# Re-Defining Financial Technology: Bitcoin

With the emergence and the rapid growth of the internet, our habits have changed drastically. With these new developments, one of the major areas affected is the financial system. Upon using the conservative banking ecosystem for hundreds of years to exchange information and money, humanity is now evolving to a peer-to-peer transaction system with Bitcoin being the leader of this act. Throughout the 1900’s, lots of new products and technologies tried to introduce new payment methods and transaction systems. Some of these products can be given as “Mondex, Digicash, HashCash, and Bitgold” which will be covered and compared with Bitcoin in the later parts of this paper. But, as of 2024 only Bitcoin is being widely used and recognised by the people of the World. This paper tries to elaborate on why Bitcoin is the most important FinTech development by comparing it with other FinTech products and developments and tries to explain the advantageous and different aspects of Bitcoin that make it popular and practically usable.

According to the Paper “Token- or Account-Based? A Digital Currency Can Be Both”, published by Rod Garratt, Michael Lee, Brendan Malone, and Antoine Martin (2020); there are 2 financial systems that can be stated as “token-based systems” and “account-based systems”. The token-based system is the system where transactions take place mostly physically and the only thing that peers should be aware of is the authenticity of the medium that is being used. The transaction happens in real time and no bookings must be kept. Whereas in the account-based system, the transaction should pass through intermediaries which also apply KYC procedures and other regulations to verify and secure the transaction. The transaction is also being booked down and accounted for. The problem with the token-based systems is that they mostly, restrict both parties to be present physically and they require parties to examine and validate the authenticity of the token that is being transferred. The account-based systems also cause some problems. The main problem is that the presence of a 3rd party is a must, and both parties should check through security steps to complete the transaction. Until January 2009, no person or institution has been able to practically merge these two transaction methods and solve their problems once and for all until Bitcoin. With the adaptation of a ledger, all the transactions are auditable like account-based systems, and tokens are used as a casual means of the payment system (Dr. Jack Rogers, 2023). Just like the token-based systems. Therefore, it proposes a new and revolutionary monetary system that no other FinTech product has proposed before.

Another major issue that Bitcoin directly addresses is double spending without the usage of an intermediatory party. According to Satoshi Nakamoto (2009), Online payments might be transmitted directly between parties without passing through a banking institution if electronic cash was only available peer-to-peer. Digital signatures help, but if a reliable third party is still needed to stop double-spending, the primary advantages are negated. Bitcoin suggests utilizing a peer-to-peer network as a solution to the double-spending issue. By hashing transactions into a continuous chain of hash-based proof-of-work, the network creates a timestamp that cannot be altered without repeating the proof-of-work (updating the UTXO Set). In conservational monetary transactions, double spending is a possibility if the person spends on 2 things at the exact same time with money, enough only for one of the payments whereas on bitcoin, it is guaranteed that only one of the payments will proceed if the amount exceeds the current balance.

It is previously stated that transactions are hashed through a continuous chain in the Bitcoin Network. To be more specific, Bitcoin uses ECDSA which is an unsymmetrical hashing algorithm unlike Swift, or even PayPal which uses a SHA-1 Algorithm. In BTC, SHA-256 is utilized for the continuity of the chain. A root called Merkle Root is fed with new transactions every 10 minutes and this root summarizes all the transactions into one single 256-bit object. According to Stig F. Mjolsnes (2011), since the length of the key of SHA-256 is larger than SHA-1, it makes the algorithm less vulnerable to cyber threats. Therefore it should be noted that the encryption of Bitcoin is relatively safer than Swift and PayPal. If we examine the previous attempts for a digital currency, neither Mondex, Digicash, nor HashCash uses a SHA-256 hashing algorithm.

So far, this paper evaluated the technical aspects of Bitcoin. The next aspect to elaborate on and compare Bitcoin with the other FinTech developments is the commercial and practical usage of the product. Since 2009, Bitcoin managed to gain a reputation and therefore the market cap has increased drastically. As of 2024, people who would like to transact information or tokens in an auditable environment where smart contracts can also be utilized have selected Bitcoin to do their transactions. One of the key aspects that paved the way for Bitcoin has been the Cypherpunks. Since the early 1980’s, cypherpunks wanted anonymity while making transactions and they wanted to avoid state-regulated currencies while doing so. These motivations led to various FinTech products but none of them could reach to mass populations and became popular. An example can be given as Digicash which was proposed by David Chaum in 1989. Parties transacting through Digicash were kept anonymous as the transaction proceeded, but since the transaction required a third party (banks), the proceeding transaction could be seen while keeping the parties anonymous. The problem with this product was that requirement of a third party was necessary. So, it was not completely peer-to-peer. Also, since the sides were kept anonymous, it hasn’t been recognized by large funds or capitals and couldn’t reach mass populations.

HahCash was another prospect that aimed to be a well-known electronic cash. It was first surfaced in 1997 by Adam Back. But the problems of involving a 3rd party couldn’t be thrust through. Therefore, it couldn’t shine among the other alternatives. But it should also be noted that real-world implementations of this digital cash have been seen in the early 2000s but like the other digital currencies to that date, it couldn’t reach to a well-defined popularity.

Mondex on the other hand is one of the other products that aimed to be a digital currency in the late 1990’s. It was an electronic cash payment system. The troubles that Mondex faced was that the users had to go through a security check and KYC procedure which was unusual at that time. So, people haven’t bothered to go through the process and it couldn’t be a popular FinTech Product in the end. If we compare it with having a Bitcoin wallet which every usual person can achieve in minutes while being at home, we can clearly observe the importance of customer friendliness affecting the total usage of a product. Also, the recognition of Mondex by banks was another issue. Not all of the banks were recognizing Mondex, therefore it was a challenge to transfer funds to a Mondex Card, whereas people can easily transfer between their Bitcoin Wallet and their fiat currency wallet in seconds today. This again shows customer experience being one of the pioneers that pave the way for these products.

If we were to compare Bitcoin with FinTech Products which remain to be popular today, we can give PayPal an example. PayPal has been used since 1998 and it is one of the most popular payment systems. It has been integrated into various stores and people can pay securely through it in different locations in the world. However, the big difference between PayPal and Bitcoin is that PayPal is a centralized medium that enables you to transfer fiat currencies to other accounts. It is completely an account-based system. Bitcoin is decentralized, and users can make transactions of a token with a limited supply which can arguably lead to being inflation-proof with each other. So, unlike PayPal, it is not another layer that is added up to the conservational banking, but it is a brand-new transaction medium that is both account and token-based.

In conclusion, Bitcoin stands out as the most significant FinTech development, surpassing earlier attempts such as Mondex, Digicash, HashCash, and even contemporary systems like PayPal. Bitcoin successfully integrates token-based and account-based systems, offering a revolutionary solution to the long-standing challenges of peer-to-peer transactions. Its decentralized nature, employing a solid SHA-256 hashing algorithm for security, addresses issues like double spending without the need for intermediaries. Unlike its predecessors, Bitcoin gained widespread popularity due to its user-friendly nature, allowing individuals to transact securely and efficiently without cumbersome security checks. The Cypherpunk movement's emphasis on anonymity further fueled Bitcoin's success. Comparing it to centralized systems like PayPal, Bitcoin's decentralized, limited-supply token-based approach presents a novel paradigm in financial transactions, making it a truly groundbreaking and influential development in the world of FinTech.

# References

*Rogers, J. (2023).*Topic 2: History of Money, Bitcoin and Blockchain. *University of Exeter. Financial Technology. https://www.exeter.ac.uk/study/postgraduate/courses/economics/fintech/*

*‌ Garratt R, Lee M, Malone B, and Martin A. (2020, August 12). Token- or Account-Based? a digital currency can be both - liberty street economics. Liberty Street Economics. https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/*

*Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf*

*Mjolsnes, S. (2011, November). A Multidisciplinary Introduction to Information Security. CRC Press.*