with the central bank while wholesale means that only specific entities (e.g., payment platform providers) would be allow to hold CBDC. Wholesale CBDC could improve settlement efficiency for domestic and especially cross-border transactions. General purpose CBDC can be either account based (e.g., settled through central bank with no anonymity) or token based and transferable in a decentralized payments system using public ledger technology.

The proper design of CBDCs is critical so as to not disrupt the services of financial intermediation offered by banks, to preserve financial stability and offer a payment landscape that can promote efficiency. The most important threat from an introduction of a general purpose CBDC is the realization of a large scale “run” on bank deposits and massive conversion to CBDCs. Note that a “digital run” would be much faster and larger compared to “traditional runs” where depositors have to physically visit a bank and convert deposits to cash. In times of a systemic bank crisis, where the central bank acts as a lender of last resort, a digital run could cause a gigantic refinancing of commercial from the central bank using loans and other securities as collaterals, implicitly converting the commercial banking system to a de a facto 100% reserve system (see balance sheet below). The likelihood of such event could hinder the ability of commercial banks to create money, increase significantly the cost of bank’s financing (deposits are a source of stable and low cost funding)

and would force the central bank to monitor and exam the credit quality of all individual assets (loans, securities etc) held by commercial banks, thereby fundamentally changing the structure of the commercial banking system. [5]

Digital Run

Central Bank	
Assets	**Liabilities**
Gold	
FX reserves	Deposit accounts (CBDC) ↑
Loans to banks (*with collaterals*) ↑	Commercial Bank reserves ↓
Securities	Banknotes
Other assets	Other liabilities
	Net worth

Commercial Banks	
Assets	**Liabilities**
Deposits at the CB ↓	Deposits ↓
	Loans from CB ↑
Loans	
Other assets	Net worth

The introduction of CBDCs in monetary unions like the Eurozone is more complicated and needs to be implemented with even greater caution. In Eurozoze there is no common deposit guarantee scheme and CBDCs will be close substitutes of government liabilities of countries with low credit risk but significantly superior compared to government liabilities of countries with higher credit risk. In times of distress a full scale run on weak countries' banking systems could occur, similarly to what happened in Greek banking sector in 2012 and 2015 but at a much larger scale and speed, that would lead to long-term and large-scale capital controls and significant fragmentation of the monetary union.

[5] Studies have proposed various "circuit breakers" to prevent digital runs, like negative interest rates on CBDC, caps on conversion or no explicit guarantee of on-demand conversion (see Kumhof, M., and C. Noone. 2018. "Central Bank Digital Currencies—Design Principles and Balance Sheet Implications." Bank of England Staff Working Paper 725, London.).