Bus Inf Syst Eng
https://doi.org/10.1007/s12599-021-00736-6

CATCHWORD

Universal Wallets

Kim Peiter Jørgensen · Roman Beck

Received: 6 November 2020 / Accepted: 18 November 2021

Keywords Blockchain · Universal wallet · Crypto wallet · Token

1 Introduction

The adoption of blockchain-based cryptocurrencies has paved the way for blockchain projects in other applications. In general, cryptocurrencies and crypto tokens are accessed through crypto wallets containing the necessary keys to transfer digital assets securely. The increased density of automation—from smart clothing, homes, and appliances, to smart cars, smart roads, and smart cities—has heightened the need for effective, resilient, and secure access to and communication with these devices. In this context, universal crypto wallets play a key role in authorizing transactions and governing activities.

Digital wallets existed long before the invention of blockchain. *Crypto wallets* are a new type of digital wallet that provide a secure environment for accessing and conducting transactions on blockchains. The next evolution of crypto wallets, *universal crypto wallets*—what we call *universal wallets*—can be considered the browsers used to navigate on blockchain (Matthews 2019; Büttgen et al. 2021, pp. 85–89), even though they are not yet as user-friendly as modern Internet browsers. Universal wallets have recently gained prominence in a range of sectors. Facebook has announced its cryptocurrency Diem (Libra Association 2020), previously known as Libra (Kastrenakes 2020; Rrustemi and Tuchschmid 2020) and accompanying wallet, Novi; this system essentially turns a Facebook account into a wallet that manages not just identity credentials but also other types of tokens. Several banks are investigating the use of wallets for cross-border transactions (Auer and Boehme 2020), while central banks are exploring wallets for handling central bank digital currency (Engert and Fung 2017). The European Union is developing cross-border services for citizens based on the European Blockchain Services Infrastructure (EBSI); these services will require the use of universal wallets to access resources and manage digital credentials. Finally, the rise of non-fungible tokens (NFTs) (Nadini et al. 2021) representing art and other assets has only been made possible via the use of universal wallets (Wang et al. 2021).

The widespread view that identity is becoming the new currency (Maurer 2020) illustrates the importance of wallets that can securely manage digital identities, identifiers, and credentials. As personal identifiers are increasingly used for trade and to provide digital and physical access to services or buildings, protecting digital identities is becoming even more important. Frequently reported security breaches demonstrate the current vulnerability of customers' data and the need for increased security. Data centers of large companies have seen countless breaches that have enabled identity theft and fraud (Toth and Anderson-Priddy 2019). Hence the focus in this paper is on universal wallets in blockchain systems, which can achieve the desired levels of security and stability. A perspective on the benefits of blockchains for self-sovereign identity can be found in van Bokkem et al. (2019).

Accepted after two revisions by Ulrich Frank.

K. P. Jørgensen · R. Beck (✉)
IT University of Copenhagen, European Blockchain Center,
Rued Langgaards Vej 7, 2300 Copenhagen, Denmark
e-mail: beck@itu.dk

K. P. Jørgensen
e-mail: kjrg@itu.dk

Published online: 08 January 2022

Universal wallets are important in situations where digital identification and blockchain-validated credentials are required. The use of universal wallets in these situations creates new types of digital interaction with reengineering of relational and societal structures (Hyperledger 2018; Schwerin et al. 2017). In an increasingly tokenized economy, using wallets to interact with blockchain services provides the needed level of information security (Ramkumar 2018). To understand universal wallets, one must first examine the context in which they are used. In this research, we discuss the meta-characteristics of wallets along with existing use cases, the socio-technical system around these use cases, and what it takes to manage digital identities and credentials through a wallet from the user's perspective. Thus, we answer the following research questions: *What are universal wallets and what functionalities do they provide for managing digital identities, identifiers, and credentials?*

In answering these questions, we contribute to the academic discourse about blockchain by directing attention to the percolating field of wallets, including the opportunities they offer for new business as well as the societal opportunities and risks they present. We first focus on the wallet itself by outlining the elements of a taxonomy for universal wallets. Next, we address the environment where users meet, manage, and use these wallets. Finally, we will provide a perspective on why universal wallets are a logical enhancement of blockchain systems.

The remainder of this paper is organized as follows: in Sect. 2, we provide the literature background and outline different dimensions of crypto wallets and universal wallets. Section 3 describes the foundations for our taxonomy, as well as the developed taxonomy itself. Section 4 discusses the implications of universal wallets, which leads into Sect. 5, our conclusion, which proposes avenues for future research.

2 Literature Background

Crypto wallets—software applications used primarily for managing cryptocurrencies—gained importance with the rise of cryptocurrencies (Lansky 2018). As of 2019, approximately 200 different cryptocurrency wallets were in use, handling more than 1600 cryptocurrencies held and used for trade by a little more than 75 million wallet users (Statista 2021a). While these figures are estimates, they illustrate the relatively broad adoption of cryptocurrencies and crypto wallets in just a few years. Bitcoin owners use wallets to keep an overview of their balance and for transferring Bitcoins. Although the term "wallet" may suggest otherwise, a Bitcoin wallet keeps track of the balance, but it does not actually *contain* the Bitcoins. A crypto wallet can be installed on a local device, such as a computer, smart phone, or external drive. Wallets installed on machines that are always online are called "hot wallets," and those stored offline, e.g., on thumb drives, are called "cold" (Jokic et al. 2019). Hot wallets are less secure, as they can be hacked via the Internet (Rezaeighaleh and Zou 2019). Whether hot or cold, crypto wallets provide encrypted protection for digital assets, tokens, personal information, and actual transactions.

2.1 Universal Wallets

Universal wallets are crypto wallets capable of storing and managing not just cryptocurrencies and tokens but also all kinds of identifiers and credentials such as identity cards or passports. This versatility makes them a key application in constructing and managing identifications, credentials, reputation scores, and privacy (Paiblock 2020). Given the scope of universal wallets, it is fair to assume that their use will continue to expand rapidly as further assets get digitized. The emergence of interoperable universal wallets was facilitated by the development and widespread use of standards for fungible and non-fungible tokens, such as ERC-20 and ERC-721. This expansion will continue with the increasing use of specialist token standards, such as ERC-1056, ERC-780, ERC-725, ERC-734, and ERC-735 for Ethereum, which facilitate universal wallets that allow users to stay in control of all kinds of identifiers and credentials, as well as cryptocurrencies and other digital assets (Drasch et al. 2020; Soltani et al. 2021). Universal wallets will likely serve as gateways to all kinds of systems based on distributed ledger technology (DLT), such as electronic marketplaces, commercial applications, or public services (Lesavre et al. 2019; Skiba 2017). Further information as well as a typology for portable universal wallets can be found in Sect. 2 ("Wallet Types") of the World Wide Web Consortium (W3C)'s draft specifications for universal wallets (W3C 2020a).

2.2 Vulnerabilities of Crypto and Universal Wallets

Given the growing use of universal wallets as gateways to interaction and user authentication, the wallets' safety and security is of high importance. The different possible attacks on universal wallets must be identified and suitable countermeasures implemented (Steinegger et al. 2014; Haigh et al. 2018). As universal wallets are the central gateway for all users to engage in digital transactions, security mechanisms need to be mature enough to handle critical transactions (Coelho et al. 2014). Hot and cold wallets present different security issues. Hot wallets, with their constant link to the Internet, provide an obvious attack vector. Because of the well-known risks that wallets might be hacked, e.g., at a crypto exchange, such exchanges employ mitigation strategies. Currently, centralized crypto exchanges keep an average of 87% of clients' funds in cold storage for greater security (The Financial Stability Board 2019). However, cold wallets are not immune from hacking, and they can be physically stolen.

In addition to the design of the wallet itself, the way the wallet is connected to different DLT systems is another attack vector that needs to be considered (Galkin and Staroletov 2019). Various approaches have been established to anonymize the flow of transactions between wallets and DLT systems, but not all operate within legal boundaries. For example, DarkWallet tries to disguise the user's identity, which allows for darknet e-commerce and black-market transactions (Buttigieg et al. 2019).

Vulnerabilities also arise from the wallet architecture itself (Schwerin et al. 2017). Errors made in the programming originate from incomplete or wrongly specified requirements; therefore, a formal or structured approach is needed when designing critical components (Turkman and Taweel 2019) of universal wallets. Due to the resilience of data written in DLT systems, it is not possible to correct errors once they have been entered. Formal development approaches seem well-suited to minimize such vulnerability errors (Bigi et al. 2015).

Vulnerabilities also result when users do not fully understand the use of universal wallets, which may lead to imprudent use that ultimately opens up an attack vector. Thus, requirements that make universal wallets user-friendly but also safe can help create usage behavior that complies with the security instruments of the universal wallet. This would indicate the need for a processual approach (Cetinkaya et al. 2019).

2.3 Interaction Among Crypto Wallet Users

As crypto wallets are access points for crypto-asset applications, one key aspect in a distributed environment is standards for connecting with other users (Balan and Ramasubbu 2009). Because this is a novel technology, standards are mostly under development at this point. One example is the Trust Over IP (ToIP) Foundation, founded by 27 organizations, hosted by the Linux Foundation and supported by several large IT service providers. The aim of ToIP is to leverage interoperable digital wallets and credentials that use the W3C Verifiable Credentials Standard (Ledger Insights 2020).

2.4 Decentralized Biometrics

In recent years there has been a significant increase in the use of biometrics (Caldwell 2015). Most of these user authentication methods and identity-proving systems rely on a centralized database, which presents a single potential point of compromise. If such a system is compromised, it poses a direct threat to the digital identities of all users. One potential solution is a decentralized biometric-based authentication method known as the "Horcrux protocol." This protocol relies on decentralized identifiers (DIDs), currently under development by the W3C, and the concept of self-sovereign identity (W3C 2020b). Another suggested solution entails implementing decentralized biometric-credential storage via blockchains, using DIDs and DID documents within the IEEE 2410–2017 Biometric Open Protocol Standard (BOPS) (Othman and Callahan 2018). Decentralized architecture reduces the need for heightened security in transactions using biometric identifiers (Mohsin et al. 2020). A wallet carried by the user can respond to queries and verify transactions, using paired DIDs related to the biometrics, and log these transactions. This query response and transaction verification is an example of how universal wallets gradually incorporate more and more features particularly with the increasing focus on identity (Maurer 2020) and its protection enabling use of wallets as an access device.

2.5 Transaction Types of Universal Wallets

To achieve widespread use, wallets need intuitive design and a positive user experience. The first generation of crypto wallets has been perceived as unfriendly and counterintuitive (Baur et al. 2015); universal wallets need to be easy to use to allow for the different transaction types they facilitate (Gainsbury and Blaszczynski 2017). Naturally, universal wallets, like crypto wallets before them, will be used for cryptocurrency trading. Even though cryptocurrencies are still mainly being traded against other cryptocurrencies, and not used as much in interchanges with fiat currencies (Wei 2018), universal wallets are being used to create new payment types, such as invoicing services charging directly from universal wallets (Wolfson 2020). Other innovative types of transactions are arising from the use of digital assets as part of the emerging token economy (Kow et al. 2017). These tokens take an intermediary role as they are often associated with a value and traded as an asset. While the tokens' legal status is not yet settled in most jurisdictions—it becomes evident that universal wallets will also be the gateway to manage new types of transactions.

Another area of new transaction types is connected to digital identifiers and the Internet of Things (IoT) (Talari 2017). Through IoT, not only computers and mobile devices will be connected, but also smart homes, smart cities, smart power grids, and so on (Hancke et al. 2013). As consequence, IoT will lead to the development of a wide range of advanced information services that are pervasive, cost effective, and accessible via universal wallets (Hancke et al. 2013). However, due to the large number of interconnected devices, cyber security in the IoT is a major challenge, and once again, relies on sound digital identity concepts to build secure authentication and authorization mechanisms (Zhu et al. 2017). A natural extension of extensive IoT connections is the empowerment of the IoT into a robot—whether a software application or an anthropomorphic manifestation. From there, it is only a small step to robots interacting independently with other robots. For example, a smart fridge might possess its own wallet giving it authority to autonomously order groceries from a food delivery service (Cardenas and Kim 2020). However, protocols that allow digital handshakes to interoperate, e.g., between a smart fridge and a supermarket chain, require standards that allow for interoperability in multi-chain and cross-border transactions (Daza et al. 2017).

3 Taxonomy of Universal Wallets

To increase our understanding of universal wallets, we developed a taxonomy based upon the functionalities of universal wallets and the ways in which they are being used and planned. Digital wallets have been with us for several decades and have many uses. In our structured literature analysis, we searched peer-reviewed publications for key terms such as *digital wallet* starting from 1990, which resulted in 4377 hits. We then narrowed these results to wallets linked to blockchain or DLT solutions; the first mention of these occurred in 2013. This narrowed our total to 2475 publications, mostly in computer science outlets. A key distinction between digital wallets on one side and crypto and universal wallets linked to blockchains and DLT systems on the other is the latters' use of cryptographic methods; the opportunities for increased safety and security in transactions and audit trails are a key driver for the use of crypto wallets in general (Moldof 2018). However, when we searched for the term "crypto wallet and DLT system" in peer-reviewed outlets, we only found 49 publications in total, including publications dealing with Novi, the crypto wallet proposed by the Diem Association (Matthews 2019).

To refine our search for publications on crypto and universal wallets, we directed our search to the various transaction types in which crypto wallets are used—i.e., not just for trading cryptocurrencies, but also for managing digital identities and other assets—as this is an indication that universal wallets are involved. As of today, most discussions of universal wallets are in non-academic publications, such as white papers on wallet functionalities or specific products. Therefore, we decided to incorporate this reservoir of information. In searching for videos, we used a video-crawler software, MovieSherlock, to identify videos on "crypto wallets"; this resulted in 41 hits. We watched the videos and noted any discussion of the functionalities and characteristics of current and projected crypto and universal wallets and integrated it into our dataset. The purpose was to be as inclusive and as up to date as possible in our research, while giving preference to academic literature wherever it was available.

3.1 Development of a Wallet Taxonomy

To outline a meaningful taxonomy, we follow the approach developed by Nickerson et al. (2013). A taxonomy can be regarded as a way of organizing knowledge. In biology it is often prescriptive, but in subject areas like information systems taxonomy is used as a descriptive tool that structures and classifies the area of interest to improve knowledge and understanding within the selected area. Nickerson et al. have outlined a widely used approach for taxonomy development in information systems, which we will apply as well.

In step 1 of the taxonomy development, we identify the purpose of the overall characterization we want to conduct, that is, determining a *meta-characteristic*: "The meta-characteristic is the most comprehensive characteristic that will serve as the basis for the choice of characteristics in the taxonomy. Each characteristic should be a logical consequence of the meta-characteristic" (Nickerson et al. 2013, p. 343). Our chosen meta-characteristic aims to support and guide researchers and crypto-wallet stakeholders and to provide deeper insights into the functionality of crypto wallets in the widest sense, beyond cryptocurrency transactions. Hence the meta-characteristic chosen is the type of digital assets managed by the universal wallets in question, mapped against the high-level functionality areas identified from our functionality scanning. Although this could be taken as two meta-characteristics, we consider the combination of these two groups as one. The approach developed by Nickerson et al. is a semi-subjective, phenomenological approach analyzing the functionality area of interest. There are no requirements for logical cohesion between the chosen dimensions, apart from the implication that they need to be within the same meta-characteristic (as the whole analysis otherwise becomes corrupted and useless). As long as the meta-characteristic is maintained, we may be able to include other wallet-relevant function areas in future use.

In step 2, the focus is put on the ending conditions of the taxonomy investigation. Here, we apply what Nickerson et al. (2013) referred to as "objective" and "subjective" ending criteria. Essentially, objective criteria establish an algorithm for continuing with the classification sorting process until no new samples are found and the taxonomy being developed has proven to be stable. Reaching a reasonably stable solution is the pragmatic way to determine when to halt the work. Thus, we examined all the sampled wallets, continuing until we had at least one object classified for every characteristic, with no new characteristics added, merged or split, or duplicated.

The subjective criteria for ending the sorting process are determined using the following taxonomy development recommendations. The taxonomy should be:

- Concise, containing only dimensions that are really needed
- Robust, "containing enough dimensions and characteristics to clearly differentiate the objects of interest"
- Comprehensive, containing "all dimensions for objects of interest"
- Extendible, allowing "for inclusion of additional dimensions and new characteristics"
- Explanatory, providing "useful explanations of the nature of the studied objects or of future objects to help us understand them" (Nickerson et al. 2013, pp. 384)

In step 3, we follow an empirical-to-conceptual approach as we build our taxonomy from examples (Nickerson et al. 2013). We consider this approach to be the best fit since our literature and empirical analyses—taking white papers, reports, and videos into consideration—provided a complete overview and no significant additional dimensions/functionality areas were found in our sort. We identified the following functionality areas:

- Scenarios: Personas and use cases
- Types of wallet data
- Encryption and security
- External storage
- Wallet utilities
- External communication

The stability of these findings makes us believe that we captured all significant dimensions and functionalities as currently reported. To allow for future developments, we have designed the taxonomy so it can easily accommodate additional categories, such as future distinct asset types and future distinct functionality (Nickerson et al. 2013).

In this taxonomy research, we focus on hot wallets or software-based wallets with completely self-managed keys, as these are most often discussed when it comes to the future use of universal wallets. The taxonomy for universal wallets as illustrated in Fig. 1 is structured on characteristics of digital assets along the horizontal "direction" and functional areas (including services) along the vertical "direction." (We avoid the word "dimension" in this context, as no metric is implied.)

Because the types of digital assets managed by wallets have already been described, in the following we discuss the functionality areas of universal wallets in more detail. The identified functionality areas are illustrated in Fig. 1 to show how cryptographic and universal wallets can be mapped against the taxonomy.

To illustrate how the taxonomy can be used, Fig. 2 illustrates a cryptocurrency wallet (e.g., for Bitcoin) and Fig. 3 a universal wallet for comparison illustrating similarities and differences.

In the following, we describe each of the distinct functionality groups. The ontology implied here focuses on key areas for universal wallets on the outlining of a taxonomy. Further detailing will entail a much finer granularity which might be relevant for some readers.

Many crypto wallets facilitate basic functions of cryptocurrency transactions, such as trading, storage, and transfer. In this research, we extend our consideration to wallets that manage additional types of tokens and credentials, including those related to identity management. Universal wallets provide further capabilities and can be used for analyzing log data for reporting or for connecting with all kinds of devices, e.g., in an IoT context (Mackey et al. 2020). Groupings of such capabilities are critical when analyzing the vastly growing number of wallets for digital identity management, as well as new functionalities when comparing with previous wallet generations.

3.1.1 Scenarios: Personas and Use Cases

Nielsen (2019) describes the use of scenarios for understanding how people and applications will work together with a new system. In this context, *personas* describe the roles a user takes, such as citizen, employee, or a member of a group. Clearly, one person can encompass more than one personas. The use cases describe the actions of these personas and why, where, and how they use universal wallets.

Crypto wallets originated as a means of storing private keys for accessing cryptocurrencies. Essentially, the first wallets contained only the private keys associated with the transactions to be conducted. Such wallets may support single or multiple cryptocurrencies, such as the Guarda wallet, which supports functions like keeping transaction records, as well as basic wallet functionalities like sending, receiving, selling, and buying cryptocurrencies. As the number of different crypto tokens representing digital value (for example gift cards or shopping loyalty awards) increases, the demand for wallets that can manage them increases as well. So far, only a few universal wallets, such as Paiblock, support a wide variety of applications. Although from an IT perspective, there are no fundamental differences between the different token-based digital assets

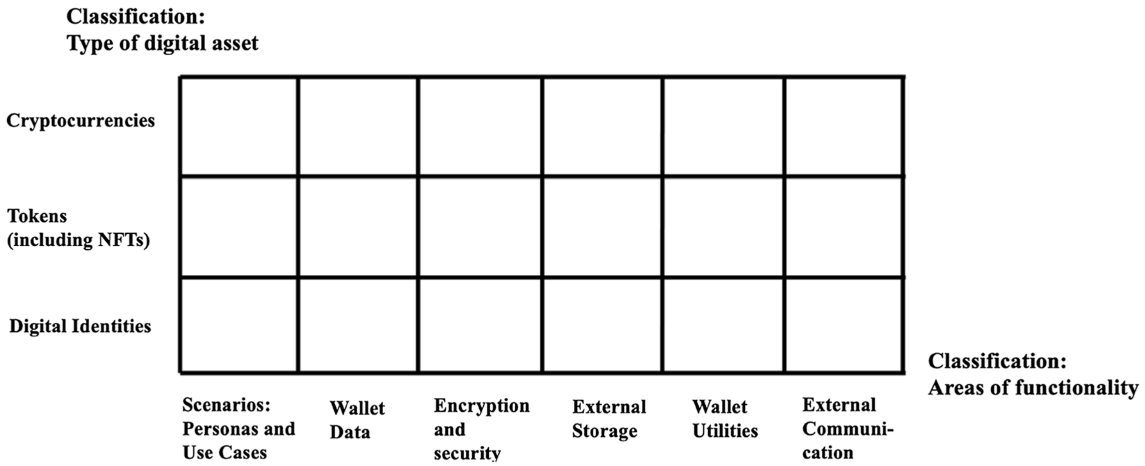

Fig. 1 A taxonomy of universal wallets for the blockchain economy

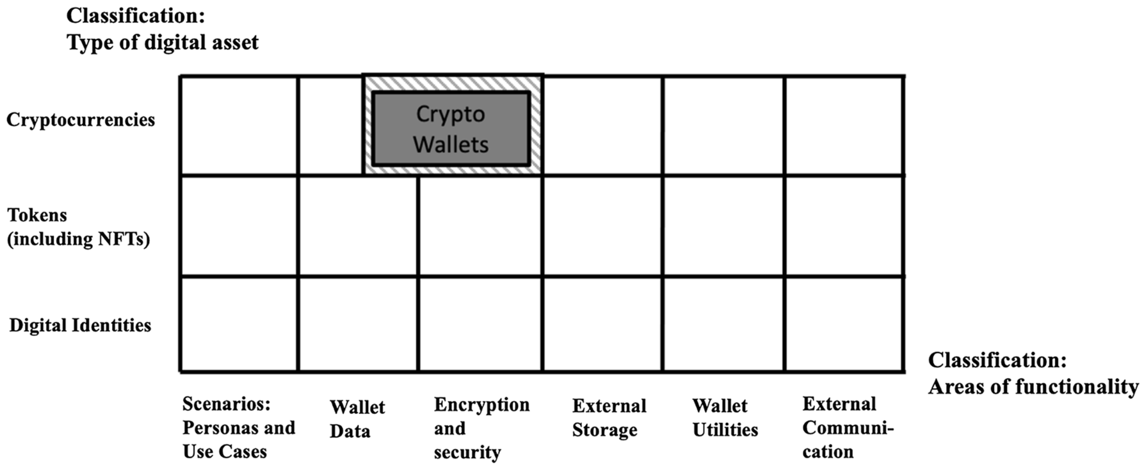

Fig. 2 The functionality of a classical crypto wallets showing the taxonomic features

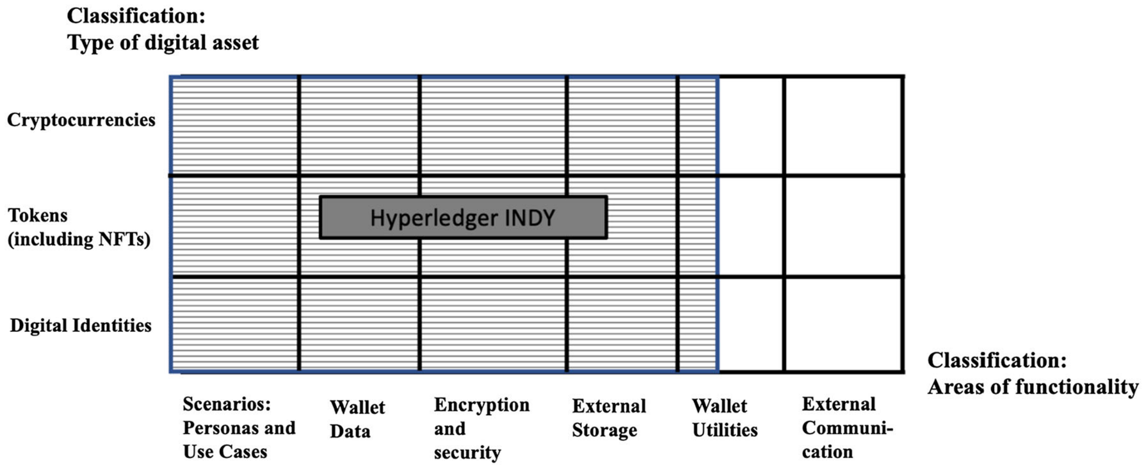

Fig. 3 The functionality of taxonomic features of Hyperledger Indy as example of a universal wallet

and, thus, no sharp boundaries within this category, societal, legal, and customary boundaries are salient, and they have Guard resulted in a host of token standards reflecting the different use cases.

Another use case is the management of personas and digital identities via universal wallets (Hohenberger and Lysyanskaya 2005). The ability to manage credentials and identifiers will be key in the future, as drivers' licenses, passports, health certificates, and other personal identity cards eventually become managed through universal wallets. This area has significant potential for commercial and societal impact (Soltani et al. 2021) as it undergirds self-sovereign identity efforts such as that undertaken by the European Self-Sovereign Identity Framework (ESSIF). Here, wallets with personal identities play a central role. For large-scale, practical use, it is important to address the different roles that may be covered by the different identifiers for the same person.

3.1.2 Types of Wallet Data

A key practical consideration is what data should be stored in universal wallets. The first-generation crypto wallets are relatively light; they host only necessary keys and call routines. As the number of application areas continues to increase, there is an increased need for covering more occasions to manage a wider range of identifiers and credentials, as well as a broader range of characteristics used to provide our unique digital identity (e.g., biometric-digital representations, tissue type markers). This may significantly increase the volume of data that a universal wallet needs to store and manage (Hyperledger 2018). The data increase may create performance challenges for universal wallets. It should be noted that even secure universal wallets should not contain all of a user's identifiers and credentials, as a wallet is not a database, and it would create a central point of failure or attack (Hohenberger and Lysyanskaya 2005).

3.1.3 Encryption and Security

A universal wallet provides security and encryption for the personal information and actual transactions stored in the wallet. This wide field of research in applied and theoretical computer science is key to the successful adoption and use of universal wallets (Xu et al. 2020; Liang et al. 2018). It should be noted that although encryption is part of security, and security also encompasses several other fields, in our context encryption is meaningfully regarded as a functionality and an inherent element in blockchain systems. Because encryption needs to be both effective and user-friendly, it seems relevant to include it as a distinctive character for a taxonomy of universal wallets.

3.1.4 External Storage

The increasing use of personal data, biomarkers, and various records has created a need for secure off-wallet storage (Gürsoy et al. 2020; Liang et al. 2018). Today, a great deal of such data is stored in file systems such as the InterPlanetary File System (IPFS) (Wang et al. 2021) or other cloud-based solutions. In a trusted DLT system, stored data, especially personal identifiable information, credentials, and personal identity data, should be handled with extra care through universal wallets, and stored in hardened, decentralized, external storage places. Pointers to off-wallet data, as well as the externally stored data itself, should be heavily encrypted (Hohenberger and Lysyanskaya 2005). Examples of the sort of data that should be stored off-wallet include transaction logs of events being stored by the user, as well as healthcare information, which needs to be accessible for at least the individual's lifetime and must be kept under the sovereign command of the data-owner (Farouk et al. 2020; Gürsoy et al. 2020; Leeming et al. 2019; Liang et al. 2018) that should be accessible at least for the person's lifetime and under sovereign command of the data-owner (Maurer 2020).

3.1.5 Wallet Utilities

Wallet utilities fall into two categories: (1) utilities built into the wallet and (2) remote utilities. These will not be deeper analyzed here. There will be a need for some utilities to read/write, send, or receive data with specialized query languages for this purpose (Hohenberger and Lysyanskaya 2005; Lesas et al. 2014). As the functionalities of the universal wallet get more advanced—and as the data includes more personal information and becomes more frequently used—there is an increasing need for tools to administer data, and for the user to be able to get an overview of status history and opportunities. Coupling the wallet with dashboard-type utilities, or "cockpits," is one way to advance these initiatives, and such project are already underway.

3.1.6 External Communication

Means of establishing practical and secure channels of communication among wallets, as well as between wallets and external entities, readers, access control systems, and so forth, are currently under development (Hohenberger and Lysyanskaya 2005; Xu et al. 2020). The wallet not only represents a user's gateway to societal services but also offers the potential of communicating autonomously between smart applications, like wallets without human involvement: As David G.W. Birch put it, "*When my* *wallet is connected to your wallet, something in its nature must change. […] In 10 years' time, my smart wallet and your smart wallet are going to be talking to each other and we won't be in the loop so much; we won't be bothered"* (quoted in Maurer 2020). Establishing communication between wallets and IoT devices is key for success with proliferation of IoT and ubiquitous computing solutions.

4 Discussion

The significance of the universal wallet may not be immediately obvious. Because of its name, one might see it as simply a storage place for cryptocurrency; but in fact, it represents the gateway to all kinds of functionalities on blockchains, as well as a means of managing one's own credentials, identifiers, digital assets, and identities. If we consider the universal wallets simply as upgraded digital wallets, we disregard the opportunities for completely new services—as well as the societal opportunities and risks they present (Büttgen et al. 2021). Universal wallets do not simply allow users to use a single device to interface with the ubiquitous intelligence generated from smart cities and essentially smart *everything* everywhere. They also offer us the opportunity to track what we do and who we interact with—not just persons, but applications and data—in a usable, effective, safe, and secure manner (Soltani et al. 2021).

For wallets to handle all the data-exchange incidents in a highly intelligent environment, they must be automated—meaning that it will be necessary to transfer some power of attorney to our wallet so it can interact smoothly with the intelligent surroundings of our daily life. That again implies the need for more capable user interfaces; these must exist partially off-wallet so that we better can analyze our data and instruct our wallet according to our wishes. Automation also raises crucial questions around security. Who is allowed to get our data, and when and why can they obtain it? These are key questions in self-sovereign identity discussions. The answers depend on how wallets manage the challenges of seamless integration, personal data integrity and data protection, and surveillance. Additionally, the likely emergence of independently acting robots with their own wallets (Cardenas and Kim 2020) raises societal and ethical considerations, as well as sparking a debate regarding possible spillover effects or other unintended second-order effects.

Why do we link universal wallets so closely to blockchains? Several benefits materialize from this: first, universal wallets, because they connect to blockchains, offer levels of safety and security that are unparalleled in current legacy systems. Second, in terms of interaction with smart local systems, IoT and robot blockchains with their decentralized architecture are unusually well-suited for the scenarios experts foresee emerging in the future. The universal wallet with their important role where authorization is necessary will be a key governing ingredient for the emerging systems that are likely to undergird future society (Liu et al. 2021). And even if specialized wallets are developed, like the digital identity products offered by Thales (Thales Group 2019), the expected increase in the number of smart devices will force us to minimize the number of contact points (like universal wallets) we apply to reach these devices. According to Statista: "The total installed base of Internet of Things (IoT) connected devices worldwide is projected to amount to 30.9 billion units by 2025, a sharp jump from the 13.8 billion units that are expected in 2021. Examples of IoT connections include connected cars, smart home devices and connected industrial equipment. In comparison, non-IoT connections include smartphones, laptops, and computers, with connections of these types of devices set to amount to just over 10 billion units by 2025" (Statista 2021b). With proliferation of 5G, 6G, and later networks, the number of connected devices will increase even more drastically, bringing opportunity for new services develop.

As more services are provided, including more diversified tokens (Draschet al. 2020; Sunyaev et al. 2021; Xu and Zou 2021) and other digital assets from services yet to be developed (Büttgen et al. 2021 pp. 85–89), and as individuals further personalize what their universal wallets contain, these wallets could develop into the user's digital twin (Kulkarni et al. 2019). The societal implications of such a development are enormous and quite unpredictable, not least in the context of demands for greater privacy and self-sovereignty, concern about the surveillance society, and the simultaneous explosion in need for access to and use of smart systems. As these qualities are derived, we will not use these in a descriptive classification context even if they are highly important.

This description and discussion of blockchain systems where wallets are an essential element is one key contribution of this paper. Another is the taxonomy, which aims to provide an overview that unites the types of digital assets a wallet handles and the functionalities relevant for managing these assets, including new areas of use like extended storage, proactive access, and transaction management.

5 Conclusions and Future Research

This paper is focused on the universal wallet itself, outlining first elements of a taxonomy for the application area and environment to manage these wallets as well as a perspective on how universal wallets are a logical enhancement of blockchain systems.

Given the important role of crypto wallets and their more expansive form of universal wallets, it is surprising that there is not more information-systems research published on wallets and blockchains. There are only a few academic publications on wallets that discuss their concepts, opportunities, and limitations. Thus, we are calling for more research in fields relating to wallets as elements in blockchain-based or blockchain-driven solutions, such as digital identities, self-sovereign identity management, tokens, and innovative uses for digital wallets and crypto wallets. Current research seems predominantly to focus on crypto wallets which, as we have seen here, offer only a fraction of the capability of universal wallets.

Our research on a universal wallet taxonomy points to several additional directions for future research. One, only lightly touched upon here, is the interaction between wallets and various digital assets, and the common and different implementations involved. The handling of a crypto token, for example, is likely quite different from that for an NFT (which might even be a piece of art to be exhibited in the wallet itself). Today's wallets operate in several contexts on very limited application platforms, and these limitations and opportunities must be further illustrated through research—as must the performance and security consequences of the expanded platforms under consideration. Further, there is a need for detailed use cases for specific industries and application areas overall where wallets are a key element, as described by Liu et al. (2021). A design-science approach could facilitate a utility perspective when it seems opportune to develop new services around such endeavors and could also provide inspiration.

Another line for research is a wallet's intelligent, automated interaction with its surroundings. This capacity is critical to successful, effective, and secure interaction between users, wallets, and their environment (Cardenas and Kim 2020). Likewise, with the increasing automation and proliferation of AI and robotic technologies, the question is not just how users will interact with these robots, but how robots will use their wallets by themselves? The increase of opportunities—including access to IoT solutions, smart cities, and ID cards, or robots that behave autonomously—emphasizes the need for policies, regulatory requirements, and new forms of self-enforcing governance and standardization. Universal wallets will enable autonomous services—AI enabled or not—which requires us to revisit the service concept as such. At present, services are typically co-created and transient; our usual models have not yet considered services that are triggered proactively and autonomously. Such "services in advance" will be possible with universal wallets as access and control points. As the availability and use of identity data shifts from manual presentation of credentials to automated, always-and-everywhere availability, many new services will emerge, with potentially large societal effects. For example, universal wallets will through NFTs make shared ownership of a car or a piece of art possible and enforceable, and authorization to buy or sell any digital asset managed by the wallet can be given on the go.

The increase in the number of interactions provides opportunity for more granular information flow (Leeming et al. 2019) and is available now for assessing transactions conducted through universal wallets. Liu et al. (2021) analyze the dynamics of such transactions through a universal wallet taking a game-theoretical and multi-agent approach to grasp the complexities and dynamics of new environments with increasingly intelligent players. Analyzing such data is another venue for research—both on-wallet as well as off-wallet. This plethora of finely granulated data also raises the possibility of a surveillance society and surveillance capitalism (Jameson et al. 2019). While some may view this as a threat, others may see opportunities.

The use of universal wallets for management and use of digital assets and identities will play a key role in modern digital transformation, extending beyond human use to use by any (more or less smart) automated entity. The wallet is a key portal for interaction with other systems including other wallets, as well as persons and services, and the interaction can take place manually between human beings or automatically via a dialogue between machines and their wallets. The different manifestations of wallets call for a structured research approach toward a wallet taxonomy, wallet affordance, as well as governance-related aspects of wallets.

Finally, there is a research area derived from services and commoditization of societal core values like trust. Here the wallet's potential to act as the user's digital twin seems key. There is a need for research into the issue of proprietary versus open-source solutions for above purposes. The societal changes that universal wallets may bring and the impact of being able to use them to stay in control of our personal data and actions has hardly been researched. The consequences could be immense, not just in terms of IT but also legally, economically, and socially.

Our purpose in this article has been to outline a taxonomy that will improve our understanding of what type of digital assets and functionalities are supported by universal wallets, in addition to assessing how universal they really are. The taxonomy focuses on groups of functionalities found in contemporary examples of such wallets. The intention is to stimulate stakeholders' interest in why, where, and how universal wallets can create more effective solutions for today's problems, as well as helping to realize and address the potential unintended consequences of those solutions (Büttgen et al. 2021 pp. 85–89). We are not aware of any similar taxonomy in this area. This could be an indication that it is still too early to formulate one. However, we are convinced that a taxonomy is urgently needed to guide discussions on functionality, services, opportunities, and limitations of universal wallets and to map these against specific use- and business cases.

References

Auer R, Boehme R (2020) The technology of retail central bank digital currency. BIS Q Rev 2020:85–100. https://ssrn.com/abstract=3561198

Balan R, Ramasubbu N (2009) The digital wallet: opportunities and prototypes. IEEE Comput Soc 42(4):100–102

Baur A, et al (2015) Cryptocurrencies as a disruption? Empirical findings on user adoption and future potential of Bitcoin and Co. In: Conference on e-Business, e-Services and e-Society. Springer, Cham, pp 63–80

Bigi G, Bracciali A, Meacci G, Tuosto E (2015) Validation of decentralised smart contracts through game theory and formal methods. In: Programming Languages with Applications to Biology and Security. Springer, pp 142–161. https://doi.org/10.1007/978-3-319-25527-9_11

van Bokkem D, Hageman R, Koning G, Nguyen L, Zarin N (2019) Self-sovereign identity solutions: the necessity of blockchain technology. arXiv preprint arXiv:1904.12816

Büttgen M et al (2021) Blockchain in service management and service research – developing a research agenda and managerial implications. J Service Manag Res 5(2):711-2–71

Buttigieg CP, Efthymiopoulos C, Attard A (2019) Anti-money laundering regulation of crypto assets in Europe's smallest member state. Law Fin Market Rev 13(4):211–227

Caldwell T (2015) Market report: border biometrics. Biom Technol Today 2015(5):5–11. https://doi.org/10.1016/S0969-4765(15)30079-5

Cardenas I, Kim J-H (2020) Robonomics: the study of robot-human peer-to-peer financial transactions and agreements. In: Companion of the 2020 ACM/IEEE international conference on human-robot interaction, pp 8–15

Cetinkaya A, et al (2019) An experimental study on decomposition: process first or structure first? In: 9th international symposium on business modeling and software design, Lisbon, Portugal

Coelho RW, Fernandes G, Proença ML Jr (2014) GAIA-MLIS: a maturity model for information security. In: 8th International conference on emerging security information, systems and technologies, Lisbon, pp 50–55

Daza V, et al (2017) CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. In: IEEE ICC SAC symposium internet of things track, Paris

Drasch BJ, et al (2020) The token's secret: the two-faced financial incentive of the token economy. Electron Mark 30(3):557–567

Engert W, Fung BSC (2017) Central Bank Digital Currency: motivations and implications. Bank of Canada, Staff Discussion Paper

Farouk A et al (2020) Blockchain platform for industrial healthcare: vision and future opportunities. Comput Commun 154:223–235

Gainsbury S, Blaszczynski A (2017) How blockchain and cryptocurrency technology could revolutionize online gambling. Gaming Law Rev 21(7):482–492

Galkin R, Staroletov S (2019) Towards methods of blockchain applications testing. Altai State Technical University. Unpublished, https://www.researchgate.net/publication/332726571_Towards_Methods_of_Blockchain_Applications_Testing. Accessed 3 Jul 2020

Gürsoy G, Brannon CM, Gerstein M (2020) Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Med Genom 13:74

Haigh T, Breitinger F, Baggili I (2018) If I had a million cryptos: cryptowallet application analysis and a trojan proof-of-concept. In: International conference on digital forensics and cyber crime. Springer, Cham, pp 45–65. https://doi.org/10.1007/978-3-030-05487-8_3

Hancke GP et al (2013) The role of advanced sensing in smart cities. Sensors 13(1):393–425

Hohenberger S, Lysyanskaya A (2005) How to securely outsource cryptographic computations. In: Kilian J (ed) Theory of cryptography conference, Cambridge. Springer, LNCS 3378, pp 264–282

Hyperledger, Wallets – Indy HIPE (2018) Presentation available via Hyperledger. http://bit.ly/2JUcIiT. Accessed 11 July 2020

Ledger Insights (2020) IBM, R3, Mastercard join open source digital identity consortium –enterprise blockchain. https://www.ledgerinsights.com/trust-over-ip-digital-identity-consortium-ibm-r3-mastercard. Accessed 12 Jul 2020

Jameson S, Richter C, Taylor L (2019) People's strategies for perceived surveillance in Amsterdam Smart City. Urban Geogr 40(10):1467–1484

Jokic S, Cvetković AS, Adamović S et al (2019) Comparative analysis of cryptocurrency wallets vs traditional wallets. Ekonomika 65(3):65–75

Kastrenakes J (2020) Libra cryptocurrency project changes name to Diem to distance itself from Facebook; Diem is 'reinforcing its organizational independence'. https://www.theverge.com/2020/12/1/21755078/libra-diem-name-change-cryptocurrency-facebook

Kow YM, Gui X, Cheng W (2017) Special digital monies: the design of Alipay and WeChat Wallet for mobile payment practices in China. In: IFIP conference on human-computer interaction, Mumbai, pp 136–155

Kulkarni V, Barat S, Clark T (2019) Towards adaptive enterprises using digital twins. In: 2019 winter simulation conference, pp 60–74. https://doi.org/10.1109/WSC40007.2019.9004956

Lansky J (2018) Possible state approaches to cryptocurrencies. J Syst Integr 9(1):19–31

Leeming G, Cunningham J, Ainsworth J (2019) A ledger of me: personalizing healthcare using blockchain technology. Front Med. https://doi.org/10.3389/fmed.2019.00171

Lesas A-M et al (2014) WOLF: a research platform to write NFC secure applications on top of multiple secure elements (with an original SQL-Like interface). Int J Adv Comput Sci Appl 5(8):20–31

Lesavre L et al (2019) A taxonomic approach to understanding emerging blockchain identity management systems. NIST. https://doi.org/10.6028/NIST.CSWP.07092019-draft

Liang X, et al (2018) Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications. EAI Endorsed Trans Pervasive Health Technol 4(15)

Libra Association Members (2020) https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf with cover letter. https://www.diem.com/en-us/white-paper/#cover-letter. Accessed 24 Aug 2021

Liu XF, Ren H-H, Liu S-H, Jiang X-J (2021) Characterizing key agents in the cryptocurrency economy through blockchain transaction analysis. EPJ Data Sci 10(1):1–13. https://doi.org/10.1140/epjds/s13688-021-00276-9

Mackey T, Bekki H, Matsuzaki T, Mizushima H (2020) Examining the potential of blockchain technology to meet the needs of 21st-century Japanese health care: viewpoint on use cases and policy. J Med Internet Res 22(1):e13649–e13649. https://doi.org/10.2196/13649

Matthews K (2019) Libra is just the beginning: insights from blockchain researchers. Scienmag. https://scienmag.com/libra-is-just-the-beginning-insights-from-blockchain-researchers. Accessed 3 Jul 2020

Maurer B (2020) Late to the party: debt and data. Soc Anthropol 20(4)

Mohsin AH et al (2020) Finger vein biometrics: taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures. IEEE Access 8:9821–9845. https://doi.org/10.1109/ACCESS.2020.2964788

Moldof A (2018) Bitcoin and blockchain insights: making digital wallets safer. Internal Auditing Mar/Apr 2018

Nadini M, Alessandretti L, Giacinto FD, Martino M, Aiello L, Baronchelli A (2021) Mapping the NFT revolution: market trends, trade networks and visual features. arXiv: abs/2106.00647.

Nickerson RC, Varshney U, Muntermann J (2013) A method for taxonomy development and its application in information systems. Eur J Inf Syst 22(3):336–359

Nielsen L (2019) Personas in use. In Personas – user focused design (pp. 83–115). Springer, London. https://doi.org/10.1007/978-1-4471-7427-1_5

Othman A, Callahan J (2018) The Horcrux Protocol: a method for decentralized biometric-based self-sovereign identity, IEEE. In: International joint conference on neural networks, Rio de Janeiro. https://doi.org/10.1109/IJCNN.2018.8489316

Paiblock (2020) Digital lifestyle. https://paiblock.app/static/digital/lifestyle. Accessed 11 Jul 2020

Ramkumar M (2018) A blockchain system integrity model. In: 17th International Conference on Security and Management, Las Vegas. https://www.researchgate.net/publication/328410774. Accessed 2 Jul 2020

Rezaeighaleh H, Zou CC (2019) New secure approach to backup cryptocurrency wallets. In: IEEE global communications conference, Waikoloa, pp 1–6

Rrustemi J, Tuchschmid NS (2020) Facebook's digital currency venture "Diem": the new frontier … or a galaxy far, far away? Technol Innov Manag Rev 10(12):19–30

Schwerin S, et al (2017) medixain: robust blockchain optimization enabling individual medical wallet architecture. Medixain. https://www.semanticscholar.org/paper/medixain-%3A-Robust-Blockchain-Optimization-Enabling-Schwerin-El-Kutbi/95ae2a6b5918674f408d43dffa1b8cdd7625864b#paper-header. Accessed 3 Jul 2020

Skiba DJ (2017) The potential of blockchain in education and health care. Natl Leag Nurs 38(4):220–221

Soltani R, Nguyen UT, An A (2021) A survey of self-sovereign identity ecosystem. Sec Commun Netw. https://doi.org/10.1155/2021/8873429

Statista (2021a) Number of blockchain wallets (2020). https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users. Accessed 16 Aug 2021

Statista (2021b) Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/)

Steinegger R, Schäfer J, Vogler M, et al (2014) Attack surface reduction for web services based on authorization patterns. In: Securware 2014, the 8th international conference on emerging security information, systems and technologies, Lisbon, pp 194–201

Sunyaev A, Kannengießer N, Beck R, Treiblmaier H, Lacity M, Kranz J, Fridgen G, Spankowski U, Luckow A (2021) Token economy. Bus Inf Syst Eng 63(4):457–478. https://doi.org/10.1007/s12599-021-00684-1

Talari S et al (2017) A review of smart cities based on the internet of things concept. Energies 10:421–444

Thales Group (2019) An ID revolution in your smartphone; https://www.thalesgroup.com/sites/default/files/gemalto/gov-info-Digital-ID-Wallet.pdf

The Financial Stability Board (FSB) (2019) Decentralised financial technologies: report on financial stability, regulatory and governance implications. https://www.fsb.org/2019/06/decentralised-financial-technologies-report-on-financial-stability-regulatory-and-governance-implications/. Accessed 3 Jul 2020

Toth K, Anderson-Priddy A (2019) Self-sovereign digital identity: a paradigm shift for identity. IEEE Secur Priv 17(3):17–27. https://doi.org/10.1109/MSEC.2018.2888782

Turkman S, Taweel A (2019) Business process model driven automatic software requirements generation. In: 9th International symposium on business modeling and software design, Lisbon

W3C (2020a) Universal wallet (2020) W3C Editor's Draft 23 October 2020; https://w3c-ccg.github.io/universal-wallet-interop-spec/. Accessed 29 Nov 2020

W3C (2020b) Decentralized identifiers (DIDs) v1.0 Working Draft 08 November 2020. https://www.w3.org/TR/did-core

Wang Q, Li R, Wang Q, Chen S (2021) Non-fungible token (NFT): overview, evaluation, opportunities and challenges. arXiv preprint arXiv: 2105.07447

Wei WC (2018) The impact of Tether grants on Bitcoin. Econ Lett 171:19–22

Wolfson R (2020) BitPay restores service to all bitcoin wallets to drive mainstream adoption. Available via Cointelegraph. https://cointelegraph.com/news/bitpay-restores-service-to-all-bitcoin-wallets-to-drive-mainstream-adoption. Accessed 4 Jul 2020

Xu Z, Zou C (2021) What can blockchain do and cannot do? China Econ J 14(1):4–25. https://doi.org/10.1080/17538963.2020.1748968

Xu B, Huang D, Mi B (2020) Smart city-based e-commerce security technology with improvement of SET network protocol. Comput Commun 154:66–74

Zhu X et al (2017) Autonomic identity framework for the internet of things. IEEE. https://doi.org/10.1109/ICCAC.2017.14