Deep Science Publishing
https://doi.org/10.70593/978-93-49910-78-2_9

DeepScience
Open Access Books

Chapter 9: Understanding the integration of blockchain, digital wallets, and smart contracts

9.1. Introduction

Although blockchain technology has been around since the launch of Bitcoin, it is still little understood and often dismissed as merely another digital gimmick. Considered technology's biggest innovation in the last five years, blockchain is a decentralized, distributed ledger on which transactions are recorded in an immutable way, deployable across diverse sectors – from finance to agriculture, from healthcare to smart cities. Crypto-currencies are one of the first and best-known practical applications of blockchain, but multiple other uses are being developed and adopted by start-ups and large enterprises alike (Buterin, 2014; Mougayar, 2016; Atzori, 2017).

Blockchain provides the technical foundation for decentralized digital currencies. Blockchain technology allows these currencies to operate without the need for a central bank, without the costs of using a third-party payment processor, and without the risks of fraud due to the fact that the entire network – whether they are transactions between computers, IoT devices or persons – has access to an unalterable ledger. Other use cases expand on this innovative, digital and decentralized use of ledgers. Tokens are used for access to services or incentives, or as representations of assets, such as gold bars, real estate, companies, and even credits in a company's loyalty plan. Tokens generated in the network through smart contracts can represent a digital currency for an application's community, the right to access a service at a determined date, or a credit in a loyalty system. In short, on a blockchain network, trust is easily established and diversely tokenized (Tapscott & Tapscott, 2018; Zwitter & Boisse-Despiaux, 2020).

9.1.1. Definition and Key Features

This section is discussing Blockchain, which is a system where records of transactions are stored over a distributed network of computers, protecting the transactions from modification. Moreover, Blockchain represents a paradigm shift in the way value is exchanged in the economy and governs the transfer of assets over the Internet. In the last few years, companies and researchers invested a significant amount of resources in the study of this technology, to explore and understand its consequences and its implications. As previously said, in a Blockchain system, transaction records are disseminated on a network of computers, known as nodes. As a result, a Blockchain database is distributed among a number of computers, with no single point of failure. Moreover, the Blockchain operates as a digital public ledger, where the transaction records can be verified by any of the nodes.

Fig 9.1: smart contracts on the blockchain

The system is based upon a consensus mechanism that ensures that modifications at any node are propagated to the other nodes. Every time a modification is made, a record of that transaction is added to the chain of digital signatures. This mechanism is what enables participants to exchange value over the Internet without relying on any third-party intermediaries. Blockchains allow participants to exchange digital assets without introducing the principal inefficiencies stemming from intermediation. In a Blockchain system, the traditional third-party broker is replaced by a network of computers that maintain an updated and publicly accessible ledger of transactions – the Blockchain. Blockchain eliminates the need for third-party intermediaries as banks and clearinghouses, enhancing efficiency through trust, security, reliability, and confidentiality. More importantly, the transfer of value is irrevocable: once a Blockchain transaction has been validated by the nodes of the network, even the sender cannot reverse it. This prevents the occurrence of the bank customer's most feared problem: transaction double-spending.

9.1.2. Historical Context and Evolution

The early days of blockchain research have recently gained renewed interest because of the emergence of practical applications using a trustworthy decentralized immutable ledger. These earliest precursors to blockchains were generally not called blockchain. Instead, they were typically called hash chains or block sequential data structures, until the landmark explanatory paper was published in October 2008 by a person or group of persons named Satoshi Nakamoto, and the Bitcoin software was released in January 2009. Nakamoto's paper was not the first proposal for electronic cash based on cryptographic principles: the idea dates back to 1983. However, among the many research and development proposals for electronic cash, Nakamoto's implementation would be the first to fully succeed, and consequently, it has become the canonical implementation of a blockchain-based system. Even now, many studies, products, and companies rely on Nakamoto's paper and the unique blockchain solutions to the Byzantine General Problem and to the Double-Spending Problem as their touchstones.

There are several important differences between Nakamoto's blockchain and previous sequential hash chains. Previous hash chains always required a single trusted party to initialize and close the chain. Bitcoin uses a unique capability-based mechanism for keeping the chain open, where all users on the network simultaneously share the responsibility for keeping the chain operational. In doing so, Bitcoin tokenizes its security, allowing users to effectively have a range of possible expenses in terms of tokens, conveniently known as transaction fees, which are paid to initiators of the next block in order to incentivize them to mine and broadcast that block. Costs of using the Bitcoin blockchain for transactions are market-based and are subject to wide fluctuations.

9.2. Digital Wallets: An Overview

Digital wallets, also called electronic wallets, are wallet solutions that store the credentials to digital assets located on a blockchain or in digital form. The range of solutions using the term 'digital wallet' varies from solutions that manage protocols and digital signatures to solutions that simply provide a mobile application interface to a banking or payment account. Digital wallets provide an abstraction over a variety of interfaces, protocols, services and solutions that have the goal of managing treasuries in the developed financial system and in DeFi. The digital wallet is the first touchpoint of the user with the world of digital assets and blockchains. Trusted digital wallets aggregate the credentials to multiple blockchain accounts in a simple application that addresses the core issues of security, safety and user experience. Wallet as the main interface to the user requires the strongest protection conceivable, as physical access to the wallet means full control of the digital assets. Hence wallets implement an array of protection mechanisms. Depending on the type of wallet, digital assets are stored as physical devices with control over private keys, especially keyboards or devices with one or multiple secure elements that utilize secure processing for secure remote management setup of digital wallets based on trusted execution environments or in the cloud. Wallet interfaces providing hot digital coin access may encrypt and obfuscate their key management functionality and accesses to private keys via API calls to external modules or even to remote trusted execution environments. However, all those mechanisms don't address the basic risk of centralized wallets that store electronically the keys to user assets because users lose access due to invalidated accounts, e.g. lost account password or invalid phone verification.

9.2.1. Types of Digital Wallets

Digital wallets are computerized systems that store payment information and passwords for numerous payment methods and websites. They allow users to make secure purchases at real-world stores, through a mobile app, or online without needing to physically swipe a debit or credit card. A digital wallet app is typically associated with a prepaid account, meaning money must be deposited into the app before purchases can be made. Users may link their bank account with the wallet to transfer money into the wallet, although some digital wallets also allow users to add money using a debit card. Furthermore, digital wallets are usually linked to a user's credit or debit card.

Digital wallets do more than allow someone to carry only their mobile phone to make credit card purchases. They can also hold boarding passes, tickets for a concert, business cards, or any other items traditionally kept in a wallet. Businesses are increasingly designing apps that serve as digital wallets and loyalty reward systems, including fast-food outlets, airlines, and hotel chains. Digital wallets are generally used for making purchases online or through an app, and the digital wallet is linked to an existing payment account.

The most common type of digital wallet is the smartphone app. Most smartphones are built with mobile wallets already on the phone. Digital wallets embedded in smartphones use near-field communication technology, which allows the phone to interface with the credit card terminal without physical contact. The phone transmits encrypted payment information to the merchant's payment system, which sends it to the payment network for verification of available funds. The app may also hold coupons and rewards information for that store, allowing customers to receive discounts or accumulate rewards through the app.

9.2.2. Security Measures and Risks

Digital wallets are a new paradigm for information storage, authentication, and remote transaction authorization. However, storing sensitive data in a secure way is a challenging task. To ensure safe transactions, a rigorous authentication process to the owner of the wallet must be applied. Security solutions can be categorized into security measures at wallet issuing, online service, and user levels. Security measures at wallet issuing and online service levels are encompassed in public key infrastructure and biometric identification, but both solutions are computer systems and thus subject to hacking threats. The vulnerability of wallet systems to hacking and denial of service attacks means that these solutions cannot be entirely trusted.

The reliability of wallets at user level remains, such as the length of backend identifiers and verifying the recipients of transactions. With regard to the web, phishing is a potential risk for wallet users. Generally, online identity security relies on the individual user through password management. However, an average user is not as competent as a specialist in preventing risks associated with weak passwords. Password strengths are reduced by the predictability of a common use of simple passwords. An increasing number of attackers are specialized in password cracking. Moreover, the time it takes to restore stolen passwords might not be recoverable after a short period. The consequence of password weakness is thus increased by new methods designed to attack password systems. An alternative solution to password management is to avoid it as much as possible.

9.3. Smart Contracts Explained

Smart contracts are computer programs stored on a blockchain that are designed to automatically execute and enforce contractual agreements between parties. They are executed on a decentralized network of nodes that validate the transaction and ensure that the terms of the contract are met before executing it. Smart contracts eliminate the need for intermediaries, such as lawyers or banks, reducing costs and streamlining the contractual process. These programs can be written in various programming languages and are designed to be tamper-proof, meaning that once deployed on the blockchain, they cannot be modified or altered.

Smart contracts can be used for a wide range of applications, including financial transactions, supply chain management, digital identity verification, and more. In finance, smart contracts can automate processes such as trading, lending, and insurance, reducing the need for intermediaries and increasing efficiency. In supply chain management, smart contracts can track the movement of goods and verify that the terms of the contract, such as delivery time and quality standards, are met. In digital identity verification, smart contracts can provide a secure and decentralized way to verify identity without the need for a centralized authority. Other potential use cases include digital rights management, healthcare records management, and voting systems.

9.3.1. Definition and Functionality

Smart contracts were a novel idea introduced in the 1990s to the area of digital currencies, where they were advanced as a way of automatically executing transactions in a trust-less environment. They were rediscovered in 2014 as part of a proposal to build an environment within which the transactions to be executed were not limited to currency issues, but could be applied to any type of digital asset. Within the framework of digital currencies, these smart contracts are simply instructions contained in a separate script that can be executed within the currency's protocol. One motivation for using smart contracts in this case is that they allow for greater privacy in the execution of non-coin-transfer transactions, as these instructions are not available to all observers of the block chain.

Smart contracts are predefined executable code that is stored in a peer-to-peer network, such that when specific conditions are met, the code is executed. When this code is executed, it has the effect of enforcing the agreement. Smart contracts have several advantages. They offer trust via the fact that they are executed in a decentralized but unchangeable environment, and they guarantee speed, lower costs, and the absence of intermediaries. There are certain aspects that need to be taken into account when using smart contracts. First, the code is immutable and even though the feedback loop is reduced, it is not prevented. Moreover, if a smart contract triggers an event, it becomes public, thus losing confidentiality. Finally, the smart contracts are executed using the currency of the protocol for the transaction fees, which may represent a hurdle.

9.3.2. Use Cases in Various Industries

Smart contracts are self-executing agreements stored on a blockchain. They facilitate, verify, and enforce the negotiation or performance of a contract, ensuring that terms are unchangeable and without the need for a third-party intermediary. Smart contracts run on the blockchain platform, processing the transaction when triggered by a user-defined input. If the validated input meets the conditions of the contract, it executes automatically. Alternatively, if it does not meet the conditions, it does not execute. Smart contracts eliminate the risk of tampering as they are predetermined agreements which execute automatically. Once a smart contract is executed, the transaction is encrypted on the blockchain.

Smart contracts excel where transparency, effectiveness, and economy are concerned. Hence, they can be applied in various industries. For example, in the banking industry, smart contracts can facilitate collateralization for various types of loans, automatically ceasing all interest payments if the collateral value declines to a certain amount. Once the loan is paid off, the collateral is released. In the financial services industry, smart contracts can facilitate trade clearing and settlement, acting as an escrow agent, an accountant, and possibly a voting committee, enabling easy access to all information needed to validate trades.

In the insurance industry, smart contracts can be used to create peer-to-peer insurance policies for agriculture. In the real estate industry, smart contracts can be used to transfer properties in an automatic way by programmatically enforcing conditions. In the supply chain industry, smart contracts can track goods and services automatically by triggering a contract condition when a good is scanned. In the digital content industry, smart contracts can be set up to automate digital goods sales in peer-to-peer fashion without a centralized distributor.

9.4. The Relationship Between Blockchain and Digital Wallets

Digital wallets are mobile applications or programs that allow users to store their funds, bank account, and credit card information, as well as enable payments and purchases via mobile devices, in addition to offering security and data protection and changes ledger features. Digital wallets store their private keys with the application's provider and are managed by centralized parties. A majority of the existing wallets fall into this category.

Centralized wallets additionally charge users fees for creating and operating a store and execute wallet services, and for peer-to-peer transfers. Centralized wallets, due to their structure, offer little to no privacy. They are especially at risk from extortionists and hackers who would want to break into the servers in case of high transactions. A single point of failure, housed on a centralized server, also means that all content will disappear if the centralized authority ceases operations or undergoes a malfunction of its server. For these reasons, decentralized wallets came into being.

Decentralized wallets allow users to carry out transactions and receive payments online using the currency of choice. They operate using private keys stored in blockchain technology. Unlike centralized wallets, decentralized wallets work without needing to depend on a centralized source or central authority. It allows users to remove intermediaries from their transactions, enabling peer-to-peer transactions with no added fees. Using a decentralized cryptocurrency wallet for transactions therefore has its advantages in privacy, security, and transaction speed.

9.4.1. How Digital Wallets Utilize Blockchain

The blockchain is a distributed digital ledger that stores information in a permutation of chronologically ordered data blocks. Each block contains an encrypted timestamp and critical information that points to the preceding block, which makes it virtually impossible to alter or destroy information on the chain. The first two words of “blockchain” explain the platform’s functionality: a block on which chains of data are recorded, which are accessible to everyone in a secure and pseudonymous manner. The blockchain is decentralized and is instead maintained on thousands of devices around the world, every device holding a copy of the ledger. These devices, called “nodes,” guarantee the trustworthiness of a particular block of data on the blockchain through a consensus mechanism. Depending on the consensus mechanism utilized, the nodes assert that everyone who has access to the blockchain network is one and the same and has not manipulated the information held within that block. Each type of blockchain has its own consensus mechanisms utilizing different methodologies to achieve that consensus.

Access to the blockchain network is granted through digital wallets, which store not only the encryption keys necessary to initiate transactions on the blockchain but also intelligent pieces of software code known as smart contracts, which execute transactions on the blockchain. Digital wallets utilize unique encryption keys that correspond with a specific public key on the blockchain ledger, which acts like a bank account number, and is used to complete transactions, which are recorded on the blockchain, acting like transaction statements. These keys serve a similar purpose to the pet naming system used to simplify browsing the Internet. Just as this system allows users to enter a more usable web address instead of the long and complicated Internet Protocol address that actually routes their access through the Internet, blockchain public keys simplify browsing the blockchain instead of relying on long and complex blockchain addresses.

9.4.2. Advantages of Blockchain in Wallet Security

Table of contents: 9.4. The Relationship Between Blockchain and Digital Wallets 9.4.1. How Digital Wallets Utilize Blockchain 9.4.2. Advantages of Blockchain in Wallet Security 9.4.2. Advantages of Blockchain in Wallet Security The centralized nature of currency and payment systems is a significant one. Service outages, and cyberattacks are some of the vulnerabilities that are evident in the management of traditional currencies. Some of the most notable examples of issues with cybersecurity in traditional payments are data leaks, and the ill-famed cases. The problem is all the more relevant in an increasingly cashless and globalized economy, where consumers demand ease of access with added security. Services that rely on standard security procedures, such as encryption keys, need to be focal point of renewed analysis. Encryption algorithms are known to be a part of simple replicable procedures; the implementation protocol is where the main difference comes from. However, this logic assumes that security is at the level of the encryption, and not of the attacker. Specialized systems change ownership of values. Money structures need to adapt to these novel opportunities in order to provide added security in their transactions. Blockchains serve a seminal role in establishing decentralized neutrality through security measures such as hashing, and address value changing. The concurrent power of the blockchain is that it eliminates need trust in centralization authorities or mediators. In the sense of the concept of uncertainty, the Blockchain offers increased resilience in sense of existing cognitive biases on probabilities. The fact that cryptocurrencies are anti-fragile means that monetary systems can offer greater equilibrium in incentive structures. Since trust in security of positive balances is possible with proper cryptographic implementations; moral hazard can thusly be eased using the Blockchain.

9.5. Integration of Smart Contracts with Digital Wallets

Digital wallets are instrumental in facilitating transactions on decentralized platforms. With the advancement of digital wallets, transactions have become streamlined and accessible for users unfamiliar with complex blockchain infrastructure. This practical utility of digital wallets is complemented by the integration of smart contracts. Smart contracts, as self-executing contracts, enhance the functionalities of digital wallets to go beyond simple transactions. The integration of smart contracts with digital wallets enables the automation of complex transactions involving predefined rules and conditions.

Smart contracts can automate different elements of a transaction process, including transaction verification, rights-transfer, and execution. The utilization of smart contracts allows users to automate transactions by pre-specifying the conditions for executing or canceling transactions. For instance, digital wallets for initial coin offerings deploy smart contracts that execute a transaction by transferring digital tokens from the issuer's smart contract to the investors' wallets upon receipt of contribution funds to the issuer's wallet. The integration of digital wallets and smart contracts removes operational friction and enhances their utility. The consequence of this smart contract and wallet integration will be more refunds to investors through smart contracts for failed token sales, reducing the risk of loss and promoting investor participation.Concluding thoughts on the integration of digital wallets and smart contracts focus on the implications for user experience and usability. Digital wallets often act as intermediaries for the execution of blockchain transactions. Interdependently, smart contracts offer more services integrated with digital wallets than simply facilitating pooled transactions on public ledgers. With such an integrated system, digital wallets will enhance the user experience by streamlining the execution of transactions and increasing operational efficiency.

9.5.1. Automating Transactions through Smart Contracts

When using digital wallets, the user’s transactions data are maintained internally on the wallet. This data must be kept secure and private, because gratuitous disclosure could potentially compromise how secure the relationship between the service provider and the user is. Therefore, unlike smart contracts, digital wallets store as little information as possible that are needed for the transactions to work. However, a smart contract does the opposite; it makes sure that the data for its scheduled operations are public to all counterparts engaged in a transaction. Also, a smart contract is capable of monitoring when the information needed for the operation is updated before its scheduled time. The smart contract triggers predefined operations at that moment in time. Therefore, the only data that a smart contract has access to are the public data on-chain. By integrating a digital wallet and a smart contract, both the digital goods and services as well as the transactions associated with them can achieve both types of results, security and transparency.

Therefore, by integrating smart contracts with wallets, we can schedule future transactions that the smart contract would execute on behalf of the wallet holder. Such transactions could require that certain predefined conditions be met, and include time constraints. For example, a smart contract acting on behalf of a digital wallet can be programmed to send a predefined fraction of the user’s cryptocurrencies to a specific crypto address if the prices of these cryptocurrencies drop below certain thresholds. These transactions could happen only at a certain time of day or be limited to a predefined length of time. Such intelligent transactions are extremely useful for crypto traders, in particular during periods of high volatility. An intelligent wallet developed in this way becomes increasingly intelligent by interacting with other smart contracts.

9.5.2. Impact on User Experience and Efficiency

Despite their potential to eliminate the need for intermediaries, the adoption of smart contracts has also faced criticism, particularly around their confirmed transaction times. Smart contracts rely on a pre-agreed means of validating transactions and condition outputs, and this means the execution time of smart contracts can be lengthy. Currently, the execution of smart contracts can take between 14 and 30 seconds depending on the time taken to confirm the transaction. However, this execution time is longer than the time currently required to initiate centralised transactions when carried out in typical user amounts. As transaction volumes increase, this centralisation transaction confirmation time is reduced, and limits around transaction size have been minimised. Nevertheless, for digital wallets processing across the blockchain, transaction costs also increase dramatically with transaction volumes. Offering smart contracts through digital wallets can provide insights into impacts on user experience and efficiency. A resulting conflict is that while user experience can be increased by facilitating frictionless interactions via using smart contracts, the increased confirmation times and expenses can negatively affect the use of smart contracts on digital wallets. As such, user experience decreases when network traffic increases. This highlights the potential need to further reduce centralised transaction confirmations, thereby increasing the likelihood that wallets will simply create transactions rather than smart contracts to manage digital assets. The increasing layer two solution popularity can increase the scope to interact with blockchain technology while managing the confirmed time. Nevertheless, such solutions are not unique to blockchain-based transactions linked to smart contracts.

9.6. Challenges in Integration

While the integration of blockchain, digital wallets, and smart contracts holds enormous potential, there are also many challenges that must be addressed. These impediments come in various forms, including technical barriers, regulatory and compliance issues, as well as integration concerns related to existing business models, privacy and security considerations, and user experience.

High-profile projects that enhance the ecosystem within which solutions are provided may assist with development; however, integrations are still hindered by a lack of standardization across systems and processes; the need for real-time interoperability among blockchains, cryptographic tokens, and financial systems; as well as scalability and traffic congestion issues. As a nascent field, blockchain technology is evolving continuously with several designs and many implementation options. In this highly fragmented environment composed of different yet interacting protocols and architectures, using various open-source and proprietary systems poses a significant problem. Without universally accepted standards or governance models for the development of a connected and efficient blockchain ecosystem, the need to build bridges from closed blockchains to existing infrastructures creates a significant gap in the overall utility and interoperability. As the injections and withdrawals of capital; cryptographic assets; and distributed tokens through exchanges, brokers, and gateways create points of potential systemic failure as large flows might congest the networks, it becomes important to reconcile trades in financial systems and blockchain ledgers seamlessly in real-time.

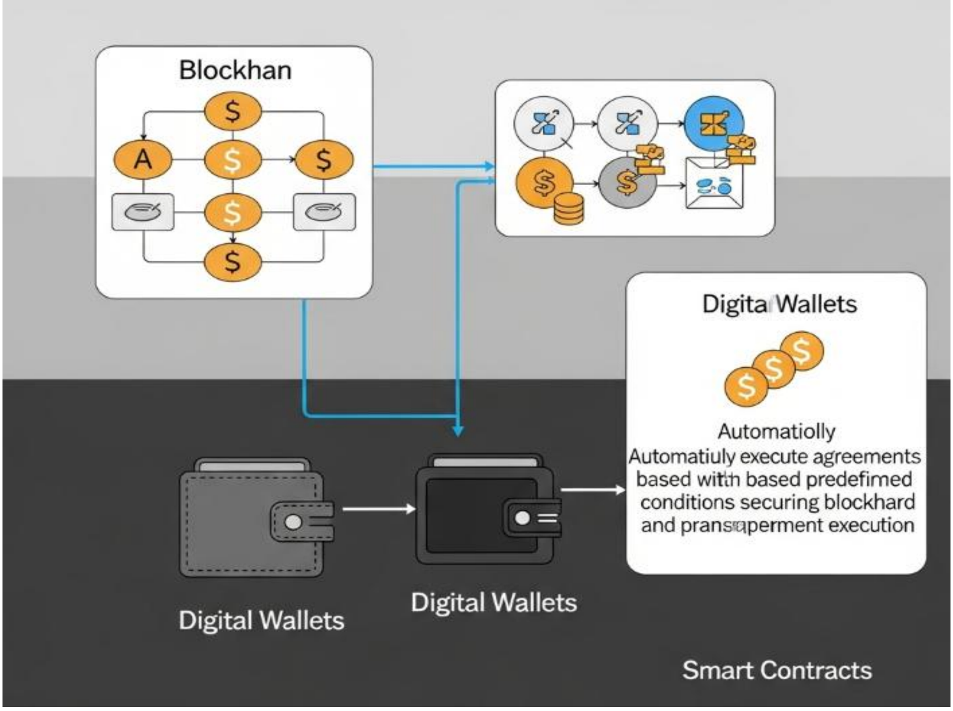
Blockhan
$
A
$
$
$
$
Digita Wallets
Automatiolly
Automatiuly execute agreements based witth based predefimed conditions securing blockhard and pransaperment execution
Digital Wallets
Digital Wallets
Smart Contracts

Fig 9.2: A Blockchain Platform for User Data Sharing Ensuring

The regulatory treatment of blockchain’s gain as income; transfer tax on the gifts of cryptographic tokens; sales tax on the currency-like services provided using tokens; and rules for exchanges, mining pools, and wallets are some of the crypto-related compliance issues that stakeholders would need to address. Their existence has an important impact on the design of solutions as implementers intend to develop a viable distributed token architecture. If every token transaction represents a taxable event, it would be impractical to use it for most commerce. Such complexity also adds friction to entry, challenging the blockchain platform’s potential for various industries.

9.6.1. Technical Barriers

Several technical barriers hinder the adoption of blockchain and its associated technologies in the domain of payments and transactions. Most currently available public blockchains suffer from scalability issues relating to high latency and limited transaction throughput. High latency in such networks is mainly caused by their reliance on a distributed consensus mechanism for transaction verification and addition to the chain. Additional delays are incurred in cases where validation difficulty is set high to protect against attacks. On the other hand, transaction throughput needs to be drastically improved in public blockchains so that they can compete with traditional payment systems that can handle thousands of transactions per second. The relatively slow transaction speed of conventional public blockchains makes them inefficient for micro-transactions, and therefore, they are yet to see widespread use in payments and financial transactions.

Although many of the issues associated with public blockchains such as high latency and low throughput can be resolved by using private and permissioned blockchains, the security of such networks is unproven. These blockchains are vulnerable to collusion-based attacks, where a coalition of users conspire to confirm false transactions. One such effort aims to solve the issue of scalability in transaction-heavy applications, including decentralized ones. In order to ensure that the network can scale to serve transaction requests for millions of users, it proposes a hybrid consensus mechanism that combines proof of work for the pub-sub layer with proof of stake in a higher layer to resolve conflicts and determine the canonical chain.

9.6.2. Regulatory and Compliance Issues

The legal landscape surrounding blockchain technology is uncharted territory. Many regulators are deliberating on how to build a regulatory framework to govern aspects of the technology, but legislation is relatively minimal. A major reason behind the lack of legislation is because many crypto assets are either not seen or treated as "money" and are considered to be property for taxation purposes only. Most regulatory authorities in countries around the world have not committed to seeing crypto assets as specific types of currency or money, and crypto assets typically bounce around in value, making it difficult to position crypto assets as a type of currency. Since allocating crypto investments can be structured similar to real estate investments or even safe-haven investments like gold, legislation is in flux and must continue to evolve over time.

Therefore, many businesses are hesitant to invest time and funds into participating in the crypto ecosystem for fear of the consequences of getting caught on the wrong side of the legal fence. If regulatory authorities do not extend protections and detailing on crypto asset investments, whether through AML or prohibit Forex transactions or exchanges, user adoption will take longer than it should, and it will be more challenging for crypto assets to get the attention they deserve. At the same time, organizations could be sued due to the nature of the launch; for example, if digital assets are sold using a smart contract that does not follow certain legal standards, customers could file suit.

9.7. Future Trends in Blockchain, Wallets, and Smart Contracts

The future of blockchain, wallets, and smart contracts is set to be shaped by emerging technologies. Blockchain could be combined with additional emerging technologies such as artificial intelligence, augmented reality, and big data analytics to create completely new cryptocurrencies and digital wallets. These technologies not only offer advanced security for digital wallets but also enable faster transactions, better user experience, improved decision-making, and also work towards helping increase the global crypto adoption rate.

As the market matures, we expect solutions to multiply that interconnect tokens and services across blockchains, wallets, smart contracts, and DeFi. This disintermediation will mean more people are organizing themselves around shared, immutable information. Young, tech-savvy users will access secure, smart wallet technology inside messaging applications. Corporations will access smart wallets through enterprise integrations, using tokenized information to handle their supply chains efficiently. The industry is working to make wallets usable and secure for regular users. Today, most users access Web3 through exchanges, and future wallet adoption will require an extensive Web3 ecosystem that includes more decentralization protocols.

The digital identity space is seeing growing interest from the Web2 sector, with hopes that Web3 can solve existing problems of centralized ownership. While no player has taken a dominant position in this multi-faceted market with different niches, products, and protocols, our outlook remains positive regarding the implementation of decentralized digital wallets. Moreover, they are the first step for users to participate in Web3 and launch a network on the blockchain from the start.

9.7.1. Emerging Technologies

Interest in emerging technologies, such as the blockchain, has grown over the last couple of years. A lot of Pan-European policy discussions focus on regulating particular use cases such as the digital economy. Blockchain in the real economy discussions are still advanced through early innovative applications, ranging from supply chain to mobility, some of which are discussed in more detail below. Blockchain technology adds a new building block to the digital economy – the programmable trust layer. This allows complementary applications throughout the technology stack, solving for fast and GDPR-compliant payment solutions that also meet AML/KYC requirements. Digital wallets are essential for mass adoption of blockchain applications. Future wallets have to become user-friendly, easy to set-up, answering consumer's needs while ensuring full compliance with all applicable legal requirements. Wallets will not only need to cover crypto transactions, but need to provide easy access to identity management solutions. Peer-to-peer identity management could ultimately be integrated into social network applications as an additional privacy-considerate feature. Communication and identification security will also be crucial for decentralized financing applications.

Scalability and privacy remain concerns for blockchain applications. However, there are promising solutions in the pipeline that will enhance and ameliorate security and privacy concerns. Automating processes through smart contracts will limit and in some cases eliminate the need for centralized trusted third parties. Smart contracts will thus have the potential to disrupt many professions. However, with the gain in simplicity and cost-efficiency, the trade-off regarding fault tolerance, foreseeability, and certainty of sanctioned breaches comes at question. The market seems to converge towards an approach that allows for hybrid solutions with human intervention at crucial decision nodes within the initiation and execution phase while employing smart contracts for the transaction execution where trusted behavior is ensured.

9.7.2. Predictions for Market Growth

The growing acceptance of blockchain technology by companies and organizations around the world is expected to lead to significant market growth for the blockchain and digital wallet ecosystems in the near future. The digital wallet sector is anticipated to grow from $1.48 trillion in 2022 to $7.58 trillion in 2028, with a compound annual growth rate (CAGR) of 32.4%. The motivations for using digital wallets include ease of use, flexibility, and the desire to automate financial services using the power of smart contracts. Digital wallets have applications for both individuals and businesses in many sectors beyond payments, including ticketing, rewards points, and gifting. However, payments are clearly a primary motivation, with digital wallet usage increasing dramatically in such sectors as travel, e-commerce, restaurant chains, and airline.

Despite the recent upheaval related to the collapse of numerous high-profile cryptocurrency exchanges and wallets, interest and investment in the blockchain and digital wallet ecosystems remains strong. Companies have invested heavily in building the infrastructure for blockchain and digital wallets. Even though these companies are not directly monetizing such extensive infrastructure investments, they are doing so to position themselves for a future in which virtual currencies play a major role in the global economy and their respective markets. Whether this future is referred to as “Web 3” or “the Metaverse,” the underlying architecture of blockchain and digital wallets will be central to this new virtual paradigm and its enabling technology.

9.8. Case Studies of Successful Implementations

Several cases exist today that demonstrate how these implementations can affect an organization’s key business processes and their risk or liability may be reduced as a result of a blockchain, digital wallet or smart contract implementation. Additional benefits can also be seen in the efficiency of the business process: a reduction in time or costs associated with the activity.

The impact that blockchain could have on the existing financial sector and facilities has long been considered since the inception of Bitcoin and the creation of the first blockchain in 2008. Banks, stock exchanges, and insurance companies work with transactions that have inherent layers of complexity related to verification and receipt confirmation managed by a centralized third party. All of this is verified against private repositories of information, which can take a day to process a transaction, validate its authenticity and ensure that the person sending the transaction has access to the funds. As the stock market and cryptocurrency asset exchanges have shown us, the volume of transactions can spike, leading to even longer verification times. The benefits that blockchain and distributed ledger systems would bring to this industry are the ability to conduct transactions faster, hold copies of information that can be easily validated and ensure the reliability of transactions through the blockchain’s inherent properties.

Real estate transactions are in the public spotlight due to their high-profile multi-million-dollar sales and the fact that the process is riddled with third-party verification agents such as title companies verifying chain-of-title paperwork, land surveyors and real estate agents. The proliferation of title insurance protects buyers from loss in the event of faulty title searches or cryptographically valid claims against parts of the chain of title that were previously owned, and the use of smart contracts could feed directly into the chain of title for the specific property, adding both purchase and sale chain transactions along with a time stamp when either activity occurs.

9.8.1. Financial Sector Innovations

In recent years, the financial sector has been one of the most innovative adopters of blockchain, digital wallets, and smart contracts. One sector of critical importance is the provision of settlement capabilities and in particular of instant settlement of retail financial transactions, whether involving payments or asset transfers. Digital currencies have given prominence to secure instruments of value transfer. The digital wallets containing these digital currencies have also been adopted as stores of value, reflected in a market with a value in excess of one trillion dollars.

Stablecoins offer other advantages. Their values are linked to a real-world currency, thereby limiting price volatility. They are, however, in their basic form, not regulated by central banks and can experience runs akin to bank runs in the event of a buildup of trust concerns. Stablecoins can be backed by real-world currency reserves or by collateralized short-term loans or creditor claims. They can be issued by private-sector players that are not regulated by central banks or by private-sector players that comply with full reserve regulations.

Recently proposed central bank digital currencies adopt the best characteristics of both private-sector solutions, as well as stablecoins and backed, segregated, fully regulated digital wallets, and allow the central bank to act as a Lender of Last Resort. Digital currencies, especially when they are instantaneously settled, allow for the instant settlement of real-time gross payment systems. At the beginning of 2023, central banks were considering whether and how to issue digital currencies, which address issues of payment settlement, financial stability, digital currency efficiency, and other practical aspects that have been raised by theoretical studies.

9.8.2. Real Estate Transactions

Transacting real estate entails so many steps and the involvement of so many agents or transaction participants that its length, complexity, and often cumbersome nature can lead to all kinds of issues. These can include unanticipated closing costs for the buyers and sellers or property value surprises when issues are suddenly brought to light, breached contracts, title disputes, and illegal activity to avoid tracking and tax liabilities. Long leases are often created, but management afterward and other property ownership events during the lease’s lifetime can also lead to disputes or just unnecessary complexities. Transfer agents; recording, title, and settlement companies; banks and other financial players underwriting, processing, and settling mortgages; bureaucracies responsible for tax assessment, appraisals, and collections; insurers providing casualty and title coverage; lawyers providing legal assistance for the transaction; and others have traditional roles in real estate transactions for good reason. Digital tools have been proposed to help facilitate various aspects of real estate transactions. Yet generally, none have performed well in terms of saving time, money, or risk to date, leading to obvious user-friendliness and efficiency concerns.

Blockchain-based digital assets, smart contracts, and digital wallets open innovation paths that could completely eliminate these historical inefficiencies while leaving or improving upon the historical transaction security provided by a variety of existing agents and bureaucracies. With property tokenization to represent both direct ownership and indirect ownership, the costs and steps of traditional property transfers, sales, purchases, and refinancing can be reduced by tokenization, while at the same time being more public, verifiable, and comfortable for various parties in the transactions, and therefore less risky. By blockchain associating automatically contemporaneous settlement procedures and documents to contracts, smart contracts allow the contract event to happen immediately while also eliminating errors and potential issues associated with partial execution of a real estate transaction.

9.9. Comparative Analysis of Different Blockchain Platforms

The term 'blockchain' has become commonly associated with a few well-known blockchain networks such as Bitcoin and Ethereum. These are public permissionless chains that function as platforms for a wide range of distributed applications that allow tokenization while leveraging smart contracts, which help in executing automated, pre-specified tasks. Beyond Bitcoin and Ethereum, there are several other plausible blockchain platforms that have emerged in recent times, trying to either solve known problems without changing the fundamental properties of the underlying technology or extending the capabilities of the technology as a whole, by changing or relaxing some of the properties that can be traded-off. In this section, we focus on the comparison between Ethereum and Bitcoin, as the two most important blockchain platforms, and some of the notable platforms that have emerged in recent times. Ethereum provides a rich programmability feature via its Turing-complete smart contract language, thereby allowing for a wide variety of possible uses. However, this flexibility comes at a cost – it could inherently lead to security vulnerabilities and issues of efficiency on the Ethereum blockchain, thus putting limits on the practical performance of the blockchain when it comes to use cases with stringent efficiency and security requirements. Bitcoin, on the other hand, sacrifices flexibility, and thus efficiency and security and is therefore not suitable for many types of smart contract-based applications, thereby also limiting the kind of deployment possible within the blockchain ecosystem as a whole. Also, Bitcoin does not provide a built-in name registry service which is a notable functionality of Ethereum. Within this context, we summarize some well-known blockchain platforms that spread out from Bitcoin and Ethereum and that are being considered for a wide variety of tasks, ranging from time-stamping and notarization to maximizing vision and security of our society.

9.9.1. Ethereum vs. Bitcoin

While Ethereum and Bitcoin both utilize blockchain technology, their shared infrastructure distinctly defines them as two separate tools for two separate use cases. After Bitcoin, Ethereum was the second successful decentralized blockchain network; several other blockchain networks have since been created based on its technology.

Bitcoin enables the transfer of Bitcoin tokens within a peer-to-peer network of peers; the tokens in Bitcoin's UTXO model exclusively represent value, in the form of limited digital cash, as an alternative to fiat money. Bitcoin doesn't possess a built-in programming language that enables developers to create custom programmable applications on top of the Bitcoin blockchain. Bitcoin is a store of value for individual transactions but has limited programmability capabilities.

Unlike Bitcoin's UTXO model, Ethereum uses an account-based model similar to how traditional bank accounts work. Unlike Bitcoin, which solely supports currency transactions, Ethereum supports tokenized asset and app execution transactions. Ethereum enables the creation and operation of decentralized applications, also known as DApps, such as games, social networks, betting applications, and decentralized financial services. DApps are created and hosted as smart contracts written in Ethereum's local high-level programming language. Smart contracts are suitable for any type of agreement that can be expressed in a decision tree format. Instead of creating DApps from scratch, developers can also create their own variations of existing DApps.

9.9.2. Other Notable Platforms

When comparing alternative blockchain platforms, we cannot disconsider Ethereum's ecosystem to the whole concept of a decentralized application. Alternatives to the Ethereum ecosystem are usually thought of as Ethereum killers. In fact, Ethereum had been forking in a fast pace to solve the gas price issues and to proceed with the switch to proof of stake. Developments in the other platforms have to be speeded up, otherwise they will lose developers, a good user interface and other intangible factors to Ethereum.

A protocol aimed at achieving blockchain interoperability allows the transfer of tokens and data across different blockchain ecosystems. Cross-chain enables an open-source platform for decentralized finance. More specifically, it allows custody bridges and atomic swaps. The custody bridge helps transaction execution with the help of a third-party. In the atomic swap, no third-party is involved during the transaction. Currently over USD 50 billion have been transferred using this protocol.

A second-layer protocol intended for micropayments works over Ethereum. It is implemented using Merkle trees. Without going into technical details, this blockchain aims to solve the speed and gas price issues faced by Ethereum. Smart contracts on this platform reference paths to the Merkle trees on Ethereum, such that only short snippets of data are inserted on Ethereum. This protocol allows several applications in various sectors such as social media, gaming and decentralized finance.

An open-source blockchain protocol is designed to scale without sacrificing speed or decentralization. It supports the building of decentralized applications while addressing the scalability needed in decentralized finance and other markets. The differences with the Ethereum platform relate to the limitations of smart contract building on Ethereum. A token is used for staking and for settlement in the network. Since 2018, this platform has collected over USD 35 million in funding from various companies.

9.10. User Adoption and Market Penetration

While the incumbent mechanisms of payments, remittances, and settlement functions are proven and trusted, the blockchain-focused models are often new, experimental, and considered risky because of technical problems, security breaches, or fraud. Monetary incentives for using a blockchain or digital wallet often do not currently exist, and the cost of conducting a transaction is high compared to the current centralized solutions. As many blockchain solutions are not yet ubiquity, the demand for using a digital wallet within the blockchain ecosystem is low yet. Thus, for the services on the blockchain to have an impact, a critical mass of participants should be achieved so that the ecosystem becomes open and transparent enough, so the others see the ripple effect. Building an attractive dApp that provides sufficient benefits or compensation for users may lure users who are willing to take the risks even with low penetration.

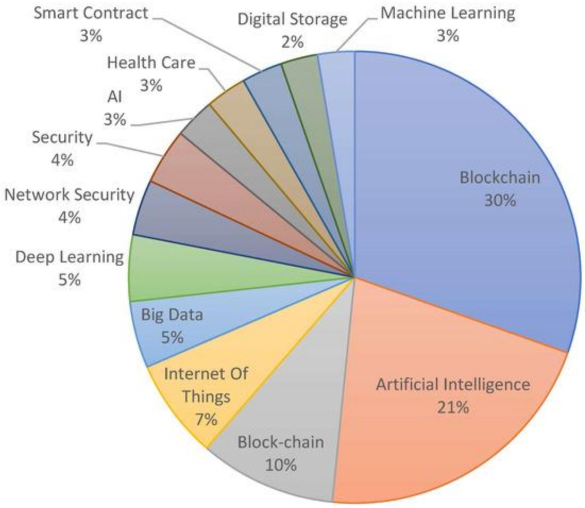

Fig : Blockchain Technology and Artificial Intelligence Together

The users and properties of the cryptocurrencies users can differ in important dimensions: the source of funds, the amount of transaction, the technology readiness, or the extent of the willingness and ability to switch. While on average cryptocurrencies users are more tech-savvy and interested in exploring new technologies, there are sizeable groups of crypto users, particularly in different geographic areas and with varying crypto assets and transaction amounts. For regulators, the heterogeneity of the user base matters not only for policy consideration but also for the considerations of technological watch.

For market players, understanding how cryptocurrency users fit in a larger picture of the crypto landscape is key to successful implementation. In business decisions on products that should integrate the blockchain, adoption in the existing nonblockchain model must be weighed against the possible competition and disruptiveness as a result of switching. This assessment also could help reinforce blockchain promoters' efforts to convince the actors on the traditional economy to create a similar offer in the blockchain ecosystem.

9.10.1. Factors Influencing Adoption

Adoption plays a significant role in the success of a promising technology. It does not only accelerate the technology's advancement, but it also improves the opportunities for enhancement. Blockchain technology is already promising beyond this decade, but there is speculation on whether it is the solution for the current financial ecosystem. Therefore, various parties are involved in the evaluation of user adoption. Lawmakers are recognizing the importance of cryptocurrencies in the financial ecosystem, while members of the banking ecosystem are disallowing third-party custodianship.

User adoption is defined as the decision by the user to receive the new technology and subsequently incorporate it into regular daily practice. However, this definition does not reflect the true nature of the question at hand. The adoption stage must be expanded to incorporate the following states of technology use: ignoring, dabbling, engaging, and experiencing. Despite cryptocurrency use growing tremendously since Bitcoin was first introduced, there is evidence of a plateau effect. Hence, it is important to explore the key segments first and then expand from there. The understanding about the key user segments can subsequently influence marketers in how they position their solutions in a competitive landscape. The influences of adoption may also be applied back as feedback to further improve the underlying technology's development.

Adoption studies in the context of financial technology are still rare. The same goes for the use of Smart Contracts or Digital Wallets. Blockchains can evolve continuously as a new way of doing things. Finding the right way of using blockchains is important for subsequent growth. Comprehensive studies which examine Digital Wallet Adoption or the User Motivation for cryptocurrency through extended Technology Acceptance Models or the Unified Theory of Acceptance and Use of Technology are limited.

9.10.2. Demographic Insights

The adoption of Web3 services is still a niche market, with dozens of solutions allowing for digital asset and identity management competing to lead the way. Despite the various approaches, challenges, and technologies behind the concept of a digital wallet and digital wallet services, they are all gateways to digital identity and interactions. Therefore, the topic continues drawing interest, speculation, funding, and talent. This section discusses the current user base of wallets to identify the challenges that lie ahead in achieving wider adoption.

As digital wallets serve multiple functions and support different use cases, in trying to understand their users and their demographics, we have to consider them in buckets based on the use case. Some wallets are direct-to-consumer solutions that promote their product as appealing to previously non-crypto-savvy audiences, with hundreds of tokens available for swaps and instant deployment of dApps direct from the wallet. Some custodial solutions allow users to trade, earning some yield on assets, but in a non-intuitive way — who knows that a transfer to an exchange could get double-dipped in fees? Some wallets offer high security and convenience promised by mobile biometrics — but storing a backup key as requested by the wallets is not something that an average user has learned to do.

9.11. Impact on Traditional Financial Systems

A common fear associated with blockchain technologies, digital wallets, and smart contracts is that they have the potential to disrupt many traditional financial systems. Indeed, by decentralizing large parts of financial systems, such technologies can provide a range of services—escrow, custody, payment, settlement, credit supply, issuance of different types of assets, insurance, and many others—without the involvement of intermediary trusted institutions. Furthermore, many of these services may be delivered cheaper and faster than those provided by those institutions.

The services provided by financial systems are typically protective or risky in nature. They include the protection of value (deposits), protection against accidents and calamities (insurance), the facilitation of transactions (money), the settlement of transactions (payments), the custodial safeguarding of property (custody), the transfer of property (settlement), the issuance of means of payment (currency), interest rate setting and management of short term risk (money markets), pricing, supply and demand of long term risk (debt and equity markets), protection against the risk of not being able to smooth consumption (credit and capital markets), property/identity verification (property registries), and the facilitation of human capital development (education). All forms of value considered—money, credit, insurance, capital goods, knowledge and skill, property, and property rights—are insurable, tradeable, or transferable on the market. Traditional financial institutions are able to position themselves on one or several of these angles and make a profit therein thanks to the provision of liquidity that reduces the operational and detailed risk of these operations.

9.11.1. Disruption of Banking Services

A wide variety of banking services and functions provide existing traditional frameworks and are used by both individual users and financial ecosystem participants to facilitate transactions. Digital wallets can be considered a lightweight version of banking. Wallets facilitate money flows and users store balances for settlement in and out of blockchains. Wallets ease cross-border payments by helping users avoid the fees charged by traditional banks. But wallets do not replace banks entirely. Unlike banks, wallets do not allow users to easily transfer fiat currency into digital assets and convert back and forth. In traditional banking, physical and digital infrastructure is maintained to service a customer base that relies on commercial banking for core financial engagements. Banks are highly regulated and earn a spread on lending versus deposit rates. They monetize ancillary transactions, including foreign transactions, cheque processing, overdrafts, cross border transfers, wire transfers, and account maintenance. Banks assist customers in safeguarding assets and monitoring transactions, but they are neither first nor foremost responsible for protection against fraud, hacking, or loss of funds. Certain banks have tighter relationships than others with individual customers, as determined by product tiering.

Banks have an impact on financial market functioning but do not actually provide stability. Banks perform due diligence on customers to verify identity and provide custodial services, which are relatively limited. Some specialized asset managers seek to maximize custodial revenues. Banks will seek to monetize transactions on integrated platforms in much the same way they do today in a digital asset ecosystem, and there are many regulations whose purpose is to ensure that the risks banks assume are kept to a minimum. The key question is whether those regulations will translate into different business models or elaborate variations on existing ones. Prior to such translation for digital asset banks, the same lenders on digital banking can provide similar services for users of digital wallets.

9.11.2. Integration with Existing Systems

The promise of blockchain-based digital wallets, permissioned smart contracts and smart debit cards is to democratize and universalize financial services by making them available to everyone with a smartphone. But in order to truly drive financial inclusion and broad-based wealth creation, we must also engage the non-blockchain smartphone users and tie in this new wave of technology with the traditional economy. This means working in parallel with existing financial infrastructure so that users can easily transfer between services and access points, and recognize and interact with surfacing smart contracts. This incremental adoption bridges crypto enthusiasm and gets legacy consumers engaged for the long haul.

Blockchain technology will need to integrate with legacy identity systems. As blockchain identity matures, consumers will begin to prefer B2C interactions that are not only convenient, user-friendly and privacy-respecting, but also display some compelling identity credential that allows the merchant to vet the consumer. For merchants that are already overwhelmed with preventing fraud in their legacy credit card backend, offering greater user security, enabling transactions to a greater majority of the population, and driving up revenue with reduced fraud risk become key incentives to adoption. Digital wallets will also need to connect with legacy payment systems. Although it is highly likely that payments will soon decouple from credit cards, with faster settlement times, broader international reach, and potentially lower fees, the majority of today's point of sale infrastructures are still hard-wired to accept card payments. In the short term, and possibly longer, digital wallets will need to both send and accept payments using card rails.

9.12. Ethical Considerations

The incorporation of blockchain technology, digital wallets, and smart contracts into various sectors raises a number of ethical questions. Issues such as privacy, security, and legality must be taken into consideration. While blockchain has a reputation for being a secure, anonymous, and unchangeable way to store transaction histories, these advantages may not apply when blockchain records are linked back to individuals or organizations, as they often are with the public blockchains utilized by cryptocurrencies. In addition, tokens and currencies issued via crypto wallets and coins have proven to be magnetically attractive to criminals and cyber-hackers. A large number of hacks against digital wallets have resulted in lost funds and negatively impacted the ethics of using these technologies. Finally, legality is a serious concern; there is much that is still unresolved concerning legal issues relative to taxation and regulation.

Accessible, immediate, and permanent records on the blockchain make companies more accountable to stakeholders at every level, including customers, employees, governments, and investors. Blockchain technology has also been a powerful tool in transforming our current society into a more transparent one. However, as previously mentioned, transacting on the blockchain is pseudonymous; therefore, these records do not have any accountability or transparency if the public cannot identify the individuals involved in the transaction. As such, cryptocurrency has established a negative image of being a medium of trade among those involved in morally dubious businesses, including organized crime and human trafficking. These issues raise ethical discussions over the true level of accountability and transparency within organizations using blockchain and to what extent we should rely on their public records as a measure of ethical conduct.

9.12.1. Privacy Concerns

Privacy is considered an important core right of individuals, and transparency for all could be a double-edged sword. Blockchain technology was first applied to electronic cash systems, where the goal was to enable digital cash transactions that cannot be reversed and also cannot be faked, but without a trusted third party to oversee the transactions. All transactions are recorded on a distributed ledger that is public and transparent to all, as the name ‘blockchain’ suggests. With the implementation of a digital wallet identifier that is not tied to any real-life identity, exposed transaction data would become a threat to user privacy. Why would it be assumed that any such identifier could be created that is unlinkable to any real identity? The chain of blocks added to the public ledger is assumed to be tamper-proof based on the consensus protocols established on the network of participant nodes. However, the consequence of placing all transaction data on a public ledger forever is that it offers data analysts unlimited opportunity to observe and analyze transaction patterns within the network, which may expose sensitive information. One might ask if privacy is even a consideration for a currency which is anchored on full transparency? True, Bitcoin is not suitable for illicit activity without some way of shielding the source and the recipient wallet addresses prior to and at the time the transaction is initiated.

A principle that fosters the emergence of blockchain technology is the absence of third-party trust issues, which is clearly seen in the protocol specifications. All cryptocurrency transactions are validated through the consensus protocols established by the blockchain. Avoiding payment processor fees while transacting on ledger chains full of transaction metadata that are not removed or selectively deleted but remain effectively “disclosed” for anyone on the public ledger – is this a proper driver for its rapid rise? If not personnel seeking to expose illicit activity for political or financial gain, why are cryptocurrency transaction analysts and data miners observing and exploiting the financial behavior of crypto users? Are there no ethical issues concerning the consultation of crypto transaction data?

9.12.2. Transparency and Accountability

Transparency is an important characteristic and promise of cryptocurrencies, DLTs, and digital currencies more generally. Given that not only central banks are creating digital versions of fiat currencies but also private sector entities are creating digital currencies, it is essential that they incorporate transparency. Central banks have fiduciary responsibility to, among other things, provide a stable currency so their information and actions should be as transparent as possible. Additionally, if digital currencies are to fulfill a store of value role, the monetary policy framework that dictates the relative scarcity of the currency needs to be transparent to prevent excessive digital currency demand or supply. Thus, central banks are expected to adhere to the same principle of transparency that applies to monetary policy, which states that when monetary policy impacts are stronger, the role of transparency in the conduct of policy becomes clearly paramount.

A unique feature of blockchain systems is that generally they contain a record of every transaction in its history. This means that if someone has the right permissions and tools, the spending and receiving of every digital currency unit can be tracked. Additionally, the fact that cryptocurrencies are not reliant on trusted third parties means that confirmation of transactions can be easily verified. Blockchain’s unique enabling technology relies on its transparent verification process to ensure no double spending takes place. One method of ensuring a more transparent process is to emulate a form of permissioned blockchain. Therefore, projects have emerged to create solutions similar to that of Bitcoin but which utilize a form of permissioned ledger. The accounts and balances on the system can be inspected at any time through a public API.

9.13. Conclusion

The convergence of blockchain technology, digital wallets, and smart contracts marks a seminal shift in the narrative of the Internet's evolution, steering it towards a 'Web 3.0', characterized by distributed architectures propagating Data Sovereignty and Trust. Blockchain, by virtue of its immutable record-keeping, introduces Data Sovereignty to ever-growing data assets and microservices, concurrently churning enterprise IT departments' processes aimed at their availability, access, and use, while instilling the value of Trust to both companies and customers. Smart contracts unravel the automation's promise that enterprise Information Systems and software have yet to exhaust and is perhaps the last great advancement in the efficiency quest of business operations.

Yet how will all that come to be? Consensus, transaction digital signatures, and native assets managed with tokens dictate digital wallets as the single most important key chain for the forthcoming new generation of digital services, vying for replacement of existing social networking, commercial commerce systems, and cryptography's banking roles. Corporate digital wallets, perhaps, are the potential Achilles' heel. All the cryptographic primitives are routed via them. They will interlace and connect disparate, proprietary layers that currently silo society from digital inclusion. Their support for regular fiat currencies cleverly seeded with liquidity may soon become our alternate digital identity model while moving the proverbial mud from the banks to non-bank commercial entities, shrinking the gap between gross domestic products and money supply at these very peculiar, unprecedented times in history.

Smart contracts presage companies and customers moving the IT department into the coding workstream. They are at the junction of risk, accountability, and transparency. The segregation of duties will be automated yet tamper-proof, and there will be no need for IT audit checks or for different IT audit trails; they will be all rolled together within the contracts, augmenting a benefit-and-incentive-driven ecosystem different from the current insurance-based risk pool mechanics.

References:

Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.

Tapscott, D., & Tapscott, A. (2018). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Portfolio.

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p4

Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper. https://ethereum.org/en/whitepaper/

Zwitter, A., & Boisse-Despiaux, M. (2020). Blockchain for humanitarian action and development aid. Journal of International Humanitarian Action, 5(16). https://doi.org/10.1186/s41018-020-00072-3