Deep Science Publishing
https://doi.org/10.70593/978-81-988918-1-5_7

DeepScience
Open Access Books

Chapter 7: The future of digital payments: Blockchain, mobile transactions, and decentralized finance

7.1. Introduction

In a bank-centered financial system, digital payments basically mean how customers access their bank deposits to settle payments. Retail payments are mostly settled through government and commercial banks, but at RTGS level, payments occur through settlement controls of the central banks. In contrast, digital payments in a decentralized currency-based financial system involve no banks or financial institutions. In brief, it is the entire banking system and not just its accounts that do not participate in digital payments.

Digital payments are the electric wiring that connects everyone at the 'exchange' and 'conversion' levels of the macroeconomic circuit, including consumers, businesses, banks, and central bank. In addition to money transfers, digital payments also provide complementary services needed in consumption and Ecommerce, such as invoicing, matching buyers and sellers, clearing, and settlement. Unlike most circuit activities, digital payments do not have a multiplier effect because of digital payments' one-for-one service charge. Digital payments also have a major role in the rapid and invisible collection of indirect taxes. Digital payment systems, whether wallet-based or interbank-based, extricate the economy from the "cash flow and multiply" mechanism that has characterized the world economy ever since barter systems were replaced by elaborate currencies. Paper currencies also have become obsolete and are headed for complete replacement by digital payments (Gai et al., 2018; Chen et al., 2019; Arner et al., 2020).

Blockchain technology consists of a distributed ledger shared by all nodes in the system, records of transactions among network participants—stored in the database as transactions, blocks, and chains—the blockchain protocol that maintains the integrity of the database, and smart contracts that automate transaction processing. The multiple and

often anonymous parties in a blockchain network are enabled to transact with others by employing cryptographic keys that are adequately protected. Cryptography protects confidentiality and authenticates transaction participants, the blockchain protocol protects data integrity by implementing the consensus mechanism ensuring that all nodes have up-to-date and correct data, and smart contracts automate the execution of transactions when predetermined conditions are met (Narayanan et al., 2016; Tapscott & Tapscott, 2018).

Fig 7.1: Blockchain and the Future of Decentralized Finance

There are several key features that collectively distinguish blockchain technology from other types of digital transaction systems. The first is decentralization. Instead of a central authority that authorizes, executes, and records transactions along with maintaining digital transaction history, blockchain distributes all these functions among the multiple nodes within the blockchain network. Transactions can occur among any two or more relay participants without the need to go through a central authority. This feature creates efficiencies in transaction costs and speed, especially in cross-border

payments that involve multiple banks clearing and settling transactions as they pass through each bank's correspondent accounts until the transactions reach their final destination.

7.2. Key Features of Blockchain

Blockchain is a decentralized ledger which means it is not managed by one entity. All data is stored in blocks and is organized into a non-alterable chain. The blocks contain necessary details such as timestamp, block identifier, and hash pointer to the parent block, and data with verification. Blockchain is secure. It establishes consensus on a decentralized network, removes possible fraud, and provides secure transactions. The data is not managed by one entity but is hosted by many nodes, all of whom have a copy of the database. These nodes ensure security such that if there is a transaction in the network, it is examined by the nodes to check for legitimacy; when certified, it is then entered as a block in the database by some of the nodes, and they are compensated in the form of cryptocurrencies. This assures that the data is backed up always and is valid for use.

The use of cryptography provides a security layer to blockchain. Unlike the familiar web protocol which protects information that is sent across the network, blockchain protects both stored data and information sent across the network. The combination of trust on a network and the cryptography makes it a digital money's system: a system where people trust the network, and cryptography provides certainty. Blockchains are trackable. Anyone can check who did what and where did the record go. Immutable means that people cannot go back in time, alter a past record, and change history as they could with an online database. The immutability of digital asset records on the blockchain makes it easier for companies to show support that their digital assets have not been tampered with. The transparency of blockchain can ensure that rights are not infringed upon.

7.2.1. Types of Blockchain

There are four basic types of blockchain. Each has its unique functionality, permissioning, and use cases. The four types mentioned here are: Consortium or Federated blockchain; Public or Permissionless blockchain; Private or Permissioned blockchain; and Hybrid blockchain.

Public or Permissionless blockchain is a class of blockchain that allows anyone to join and participate. It is completely decentralized in nature and open to all. Anyone can create a wallet and mine (or stake) on the network. All the transactions in a public blockchain are not only stored on the blockchain ledger and verifiable by its members,

but are also open to the public. Therefore, these blockchains are best suited for cryptocurrencies or coins. In fact, public blockchain are better for use cases where trust is an issue.

Private or Permissioned blockchain are private, and allow only a pre-selected group to join. Access is not open to all. Therefore, they are not truly decentralized and run on a centralized structure. The whole network is maintained by a single trusted entity, though multiple parties may be provided with access. No one outside the group can view and verify the transactions. Private blockchains are recommended for use cases that have a select group of parties involved and wish to conduct transactions privately without outside interference.

Federated or Consortium blockchain are managed by a group of organizations. Nodes are selected and can be controlled by an outside entity. Access to this type of blockchain is provided to only selected participants. Not all transactions are visible to the public. A hybrid blockchain is one that possesses features of both the public and the private blockchain. While the private side of the hybrid model provides an organization with control over who views what on the blockchain, the public side ensures transparency and security.

7.3. Mobile Transactions: Current Trends

The swift adoption of mobile technology has spurred on the number of mobile transactions and led to increasing interest in mobile payment solutions. The global shift to mobile and digital transactions has created a property-hot landscape for digital payment and app-driven start-ups in developing markets, led by a prominent mobile payment service, which has attracted millions of users in various countries, as well as in markets like Asia and Latin America. It has also provoked fierce efforts from the established banks and credit card companies, facing growing competition from cardless payments. Indeed, across all global fintech markets – payments, lending, investment management, digital banking, insurance and technology solutions – growth in mobile payments and P2P capabilities offers a tantalizing prospect.

While the consensus runs that mobile payment solutions operate in a separate market from digital currencies, the two areas are starting to overlap. Blockchain projects are developing fast solutions that bypass traditional banking systems and allow for cheaper cross-border transactions. Security issues are front and center: a series of high-profile hacks of cryptocurrency wallets have exposed vulnerabilities. Lack of mass market human behavior changes, convincing users to overcome their local inertia, are another barrier to the wider uptake of digital currency solutions. Nonetheless, the potential for the use of blockchain technology in mobile transactions is great.

7.3.1. Growth of Mobile Payment Solutions

Several companies that existed before the advent of mobile platforms have jumped onto the mobile payments bandwagon. Recently, a mobile payments application for Apple devices was released. A mobile payment solution allows users to access their accounts and make purchases from wherever they are, using a device's Wi-Fi connection. Other similar services have also emerged and gained popularity among merchants. A startup has focused on pushing electronic tipping, allowing people to tip for services via phone. With this service, a third party would accumulate users' credit balances, allowing merchants to carry out some transactions without fees. Money on account, however, would not earn interest because of the way the liability is structured.

The merger between the banking sector and telecommunication infrastructure opened the door for another successful solo venture in this area: SMS banking. An example of SMS banking is a service offered in various countries by an ATM operator and networks service provider. Users set an ATM withdrawal amount on their mobile phone and send a text message to a service number to authorize the application. Minutes later, users receive a text back with a special PIN code. To complete the withdrawal, the code and account number must be typed into the ATM, which is programmed to accept withdrawals only from pre-registered customers at scheduled times. Encryption is used to secure the service. The operator is not directly responsible if a device is stolen or robbed.

7.3.2. Security Challenges in Mobile Transactions

Mobile payments, characterized by their ease of use and other positive user-assisted factors, also feature serious hurdles in terms of implementation regarding security. The most noteworthy point is that mobile devices are subject to less physical control than card-based transactions, both the point of sale and the possession of the mobile itself. In addition, distant interactions within both payment-related processes and the provisioning of services can be held explicitly responsible for the success or failure of a conclusion.

Mobile payment systems have possible entries such as mobile malware and spyware fallacies, which may intercept sensitive data being communicated between different system components. Specific vendor solutions implement an in-depth authentication method that attempts to minimize risks. The presence of trustworthiness can act against possible attacks. Conversely, customers trust the different service providers who

implement multiple security-enhancing factors such as fingerprints, cell ID, and PINs to carry out successful authentication procedures.

Another methodological hurdle is user awareness. Prospective users should know about safe usage techniques through education and training. Several security frameworks for mobile services and/or payment tools have already been developed, focusing on technical as well as policy aspects; security-related criteria of various mobile payment systems have already been evaluated. Related studies report high system risk level for more conventional mobile payment methods, and the most vulnerable parts of mobile payment-related services are non-finance-related ones. These two observations point to the necessity for more technical security enhancements in the field of mobile transactions, as well as for educating users on using current systems and on general behavioral safety issues. Both these findings can be supported through scenarios that include urges to deliver security-related protocols and other related provisions to interested parties.

7.4. Decentralized Finance (DeFi) Explained

To some people, all these new DApps and protocols that bring liquidity and credit, or stamp a bond, into the blockchain universe are all labeled as "DeFi". For some, that's enough and they consider that a big enough mess to be in. For other crypto enthusiasts, DeFi is the sum of several pieces of infrastructure with a clear utility: it is all about making transactions, lending, and borrowing assets; trading derivatives; exchanging foreign currency; and offering insurance - all without intermediaries and with transparent protocols. In this case, what better label for that universe than its functionality? In this sense, DeFi not only refers to specific pieces of DeFi infrastructure, but it defines a whole industry of protocol-based transactions and services. This paper adopts the latter definition. Hence, in this work, DeFi is the FinTech universe on an open blockchain, especially on Ethereum.

Why would anyone take a $200 debit card from a bank, when a $20 one would do? Or pay up to 3% fees per transaction, toward a bank, a card issuer and the payment processors, when you could pay a few cents, to strung together smart contracts? Moving funds in crypto, it turns out, is actually a lot easier than moving funds in fiat. One does not even have to pay gas fees; transfers using a stablecoin are almost instant and the assets just live on the Ethereum blockchain. Centralized exchanges are usually responsible for the relatively high costs of fiat-crypto transfers, but recent innovations in decentralized finance (DeFi), like liquidity mining, have made market makers in gas fees abundant.

7.4.1. Core Principles of DeFi

DeFi is an open-source financial system, built on the Ethereum blockchain. It consists of decentralized protocols and services that offer a wide range of sophisticated functionalities, many of which are practically indistinguishable from those provided by centralized financial services. In fact, the combination of DApps and decentralized protocols built on DeFi has produced a huge expansion of financial services being offered and used, even in totally new areas of finance, such as blockchain-based non-fungible tokens or mixed-use services like a DApp for finding rideshare workers and riders, that lets users transact payments directly in the app using the blockchain.

DeFi has several core principles that set it apart from traditional finance. First, the DeFi ecosystem is open to all. Anyone with a smartphone and internet access can access DeFi financial services anytime, anywhere. Second, DeFi is built on trustless protocols — anyone can write, execute, and audit DeFi code without requiring permission from any organization. This codified trust allows DeFi DApps to work on a peer-to-peer basis, thus minimizing centralized control, costs, and risks. Third, cryptoassets are the foundation of the DeFi ecosystem. Owners of cryptoassets can use them directly to build, and transact on, these DeFi protocols without the need to convert crypto to fiat currency. Fourth, DeFi adopts the best of blockchain technology, blockchain transparency, strong programmability in smart contracts, and algorithmic guarantees in a code-based trust environment. Features such as teamless identity, low cost of entry/exit, DeFi composability, and algorithm-driven direct peer-to-peer transactions minimize the costs associated with outdated financial services and create new, and very disruptive consumer value propositions.

7.4.2. DeFi vs Traditional Finance

As much as DeFi looks to revolutionize traditional financial services, there are certain aspects of finance that they've borrowed wholesale. Managing identity is the one area where DeFi has a distinct advantage over TradFi. In DeFi, our identity is linked to a wallet which is completely anonymous to all except the owner. Furthermore, there is no centralized server that can be hacked or records that can be lost. Our online identities are less secure as we're reliant on centralized organizations to manage authentication protocols and servers. Because of this centralization, we also lose control of our data, exposing us to the risk of censorship, surveillance, and hacking.

Scalable transactions, low gas fees, and fraud protection are advantages that favor TradFi. Currently, DeFi is still in its infancy, mainly because of low transaction speeds, high gas fees, and the potential for fraud. By switching to blockchain-based databases, TradFi moves to a more decentralized solution that can handle transactions in real-time,

at scale, whilst remaining secure. This will be useful for mission-critical operations that we want to monitor live. Rapid access to treasury operations can thwart attempts at fraud. For example, a minute-long wait on a quarter-billion-dollar bank transfer to the wrong account can prevent a potential multimillion-dollar loss. Having an auditor chomping at the bit for a transaction to go through could help deter shady activity amongst bank executives or executives of companies that accept bank transfers.

7.5. Cryptocurrencies and Their Role in Digital Payments

Cryptocurrencies are typically distinguished from other digital currencies by their decentralized and open characteristics. Three types of currency, however, have similar properties. Those are loyalty points, national digital currencies, and private central bank digital currencies. Cryptocurrencies operate in a different way. Functions of both “digital currency” and “cryptocurrency” conduct against an operation backboned by a totally decomposed infrastructure, relying on consensus through the blockchain among included participants, so no central authority problem exists. Cryptocurrencies, like other digital currencies, seek to imitate national currencies' circulating function. Cryptocurrencies are governed by rules determined in coded protocols that use trustless and permissionless technology. Unlike other digital currencies, which are typically generated by private firms or institutions issuing unique data tokens linked to some redeemability condition compliant operation or liquidity condition guaranteed by the issuer, cryptocurrencies are non-fiduciary currencies that incorporate programmability.

Backed by two engines, currency networks' demand side and transaction cost's supply side, cryptocurrencies favor the reduction of transaction costs against traditional payment systems. Payment systems hold fewer weaknesses than cryptocurrency networks hold advantages in order to absorb the grand scale of payments activity's extreme concentration pressure. The situation remains the same even in the Web3 environment emerging with blockchain technology, based on a shift from data legibility to data availability, based on controlled self-custody of data and user behavior authorization for data transaction through the token held. Cryptocurrencies are not used yet to process day-to-day micropayments for, for example, postal stamps, phone calls, or, larger goods, such as cabs and gas, reimbursable for value in cash.

7.5.1. Major Cryptocurrencies Overview

Cryptocurrency exists today primarily in the form of tokens launched with their own independent iterations of blockchain protocols. Bitcoin led the way, released in early 2009, and paved the way for hundreds of imitators. Bitcoin was the first decentralized cryptocurrency, created as an open-source protocol to be enhanced and developed by a

community of independent and company-facilitated developers. Bitcoin's open-market model spawned competition by allowing other tokens, a.k.a. coins, to freely innovate on and create economic systems, and all-in competition that perpetually nourishes Bitcoin's long-run scarcity properties. Because Bitcoin was the first cryptocurrency and created a breakthrough leap in the potential utility of money, the Bitcoin network has the largest value capture of any cryptocurrency, and thus is the foundation upon which other cryptoassets rely. Bitcoin's monopoly on cryptocurrency consumes more electricity and processing power than any stock exchange, and sustains absolute power over nearly every other independent blockchain, even Ethereum, the second largest.

In what may seem like irony, or just business, early influential cryptographic currency libertarian developers also realized that less competitive alternative proof of all cryptoassets could be engineered to monetize excess capacity and increase the attractiveness of using payment systems other than Bitcoin. These creators positioned their protocols as being independent from Bitcoin's competitive-defensive, scarcity-driven imperative and as enabling whole new classes of decentralized financial applications. Ethereum pioneered an implementation of smart contracts: sets of conditions defined in software, what we might someday call bots, that can autonomously activate and send out or receive cryptocurrency based on their deployment provisions.

7.5.2. Adoption of Cryptocurrencies for Payments

Despite their merits, cryptocurrencies have not seen mass adoption as payment methods. The average volume of Bitcoin daily transaction counts was around 2 million between December 2018 and December 2022, while the global number of digital payments in 2022 reached 1.1 trillion. A comparatively small number of Bitcoin transactions does not pose serious problems for the Bitcoin ecosystem, especially considering that Bitcoin is not currently used for large-scale payments. The low adoption of cryptocurrencies as payment methods might also indicate a lack of need, as most consumers around the world already have bank accounts and access to regular channels of payment. However, other analysts also point to the high transaction costs and scalability issues of Bitcoin and other cryptocurrencies that coincide with transaction peaks.

Bitcoin was initially designed to be a cheap and secure store of value and means of payment for the Internet. The emergence of Coinjoin, the Lightning Network, Meredo, and the Liquid Federation Protocol as low-cost and quick add-ons to Bitcoin are currently trying to reclaim Bitcoin's original purpose in a decentralized way. Coinjoin allows users to pool their coins and make it seem like they are transacting with other wallets in the pool. The Lightning Network builds a second layer on top of Bitcoin for microtransactions. Meredo uses the Lightning Network to facilitate instant payments while guaranteeing privacy. Liquid is poised to be the default centralized option for those

who want faster transactions in Bitcoin and tokens. Liquid uses side chains secured by a pluralistic multi-signature of elected functionaries to process transactions faster and cheaper than the BTC layer.

7.6. Regulatory Landscape for Digital Payments

When compared to the global payments landscape, the regulation of digital payments faces the challenge of protecting the scale and facilitative nature of payment systems while at the same time preemptively imposing the risk management discipline that is associated with financial systems. Global payments regulations have coalesced around four broad themes: payment instrument rules, participant access rules, operating rules, and consumer protection rules. Within these broad categories, there are two important features that have emerged around how payment systems have been regulated — the prevalence of voluntary membership-based rules and operating rules. Payment systems are framed as private utilities whose ancillary public good characteristics are recognized and compensated at the margin. Only in the case of failure to resolve asymmetric risk allocation or information concerns would mandatory regulation kick in and only in a light-touch manner, applying to the payment instruments or participants most at risk. Consumer protection regulations are also important as an additional layer of protection.

The bulk of payments regulation revolves around the security and operational efficiency of payment systems. The objective is to ensure the availability, speed, resiliency, and efficiency of payment systems. The actual monitoring of these attributes of payment systems is often delegated to central banks on behalf of the broader public. Payment systems, in this regard, are more akin to public services such as power, water, or rail than a public good like national defense. That is because payments are not just a transfer of funds from one financial institution to another. They play a much larger role in financial intermediation. And when they fail, it is not just the parties to the transaction that are affected but the wider economy as a whole. Regulations and safeguards have been established around payments for this reason. An increase in the digitalization of payments does not change this foundation of why payments are so regulated. It simply means that a new format with new risk features has emerged. The challenge for regulators is to understand those new features and how to adapt the existing rules so that they remain appropriately proportionate.

7.6.1. Global Regulatory Approaches

Diverse regulatory approaches and policies have been adopted and implemented in different countries and regions of the world. In the U.S. and Brazil, the government and central bank have taken the lead in defining payment systems and establishing

infrastructure as part of a public utility. In Switzerland, a public-private partnership is responsible for oversight of retail payment systems. In the Eurozone, regulation is more flexible and broadly applicable to all payment service providers and includes transparency and consumer protection regulation. Other countries, such as the UK, have preferred self-regulatory mechanisms with a light touch regulatory framework. In comparison, Korea has extensive regulation that is specific to designated services and providers.

Payment system development stages greatly influence regulatory responses and policies. Advanced economies like the Eurozone may rely on industry codes and flexible framework regulation at the early stage of digital payments growth, while a stronger regulatory response is warranted as payment systems mature and reach critical mass. Other factors can also have a strong influence. Government views on digital currencies, trust in private payment initiatives, the importance of privacy and data protection, and the role that digital currencies should play in a country's payments system can strongly influence the design of a payment system.

As digital payments grow, regulation will increasingly focus on areas like security, data protection, and competition. Public policies may also evolve to include operational resilience and availability, as countries transition from cash to digital payments. Cybersecurity risks associated with equipment, software, systems, and networks used in digital finance are expected to be more serious, given the threat posed by both state-sponsored and non-state actors. In response, industry and government must collaborate to adopt measures to strengthen the cybersecurity of payment systems.

7.6.2. Challenges in Regulation

Digital payments have transformed the way individuals and businesses exchange value and conduct commerce. While increased convenience, lowered transaction costs, and reduced settlement risk are some of the many benefits of digital payment systems, their fast-paced growth and the evolution of business models within the sector have posed challenges to regulators around the world. With many providers dabbling in multiple payment functions, spanning stored-value facilities, credit provision, remittance services, currency exchange, that may be tied up with other nonpayment functions such as e-commerce, ride-sharing, accommodation leasing, and customer loyalty programs, some of them are under the purview of regulatory authorities in multiple jurisdictions, while others are not. Compounding this patchwork of jurisdiction is the global nature of the digital economy, wherein funds flow across borders, with users and businesses residing in different countries. This has only heightened the difficulty of striking an appropriate balance in regulation. It is not uncommon for a legitimate payment function to be subject to different regulatory standards depending on the provider's location.

Therefore, clear and consistent regulations across the globe will enable the demand-side security of such services and allow for seamless and low-cost payment options across borders.

The growing presence of private providers has also challenged regulators to maintain a payment ecosystem that is secure, equitable, and efficient. With a few of these providers controlling the bulk of the market, there are growing concerns regarding the security and resilience of payment services in times of distress, the protection of sensitive information privacy, and the supervision around anti-money laundering and consumer risk. In addition, regulators have struggled to adapt effectively to the technology and business model changes. New services, such as instantaneous settlement, are possibly outside the scope of existing regulations. While ensuring that financial stability, consumer protection, and payment integrity risks associated with these new entities and services are adequately addressed, regulators also need to ensure that their interventions do not stifle the competition, innovation, and lower-cost services that are holding the potential for advancing financial inclusion.

7.7. Technological Innovations in Payment Systems

Financial technology is changing the future of payments. Modern payment systems are and will continue to be enhanced and reinforced with new and improved innovative technology shaping the global real-time economy. Financial institutions use technology such as open APIs, cloud computing, and artificial intelligence to create the infrastructure and payment products required for the next phase of globalization. The challenge now becomes creating seamless products and services that consumers will actually use. Financial institutions, both traditional and new entrants such as retail and tech companies, will need to believe in the power of the Digital Wallet and the importance of fintech in this mobile-first economy.

Artificial intelligence is a key emerging technology. AI has the potential to reduce costs, increase efficiency, enable innovation, avert risk, and ultimately change the way consumers and companies interact with the world. In payments, AI is being adopted to improve anticrime defenses, bolster sentiment analysis, and enhance customer experience through personalization, and will soon be used to detect client pain points and help deliver fully online account opening and transaction journeys.

Fig 7.2: The Future of Payments

AI can also help improve risk assessment, tach the commercialization of compliance as a service, and sophisticate payment security through biometrics and behavioral analytics. In short, AI will significantly enhance the consumer experience. Business process reengineering may include automating the customer service function. Conversational platforms using natural language understanding/chatbots can automate much logic, allow human operators to focus on more complex clients issues and thereby increase job satisfaction, and reduce service center costs. Over time, improving technology and accompanying falling costs will allow chatbots to respond to a wider variety of requests. Such improved technology, now augmented by AI machine learning, will eventually move conversational platforms into voice-logic services.

7.7.1. Artificial Intelligence in Payments

AI is a powerful technology that enables computers to perform operations that would normally require human intelligence. In the payment services industry, AI is highly relevant. AI is largely used for predictive analytics, the advanced technology that makes predictions about the future. As it requires access to vast amounts of historical data that are difficult to analyze for human brains, predictive analytics is based on complex formulas that use techniques like data mining, statistics, modeling, machine learning, and artificial intelligence. AI can use previous behaviors and experiences to predict the probability of future behavior. Simply put, AI in the payments sector can help stakeholders and customers easily analyze substantial amounts of data that they may need to make critical business decisions.

AI solutions can automate and personalize customer service. The principle is pretty much the same as in the retail sector where chatbots can answer customers' questions in real-time. AI solutions can also provide businesses with intelligent, flexible chat assistance that enables financial institutions to communicate with their customers and provide relevant product information at any time of the day or night. These solutions can analyze customers' previous purchases and take contextual factors into account to offer personalized message prompts or suggestions. Not only that, AI can also help major payment service providers and public authorities determine vast amounts of data in real-time in order to protect against fraud. Algorithms can automatically spot discrepancies with previously recognized spending behavior, for example, identifying atypical purchases that could indicate credit card cloning.

Moreover, AI can identify unique transaction patterns that reflect corporate culture and likely disallow unique purchase transactions. For example, payment solutions providers can help companies analyze vast amounts of transactions to determine acceptable patterns. Then companies or banks can configure automatic alerts to notify companies of anomalies for new transaction patterns. Such technologies can be permanently working in the background to stop card cloning before it happens, essentially eliminating the need for notifications to confirm purchases.

7.7.2. Internet of Things (IoT) and Payments

The seamless integration of technology with our daily lives has transformed how we interact with the world around us. What once were inanimate objects now form a cohesive network, constantly sending and receiving data. This interconnectivity allows for the automation of mundane tasks; devices can make decisions on behalf of their owners without input, like replenishing groceries while we are out of town. With an overarching theme of efficiency, these advancements have posed difficult questions for

traditional transactions and payment systems: if a washing machine can order and purchase detergent, how is it supposed to pay the store? Who gets in on the action, and how? And what happens to a society that embraces all of these conveniences as a normative way of life?

Leveraging the conveniences of this enhanced connectivity, emerging concepts like smart car payments and autonomous convenience stores are placing demands on traditional methods of conducting and processing transactions. Perhaps the most talked-about of these developments is the concept of frictionless payment systems, in which devices are capable of monitoring owners and conducting transactions on a user's behalf without any action required on the part of the user. To enable these systems, it is expected that leashless transactions will become increasingly common. In addition to being seamlessly executed, these payments are expected to be instantaneous. IoT-based payments may also run without transaction fees or service charges and will be available 24/7.

7.8. Consumer Behavior and Digital Payments

7.8.1. Changing Consumer Preferences Consumer preferences have always played a significant role in the adoption of new technology and payments. Social and demographic factors are a main driver of acceptance but also affect how consumers utilize products and technology and how their experience may differ. What factors within consumer behavior will affect payment strategies now and in the future? Payment companies are constantly innovating and coming up with new payment modalities but there is an absence of new payment modalities that are successful. The introduction of non-embossed card a few decades back in a market of embossed cards is a testament to this point. Despite what payment companies want, convenience is the main driver for selection of a payment tool. Consumers are not willing to accept new payment and authentication modalities unless they are easier and faster than existing mass market payment tools that are optimized for speed such as a contactless payment card in a payment terminal. A successful new payment tool will have to overcome an important challenge. Payment tools which large numbers of consumers already use have gained strength through network externalities. This means that all merchants already have the infrastructure to accept these payment types and large numbers of consumers own these payment tools. It is therefore inevitable that such established payment modalities will dominate the retail payments landscape in the foreseeable future. This creates a very high barrier for companies that want to launch successful new payment tools. 7.8.2. Impact of COVID-19 on Payment Habits.

7.8.1. Changing Consumer Preferences

Research shows that the ability to make payments digitally is important to many consumers. A fractional change in the amount of consumers that care about such capabilities implies that a greater number of users may be delaying adoption of digital payments. Cryptocurrencies increase consumer choice for payment assets, and an increasing amount of consumers putting importance on digital payment capabilities could drive banks to adopt the new payment technology more readily. Factors such as generation, income, and education level impact how users view the relevance of digital payments when utilizing fiat. The willingness-to-pay by consumers for the costs of cryptocurrency transactions on crypto networks may be correlated with a desire for digital payment capabilities. Digital currencies are a more affordable alternative for international transactions than conventional payment processors and banks.

As offerings of digital forms of the U.S. dollar and other fiat currencies gain momentum, people oftentimes favor their fiat-denominated digital options compared to cryptocurrencies as payment mechanisms. Unlike the existing forms of digital currency being explored and expanded by suppliers, cryptocurrencies are supported by blockchain consensus validation and not issued by authorities. This makes cryptos a more attractive option for facilitating payments for cross-border purposes. These currencies are not subject to illicit transaction bans and payment processing censorship since they do not rely on centralized gatekeepers. Moreover, market makers stand ready to translate tokens from one crypto network into another using smart contracts.

7.8.2. Impact of COVID-19 on Payment Habits

Not surprisingly, the COVID-19 pandemic had a great impact on consumer behavior and payment habits. People turned to online shopping to avoid stores. Forcing consumers to stay confined at home during months, many turned to e-commerce for the first time in their lives, starting a process of digitization that naturally extended to their payments. E-commerce payment methods became critical for consumers to enjoy their online shopping experience. Grocery and food delivery services began to offer fresher produce, expanded their selection of offer, and guaranteed faster delivery times. E-commerce adoption was expected to last beyond the pandemic and to transform the way people consume. This accelerated trend for home delivery meant that the in-store experience would last longer and that people would visit shops and restaurants less frequently. At the same time, more families and friends were digitally connecting with each other through apps and negotiating money moves. Relationships changed with more people splitting bills, gifting each other money, or giving money to those in need. Years of behavioral studies had concluded that people tend to pay the same way for gifts, bills, and support payments. As these digital-first payment flows became part of consumers'

daily lives, both the demand for and use of digital wallets continued to grow. Money conversations and considerations went virtual during lockdowns. At-home digital money moves scaled globally as more families and friends found themselves physically dispersed. Partly in agreement with most previous studies, mass economic dislocation was followed by changes in consumer payment preferences. Cashless transactions were accelerated and the need for speed and simplicity had never been more evident than in this period of uncertainty.

7.9. Future Trends in Digital Payments

Over the next decade, the digital payments space will be redefined by advanced technologies such as Artificial Intelligence, Machine Learning, robotics, blockchain, digital currencies, machine vision, and smart contracts. Digital payments will become faster, more secure, less expensive, and more real-time basis-enabled thanks to emerging innovations and breakthroughs in quantum computing, biometrics, near field communication, and a unique client experience. Infrastructure upgrades to existing centralized payment networks will support the implementation of real-time settlement and add additional safeguards against fraud and cybercrime. Digital wallets will make it easier for consumers and corporate clients to organize multiple accounts and digital assets, and by simplifying the online and cross-border shopping experiences, revolutionize e-commerce. Using digital identity and biometric authentication, and leveraging AI and ML for real-time fraud detection, customers will navigate frictionless experiences in both digital and physical worlds, becoming less aware of the payment processing. Central banks and commercial banks will launch digital currencies supported by payment infrastructures that enable economic actors to transact on a nearly real-time basis.

Fintech companies will lead innovation in global digital payment solutions. As the local-to-global presence of digital assets and economic actors in emerging markets expands, new players will fill gaps left by incumbent banks utilizing emerging technologies, offering a range of financial services from the digitalization of the cash economy to trade policies and trade finance, all tied to current account flows and access to foreign currency. Fintech companies will enter a multitude of locations working in partnership with other fintech players, banks, telecommunications, and technology companies. Tokenized economic assets will promote digital identity and digital currency solutions. Emerging standards will help democratize access to financial services while enhancing customer experiences. Enhanced APIs will lower the implementation time and costs of integration. Data-driven insights will assist automated customer onboarding and transaction monitoring, while embedded finance will become the norm.

7.9.1. Emerging Payment Technologies

Despite the above-mentioned structural advantages of money, a business does not need to implement one of the official versions of money as the center of its internal payment system or as the medium for payments in commerce. It can build it entirely on top of credit if it thinks this is better. It can reciprocally dispense credit written on itself to credit-constrained counterparties. In that case, the exchanged assets will not be money, for these transactions will create no net balances in the aggregate. It can also dispense its own tokens as credits or discounts. In that case, the exchanged assets will not be money either. The tokens will serve as an additional layer that sits above the money payment system. Notably, it is not only non-state actors, such as businesses and tech firms, that can do this. Central banks can also build their national payment systems entirely on top of credit relationships. The way to do it is to allow designated banks to create aggregated balances, where all deposits at the central bank are netted out, and let all market participants credit equally.

In the near future, central banks will explore going down this path to provide a frothier layer in the payment system. They may also ramp up support for private forms of tokens by backing stablecoins that have reached a certain stage of maturity. A step in this direction could be the notification of the firms involved in the production of mature stablecoins and approval of their services. Other likely central bank interventions would be pressuring commercial banks to lower the user costs of their token services or encouraging the development of token services by banks and tech firms. Alongside these crypto-assets and central banks' efforts, new payment technologies will emerge to restore functionality to the traditional payment services that crypto-assets are gradually siphoning off.

7.9.2. The Role of Fintech Companies

Fintech companies have emerged as key players in the digital payment sector. Rising from the ashes of the housing crash and central bank-induced zero interest rate policy, they successfully siphoned institutional capital away from the tech public equities and hospitable monetary regime back into retail equity portfolios. Companies with significant first mover advantages in the digital payments vanguard quickly scaled to IPO, creating market validation for dozens of newly formed competitors as part of a record tech IPO class. The record class of post-IPO tech companies is emerging from a decade of ecosystem-enabling rampant venture capital irrationality featuring both fundamental business model challenges. Embracing the concept of financial services unbundling, they dismiss traditional banks as too slow to respond, mired in insufficiently agile legacy computer systems, in risk-averse corporate atmospheres. The emergence of the concept of embedded finance is resulting in the unbundling of services traditionally

offered by banks but offered ad hoc by disparate solutions offering niche solves for limitations in the offerings of traditional banks.

Through best-of-breed day-to-day operations, these service providers are extracting customer or user data and establishing their brands with a pervasive frequency of contact. This creates disaffection for the antiquated, outdated traditional bank. These fintech companies are engaging in a viciously competitive race for eye-watering instant gratification for market share from the habitually regarded bank of choice. By designing superior user experiences powered by innovative technology, they are prompting a response from the established banks that have been hacking away at digitization of the pre-existing banking sector. Between the onslaught of the attack of the fintech Upstarts and the speed of the digital investment in simplicity by the Big Banks, a full-blown exciting revolutionary upgrade to functionality, security, transparency, privacy, and safety of the services offered is destined to unfold.

7.10. Challenges and Risks in Digital Payment Systems

The rapid rise of digital payment systems has not been without complexity and challenges that may hinder their development. The security of internet-connected payment services has been compromised by hackers that steal login details and drain accounts. Roadblocks remaining to unauthorized parties gaining access include cyber security issues, lack of trust in financial services, heightened cybersecurity investment costs, inadequate payment defense mechanisms, and the unregulated cryptocurrency and mobile payment services segments. The digital divide surrounding fintech companies offers little incentive for some partners and institutions to encourage the digital evolution in the developed world, let alone in emerging and developing countries. Pre-existing regulatory frameworks may inhibit the establishment of effective, unified solutions. Granting third parties access to customer bank accounts can cost banks their client relationships, especially if, through a bank's reluctance to build partnerships with fintechs, those entities end up offering better rates for the customer.

Without security and trust, the regulatory environment will hamper the growth and acceptance of digital payment systems across customer segments. Critical improvements and services must be enhanced to lure various clients to use digital currencies, such as expansion of crypto businesses, institutional investors, or the mainstream global payments ecosystem, better solutions and services needs when using digital payment systems and a heightened awareness of system advantages and risk mitigation measures. Additionally, currency fluctuating volatility and regulatory scrutiny make digital payment processes infeasible. A third significant obstacle to smoother digital transaction adoption is the pre-flight latency in addition to post-distribution processing times demanded by existing blockchain networks, since quicker transaction confirmations are

fundamental for small transaction payment systems and also for transactions at physical locations. It cannot be denied that the technological requirements tied to blockchain digital systems, mobile payment transaction services, contactless-tech options, plus digital coin solutions vary from market to market.

7.10.1. Fraud and Cybersecurity Risks

With the rapid growth of digital payments, criminal activities are also in expansion, with an increase in online fraud and scams. Criminal organizations are beginning to scale the development of their operations to take advantage of the growing cryptocurrency and fake economics, looking at these markets and all their peripheries as a source of easy money. Scams are currently taking over the field, and they are driving away legitimate players. Nobody wants to trade or even just hold a cryptocurrency that has a very high number of rug pulls or other scams; untrustworthiness drains liquidity from any market. Educational level seems to play a paramount role, since educated users are less likely to respond to scam attempts.

However, despite the existence of highly visible and discussed incidents, cryptographic currencies have fewer points of exposure. The rewards are greater for ATM thieves, merchant site credit-card security breaches, and hacking companies that are storing customers' credit cards, but this is compensated for by the volume of transactions and the added liability issues related to credit-card chargebacks. Fraud issues ought to lessen over time as structured transaction data becomes available, but it is also true that privacy may be compromised and, seeing how much value users attach to the security and privacy of their transactions, cryptocurrencies losing the battle on fraud might find users unwilling to share data for transaction clearance and verification. Of course, this is a long-term picture, but it is fact that companies make money with fraud too. Cyber security threats include Denial of Service attacks and data breaches involving digital assets.

The level of tolerance for cyber security lapses is generally low, and the fact that failure creates profit opportunities for others will lead to increased attention in the industry, both from researchers and government bodies trying to put standards and protocols in place. Cyber security hazards can be lessened through the introduction of insurance and guarantees at the transaction level, as it is the case with credit cards.

7.10.2. Technological Barriers to Adoption

One practical problem is that many of blockchain's transaction systems currently work much more slowly than legacy systems, such as credit card systems. Low transaction

speeds directly affect digital payments. Although Bitcoin has allowed very limited instantaneous transactions through services, in general Bitcoin (and Ethereum) transactions can take an average of 10 to 12 minutes to be confirmed, and hundreds of dollars in transaction fees may be needed for priority status. Even proof-of-stake systems are not yet close to processing rates of traditional systems. Additionally, without highly-lucrative transaction fees, the networks are not currently able to offer the enormous incentive systems necessary to support a network of full nodes that can guarantee independence and neutrality from both state and third-party actors in transaction systems. Currently, the nodes on the Bitcoin network that have the full records are able to confirm transactions in part because owners are being paid from transaction fees on a per-transaction basis. Without transaction fees to create these powerful incentives for miners from transaction costs, and with the recent acknowledged centralization of mining on Bitcoin, the ability of the system to process vast numbers of transactions seems limited.

The privacy and anonymity issues also are serious challenges. Most currently-available systems for digital transactions make it easy to trace any type of transaction on any payment channel. When you use a credit card, for instance, you are relying on the bank to abandon false pretexts and untrustworthy partners that want your transaction information, and the credit card company keeps the information secure. The full transaction history held by miners and other actors currently would violate a key operating condition behind the advantages of digital transactions when compared to other forms of monitoring. An efficient decentralized payment system must allow the private and quick execution and storage of digital payment transactions done without compromising the fund's security, but enable record-keeping, audit, and tracing of illicit transactions as needed. Currently-available systems do not achieve this.

7.11. Case Studies of Successful Digital Payment Implementations

In the sections that follow, we more closely examine some successful (and failed) implementations of digital payments systems to demonstrate a diversity of approaches and the lessons that can be learned from the implementations of others. Note that "success" or "failure" is unavoidably subjective. For our purposes, a "successful" implementation is one that provides at least some users with a convenient, low-cost, low-friction method of effecting transactions. A "failed" implementation is one that has not stood the test of time. Note also that our success or failure considerations are in relation to the implementation of the payments mechanism itself, and not necessarily the purpose of that payment mechanism. For instance, some have considered certain illegal digital marketplaces a success because they provided a safe haven for the trade of illegal goods, thus "filling a market gap" that otherwise would have likely included violence and

disorder. However, such crime-based success is somewhere far afield from this text, given its focus on legitimate private commerce activities that are seamless, low-friction, efficient, and non-violent.

Sadly, many of today's remaining digital payments systems that are not yet clear successes often bear a close resemblance to the more sophisticated, fully functional, successful systems of the past, such as various easy-to-use, instant-transaction, clear-payment, cross-border money-transfer systems that once made certain platforms ubiquitous. Customer backlash (in the form of transaction charge complaints and high transaction charge non-use), counterparty abuse (linking service to counterparty with exposure), and counterparty fraud have certainly had their effect in limiting these early, untethered versions of several similar digital payment implementations.

7.11.1. Global Case Studies

Commercial organizations and governments want to give you the choosing power to spend your hard-earned cash how and when you see fit. Years of customer-centric culture at large corporates, combined with swathes of digital transformation and the rise of new entrants wanting to disrupt the traditional banks, have resulted in the digital economy and eCommerce environment we see today where the consumer is firmly in the driving seat. One consequence of this is that finding the right solution for organizations to empower their customers is not so straightforward – what works for one may not work for others.

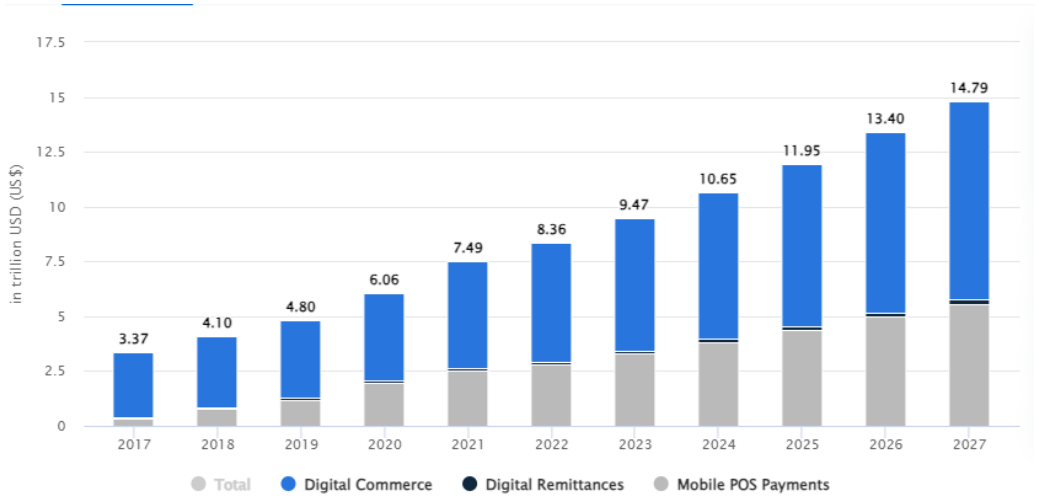

Fig : Digital Payment Systems

Payment solution providers may therefore talk about their world-class product or payment gateway but the truth is, they offer solutions that work best in specific

situations. This can depend on geography, currency types, target consumers, customer demographics – age, gender, culture, etc. The success of these solutions is proven by case studies of product implementation and rollout by various organizations and often in various parts of the world, given the consumer choices described above.

Through this report, we have reviewed several case studies in successful today's digital payments landscape. Some are from the Western Hemisphere, with the USA leading the way and a few EU countries, Singapore and of course China providing stiff competition. Others are from the East, where the digital economy is spearheaded by various countries in the Association of South-East Asian Nations region, of which Indonesia is the largest society and therefore keenest to spearhead digital transformation. Yet another group comprises the pockets of cash-strapped people in Afghanistan and the associated digital payments choices available to them. These case studies are indicative of the solution providers either working alone or partnering with commercial organizations or government institutions to allow for the unbanked to be provided the facility to use digital payment methods.

We will begin with case studies from the West, but this will be followed by digital payment solution implementations from various countries in the East.

7.11.2. Lessons Learned from Failures

A careful evaluation of the failures of numerous unsuccessful digital payment efforts provides important lessons for the future implementation of digital payments. The role of the private sector is crucial in determining the formation of digital payment platforms that effectively serve consumer needs and population priorities. Digital payments are best introduced and established in economies in which the populations already have access to banking facilities that include checking accounts, debit cards, and credit cards. An introductory focus on the upper-income segment where demand is greatest can motivate early enthusiasm and provide the seed money for future growth. Digital payments will never achieve scale if the low-income population does not embrace them. The key to acceptance with this group is to provide simple devices that are issued free of charge or at very low cost and link their ability to make or receive payments to incentives that encourage frequent use. The mobile phones that can provide access to digital payments are often owned by members of the low-income population, so a successful strategy also has to find ways of encouraging them to share access to this payment platform. Merchant acceptance is critical. Merchants must be encouraged to adopt point-of-sale devices that will accept transactions and charged minimum fees for use, or preferably none at all, for low-value transactions. These payments can be bundled

with a primary product or service providing an immediate benefit to the seller. Only when low-value transactions become frequent will it be profitable for merchants and payment companies to invest in technology and equipment. For that reason, the digital payment technology at the center of the ecosystem must be easy to use while having no per transaction costs ambiguities to confuse those characterized by low literacy. If business is encouraged to invest, the technology will subsequently have to satisfy their concerns about being expensive to install and use and inappropriate to the nature of their enterprise as well.

7.12. The Future of Cash in a Digital World

The rise of digital currencies and cashless systems does beg the question — what is the future of cash? Will consumers make the switch, or will the aged comfort of cash persist through generations? The answer is quite subjective. While the cashless generation grows ever more centered around mobile wallets, cryptocurrency, and swift money transfers, there is still a contingent of society passionately devoted to cash — the older generation. For them, it is a sign of financial stability that doesn't rely on technology vulnerable to glitches and hacks. It is a control factor that doesn't shift depending on regulations and market value of currency. Moreover, what could a transition to an entirely cashless digital world mean for financial stability for disadvantaged people? Cash is essential for unbanked consumers and small business owners who would otherwise be hindered by fees inherent in card payments. If the proposed benefits of connected technologies were to eliminate the need for cash, that could spell catastrophe for that niche of society. The ultimate fact is that the aging generation is uneasy about new technologies, and that sentiment will likely never change. Nevertheless, as future generations find convenience through digital currencies, cash will likely continue its decline.

So in what direction does cash evolve? Reports on predictions about cash are a mixed bag. Some state that cash will continue to dwindle, but invariably be needed for certain transactions. Others believe that a seamless transition into digital currency and cashless systems would lead to cash's demise. While that may be premature, there are also reliable predictions that point towards cash still being around for a long time to come, with an evolution of its own. What that could entail includes the following: enhanced currency security with physical attributes that respond to hi-tech capabilities of the future such as anti-counterfeit features and money that reacts to touch functionality. The future is hazy for cash, but while there are still proponents that place favor upon the control and security of cash, it will remain relevant for some time to come.

7.13. Conclusion

The rapid advancement of technology and supportive government policy is prompting advertisers to rethink payment options for bringing customer convenience, information analytics, and budget control. Businesses around the world and sector are jumping to explore the digital payment ecosystem for both internal and external transactions. The digital commerce boom is slowing down, yet spending trends show that people plan to spend more online over time and want to see new progress. Emerging technologies also promise smoother and faster transaction experiences and new customer-oriented payment models. We observe that the digital future of payment will likely be built on three pillars: open financial systems; seamless and connected payments; and trusted transactions and verifications.

Digital currencies will facilitate smooth cross-border payments and enable real-time gross settling of interbank transactions in the future. Cross-border payments today are governed mostly by relation banks; they depend on services on offer being acceptable to both sides, and messages being exchanged following international standards. Using blockchain to process and store messages, however, allows banks to implement verification protocols according to their own criteria. This would make it much less sensitive to questions of trust to whom in a country the funds are being sent. Clearing houses would be likely to rely more on KYC rules and less on purely commercial considerations. Thus the future is promising for a global payments ecosystem centered on digital currency issuance and a business environment where CBDC and private currency systems co-exist and facilitate each other.

The next decade and beyond will likely be characterized by the assimilation of technology into payment infrastructures. Financial services companies will witness the vertiginous growth of payments as infrastructure. Society and businesses would begin to partner with fintechs as technology platforms to support a new wave of innovation in how payments are viewed and executed. They are using payments as a customer relationship tool and exploring the potential of these insights to monetize payments. The digitalization of payments and the evolution of payment ecosystems have only just begun. It promises to be a long and fruitful journey.

References

Tapscott, D., & Tapscott, A. (2018). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

Arner, D. W., Barberis, J., & Buckley, R. P. (2020). The rise of digital finance: Financial inclusion, mobile money, and the FinTech revolution. Journal of Banking Regulation, 21(4), 299–312.
Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. Journal of Network and Computer Applications, 103, 262–273.
Chen, M. A., Wu, Q., & Yang, B. (2019). How valuable is FinTech innovation?. The Review of Financial Studies, 32(5), 2062–2106.