

Master of Financial Technology

FNT 628

**Blockchain and
Cryptocurrencies**



Lecture 8

FNT 628

Blockchain and Cryptocurrencies

Prepared by Dr. Yara Ibrahim

www.midocean.ae

Cryptocurrency

Introduction

- To understand cryptocurrencies, we need to distinguish between what they were envisioned to be and what they currently are.
- the ambition in Nakamoto (2008) was to create a fair, borderless, and secure currency that can be trans- acted in a secure way across a network of anonymous participants.
- this stood on the shoulders of decades of innovation in databases, cryptography and network protocols, which all combined to give the innovation of blockchain technology.
- From a technical perspective, the real achievement of Bitcoin relies on the coordination of the underlying features of blockchain technology, embedded with a pre-programmed economic incentive scheme (akin to a monetary policy).

Introduction

- Blockchain technology enables an exchange of trust via a tamperproof, publicly auditable record of transactions between parties with no requirement of a pre-existing trust in each other or need for a central authority to govern and manage the network.
- The initial underlying philosophy behind the Bitcoin system (or broadly any 'decentralised' network) was to ensure that no one entity can act to censor transactions or prevent person(s) from joining the network. Rather, each participant in the network has a 'voting' right given they have computational processing power.
- In the context of this chapter, cryptocurrencies are any form of currency that only exists digitally as part of a payment system that has no central issuing or regulating authority and uses a decentralised system to record transactions and manage the issuance of new units/tokens, and that relies on cryptography to prevent counterfeiting and fraudulent transactions. This definition excludes 'Central Bank Digital Currencies' (CBDCs),

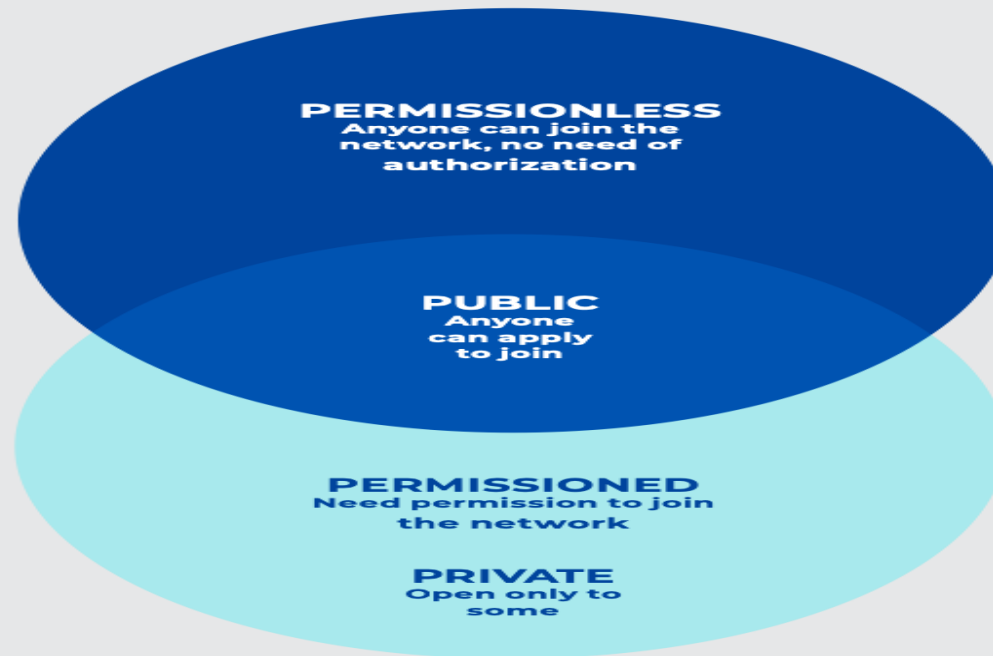
Permissionless and Permissioned Blockchains

- To understand the difference between permission-less and permissioned blockchains, it is important to understand how the source code of the software applications is managed (that is to view code, copy it, learn from it, alter it, or share it).
- Most cryptocurrencies are based on decentralized permission-less blockchains, including Bitcoin and Ethereum, whose transparency is built on open-source code (accessible to everyone on the network). Permission-less blockchain-based cryptocurrencies allow anyone to access the Bitcoin code, inspect it, copy it and improve it.

Permissionless and Permissioned Blockchains

- Permissioned blockchains on the other hand are typically more centralized, closed systems, whereby there is a known custodian of the blockchain network who qualifies participants based on certain pre-defined criteria in order to access and use the blockchain data.
- Permissioned blockchains are typically used by large, private groups of enterprise organisations who require a great deal of trust, as they are likely to be using the blockchain for its technological efficiency gains in specific use cases, as opposed to its economic digital currency features and capabilities.

**Permissionless and
Permissioned Network**



Ledgers

- Ledgers have existed and evolved as a form of accounting for over a millennium. For example, ledgers were found to be used by Mesopotamians (modern day Iraq) as far back as 3200 BC to record expenditures, traded goods and record accounts payable on Clay Tablets (kept safe in temples, considered banks of the time).
- Then ledgers were used in 633 BC by Persian civilizations as an auditing tool to regulate the collection of alms (wealth tax).
- During the Middle Ages, there was a scarcity in gold across Britain, which caused a decline in circulation of coins; as a result the Exchequer introduced tally sticks as a physical proof of payment, whereby the stick would be split in half.
- One half was kept as stock by the payer (contract), and the other half as debt retained by the Exchequer. Hence, when accounts were audited, the pieces were fitted together to check they 'tallied'.

Ledgers

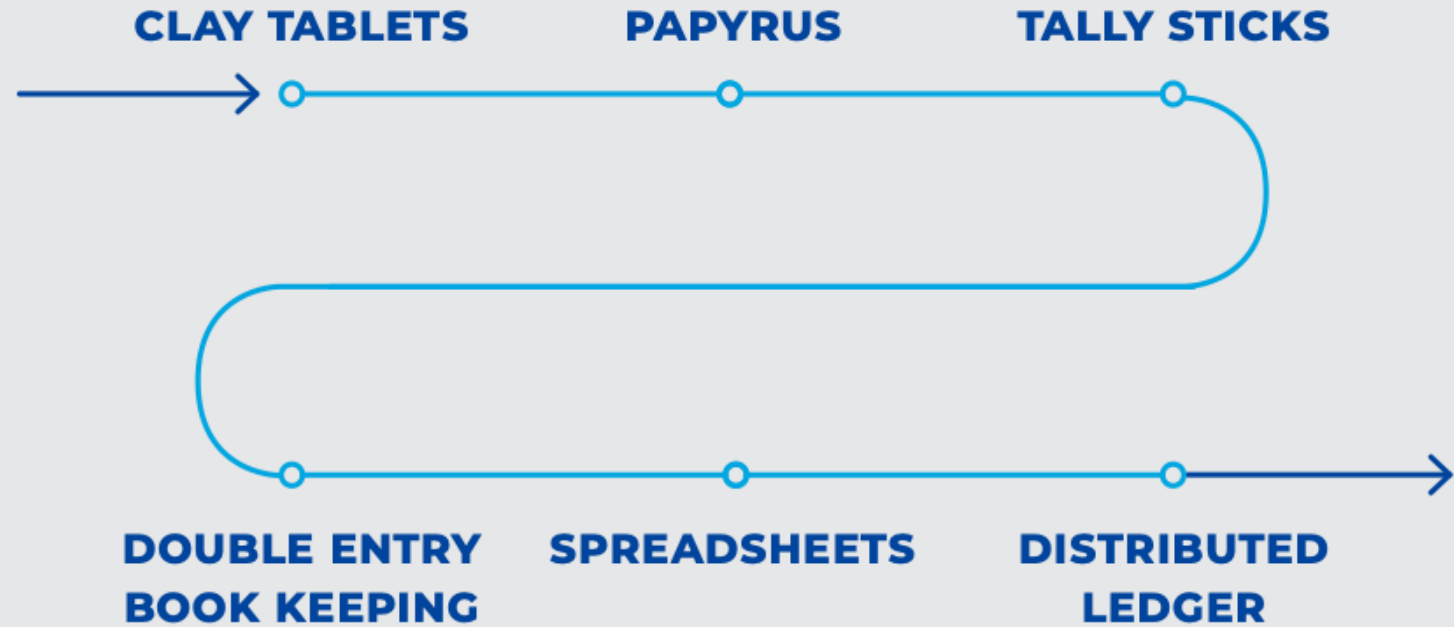
- By the 14th century, tally sticks had spread across Europe, fundamentally acknowledging the emergence of debt and contracts, which were used to pay wages to workers and taxes to the state, and also traded to buy and sell items, similar to coins.
- They were different in that they also acted as an 'IOU' pledge, whereby whoever issued the stock was liable to pay in gold who- ever owned the other half of the stick.
- Thus, the stock had a value in gold, and could be spent accordingly to the same value of actual gold.
- Thus far, a 'ledger' is defined as an information store that keeps a final and definitive records of transactions, and a 'transaction' is defined as a smallest unit of work process resulting in a state change

Ledgers

- By 1497 Merchants in Venice had advanced accounting systems to create a new financial services industry. This was captured by the Italian church father and mathematician Luca Bartolomes Pacioli, who published the first book on double entry system of accounting, highlighting that any given new transaction fundamentally changes either the debit or credit position of the account, to give an actual value of a business.
- Other than advancements in technology and general digitalisation, accounting and bookkeeping have not really progressed beyond Excel spreadsheets and have become more complex, which requires qualified professionals to maintain accounting re- cords across multiple accounts (ledgers).
- From an accounting perspective, key advancements in blockchain technology are the abilities for participants to share one single synchronised, distributed ledger of transactions, and for the underlying consensus protocol (a set of rules) to successfully ensure each node on a network agrees on the data being shared on the ledger.

Ledgers

FIGURE 10
**Historical Evolution
of Ledgers**



Source: Coindesk, 2019.

Networks

- Blockchains, or DLTs, consist of a network of nodes, where a network is defined as an interconnected system of things.
- The best way to understand the relationship between nodes and networks is a *visual representation* seen in Figure 11 where decentralized networks have multiple sources of control and distributed networks distribute control equally across all participants in that network, whereas centralised networks have one central source of control.
- The Rand Corporation described these networks back in the 1960s (Barand, 1964), describing the type of interconnection between the nodes and the type of information flow between them for transaction and/or the purpose of validation.
- For efficiency reasons, systems have historically been designed in a centralised manner. This centralisation dramatically lowers the costs for system configuration, maintenance, adjustment (and the costs of arbitration in case of conflict) as this work must be performed only once in a central place.
- While highly efficient in many situations, this kind of systems induce a single (or very limited set of) point(s) of failure and suffers from scalability issues (Tasca and Tessone, 2018).

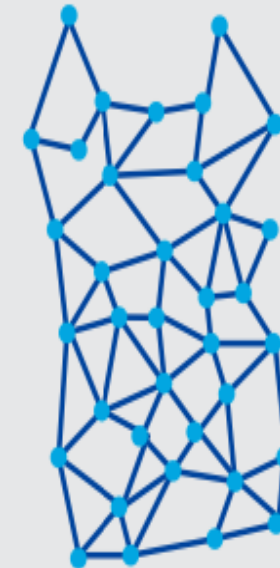
FIGURE 11
**Centralized,
Decentralized
and Distributed
Ledger
Technology**



Centralized



Decentralized



Distributed

Image Source: Baran, 1964.

Networks

- In a highly centralised system, all the nodes (and all the users on a node) are connected to the central node (a 'dictator' model). Most social and monetary networks are centralised systems, where all participants have relationships with centralised hubs (i.e. a central bank).
- However, the Internet was not really designed to be like that (i.e. for centralised business models), rather, for information to be decentralised and accessible and not controlled by one central hub.
- The distributed network on the other hand, maintains a strong sense of locality with no tiered hierarchy, critically meaning if one node falters, the whole network will not be taken out.
- Both have advantages and disadvantages, making it hard to prescribe a relative value to each extreme end.
- The centralised system is very efficient but more susceptible to single-point failure whereas a distributed system is robust with no reliance on a central authority, however it could take a long time for data to pass across

BITCOIN Motivation

- The motivation behind Bitcoin and other DLT apparatuses involves the application of cryptography to monetary networks in order to eliminate trusted third parties across messaging systems.
- Most people already use cryptography when using internet applications, in sending or signing off on packets of data or messages (e.g. the https protocol for internet browsing or Whatsapp for secure peer-to-peer messaging).
- *Encrypted* messages prevent observations from an intermediary and *signing* preventing tampering of data have eliminated the need to trust a third party to carry the message, for example SMSs where data packets go through centralised data exchanges usually administered by Telcom service providers.
- When considering the innovation of blockchain, it allows the same, the elimination of third parties in financial transactions through the use of payment tokens.

BITCOIN Motivation

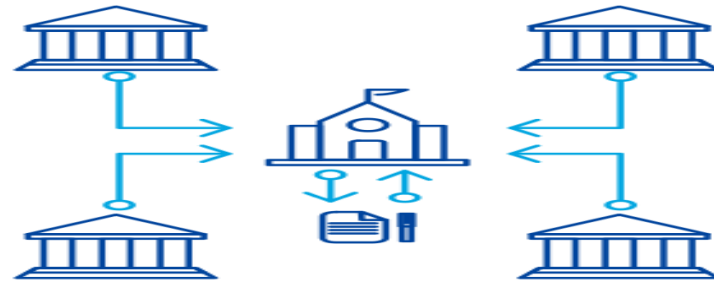
- Some of the benefits of blockchain technology applied to monetary systems are:
- ▷ **Decentralisation** – no single point of trust, no single point of control (no central authority), no single point of failure
- ▷ **Security and Anonymity** – non-repudiation and irreversibility of records with pseudo-anonymous transactions.
- ▷ **Transparency, Auditability, and Governance** – anyone can join participants can verify the veracity of records directly, without external querying.

BITCOIN Motivation

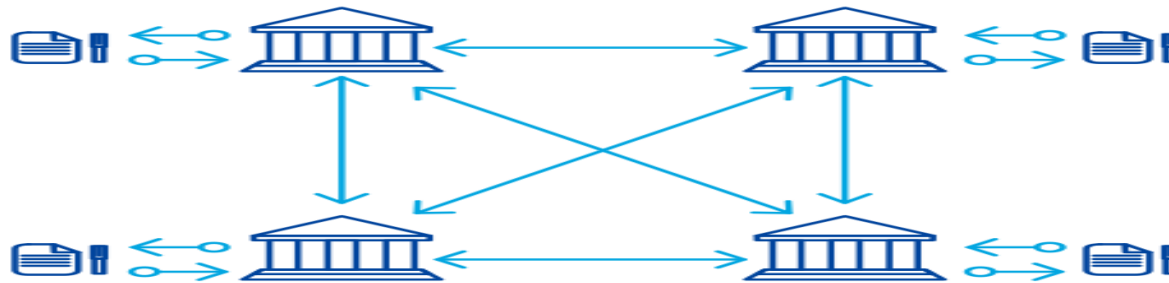
- The focal point here is not money itself, but the way money is used and managed (system of payments), specifically with no intermediation.
- In fact, cryptocurrencies have several similar characteristics to cash (low transaction cost, quasi-anonymity).
- The key difference envisioned by Nakamoto was the stripping out of a centralized authority and clearing house for money, instead having transactions verified by a global group of participants using blockchain technology

FIGURE 13

Centralised and Distributed Ledger Monetary Systems



CENTRALIZED LEDGER



DISTRIBUTED LEDGER

Source: Ward, 2019.

Why Decentralize?

- When considering existing (digital) business models, which are all predominantly centralised, there are certain risks involved to network users.
- Some of these risks include:
 - ▷ **Single-point failure**
 - ▷ **Exclusion, abuse, and mistrust**
 - ▷ **Low Transparency and high transaction fees**

Single Points of Failure

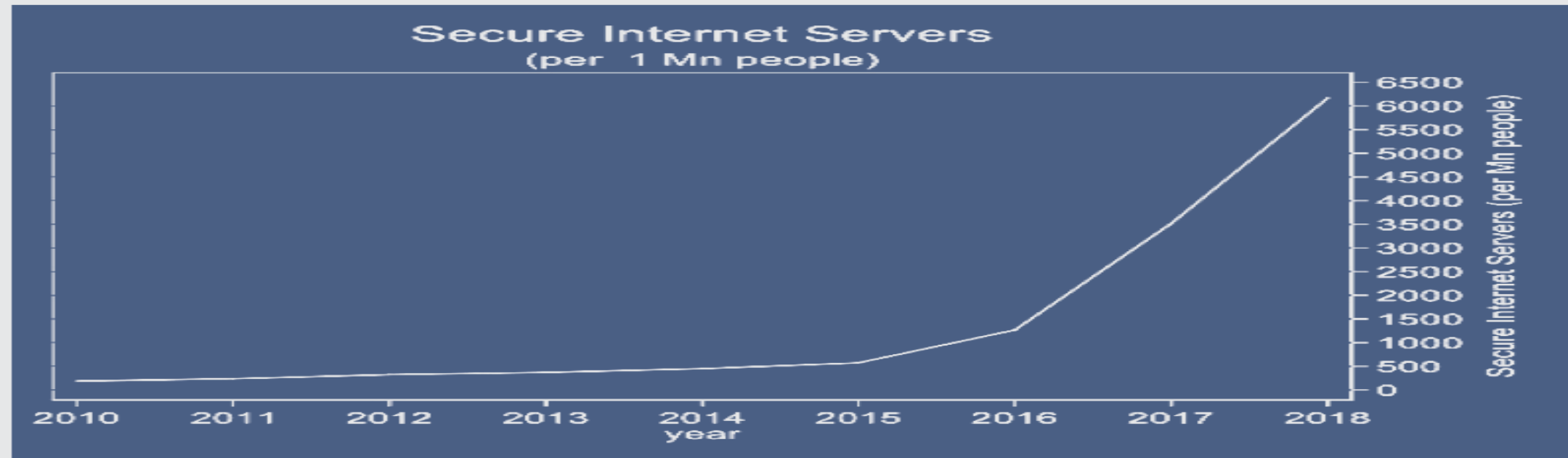
- Peer-to-peer decentralized payment system is inherently more robust than a payment system requiring an intermediary or clearing house.
- Bitcoin achieves this by using a blockchain-based consensus mechanism to manage an agreement on the state of a distributed database. While the network relies on the underlying Internet connectivity (which is itself decentralised), there is no single entity whose failure would disrupt the network.
- Centralised payment systems are exposed to failures of hardware and breaches of security procedures which, in the worst cases, can bring the whole payment network down (as was the case for Visa in Europe on 1 June 2018).
- Having a decentralised network ensures that the failure or break down of any node cannot disrupt the entire system.
- For example, if a central clearing house (say the central bank) was to suffer an attack, this would prevent the entire monetary system from functioning in a centralised system; whereas, an attack on a server in the Bitcoin network would have no effect on the functioning of the system (i.e. users could still make transactions using Bitcoin).

Exclusion, abuse and mistrust

- Blockchain-based permissionless cryptocurrencies have, by design, a uniquely low barrier for entry – any individual can participate in the payment system as long as they have access to an Internet connection.
- This makes it possible for anyone to actively participate in the system and ensure the accountability of others in the network.
- With 1.7bn people in the world without access to a bank account, regular payment providers have often failed to provide access to an effective payments system.
- This is especially true in the midst of a worldwide surge in access to the Internet and secure internet servers as can be seen in the Figure 14 below.
- The decentralized network also prevents a centralized authority from excluding members participation or abusing their unique position as the only group with access to a private ledger.
- This lack of transparency in a centralized system can lead to popular mistrust, which is remedied by allowing all participants access to a common decentralized ledger.

FIGURE 14

World Internet Users and Secure Internet Servers



Data Source: World Bank, 2019.

High Transaction Fees

- With the invention of electronic transfers (credit cards, debit cards, etc.), financial transactions have become considerably cheaper and more efficient over the past thirty years.
- There do remain some types of transactions which require significant third-party fees to complete.
- The most prevalent of these would be transactions involving multiple currencies (i.e. remittances, tourism, imports/ exports of goods and services).
- For example, looking at data from the World Bank for remittance fees over the 2011–2017 period, we can see that remittance fees to some countries are still close to 20%, and still range around 10% in strong emerging economies like China and Thailand.
- A more extreme, and persistent, example of high third-party fees is the exchange of currencies at international airports.

Security and Anonymity of Participants

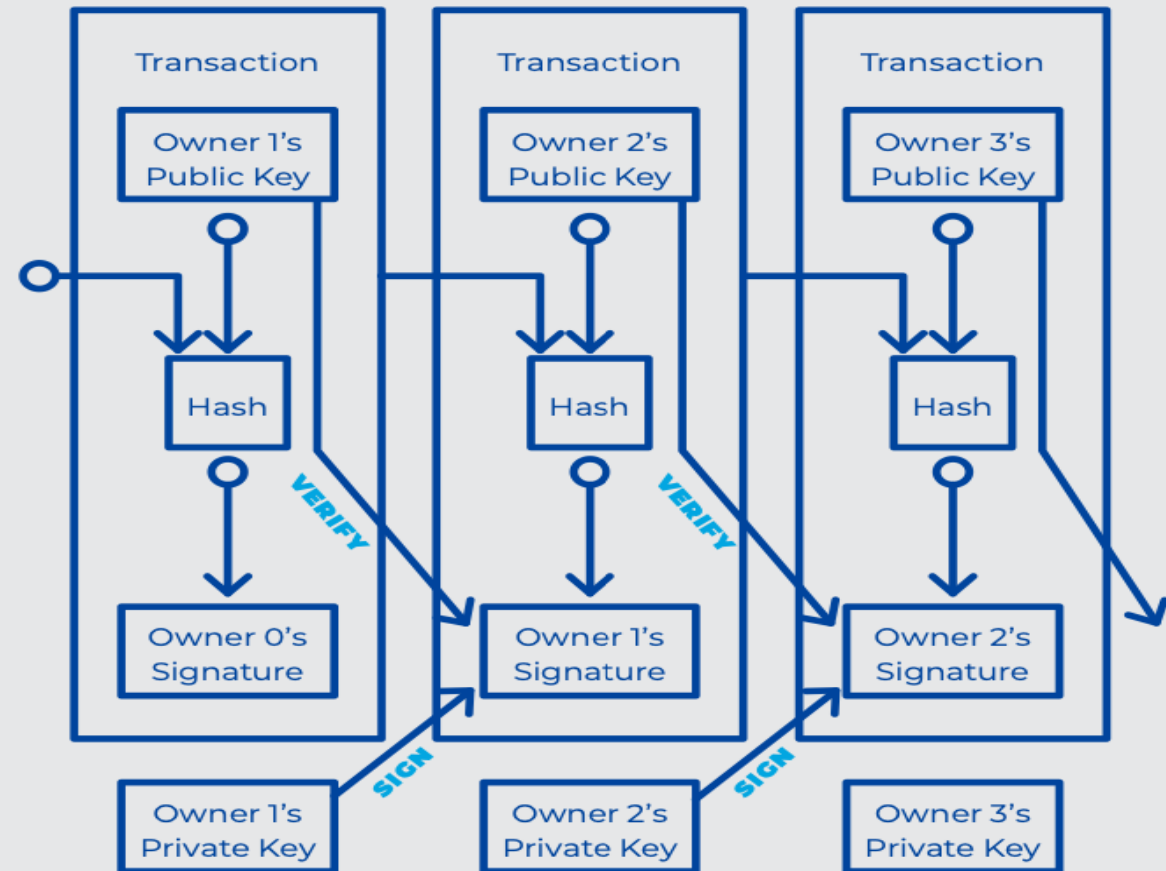
- While blockchain-based transactions are public by the nature of the payment protocol, blockchain-based cryptocurrencies are 'pseudonymous'.
- Transactions can be linked to the public keys they originated from and were sent to, but it is much harder to establish a link between a public key and the identity of the person making the transaction.
- Notably, the transaction is 'pseudonymous' not only from the broader public, but also from the other counterparty – not unlike a cash transaction between two strangers.
- This security and anonymity removes the risk of a financial intermediary misusing client details, having them unintentionally stolen or legally sharing them with third parties (e.g. a suppressive government) without the explicit consent of the client.
- This pseudo-anonymity also helps to overcome some of the problems with purely anonymous cash.
- For example, large movement of funds could be followed as they move through the network, allowing for law enforcement to track conspicuous transactions across the globe.

Transparency, Auditability and Governance

- Similar to banks, blockchain-based cryptocurrencies record all transactions in a secure and immutable ledger.
- The blockchain is a transactions ledger of tokens where the entire history of transactions is recorded.
- One block contains a group of transactions and has a unique pointer that refers to previous blocks in the chain. In contrast to centralized systems or banks, in the case of Bitcoin, the ledger is not stored in one 'safe' place.
- Instead, everyone using Bitcoin (i.e. who has the core software) is connected through a peer-to-peer network and saves a replica of the Bitcoin's blockchain (ledger).
- There are many replicas of the same ledger existing on multiple machines, guaranteeing its safety against system failures or attacks and full transparency for all users on the network.
- Effectively, this means that anyone can access and audit records of all pseudo-anonymous transactions and does not require intervention or permission from a third party (i.e. a central bank).

FIGURE 16

Blockchain Transactions



Source: Nakamoto, 2008.

Why Decentralize?

- In summary, Cryptocurrencies propose to remedy three issues that exist in the current system of payments, mainly, the single point of failure that naturally emerges from centralized / monopolised money, the anonymity of participants, and the exclusion, abuse and trust of users in a system where money is monopolised by potentially irresponsible policymakers.
- Blockchain-based cryptocurrencies also provide a secure environment to transact with no need for expensive third parties and full transparency to all members of the network using a common distributed ledger.
- Lastly, the rules governing these currencies are democratised to allow for members to participate based on publicly available consensus protocols.

Cryptocurrencies in Practice

- In practice, cryptocurrencies (including Bitcoin) have become something different than what was envisioned by Nakamoto (2008). While there is a great deal of competition (Hayek money) in the cryptocurrency market, Bitcoin and other high-profile cryptocurrencies have failed to stabilize their value and subsequently increase their level of trust and acceptability.
- There are also challenges when comparing specific features of cryptocurrencies discussed in theory with cryptocurrencies in practice.
- From 2013, the growth in the number of cryptocurrencies has been impressive. A 2019 Institute and Faculty of Actuaries paper reported that there were 66 varieties of crypto-assets in 2013, 644 in 2016, 1,335 at the end of 2017, and 2,116 in January of 2019.
- (Rochemont and Ward, 2019) The same trend has occurred in terms of market capitalization, where crypto-assets have grown exponentially from around USD 10 billion at end-2013 to USD 572.9 billion at end-2017.
- In terms of trading platforms for crypto assets, as of April 2018, the number had exceeded 10,000. (Rochemont and Ward, 2019)

Cryptocurrencies in Practice

- Cryptocurrencies are purchased with an underlying unit of account (central bank-issued money). This allows us to see what currencies are being converted into crypto- currencies, similar to looking at debt or equity by currency type to get an idea of who is holding that debt or equity.
- In August of 2014, a Bank of England Report estimated that almost 60% of Bitcoin trading was against the Chinese renminbi, 32% traded against the US dollar, 3% against the euro and 1.2% of trading was against the British pound (Ali et al, 2014).
- Since the publication of these figures, there have been significant changes in this composition.
- After a 2017 Chinese government ban on trading bitcoin using renminbi, this composition looks dramatically different as of August of 2019.
- In the 30 day period leading up to August 24th, the US dollar made up around 43% (up from 32%), euro made up around 21% (up from 3%), yen made up around 14% and British pound made up around 13% (up from 1.2%).
- Given the current state of cryptocurrencies in practice, there remain several barriers to overcome when comparing these with the objectives from Nakamoto (2008) discussed above in Section B. We can classify some of these challenges as relating to:

▷ **Token Supply**

▷ **Decentralization**

▷ **Security and Anonymity**

▷ **Transparency and Governance**

Token Supply

- The supply of many cryptocurrencies increases at a fixed ‘controlled’ rate every year and is not actively managed by any centralized authority, which has led to wide swings in their value – for example, the value of 1 Bit- coin climbed to almost 20,000 USD to fall back to around 3,000 USD before slightly rebounding and fluctuating around 10,000 USD over a short two-year period.
- In practice, the supply of Bitcoin is increased at a fixed rate by rewarding miners who are incentivized through award determined by a fixed schedule pre-programmed in the Bitcoin source code.
- As of 2019, the reward amounted to 12.5 BTC; however, every 210,000 blocks Bitcoin halves this reward to regulate the total supply of Bitcoin.
- Miners also can be rewarded by fees attached to the transactions they help record in a decentralized ledger.

Token Supply

- Because the supply of money cannot be actively adjusted to meet demand dramatic fluctuations in value of the most popular cryptocurrencies have occurred since their inceptions.
- This has led many observers, based on the three basic characteristics of money (unit of account, store of value, means of exchange) to rightly conclude that most cryptocurrencies are, in fact, not money.
- In response to the large fluctuations in value, a second generation of cryptocurrency has been designed that pegs a token's value to an existing currency or basket of currencies.
- 'Stablecoins' are currently being used primarily as a tool for exchanges to trade between fiat and cryptocurrencies, and privately between large enterprises to settle trades.
- While stablecoins are very new at the time of writing this report, the future looks optimistic as evidenced by some high-profile projects listed below in Table 3.

Decentralization

- Several advantages of blockchain-based cryptocurrencies were identified, over other forms of money, mainly, overcoming the risks associated with single point failures preventing exclusion, abuse and mistrust, and reducing unreasonably high fees.
- In practice, these still have barriers to overcome.

Single Point of Failure

- While the mining activity is, in principle, decentralised and has very low barriers to entry (a computer with Internet access), over time there are incentives for a degree of centralisation in the activity.
- With centralisation of mining activity, the issue of Single Point of Failure is no longer resolved through a decentralized network, since a large mining pool could compromise the integrity of the whole network.
- For example, a dishonest miner who has more than 50% of the total ability of the network to generate blocks may be able to successfully confirm fraudulent transactions.
- Another factor which would lead to further centralisation is the very low expected payoff to individual miners – a single miner has an extremely low chance of finding a solution to the block.

Exclusion, abuse and mistrust

- As discussed above, the centralisation of mining could lead to a situation where a few cooperating pools have more than 50% of a network's hash-rate, in which case
- In July 2014 the mining pool Ghash.io exceeded 50% of Bitcoin computational power. This is not the only option to break the honest mining assumption; another possibility is collision between miners. In fact, there are different possible attack strategies, incentives and condition in which the stability of the consensus mechanism is in threat (Bahack, 2013; Garay, 2014; Sirer, 2014).
- This possibility of miners, along with influential players altering and forcing specific rules on the Bitcoin network challenges the assumptions of decentralisation. Recently, the Bitcoin community witnessed a panic by a suggestion of Binance CEO of "reorganizing the chain" after the exchange was hacked and lost \$40 million in Bitcoin.
- Fortunately, influential actors advised not to go through with the idea in fear of losing trust in Bitcoin. This conclusion was the main argument of Nakamoto against the majority miner attack, where he argued that "in the long term, it is better to play by the rules" (Nakamoto, 2008).

Lower Fees

- Despite not being classified as money, Bitcoin has succeeded in providing a cheap way of transferring large amounts of capital.
- While the transaction fees have changed significantly over time, on average it cost less than \$1 to have a transaction settle on blockchain with an expected time of 10 minutes (one block).
- The challenge comes when we consider a network for micropayments, as the blockchain fee is (approximately) fixed regardless of the value of the transaction.
- This makes day to day transactions using Bitcoin no cheaper than using a debit, a credit card or other third-party payment systems. There are plans to ramp up the speed and efficiency of Bitcoin transactions, which could help to bring down costs in the future.
- There also exist significant, and well-documented, electricity costs associated with Proof of Work frameworks, requiring huge amounts computational power for a vast network of users, the scale of which was perhaps not envisioned by Nakamoto in 2008.
- The electricity requirements for solving blocks makes this a popular activity in countries with subsidized electricity such as Mongolia. This creates additional issues regarding the degree of centralised control for consortiums in a supposedly decentralised network.

Security and Anonymity

- For all practical purposes, Bitcoin provides 'pseudo-anonymity' only. As the history of all transactions is openly available, with sufficient investigative resources one can often statistically infer the identity of a person behind a public key.
- There exist useful advantages of cryptocurrencies in sending international transfers to countries where they would otherwise be seized by the banking system, as well as a store of value in countries with rampant inflation rates.
- There has been little evidence of governments in countries expending significant effort in curbing this activity.
- Another important drawback of currencies that are anonymous and fully independent of state control relates back to the same arguments made by Sands (2016) and Rogoff (2017).
- If a given type of currency offers anonymity and the guarantee that nobody, including law enforcement, would be able to access the record of transactions, it is very likely that criminals would use this for their financial transactions. In fact, from the perspective of those who wish to perform illegal activities, fully anonymous digital currencies are even better than cash.
- At least cash has a serial number in most countries, which helps to trace its path.
- Moreover, because of its physical nature, transferring large amounts of cash is a cumbersome activity that requires a lot of effort from criminals. With a non-track-able digital form of money, illegal financial transactions could be done instantly and on a global scale.

Governance and consensus protocols

- While the intention of Proof of Work consensus protocols like Bitcoin was to create a democratic decentralised system where all participants have some ability to contribute, it has been found that “the distribution of computing power in Bitcoin reveals that the power of dedicated ‘miners’ far exceeds the power that individual users dedicate to mining, allowing few parties to effectively control the currency” (Gervais, Karame, Capkun, and Capkun, 2014).
- At the time the cited article was published, the top-three (centrally managed) mining pools controlled more than 50% of the computing power in Bitcoin.
- Further- more, Bitcoin users do not have any direct influence over the appointment of the administrators making governance frameworks, which is not very dissimilar from those found on Monetary Policy Committees in Central Banks.

Governance and consensus protocols

- In summary, cryptocurrencies are struggling uphold their creator's objectives.
- To date, no existing cryptocurrency has been universally successful in fulfilling the role of 'money'.
- This is partly due to the technical issues raised throughout this chapter, and partly due to the fact that policymakers, academics and the general public have all held generally negative attitudes about the prospects of money being issued and managed in a decentralized framework and/or by private sector actors.
- From this perspective, central banks in most advanced economies have built a trust premium compared to private sector companies, which should make them better candidates for issuing money and managing/regulating financial transactions.

References

- Li, R., Barrdear, J., Clews, R. and Southgate, J. (2014) The Economics of Digital Currencies – BOE Quarterly Bulletin 2014 Q3
- Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014) Innovations in payment technologies and the emergence of digital currencies – BOE Quarterly Bulletin 2014 Q3
- A. Gervais, G. O. Karamé, V. Capkun and S. Capkun, "Is Bitcoin a Decentralized Currency?," in *IEEE Security & Privacy*, vol. 12, no. 3, pp. 54-60, May-June 2014.
- Baran, P. *On Distributed Communications*. Rand Corporation, 1964.
- Barrdear, J. and Kumhof, M. (2016). The macroeconomics of central bank issued digital currencies. BOE Staff Working Paper No. 605
- Benes, J. and Kumhof, M. The Chicago Plan Revisited. IMF Working Paper WP 12/202.
- Bernanke, B., & James, H. (1990). The Gold Standard, Deflation, and Financial Crisis in the Great Depression: An International Comparison. *NBER Working Paper* No. 3488.
- Bordo, M. (1995). Is There a Good Case for a New Bretton Woods International Monetary System? *American Economic Review*.
- Bordo, M. (2018). The imbalances of the Bretton Woods System 1965 to 1973: U.S. Inflation, The Elephant in the Room. *NBER Working Paper* No. 25409.
- Bösl, S. M. (2019) Mehrheit der Deutschen skeptisch bei Facebooks Libra. <https://www.finanzwende.de/presse/mehrheit-der-deutschen-skeptisch-bei-facebooks-libra/?L=0>
- Craig, B. (1996). Competing Currencies: Back to the Future? *Federal Reserve Bank of Cleveland Economic Commentary*.
- Doidge, F. and Exton, J. (2018) Cracking the code on cryptocurrency. ING International Survey Mobile Banking – Cryptocurrency June 2018
- du Toit, G., Bradley, K., Swinton, S., Burns, M. and de Gooyer, C. (2018) In Search of Customers Who Love Their Bank. Bain and Company Report, November 14, 2018
- Eichengreen, B. (1986). The Bank of France and the sterilization of gold, 1926-1932. *Explorations in Economic History*.
- Endres, A. (2009). Currency Competition: A Hayekian Perspective on International Monetary Integration. *Journal of Money, Credit and Banking*.
- Exton, J. From cash to crypto: The Money Revolution. ING International Survey ING International Survey, New Technologies, September 2019 September 2019
- Fisher, I. (1936). 100% Money and the Public Debt.
- *Economic Forum Spring Number, April-Jun.*
- Friedman, B. (1999). The Future of Monetary Policy: the Central Bank as an Army with only a Signal Corps? *International Finance*.
- Hanke, S. and Kwok, A. (2009). "On the Measurement of Zimbabwe's Hyperinflation", *Cato Journal*, Vol. 29, No. 2 (Spring/Summer 2009).
- Hayek, F. (1978a). *Choice in Currency*. Chicago University Press.
- Hayek, F. (1978b). *The Denationalization of Money: An Analysis of the Theory and Practice of Concurrent Currencies*. Chicago University Press.
- Hoppe, H.-H. (1994). How is Fiat Money Possible? -- or the Devolution of Money and Credit. *Review of Austrian Economics*.

References

- Kaminska, I. What mobile money giveth, it also taketh away. FT Alphaville, November 23, 2015. <https://ftalphaville.ft.com/2015/11/23/2145684/what-mobile-money-giveth-it-also-taketh-away/>
- Kaminska, I. (2015). Mpesa: the costs of evolving an independent central bank' FT Alphaville, July 2015. <https://ftalphaville.ft.com/2015/07/15/2134081/the-collateral-velocity-and-sovereign-costs-of-mobile-money/>
- Kindleberger, C. (1989). *Economic Laws and Economic History*. Cambridge University Press.
- Lawson, Tony (2016) 'Social positioning and the nature of money', *Cambridge Journal of Economics*, 40 (4): pp. 961–996.
- Lawson, Tony (2018) 'Debt as money', *Cambridge Journal of Economics*, 42 (4): pp. 1165–81.
- Lawson, Tony (2019) *The Nature of Social Reality: issues in social ontology*, London and New York: Routledge.
- Morgan Jamie, and Brendon Sheehan (2015) 'The Concept of Trust and the Political Economy of John Maynard Keynes, Illustrated Using Central Bank Forward Guidance and the Democratic Dilemma in Europe', *Review of Social Economy*, 73 (1): 113–137.
- Nakamoto, Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System, paper downloaded from <https://bitcoin.org/bitcoin.pdf> on 01/09/2018.
- Pratten, Stephen (2017), 'Trust and the social positioning process', *Cambridge Journal of Economics*, Volume 41, Issue 5, 1 August 2017, pp. 1419–1436.
- Minsky, H. P. (1992). The Financial Instability Hypothesis. *Levy Economics Institute Working Paper*.
- Minsky, H.P. 1994. Financial instability and the dedine (?) of banking: future policy implications. Working paper No. 127, October 1994. The Jerome Levy Research Institute of Bard College.
- Mundell, R. (2000). A Reconsideration of the Twentieth Century. *American Economic Review*.
- Rochemont, S. and Ward, O. (2019) Understanding Central Bank Digital Currencies (CBDCs). Institute and Faculty of Actuaries, March 2019.
- Simons, H. (1946), "Debt Policy and Banking Policy", *Review of Economic Statistics*, 28 (2), 85–89.
- Temin, P. (1989). *Lessons from the Great Depression*. Cambridge University Press.
- Tasca, Paolo and Tessone, Claudio, Taxonomy of Blockchain Technologies. Principles of Identification and Classification (March 31, 2018). Available at SSRN: <https://ssrn.com/abstract=2977781> or <http://dx.doi.org/10.2139/ssrn.2977781>
- Varston, N (2012) Trust and Reputation in Financial Services. Driver Review DR30. Foresight, UK Government Office for Science
- Weir, M. (2019) Boom in the Benjamins. IMF Finance & Development, June 2019, Vol 156, No. 2
- Wolf, M. (2014, April 24). Strip private banks of their power to create money. *Financial Times*.
- Adrian, T. and Mancini-Griffoli, T. (2019). The Rise of Digital Money. IMF Fintech Notes, July 2019
- Barker, J.; Clayton, E.; Dyson, B. and Mearns, J. (2016) Broadening Narrow Money: Monetary Policy with a Central Bank Digital Currency. Bank of England Staff Working Paper No. 724.
- Bech, M. L., Faruqi, U., Ougaard, F., & Picillo, C. (2018). Payments are a-changin but cash still rules. BIS Quarterly Review, March.
- Berentsen, A., & Schar, F. (2018a). The case for central bank electronic money and the non-case for central bank cryptocurrencies.
- Berentsen, A., & Schar, F. (2018b). A short introduction to the world of cryptocurrencies.
- Bordo, M. D., & Levin, A. T. (2017). Central bank digital currency and the future of monetary policy (Tech. Rep.). National Bureau of Economic Research.

References

- Broadbent, B. (2016). Central banks and digital currencies. Speech at London School of Economics.
- Brunner, K. and Meltzer, A. H. (1971) The Uses of Money: Money in the Theory of an Exchange Economy. *The American Economic Review* Vol. 61, No. 5 (Dec., 1971), pp. 784-805
- Carstens, A. (2019). The future of money and payments. Speech by General Manager of the BIS at the Central Bank of Ireland, Whitaker Lecture.
- Coeur, B., & Loh, J. (2018). Central bank digital currencies. CPMI Papers.
- Dyson, B., & Hodgson, G. (2016). Digital cash: why central banks should start issuing electronic money. Positive Money.
- Engert, W., Fung, B., et al. (2017). Central bank digital currency: Motivations and implications. Bank of Canada.
- Fisher, I. (1936). 100% money and the public debt.
- Goodfriend, M. (2016). The case for unencumbering interest rate policy at the zero bound. In Federal reserve bank of kansas citys 40th economic policy symposium. Jackson Hole, wy. august (Vol. 26).
- Gurtler, K., Nielsen, S. T., Rasmussen, K., & Spange, M. (2017). Central bank digital currency in denmark? Analysis.
- Keynes, J. M. (1930). *A Treatise on Money*. Macmillan and Co. Ltd. St Martin's Street, London, 1930
- Kumhof, M., & Noone, C. (2018). Central bank digital currencies-design principles and balance sheet implications.
- Lagarde, C. (2018). Winds of change: The case for new digital currency. Delivery by IMF Managing Director, Singapore Fintech Festival.
- Lowe, P. (2017). An eaud. Address to the 2017 Australian Payment Summit, Sydney, Australia, 13 December, 2017
- Mersch, Y. (2017). Why europe still needs cash. Contribution by Yves Mersch, Member of the Executive Board of the ECB for Project Syndicate, 28 .
- Raskin, M. and Yermack, D. Digital Currencies, Decentralized Ledgers, and the Future of Central Banking. NBER Working Paper No. 22238
- Riksbank, S. (2017). The riksbanks e-krona project. Riksbank Studies, Report, 1 .
- Rogoff, K. S. (2017). The curse of cash: How large-denomination bills aid crime and tax evasion and constrain monetary policy. Princeton University Press.
- Sands, P., et al. (2016). Making it harder for the bad guys: the case for eliminating high denomination notes. Harvard Kennedy School, Mossavar- Rahmani Center for Business and Government.
- Skingsley, C. (2016). Should the riksbank issue e-krona? speech at FinTech Stockholm, 16 .
- Smithin, J. (ed) (2000). *What is Money?* Routledge Press
- Tobin, J. (1986). Financial innovation and deregulation in perspective. Cowles Foundation for Research in Economics at Yale University.

References

- Woodford, M. (2000). Monetary policy in a world without money. *International Finance*, 3 (2), 229–260.
- A. Laszka, B. J. (2015). When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long- Term Impact of Attacks Between Mining Pools. *Workshop on Bitcoin Research*.
- *all cryptocurrencies*. (2012). Retrieved from coinmarketcap: <https://coinmarketcap.com>
- Androulaki, E. K. (2013). Evaluating user privacy in bitcoin. *International Conference on Financial Cryptography and Data Security* (pp. 34-51). Springer.
- Bahack, L. (2013). *Theoretical Bitcoin Attacks with less than Half of the Computational Power*. Retrieved from arXiv preprint arXiv:1312.7013.
- Barrera, C. &. (2018). SSRN . Retrieved from Blockchain upgrade as a coordination game.: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192208
- Courtois, N. T. (2014). *On the longest chain rule and programmed self- destruction of crypto currencies*. Retrieved from arXiv preprint arXiv:1405.0534.
- Gervais, A. K. (2014). Is bitcoin a decentralized currency? *IEEE security & privacy*, (pp. 54-60).
- Herrera-Joancomartí, J. (2014). Research and challenges on bitcoin anonymity. *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* , 3-16.
- J. Garay, A. K. (2014). *The Bitcoin Backbone Protocol: Analysis and Applications*. Cryptology ePrint Archive, Report 2014/765.
- Laurie, B. (2011). *An Efficient Distributed Currency*.
- M. Babaioff, S. D. (2012). On Bitcoin and Red Balloons. *SIGecom Exchanges*, 56–73.
- Meiklejohn, S. P. (2013). A fistful of bitcoins: characterizing payments among men with no names. *The 2013 conference on Internet measurement conference* (pp. 127-140). ACM.
- N. T. Courtois, M. G. (2014). Optimizing sha256 in bitcoin mining. *Cryptography and Security Systems*.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <http://bitcoin.org/bitcoin.pdf>
- Sirer, I. E. (2014). Majority is not enough: Bitcoin mining is vulnerable. *In Financial Cryptography*.
- T. Bamert, C. D. (2013). Have a snack, pay with Bitcoins. *IEEE P2P*.



Thank You